НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ГУМАНІТАРНО-ПЕДАГОГІЧНИЙ ФАКУЛЬТЕТ

УДК 327-049.5:004-049.5

ПОГОДЖЕНО
Декан факультету (Директор ННІ)
гуманітарно-педагогічного факультету, кандидат філософських наук, доцент

_____Савицька І.М.
"__" _____ 2023 р.

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ
в.о. Завідувача кафедри
міжнародних відносин та суспільних комунікацій, кандидат історичних наук, доцент

_____Хвіст В.О.
"__" _____ 2023 р.

МАГІСТЕРСЬКА РОБОТА
на тему:

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА СУЧАСНОЇ СИСТЕМИ МІЖНАРОДНОЇ БЕЗПЕКИ

CYBER SECURITY AS A COMPONENT OF THE MODERN INTERNATIONAL SECURITY SYSTEM

Спеціальність: Міжнародні відносини, суспільні комунікації та регіональні студії

Магістерська програма: Міжнародні відносини, суспільні комунікації та регіональні студії

Програма підготовки: освітньо-професійна

Гарант освітньої програми

_____ Кандидат історичних наук, доцент Кравченко Н.Б.

Керівник магістерської роботи
доцент кафедри міжнародних відносин суспільних комунікацій та регіональних студій Гольцов А.Г.

Виконав(ла) Кириченко Е.Д.

КИЇВ – 2023

НАЦІОНАЛЬНИЙ УНІВЕРСТИТЕТ
БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ГУМАНІТАРНО-ПЕДАГОГІЧНИЙ
ФАКУЛЬТЕТ

ЗАТВЕРДЖУЮ
в.о. Завідувача кафедри міжнародних відносин
і суспільних наук
Хвіст В.О.
“__” ____ 2023 р.

ЗАВДАННЯ
ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
СТУДЕНТУ
Кириченко Богдан Дмитрович

Спеціальність 291 **«Міжнародні відносини, суспільні комунікації тарегіональні студії»**

Освітня програма **«Міжнародні відносини, суспільні комунікації та регіональні студії»**

Орієнтація освітньої прогами **освітньо-професійна**

Тема магістерської роботи: **«Кібербезпека як складова сучасної системи міжнародної безпеки»**

Затверджена наказом ректора НУБіП України від 28 листопада 2022 р.

Термін подання завершеної роботи на кафедру «__» _____ 2023 р.

Вихідні дані до магістерської роботи:

1) Наукові дослідження з питань вивчення розвитку кібербезпеки в Україні та світі;
2) Вітчизняні та зарубіжні літературні джерела з проблемидослідження;

Перелік питань, що підлягають дослідженню:

- проаналізувати науково-термінологічні засади сучасних досліджень кібербезпеки у складі міжнародної безпеки;
- дослідити сучасний стан кіберзлочинності у світі, та які методи кібератак найбільш поширені наразі;

- з’ясувати ефективність вжитих заходів України та провідних держав у боротьбі з кіберзагрозами;
- аналітика отриманих даних, виявлення сильних та слабких сторін;
- аналіз сучасної міжнародної правової бази та тенденцій у боротьбі із кіберзлочинністю.

Дата видачі завдання «__» _____ 2022 р.

Керівник магістерської роботи _____ Гольцов А.Г.

Завдання прийняв до виконання _____ Кириченко Б.Д.

РЕФЕРАТ
магістерської роботи
студента магістратури гуманітарно-педагогічного факультету
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»,
освітньо-професійної програми «Міжнародні відносини, суспільні комунікації та регіональні студії»
Національний університет біоресурсів і природокористування України
Кириченка Богдана Дмитровича
на тему: «Кібербезпека як складова сучасної системи міжнародної безпеки»

Кваліфікаційна робота складається зі вступу, 3 розділів, висновків, списку використаних джерел з 171 найменувань.

Робота зосереджена на питанні сучасного стану кібербезпеки міжнародного середовища, приділяючи особливу увагу нормативно-правовій базі регулювання інформаційно-комунікаційних технологій, досвіду зарубіжних країн та України у протидії кіберзлочинності, а також останніх зрушень у питанні подальшої співпраці на глобальному рівні.

Сучасне суспільство тісно пов'язано з інформаційно-комунікативними технологіями, пронизуючи його зверху-вниз ІКТ перетворилось із засобу, який спрощує життя людини на зброю масового ураження. Тепер під ударом опинились не просто окремі індивіди, а цілі держави та союзи. І чим більш залежними від технологій ми стаємо, тим складніше стає захищати наш інформаційний простір та конфіденційну інформацію. Оскільки зараз усі критичні об'єкти зберігають інформацію у цифровому форматі – необхідність покращення заходів та методів для захисту від кіберзагроз, як ніколи, актуальна.

До того ж, в контексті відкритої війни між Україною та Російською Федерацією, необхідно проаналізувати уже здобутий власний досвід та досвід наших партнерів, щоб прослідкувати міжнародні тенденції у протидії кіберзлочинності та притягненню винних до відповідальності.

Ключові слова за темою кваліфікаційної роботи: кібербезпека, кіберзахист, кіберзлочинність, інформаційно-комунікаційні технології (ІКТ), інформаційно-телекомунікаційні системи (ІТС), кібершпигунство, міжнародна співпраця, кіберінциденти, кіберзагрози.

АНОТАЦІЯ

Кириченко Богдан Дмитрович. Кібербезпека як складова сучасної системи міжнародної безпеки. Кваліфікаційна робота на здобуття ступеня магістр за спеціальністю 291 «Міжнародні відносини, суспільні комунікації та регіональні студії». – Національний Університет біоресурсів і природокористування України, Київ, 2023.

Зміст анотації:

Об’єктами дослідження виступає сучасна система міжнародної безпеки, яка на сьогоднішній день є невід’ємною та значною частиною загальної міжнародної безпеки.

Предметом дослідження є кібернетична безпека в сучасній системі міжнародної безпеки.

До цього входять і безпосередньо вжиті заходи, що були задекларовані урядами держав та світовою громадськістю у їхніх правових документах та міжнародних конвенціях, і наслідки від них для кібербезпеки.

Методи дослідження. В своїй роботі ми вдавались до наступних методів: робота з першоджерелами (безпосередньо нормативно-правові акти та урядові звіти), аналіз тематичної літератури, провідних науковців у сфері кібербезпеки, заяв представників влади та публікацій українських та міжнародних ЗМІ; системний підхід; метод порівння, метод аналогій; синтез та дедукція, узагальнення при визначенні проблем та перспектив розвитку кібербезпеки в Україні та світі.

Отримані нами результати можуть бути використані як науковим співтовариством, що безпосередньо займається питанням сучасного стану світової кібербезпеки, так і владними посадовцями задля провадження змін у законодавчі акти держави, з метою уніфікації термінологічної та нормативно-

правової бази з кібербезпеки України в контексті євро-атлантичної інтеграції, а також перейняття міжнародного досвіду та покращення захисту нашої держави від кібератак.

Отримані результати стосуються безпосередньо подій, що розгорнулися в Україні та світі в останні роки. Наша робота зачіпає безпосередньо аналіз дій впроваджений українською владою та міжнародною спільнотою в ретроспективі від минулого до сьогодення: від самого започаткування тих заходів – до практичного впровадження, та тих наслідків, які прослідували за цим. До того ж, автором зачіпається питання саме сучасних методів кіберзлочинців, та який вплив вони несуть для держави.

Кваліфікаційна робота складається зі вступу, 3 розділів, висновків, списку використаних джерел з 171 найменувань. В першому розділі роботи розкрито теоретико-методологічні аспекти дослідження світових моделей підходу до трактування кібербезпеки; у другому розділі досліджено світові моделі підтримки державами кібербезпеки, методи, якими вони при цьому користуються, а також досвід України; в третьому розділі виконано аналіз сучасного стану світової кібербезпеки та який потенціал у глобального співтовариства у поглибленні подальшої співпраці у цій сфері. Зміст кваліфікаційної роботи викладено на 85 сторінках друкованого тексту.

Ключові слова за темою кваліфікаційної роботи: кібербезпека, кіберзахист, кіберзлочинність, інформаційно-комунікаційні технології (ІКТ), інформаційно-телекомунікаційні системи (ІТС), кібершпигунство, міжнародна співпраця, кіберінциденти, кіберзагрози.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

Інформаційно-комунікаційні технології	ІКТ
Інформаційно-телекомунікаційні системи	ІТС
Агентство Національної Безпеки	АНБ
Асоціація держав Південно-Східної Азії	АСЕАН
Організація з безпеки і співробітництва в Європі	ОБСЄ
Рада Європи	РЄ
Організація економічного співробітництва та розвитку	ОЕСР
Шанхайська організація співробітництва	ШОС

ВСТУП

Актуальність теми дослідження. XXI століття ознаменувало стрімкий розвиток інформаційно-комунікаційних технологій (ІКТ), які полегшили життя людини у сучасному світі. Тому, дедалі частіше лунають заклики про те, що світове суспільство переходить до тотального перенесення своєї діяльності у кіберпростір. Україна також не залишається осторонь цього процесу, впроваджуючи і реалізуючи стратегію «Держави в смартфоні», яка має на меті спрощення взаємодії громадян з владними органами. Та сама «Дія», яка дала можливість мати електронні документи, подавати заявки, отримувати квитанції та довідки, і все це у власному ж телефоні.

Проте, на жаль, існує й інший бік розвитку ІКТ. Дозволивши технологіям стати частинкою нас, ми стали й більш уразливими для зловмисників. Перенісши усю інформацію у цифровий світ, ми тим самим впевнені, що там вона буде в безпеці і ніхто окрім нас не зможе її отримати. На жаль, це не так. Тому, як і аналогові носії, наші дані в мережі можуть потрапити у руки тих, хто захоче ними скористатися для власних цілей, як то шантаж або перепродаж. І це стосується як звичайних громадян, так і цілих держав. Саме тому уряди країн світу намагаються убезпечити себе та своїх громадян від потенційної небезпеки у кіберпросторі, через впровадження нормативно-правової бази, а також створення відповідних органів контролю.

Тож, у контексті досвіду України, провідних держав світу, а також нашого безпосереднього геополітичного та геостратегічного ворога, Російської Федерації, варто дослідити наскільки ефективно працює та чи інша система, які її сильні сторони та який нинішній стан розгляду цього питання на світовій арені.

Ступінь дослідження теми. Свої роботи, присвячені питанню методів забезпечення кібербезпеки, аналізу сучасних правових документів, які стосуються цієї теми, а також оцінки ефективності вжитих заходів, присвятили

такі українські дослідники і теоретики міжнародних відносин, як Баранов О.А., Безуглий Д., Капітоненко М.Г., Липкан В. А., Дубов Д.В., Діордіца І. В., Фурашев В.М. та зарубіжні автори, такі як Аморосо Е., Бузан Б., Уевер О., Уайлд Дж., Річард А. Кеммерер, Дженіфер Льюіс, Болдуїн Д.А. та інші.

Об'єктом дослідження виступає сучасна система міжнародної безпеки, яка на сьогоднішній день є невід'ємною та значною частиною загальної міжнародної безпеки.

Предметом дослідження є кібернетична безпека в сучасній системі міжнародної безпеки.

До цього входять і безпосередньо вжиті заходи, що були задекларовані урядами держав та світовою громадськістю у їхніх правових документах та міжнародних конвенціях, і наслідки від них для кібербезпеки.

Метою цієї роботи є виявлення сучасних проблем захисту кібербезпеки в системі міжнародної безпеки, визначення шляхів їхнього розв'язання.

Отож, **Завдання**, які ми перед собою ставимо наступні:

- проаналізувати науково-термінологічні засади сучасних досліджень кібербезпеки у складі міжнародної безпеки;
- дослідити сучасний стан кіберзлочинності у світі, та які методи кібератак найбільш поширені наразі;
- з'ясувати ефективність вжитих заходів України та провідних держав у боротьбі з кіберзагрозами;
- аналітика отриманих даних, виявлення сильних та слабких сторін;
- аналіз сучасної міжнародної правової бази та тенденцій у боротьбі із кіберзлочинністю.

Методи дослідження. В своїй роботі ми вдавались до наступних методів: робота з першоджерелами (безпосередньо нормативно-правові акти та урядові звіти); аналіз тематичної літератури, провідних науковців у сфері кібербезпеки, заяв представників влади та публікацій українських та міжнародних ЗМІ; системний підхід; метод порівняння, метод аналогій; синтез та дедукція, узагальнення при визначенні проблем та перспектив розвитку кібербезпеки в Україні та світі.

Хронологічні рамки дослідження. В нашій роботі за основу були взяті події періоду кінця 90-х років XX століття й до сьогодення.

Територіальні рамки. Аналітика була проведена відносно України та провідних країн світу, таких як: США, ЄС, комуністичний Китай (КНР), РФ та Індії.

Наукова новизна. Отримані результати стосуються безпосередньо подій, що розгорнулися в Україні та світі в останні роки. Наша робота удосконалює безпосередньо підхід до аналізу дій впроваджений українською владою та міжнародною спільнотою в ретроспективі від минулого до сьогодення: так як ми можемо прослідкувати їх від самого започаткування – до практичного впровадження, та тих наслідків, які прослідувати за цим. До того як, набуло подальшого розвитку питання саме сучасних методів кіберзлочинців, та який вплив вони несуть для держави.

Теоретичне значення. Дана робота, беручи за основу дослідження сучасних науковців та теоретиків міжнародної безпеки, може послужити базисом для наукових робіт та студентських праць. Бо прослідковуючи шлях історичного процесу формування кібербезпекових заходів, та те, який вплив вони мали на міжнародну політику та безпеку сьогодення, ми даємо власну оцінку цих подій, що може бути використано у подальших дослідженнях цієї теми.

Практичне значення. Отримані нами результати можуть бути використані як науковим співтовариством, що безпосередньо займається питанням сучасного стану світової кібербезпеки, так і владними посадовцями задля провадження змін у законодавчі акти держави, з метою уніфікації термінологічної та нормативно-правової бази з кібербезпеки України в контексті євро-атлантичної інтеграції, а також перейняття міжнародного досвіду та покращення захисту нашої держави від кібератак. Також, матеріали дослідження можуть бути використанні при викладанні в закладах вищої освіти низки навчальних курсів, таких як «Міжнародні відносини та світова політика» та «Міжнародна безпека».

Інформаційною базою роботи стали нормативно-правова база, літературні джерела та статистичні матеріали щодо розвитку кібербезпеки, спеціальні монографічні й періодичні джерела, Інтернет-ресурси, офіційні сайти тощо.

Апробація результатів дослідження. Частина даної роботи, а особливо розділ про сучасний стан кібербезпеки України, була використана при написанні тез для IV Всеукраїнської студентської наукової конференції «Формування сучасної науки: методика та практика» (м. Київ), у розділі «Міжнародні відносини», 14 жовтня 2023 р.

Публікації. Тези було опубліковано у збірнику тез вище зазначеної конференції, у співавторстві з науковим керівником:

- Кириченко Б. Д., Гольцов А. Г., «Міжнародна підтримка кібербезпеки України в умовах відкритої війни проти Росії» // *«Формування сучасної науки: методика та практика»*: зб. матеріалів IV Всеукр. студ. наук. конф. Київ: УКРЛОГОС Груп. 2023. С. 75 – 76.

Структура роботи відбиває поставлені перед дослідженням цілі та завдання. Загальний обсяг роботи становить 122 сторінки, з них основного тексту – 85 сторінок. Робота складається зі вступу, 3 розділів, 8 підрозділів,

висновків, списку джерел та літератури (171 найменування українською, російською та англійською мовами).

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ КІБЕРБЕЗПЕКИ В СИСТЕМІ МІЖНАРОДНОЇ БЕЗПЕКИ

1.1. Система міжнародної безпеки. Роль та місце кібербезпеки

Забезпечення мирного співіснування держав світу завжди було основною темою для дискусій серед дослідників та теоретиків міжнародних відносин. І дійсно, історія показує, що людство прагне до встановлення певної системи правил та обов'язків, які б мали на меті регулювання міжнародних відносин, а також впровадження єдиних норм та цінностей, що б лежали в основі міжнародного миру.

Саме у цьому і є головне покликання системи міжнародної безпеки. У цьому плані необхідно розуміти, що мета такої системи, як відзначає Капітоненко Г., на сучасному етапі має містити наступні критерії: утвердження мирного співіснування, як універсального принципу міждержавних відносин; забезпечення рівної безпеки для всіх держав; створення дієвих гарантій у різних сферах життєдіяльності; недопущення використання зброї масового знищення та її повна ліквідація; повага суверенних прав кожного народу; справедливе політичне врегулювання міжнародних криз і регіональних конфліктів; зміцнення міждержавної довіри; вироблення ефективних методів запобігання міжнародному тероризму; викорінення геноциду, апартеїду, вилучення з міжнародної практики всіх форм дискримінації, запровадження нового економічного порядку, що забезпечує рівну економічну безпеку всіх держав. І тут головне, щоб система несла у собі ідею попередження та недопущення війни, застосовуючи справді робочі методи до дипломатичного вирішення кризових питань між державами, не доводячи ситуацію до критичної точки [1].

Якщо розглядати концепти бачення міжнародної безпеки, варто згадати Е. Н. Карра та Ганса Моргентау, які вважали, що міжнародна система

розглядається як досить жорстока арена, на якій держави намагатимуться досягти власної безпеки за рахунок своїх сусідів [107]. Міждержавні відносини розглядалися як боротьба за владу, оскільки держави постійно намагалися скористатися одна одною. Згідно з цією точкою зору, навряд вдасться досягти постійного миру. Все, що можуть зробити держави, це спробувати врівноважити силу одне одного, щоб не дати будь-якій з них досягти глобальної гегемонії. Відносячись до реалістичного крила трактування міжнародних відносин та спираючись на концепт сильних національних держав та суверенітету. Характерною рисою міжнародної політики реалістами вважається анархічність та відсутність влади регулювати взаємодію між державами. Реалізм базуються на трьох основних припущеннях: згуртованість, егоїзм та утримання влади. Згідно з класичними реалістами, більшість конфліктів між державами відбуваються тому, що люди, які вповноважені здійснюють зовнішню політику держави, діють зі своїх егоїстичних бажань, і саме вони є визначним фактором формування політики власне держав, яка зрештою і приводить до конфлікту. Отож, виходячи з їхнього бачення, можна сказати приблизно наступне: війна – неминуча, а мир – лише тимчасове явище [167].

На противагу «песимістичного» бачення міжнародної взаємодії реалістів, ліберальне крило теоретиків міжнародних відносин стверджує, що саме міжнародні інституції відіграють ключову роль у співпраці між державами. Як відзначають у своїй роботі Шираєв Е. Б. та Зубок В. М. [155], ліберали відходять від визначної ролі саме національних держав та егоїстичних мотивів їхнього керівництва, та стверджують, що окрім них – вплив на міжнародні відносини, і зокрема міжнародну безпеку здійснюють також транснаціональні корпорації, міжнародні інституції та міжнародна культурна дипломатія (зокрема й туризм). Держави при цьому взаємодіють різними способами, за допомогою економічних, фінансових і культурних засобів; безпека, як правило, не є основною метою взаємодії між державами; і

військові сили зазвичай не використовуються. Ліберали також стверджують, що міжнародна дипломатія може бути дуже ефективним способом змусити держави взаємодіяти одна з одною чесно та підтримувати ненасильницькі рішення проблем. Маючи відповідні інституції та дипломатію, ліберали вірять, що держави можуть працювати разом, щоб максимізувати процвітання та мінімізувати конфлікт [154].

Взагалі, дослідники Чернега О. Б. та Іваненко І. А. у своїй роботі «НАТО та система міжнародної безпеки», відзначали наступне: «Під поняттям «системи міжнародної безпеки» слід розуміти комплекс взаємопов'язаних міждержавних відносин та організацій, політичних, дипломатичних, економічних, військових і суспільних заходів, що спрямовані на забезпечення колективної безпеки держав і народів. Основними елементами системи міжнародної безпеки є основні принципи безпеки, міждержавні механізми та структури, міжнародно-правові норми, багатосторонні договори, які створюються, приймаються та функціонують з метою запобігання військовим зіткненням, їх локалізації, врегулюванню політичних, економічних і воєнних-стратегічних протиріч політичним шляхом, а також спеціальний режим контролю за міжнародною, особливо військовою діяльністю та відповідний режим інформації» [74].

Розглядаючи нинішню систему міжнародної безпеки необхідно дивитися на неї через призму бажання провідних держав після завершення Другої світової війни, побудувати таку структуру, яка б несла у собі загальне бажання усього світу до утвердження довготривалих мирних відносин зі спрямування на добробут усіх людей, а також вирішення питань через дипломатію. Невдалий досвід Ліги Націй спонукав до впровадження такої системи, яка б не носила у собі дискримінаційний характер для жодної сторони, а також містила у собі єдині права та обов'язки. Головна роль миротворчого процесу у цьому плані покладалася на Організацію Об'єднаних Націй та підконтрольні їй структури. Статут ООН мав у собі чіткий принцип,

а саме принцип неподільності світу, що вимагає від держав реагування на будь-які порушення миру і безпеки у будь-якій частині світу, їх участь у спільних діях, спрямованих на запобігання або ліквідацію існуючої загрози [62].

Відповідно до Статуту Організації Об'єднаних Націй система колективних заходів полягає у: заходах по забороні загрози силою або її застосуванні у відносинах між державами; заходах мирного дозволу міжнародних суперечок; заходах роззброєння; заходах з використання регіональних організацій безпеки; тимчасових заходах по припиненню порушень миру; примусових заходах з безпеки без використання збройних сил; примусових заходах безпеки з використанням збройних сил.

В міжнародному праві, під колективною безпекою розуміється система спільних дій держав, що встановлена Статутом Організації Об'єднаний націй з метою підтримки міжнародного миру і безпеки, запобігання та протидії актам агресії. Водночас, якщо розглядати колективну безпеку, як систему спільних дій держав, то можна виокремити перелік її структурних елементів, серед яких:

- загальноприйняті принципи сучасного міжнародного права (принцип незастосування сили або погрози силою, принцип непорушності кордонів, принцип територіальної цілісності, принцип невтручання у загальнодержавні справи);
- колективні заходи, що спрямовані на запобігання та усунення загроз миру та актів агресії (являють собою дії неозброєного або збройного характеру, які здійснюються державами та організаціями, уповноваженими на підтримку, відновлення міжнародного миру та безпеки);
- колективні заходи щодо обмеження і скорочення озброєнь, що мають кінцеву мету – повне роззброєння [62].

На фоні створення системи колективного контролю над міжнародною безпекою в глобальному плані, і постає питання безпеки на нижчих рівнях, оскільки хоч світ наш наразі є переплетений як економічно та інформаційно, тим не менше, говорячи про ситуацію в цілому, варто зазначити певну тенденцію до стереотипізації чи навіть спотворення розуміння різними державами реальної ситуації у різних куточках світу. Цей фактор вкрай негативно впливає на клімат всередині владних кабінетів світових держав, а отже викривлює їхній погляд на методи вирішення проблем. З іншого ж боку, ООН – це радше дорадча структура аніж імператив, а тому її поради можна як виконати, так і проігнорувати. Тому, з метою більш якісного розуміння та забезпечення міжнародної безпеки на регіональному рівні, створюються організації, що мають на меті забезпечити мирне співіснування держав, які там знаходяться, покращити економічний та політичний клімат між ними, а також забезпечити стабільний розвиток країн-членів. Серед таких, достойними згадки є: Організація з Безпеки і Співробітництва в Європі (ОБСЄ), організація, що об'єднує у собі 57 країн Європи, Центральної Азії та Північної Америки, та забезпечує комунікацію між державами, охоплюючи як політичний аспект, так і військовий, економічний та людський [44]; Європейський Союз (ЄС), в рамках якого здійснюється співпраця між європейськими державами-членами, заради координації спільної загальноєвропейської політики, а також розвитку добросусідства та недопущення конфлікту всередині європейського континенту, оскільки досвід обох Світових воєн показав, що саме Європа – стала місцем початку цих кривавих подій минулого [85]; Ліга арабських держав (ЛАД) – що є об'єднанням держав арабського світу, та створена для того щоб забезпечити інтереси цих країн у світі, а також співпраці держав заради їхнього економічного та політичного процвітання [42]; Шанхайська Організація Співробітництва (ШОС), ініціатива що об'єднує у собі країни Центральної та

Східної Азії, декларуючи співпрацю та добросусідські відносини між цими державами, а також зміцнення політико-економічної співпраці [26].

Та окрім регіональних організацій, що створені на основі політичної та економічної співпраці, існують іще й організації, що носять оборонний характер та безпосередньо стосуються військового потенціалу та збройних сил конкретних держав, що об'єднуються саме задля забезпечення колективної безпеки у разі якщо одній зі сторін загрожує небезпека. Такими організаціями зокрема виступають Організація Північноатлантичного договору (НАТО), яка об'єднує у собі 31 країну Європи та Північної Америки [43]; в певному сенсі, її клон у вигляді Організації Договору про колективну безпеку (ОДКБ), що об'єднує у собі Білорусь, Вірменію, Казахстан, Киргизстан, Росію та Таджикистан [45]. Такі структури одразу ставлять собі за основу саме військовий аспект безпеки, та діють відповідно до того, щоб забезпечити колективну оборону кожної з країни учасниць.

Проте безпека, у її класичному трактуванні, покриває далеко не усі виміри сучасного світу. Зокрема, у контексті розвитку технологічного процесу на планеті, ми постійно стикаємося з питанням сучасних заходів безпеки у кіберпросторі. Впровадження сучасних інформаційних технологій у всі сфери нашого життя, починаючи з телефонів у наших руках, та закінчуючи гігантськими серверами з секретною інформацією у державних структурах, потенційно несуть у собі інтерес осіб чи груп осіб, які б воліли скористатися ними задля отримання вигоди. До того ж, глобалізація та діджиталізація інформаційних відносин між індивідами та державами породжують загальносвітову тенденцію до зростання кількості злочинів у кібернетичному просторі. На сьогодні кіберзлочинність може нести у собі загрозу не тільки у питаннях прав та свобод громадянина, але й національних інтересів держав, при цьому не віднуваючи жодних кордонів ні фізичних, ні цифрових.

Світ зіткається з високою вразливістю кіберпростору перед обличчям ворожих кібератак, дій злочинних бандитських угруповань, хакерів, а також, груп та осіб з сумнівними намірами, які мають доступ до службових документів та інформації (вони ж інсайдери), що потенційно можуть надати їх для кола зацікавлених сторін. І подібні ситуації негативного кібер-впливу стають частішими. Вони більш організовані, та з кожним днем стають легшими та доступнішими в плані реалізації [64].

А зважаючи на те, наскільки буремно та стрімко зростає попит на цифрові та хмарні носії інформації, держави світу постають перед питанням захисту свого населення, а також інформації в умовах тотальної світової мережі. Кібер-фронт, як би автор назвав цей напрямок безпеки, наразі є одним із найважливіших у світі, а надто для України та колективного Заходу в умовах відкритої війни з Російською Федерацією (РФ) та блоком держав які її спонсорують та підтримують безпосередньо чи опосередковано. Бо з кожним днем, всесвітня мережа росте та пускає своє коріння все глибше і глибше. Створюються нові способи обману та отримання даних в обхід систем захисту, удосконалюються схеми кібер-шахрайства, що проявляються, наприклад, у: хакерських атаках, фішінг-операціях, зливах секретної інформації, поширення вірусів, «троянівських» програм, тощо [5].

Саме тому, створюється система заходів, що несуть у собі мету – протидіяти подібного роду злочинцям, які діють у кіберпросторі. Подібний комплекс заходів і прийнято називати «Кібербезпека». Сам термін, як відзначає у своїй роботі Баранов О.А. [3], з'явився у широкому загалі у 1990-х роках у США, коли на зламі тисячоліть технології досягли своєї розповсюдженості у світі настільки, що питання безпеки цього кіберпростору потребувало регуляції та регламентації на державному та міжнародному рівнях.

Проте, варто також відзначити, що досі існує розбіжність у точності визначення цього поняття у міжнародних нормативно-правових актах. Юриспруденція різних країн світу досі не може прийти до єдиного уніфікованого визначення даного поняття для застосування у міжнародній практиці, чим неабияк створюють проблему для правоохоронних органів в питанні притягнення винних до відповідальності. І тому, подібний напрямок є дуже важливим та перспективним для подальшого опрацювання та дискусій на глобальному рівні [8].

Боротьба ж натомість з кіберзлочинністю часто стає справою, яка потребує рішучості від урядів та держав за принципом «робити на вчора». Так як, зважаючи на швидкість модифікації та вдосконалення квантового простору, зацікавлені сторони будуть і самі покращувати власні засоби для досягнення мети. Законодавча ж база держав часто пасе задніх у питанні актуальності методів, які лежать в основі їхньої боротьби. Через це ми й можемо спостерігати прогалини у нормативних документах, якими й користуються хакери та кібер-злочинці.

Отож, із зазначеного вище, робимо висновок про те, що кібербезпеку можемо класифікувати, як комплекс заходів та рішень які спрямовані на те, щоб забезпечити безпечне користування всесвітньою мережею, а також захистити важливі системи та інформацію від потенційних атак ззовні чи викрадення зсередини [37].

При цьому, коли питання заходить про безпеку, варто також відзначити, що будь-яка дія спрямована на захист, по суті є одним із засобів здійснення безпекових процедур. Сукупність же таких дій являють собою «систему забезпечення безпеки». Звертаючись до праць Ліпкана В. А. [30], а саме його монографії «Національна і міжнародна безпека у визначеннях та поняттях», отримаємо досить чітку дефініцію цього поняття, цитата: «система забезпечення безпеки – механізм із вироблення, перетворення і реалізації

концепції, стратегії і тактики у сфері безпеки за допомогою скоординованої діяльності державних і недержавних структур; сукупність організаційно об'єднаних органів управління, сил і засобів, призначених для вирішення завдань щодо забезпечення національної безпеки».

Кожна країна при цьому визначає свої аспекти роботи системи забезпечення, як у розрізі роботи спеціальних органів, яких наділяють функціями регуляції питань кібербезпеки держави та користувачів, так і заходів спрямованих на забезпечення цієї самої кібербезпеки. При цьому, коли постає питання роботи відомств регуляції, на законодавчому рівні затверджується розподіл завдань та обов'язків, які мають ними здійснюватися. В процесі їхньої роботи мають бути визначені потенційні загрози національній безпеці, питання класифікації кіберзлочинів за ступенем тяжкості та зони відповідальності, а також інформування вищих органів про кіберінциденти, які мали місце бути за час роботи відомства. До таких прийнято відносити ситуації за яких, у ненавмисному порядку, було спричинено подію чи ряд подій, які містили у собі потенційні ознаки кібератаки. Забезпечуючи інформацією відносно цих випадків, держава має змогу відслідкувати та запобігти ескалації проблеми, що в свою чергу показує ефективність цих заходів [49].

Та одного бажання держави зазвичай буває замало. І постає питання того наскільки розвинуто механізм комунікації з суспільством та приватними підприємствами, як основними користувачами мережі. В такому випадку зазвичай вдаються до кампаній на тему того наскільки важливий діалог між владою та суспільством, зокрема в кібер-інформаційному просторі. В таких випадках, якщо користувач або стає жертвою кіберзлочинця, чи є свідком забороненої діяльності, він може своїми діями допомогти відповідним органам держави притягнути зловмисників до відповідальності [36].

І так як ми вже торкаємося питання кіберзлочинів, яким необхідно протидіяти, то до них відносяться не тільки хакерські атаки та шахрайські схеми, але й розповсюдження небажаного контенту, які несе у собі характер загрози чи з морального, чи безпекового боку. Тому, якщо звертатися до праць Вдовенка С. Г., умовно їх можна розділити на категорії за об'єктом здійснення злочину та характером використання предмету злочину, а саме комп'ютерних технологій [7].

До першої категорії ми можемо віднести злочини: які пов'язані з отриманням економічної вигоди; такі що зачіпають особисті права та недоторканість приватної сфери; і, звичайно, справи які зачіпають державний сегмент та національну безпеку. В таких випадках, засоби масової інформації та державні посадовці звикли використовувати до таких людей термін – хакер. Але цей термін логічно використати лише тоді, коли саме питання стоїть у площині отримання зловмисником прибутку чи помсти. Натомість, коли питання не стоїть у грошах, а радше у площині переконань та ідеології, яку суб'єкт намагається донести через вчинення кібератаки – подібних людей називають хактивістами. Через використання DDoS-атак (атака на комп'ютерні системи органу, організації, установи з метою порушення доступності атакованих веб-ресурсів. Створюється перевантаження системи за рахунок великої кількості запитів на сторінці) вони можуть оприлюднити небажану конфіденційну інформацію об'єкта своєї атаки, щоб змусити їх до співпраці [33].

До другої категорії ми відносимо те, як саме та за яких обставин зловмисниками було використано комп'ютер чи комп'ютерну систему. Умовно їх можна розділити на три групи:

1. *Комп'ютер є предметом злочину.* В цьому випадку злочинець, заволодівши доступом до чужого пристрою, виконує пряму деструктивну функцію, яка спрямована на отримання

несанкціонованого доступу, пошкодженні та спотворенні інформації на носії іншої сторони;

2. *Комп'ютер використовується як знаряддя злочину.* В цьому випадку злочинець, використовуючи особистий комп'ютер чи комп'ютерну систему, застосовує їх для незаконного отримання та заволодіння інформації зі стороннього носія, чи отримання контролю над ним;
3. *Комп'ютер є інтелектуальним засобом.* В цьому випадку злочинець, використовуючи комп'ютер чи комп'ютерну систему, розміщує у вільному доступі певний контент, який носить заборонений характер (сцени насилля, порнографічні матеріали, компрометуючі матеріали) задля отримання вигоди, як грошової, так і ідеологічно-інформаційної [6].

1.2 Науково-концептуальні підходи у розумінні кібербезпеки

Отож, щоб розкрити питання того, що саме ми вкладаємо у визначення кібербезпеки, звернемося до офіційних документів, які містять у собі визначення цього поняття. У чинному Законі України «Про основні засади забезпечення кібербезпеки України» від 17 серпня 2022 року, у Статті 1, можемо прочитати наступне: «Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [52].

У цьому ж законі, можемо також отримати визначення до понять кібероборона та кіберзахист. Цитата: «Кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на

запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем»; «Кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії» [52].

Зазвичай, у нашій державі було прийнято за основу розуміння того, що кібербезпека та національна безпека є по суті своїй синонімами. Ця концепція навіть була викладена у нормативно правових документах як Стратегія кібербезпеки України та Закону України «Про основи національної безпеки України». І як правильно зауважив у своїй роботі дослідник Діордіца І.В. в своїй роботі «Система забезпечення кібербезпеки: сутність та призначення», подібний підхід є хибним. Там під кібербезпекою розуміється, цитата: «стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів [16].

Водночас, як відзначає Діордіца І. В., зважаючи на те, що відкритість процесів розроблення документів м'яко кажучи питання досить дискусійне, поява такої формули побудови даного поняття свідчить про небажання авторів подібних нормативно-правових актів прислуховуватись до думок наукового співтовариства і їхнє несприйняття аргументів щодо неправильності і помилковості співставлення безпеки та стану захищеності [16].

Кожна держава в цьому плані, індивідуально та на власному законодавчому рівні визначає сфери, які вона буде відносити до кібернетичної безпеки. Зокрема це стосується таких пунктів як:

- точний перелік об’єктів і суб’єктів забезпечення кібернетичної безпеки;
- стратегічні цілі і завдань, які стоять перед державою на національному та міжнародному рівнях;
- практичних можливостей реалізації національних інтересів [16].

На нинішньому етапі, виходячи з проведеного дослідником аналізу елементів національної системи кібербезпеки, подання на загал поняття кібернетичної безпеки, поки використовується у вищих колах лише як складова частина поняття інформаційної безпеки. Це аргументується тим, що сутності та природа загроз, методів, засобів і заходів у них однакові і обмежені тільки рамками кіберпростору.

При цьому, як говорить у своїх записах Войціховський А. В. [11], підходи до формування стратегій кібербезпеки у кожній державі відрізняються саме у контексті підходу до нього з боку законодавчої основи, яка лежить у нормативно-правових документах.

У цьому випадку, ми розглядаємо основоположні документи, які містять у собі питання кібербезпеки. У них зазвичай описуються такі питання:

- створення державної системи управління у сфері забезпечення кібербезпеки;
- виокремлення відповідного механізму, який надає можливість як приватним так і державним зацікавленим сторонам обговорювати проблеми забезпечення безпеки національних інформаційних систем;
- упорядкування стратегічних основ політики у питаннях безпеки та механізмів регулювання, відповідний розподіл завдань, прав та відповідальності для приватного і державного секторів (наприклад, обов’язкове інформування про кіберінциденти, оцінка загроз, розробка критеріїв віднесення об’єктів до критичної інформаційної інфраструктури тощо).

Сьогодні більшість держав світу успішно проводять політику посилення кібербезпеки. У цьому плані, з міжнародної точки зору, за Номоконовим В. А. та Тропиною Т. Л. можна виділити три основні моделі правового врегулювання поширення інформації в мережі Інтернет.

1. Перша модель передбачає повний, та всеосяжний контроль держави над всесвітньою мережею. Подібної моделі притримується такі країни як, наприклад, Китайська Народна Республіка, де майже весь Інтернет перебуває під повним державним контролем. Між іншим, певні елементи китайського досвіду сьогодні впроваджуються в практичну площину в країні-агресорі Російській Федерації.
2. Друга модель вимагає від провайдера відповідальність за будь-які дії користувача. До прикладу, у Франції провайдерів було зобов'язано надавати відомості про авторів сайтів на вимогу третіх осіб..
3. Третя модель регулювання безпеки в мережі прописує звільнення провайдера від відповідальності в разі, якщо він виконує певні умови, пов'язані з характером надання послуг і взаємодії із суб'єктами інформаційного обміну. Так, в Німеччині відповідальність провайдерів за розміщення нелегального контенту на Інтернет-ресурсах, що знаходяться в їх мережі, настає лише в разі, якщо вони самі є власником інформації або свідомо поширювали її з посиланням на інші джерела. До країн у яких поширена ця система також належить Японія [40].

В свою чергу, іноземні автори у цьому питанні сходяться на іншій думці. Зокрема у концепції викладеній дослідниками Деном Крейгеном, Надькою Діакун-Тібо та Ренді Перс, у своїй роботі «Defining Cybersecurity»[100], де вони оглядали підхід західних вчених у розумінні поняття кібербезпеки, зазначали наступне. Відносно того, що саме стосується терміну «безпека», то в розглянутій ними літературі воно не має широкого визнання, і цей термін, як відомо, важко визначати в загальному сенсі. За Бузаном, Уевером і Уайлдом

[91], дискурси безпеки обов'язково включають і прагнути зрозуміти, хто надає захист, з яких питань (загрози), для кого (опорний об'єкт), чому, з які результати і за яких умов (структура).

Хоча існують більш конкретні форми безпеки (наприклад, фізичні властивості, властивості людини, властивості інформаційної системи або математичні визначення для різних видів безпеки), цей термін набуває значення на основі власної точки зору та того, що ви цінуєте. Це залишається спірним терміном, але центральним принципом безпеки є відсутність небезпеки чи загрози [143]. Крім того, хоча вони відзначили, що безпека є спірною темою. Дослідник Болдуїн [88] у своїй роботі стверджує, що цей термін не можна використовувати для позначення як «виправдання для того, щоб не сформулювати власне уявлення про безпеку максимально чітко і точно».

У результаті їхнього огляду літератури було відібрано дев'ять визначень кібербезпеки, які, на думку дослідників, надають матеріальні перспективи:

1. За Річардом А. Кеммерером — професором лідерства в інформатиці та колишнім завідувачем кафедри інформатики Каліфорнійського університету, дається наступне визначення: «Кібербезпека в основному складається з захисних методів, які використовуються для виявлення та запобігання потенційним зловмисникам» [126].
2. Дженіфер Льюіс, доктор наук та спеціаліст у сфері біоінженерії та сучасних технологій Національної академії винахідників США пропонує наступне визначення: «Кібербезпека передбачає захист комп'ютерних мереж та інформації, що в них міститься, від проникнення та зловмисного пошкодження чи збою» [129].
3. Едвард Г. Аморозо — американський професіонал із комп'ютерної безпеки, підприємець, письменник і викладач, чиї дослідницькі інтереси зосереджені на методах і критеріях вимірювання надійної

розробки програмного забезпечення, у своїй роботі «Cyber Security» пропонує наступне визначення: «Кібербезпека передбачає зниження ризику зловмисної атаки на програмне забезпечення, комп'ютери та мережі. Це включає інструменти, які використовуються для виявлення зломів, зупинки вірусів, блокування зловмисного доступу, примусової автентифікації, увімкнення зашифрованого зв'язку тощо» [84].

4. Міжнародна спілка електрозв'язку – міжнародна організація, що визначає стандарти та дає рекомендації в галузі телекомунікацій та радіо, зазначає наступне: «Кібербезпека — це сукупність інструментів, політик, концепцій безпеки, заходів безпеки, інструкцій, підходів до управління ризиками, дій, навчання, найкращих практик, гарантій і технологій, які можна використовувати для захисту кіберсередовища, організації та активів користувачів» [124].
5. «Здатність захищати або захищати використання кіберпростору від кібератак» – саме таке визначення дає кібербезпеці Комітет із систем національної безпеки (CNSS), міжурядова організація Сполучених Штатів, яка встановлює політику безпеки систем безпеки США [95].
6. Міністерство громадської безпеки Канади, відповідальним за більшість питань громадської безпеки, управління надзвичайними ситуаціями, національної безпеки та готовності до надзвичайних ситуацій у Канаді, дає наступне визначення кібербезпеці: «Сукупність технологій, процесів, методів і заходів реагування та пом'якшення, розроблених для захисту мереж, комп'ютерів, програм і даних від атак, пошкоджень або несанкціонованого доступу з метою забезпечення конфіденційності, цілісності та доступності» [145].
7. «Мистецтво забезпечення існування та безперервності інформаційного суспільства нації, гарантування та захист у

кіберпросторі її інформації, активів та критичної інфраструктури» – визначення запропоноване бразильськими дослідниками Клаудією Канонгія і Рафаелем Мандаріно [92].

8. Oxford University Press пропонує наступне визначення кібербезпеки: «Стан захисту від злочинного або несанкціонованого використання електронних даних або заходи, вжиті для досягнення цього» [143].
9. «Діяльність або процес, здатність або спроможність або стан, за допомогою якого інформаційно-комунікаційні системи та інформація, що в них міститься, захищені від та/або захищені від пошкодження, несанкціонованого використання, модифікації чи експлуатації» – визначення запропоноване Міністерством національної безпеки США. [104].

Хоча деякі з цих визначень містять посилання на нетехнічну діяльність і взаємодію людей, вони демонструють переважання технічної точки зору в літературі. Як зазначив Кавелті [93], дискурс і дослідження кібербезпеки «неодмінно змішуються до контекстів і умов, які визначають процес, за допомогою якого ключові суб'єкти суб'єктивно приходять до спільного розуміння того, як виробити загальну концепцію загрози безпеці та в кінцевому підсумку реагувати на неї». Відповідно, у конкретному контексті наведені вище визначення є корисними, але не обов'язково забезпечують цілісне уявлення, яке підтримує міждисциплінарність. Повертаючись до обговорення досліджень питання захисту, посилаючись на роботи Бузана, Уевера і Уайлда [91], будь-яке визначення має бути в змозі охопити розуміння актора, суб'єкта, референтного об'єкта, намірів і цілей, результатів і структури. У огляді представленому Деном Крейгеном, Надьєю Діакун-Тібо та Ренді Перс, не було знайдено універсального визначення, яке було б всеосяжним, впливовим та об'єднуючим. Кібербезпека на їхню думку, це складний виклик, який потребує міждисциплінарного обґрунтування, отже, будь-яке кінцеве визначення має залучати на даний момент різнорідних

зацікавлених сторін у сфері кібербезпеки, водночас бути неупередженим, значущим і фундаментально корисним.

Тому, дослідниками було запропоноване наступне визначення, яке об'єднує ключові концепції, взяті з оглянутими ними джерел: «Кібербезпека – це організація та сукупність ресурсів, процесів і структур, які використовуються для захисту кіберпростору та систем, що підтримують кіберпростор, від подій, які не відповідають де-юре та де-факто фактичні права власності» [100].

Девід Стаблі, генеральний директор «7 Elements», компанії яка має спеціалізацію на тестуванні ІТ-безпеки, в Единбурзі, яку він заснував після 13 років досвіду роботи в галузі тестування кібербезпеки Сполученого Королівства, у своїй статті зазначає, що кібербезпека є широко вживаним терміном, про який більшість людей уже чули. Багатьом доведеться розуміти цей термін, якщо їм доручено захистити інформаційні системи [159].

Однак існує багато визначень, у яких використовується слово «кібер», і я вважаю, що вони часто плутають, наприклад: «Кібербезпека передбачає захист інформації та систем від основних кіберзагроз, таких як кібертероризм, кібервійна та кібершпигунство».

На жаль, його часто використовують як частину рекламної пропозиції, і його часто можна зловживати для створення стану страху, невизначеності та сумнівів, спрямованого на підвищення інтересу до продукту чи послуги. В своїй практиці, люди часто зустрічатимуть такі терміни, як кіберзлочинність, кіберстратегія, поінформованість про кібербезпеку та кіберзагроза.

Отже, дивлячись на те, як визначити кібербезпеку, якщо спиратись на наше розуміння кібербезпеки, можемо побачити, що ми зараз говоримо про безпеку інформаційних технологій і комп'ютерів. Це, по суті, старомодні засоби контролю інформаційної безпеки.

Тому Девід Стаблі відзначає, що поняття «кібербезпека» слід замінити на: "Інформаційна безпека". Чим в принципі його концепція є дуже схожою до тієї, яку сповідують наші вітчизняні автори [159].

Також, деякі з українських дослідників вважають, що підхід до нормативно-правового розуміння загальнонаціональної та інформаційної безпеки містить у собі як поняття того наскільки добре захищені життєво важливі інтереси людини й громадянина, а заразом, держави. При цьому, як відзначається, потрібно надати сталий розвиток суспільства, при якому будуть присутні своєчасні виявлення, запобігання і обов'язково нейтралізація потенційних та нагальних загроз національним інтересам. Особливо це стосується площини функціонування інформаційно-телекомунікаційних систем (ІТС).

Подібним варіантом подачі визначенням кібербезпеки, дослідники визначають в якості об'єкта загроз – національні інтереси у сфері функціонування інформаційно-телекомунікаційних систем, що вкрай зменшує діапазон можливих життєво важливих інтересів людини і громадянина, суспільства і держави [159].

До того ж, можливість використання в якості критерію ступеню захищеності інтересів людини і громадянина, суспільства і держави, критерій, на зразок «стабільний розвиток суспільства» не дозволяє диференціювати методологічну основу при оцінці рівня подібної захищеності, оскільки непросто дати кількісні та якісні оцінки «стабільного розвитку».

Дослідник Фурашев В.Н. [72] у своїй роботі дає визначення поняттю «кібербезпека» – як стан здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу інформації.

При цьому трактуванні, досить важливою методологічною складовою для визначення обсягу юрисдикції для поняття «кібербезпеки», є дослідження

та розуміння об’єкта потенційних загроз, а також при цьому чітко розрізняти види та типи можливих збитків завданих такими загрозами. Ця інформація та чітке розуміння ситуації мають високу цінність, яку можна та потрібно застосовувати на практиці. Оскільки, саме від них залежатиме змістовна частина формування стратегій кібербезпеки, і при всьому тому, рівень охопленості об’єктів, які підпадають під такі дії відносно убезпечення кібербезпеки, а також рівень та склад інституційних органів, та перелік і обсяги ресурсів, що мають бути при цьому задіяні.

Так як ми розглядаємо саме цільове призначення таких систем, що складаються з комп’ютерних систем та телекомунікаційних мереж, ми робимо висновок про те, що можливі загрози які носять кібернетичний характер, в першу чергу націлені на порушення та виведення з ладу обігу інформації. За таких обставин, мова може вже йти як про фундаментальні системні загрози, що напряму несуть у собі мету – порушення обігу інформації. І тоді мова йтиме про порушення на будь-якому з його етапів – будь то створення, поширення, використання, чи зберіганні і знищенні інформації. При всьому тому, тоді ми можемо отримати кіберзагрози, що пов’язані з недостовірністю, несвоєчасністю і неповнотою інформації. Ба більше, до подібного типу загроз слід також віднести загрози, що можуть бути пов’язані з несанкціонованим використанням та поширенням інформації, порушенням її цілісності та конфіденційності [15].

Висновки до розділу 1

Концептуальний підхід до характеризації питання прописування різнобічних аспектів, які містить у собі термін «кібербезпека», є нагальним у сучасному світі. І попри те, що саме термінологія та чіткість запропонованих дослідниками визначень є досить суперечливими з точки зору кожної зі сторін, тим не менше кожна з них не настільки далека від істини. Зрештою, всі вони сходяться на думці, що кібербезпека – є певним комплексом методів та інструментів, за допомогою яких здійснюється захист даних користувачів.

Система забезпечення кібербезпеки являє собою цілісну систему, складові частини якої тісно переплетені між собою. Основними елементами цієї системи є її суб'єкти та об'єкти.

Як і при визначенні основних об'єктів системи забезпечення кібербезпеки, також слід визначати національні цінності, а з ними і національні інтереси держави. Суб'єктами забезпечення безпеки кіберпростору, незалежно від форми власності, виступають державні структури, органи місцевого самоврядування, підприємства, установи, організації. Вони і впроваджують проектування, та використання складових критичних об'єктів національної інформаційної інфраструктури або забезпечують їх кіберзахист.

Головною метою системи забезпечення кібербезпеки є сприяння у досягненні цілей кібернетичної безпеки. При цьому, глобальною складовою даної системи можна вважати забезпечення упорядкованого існування інтересів особи, суспільства і держави шляхом здійснення перевірок, діагностування; виявлення та ідентифікацію, запобігання та припинення, мінімізацію та нейтралізацію дії внутрішніх і зовнішніх загроз і небезпек.

РОЗДІЛ 2: ЗАХИСТ КІБЕРБЕЗПЕКИ В ПОЛІТИЦІ ДЕРЖАВ СВІТУ

2.1 Американський та європейський досвід у забезпеченні кібербезпеки

Сполучені Штати Америки, як одні з тих, хто став першопроходьцем у створенні системи кіберзахисту для своєї держави, завжди спиралися на парадигму того, що саме технологічний прогрес та впровадження новітніх комп'ютерних систем – є запорукою розвитку, а також зміцнення потенціалу держави та світу загалом [162]. Тому, у 2005 р. у США за підтримки уряду було впроваджено «Федеральну програму Дослідження та розробка мереж та інформаційних технологій» (Networking and Information Technology Research and Development (NITRD)). Щорічно з американського бюджету виділяється 2,5 мільярда доларів на її функціонування. Загалом програма NITRD спрямована на те, щоб розвивати та впроваджувати наукові дослідження й розробки, які мають на меті забезпечення технологічного лідерства США в сфері створення сучасних мереж, обчислювальних систем та приладів, а також програмного забезпечення. На плечі даної програми покладено втілення ряду заходів, які безпосередньо зачіпають питання швидкої розробки та задіяння технологій для забезпечення національної безпеки, а саме зміцнення національної оборони і національної безпеки та підвищення конкурентоспроможності США на світовому ринку технологій, стабільне економічне зростання та добробут для громадян [83, 170].

Пізніше, в дусі програми NITRD, Президентом США, у 2011 році, було підписано «Міжнародну стратегію дій у кіберпросторі (Процвітання, безпека і відкритість в мережевому світі)» (International Strategy for cyberspace (Prosperity, Security and Openness in a Networked World). В ній було прописано та регламентовано план США відносно питань співпраці між державами та народами світу, з метою реалізації парадигми кібербезпеки. Там же було визначено головні характеристики цієї стратегії: відкритість держав для

інновацій; взаємодія у питаннях кіберпростору по всьому світу; довіра між країнами та партнерство.

Початок же здійснення реальних заходів відносно протекції кіберпростору США від зовнішніх та внутрішніх ворогів, що і нині лежить в основі дій Білого Дому, було запропоновано колишнім Президентом Джорджем Бущем, який 8 січня 2008 року видав директиву із забезпечення національної безпеки № 54 (National Security Presidential Directive 54 – NSPD-54) та NSPD-54 безпеки № 23 (Homeland Security Presidential Directive 23 - HSPD-23). Цей комплекс заходів отримав назву Комплексна національна ініціатива забезпечення кібернетичної безпеки (The Comprehensive National Cybersecurity Initiative (CNCI)) [161].

CNCI містить у собі достатньо широкий спектр тісно пов'язаних напрямів діяльності, які мають на меті задовольнити вирішення досить масштабних завдань, спрямованих на посилення захисту кіберпростору США у довгостроковій перспективі. Виконанням цієї програми займаються відомства починаючи від місцевих адміністрацій, і аж до федеральних органів США.

У програмі чітко прописано завдання які ставляться перед органами забезпечення кібербезпеки держави, а саме:

1. Перед відомствами ставиться питання дефініції так званої, «лінії оборони» від можливих атак ймовірних противників, а також забезпечення необхідних умов для отримання інформації безпосередньо фахівцями федерального уряду про точки вразливості національних комп'ютерних мереж, загрози безпеці та інциденти, які мали місце при функціонуванні автоматизованих систем, що забезпечують життєдіяльність держави США.
2. Контррозвідувальні органи США мають забезпечувати захист інформаційної безпеки на всіх можливих рівнях через розширення

своїх технічних та оперативних можливостей. До того ж, впроваджується чітко регламентоване надання каналів поставок федеральним відомствам, владним структурам штатів, органам місцевого управління та приватним фірмам ключових інформаційних технологій у закритому форматі. Подібний захід спрямований на те, щоб вороги США не мали змогу дістатися до технологій та систем, які складають собою ядро американської безпеки.

3. Виконання комплексу заходів що мають на меті розширення системи підготовки фахівців з інформаційної безпеки, підвищення ефективності координації між науково-дослідницькими та дослідно-конструкторськими роботами у цій сфері, що отримують фінансування з федерального бюджету, а також впровадження дієвих механізмів їх своєчасної переорієнтації, з метою виключення невиправданих витрат на здійснення досліджень, які дублюють один одного [29].

За рік же до того моменту, як була представлена CNCI, а саме у 2009 році, Президенту США було представлено звіт під назвою «Огляд політики в кіберпросторі» (Cyberspace Policy Review). У ньому зокрема йшлося про аналіз стану галузі захисту інформації, та рекомендації спеціальної комісії відносно покращення систем охорони кіберпростору Америки. Там же, голові держави було запропоновано створити пост координатора з питань кібербезпеки, який мав регулярно доповідати йому про ступінь захищеності комп'ютерних систем США та про заходи, що проводяться у цій сфері [170].

В результаті цих дій, у США було створено таке об'єднання адміністративних структур, яке спроможне забезпечити організований та єдиний похід до протидії кібератакам на США.

Запроваджені заходи стали для США новою віхою у питанні убезпечення своєї національної безпеки на кібернетичному рівні. До того ж,

саме питання кадрового забезпечення цих дій є досить актуальним з точки зору того, що подібні проекти вимагають досить великих вкладів в плані мізків.

Тому, у згаданій раніше «Комплексній національній ініціативі забезпечення кібербезпеки» (Comprehensive National Cybersecurity Initiative), прийнятої урядом США, прописано запровадження спеціальної та загальної кіберосвіти має стати Національною стратегією кіберосвіти за аналогією Національної стратегії з «модернізації» -Х роках (8 розділ стратегії).

У цьому плані, наступною після «Комплексної національної ініціативи забезпечення кібербезпеки» стала «Президентська національна ініціатива в галузі кіберосвіти», яку було прийнято 19 квітня 2010 року [35]. У ній йдеться насамперед про те, що Агентство Національної Безпеки (АНБ), яка по суті має координувати питання, що стосуються підготовки кадрового забезпечення для кіберструктур США, впроваджує програму CAE-CO (Центр академічної майстерності в області Кібероперацій). Програма має на меті підготовку студентів для роботи в правоохоронних органах США, проводити розвідувальні операції, та розслідувати кіберзлочини. Головним завданням програми є скорочення імовірних вразливих місць у національній інформаційній інфраструктурі безпосередньо через сприяння покращенню якості вищої освіти та наукових досліджень у сфері кібербезпеки, підготовки більшої кількості фахівців, які б отримували практичні навички в рамках різних дисциплін.

В цій ініціативі чітко прописано коло відповідальних органів, а також цілі, які перед ними ставляться:

1. Інформування відомств національної кібербезпеки. Органом виконання цього завдання призначено Департамент внутрішньої безпеки (Department of Homeland Security – DHS).

2. Формалізація питань кібер-освіти. Відповідальний орган – Управління науково-технічної політики Департаменту освіти (Office of Science and Technology Policy).
3. Федеральна структура робочої сили у галузі кібербезпеки. Орган відповідальний за втілення цього - Офіс управління кадрами (Office of Personnel Management). Він має провести роботи з визначення навичок та компетенцій для посад у федеральному уряді, пов'язаних з питаннями забезпечення кібербезпеки та розробки нових правил щодо залучення кваліфікованих кадрів.
4. Навчання персоналу з кібербезпеки та їхній професійний розвиток. Відповідальна структура – Міністерство оборони (DoD), Адміністрація Директора Національної розвідки (Office of the Director of National Intelligence (ODNI)), Міністерство національної безпеки (Department of Homeland Security (DHS)) [35].

Одним із основних завдань «Комплексної національної ініціативи забезпечення кібербезпеки» є також вибір навчальних та наукових закладів, які мають займатися забезпеченням кібербезпеки. У питання їхньої компетенції входить і підготовка якісних кадрів. Дана процедура має проводиться на конкурсній основі серед навчальних та наукових закладів, в програму яких входить поглиблене вивчення технічних та міждисциплінарних навчальних програми, які зосереджені на таких галузях, як інформатика, обчислювальна техніка та електротехніка [94, 128].

Повертаючись же до більш сучасного стану кібербезпекових заходів США, то варто згадати, що 20 вересня 2018 року Міністерство оборони США представило Стратегію з кібербезпеки адміністрації Президента Д. Трампа [138]. Цей документ має на меті спростити сам процес узгодження кібербезпекових питань між силовими й оборонними відомствами. Відзначається також тенденція до того, що американці стають все більш залежними від сучасних цифрових технологій, чим у свою чергу стають більш

вразливими до таких загроз, як: корпоративні порушення безпеки, фішинг та шахрайство в соціальних мережах, кібератаки тощо. У Стратегії кібербезпеки США були заразом додані нові інструкції відносно дотримання безпеки в кіберпросторі для усіх федеральних відомств.

Між іншим у цій стратегії чітко прописаний наступальний характер Сполучених Штатів у міжнародному кіберпросторі. Положення даної стратегії, які попередніх, прийнятих Білим Домом, відзначають необхідність просування забезпеченості безпеки американських користувачів, а також державних органів від можливих атак з боку хакерів та спецслужб іноземних держав. Мова передусім йдеться про Китайську Народну Республіку (він же – комуністичний Китай (КНР)), Російську Федерацію, Ісламську Державу Іран, Північну Корею (Корейську Народну Демократичну Республіку) [138]. У документі також йдеться про те, що американські спецслужби матимуть більш розв'язані руки у питанні кібербезпеки та можливих дій у відповідь відносно потенційних порушників. Знову ж таки, дя програма несе у собі кілька важливих для кібербезпеки США завдань. Зокрема, у пріоритеті розробка та створення міжнародної політики відносно регуляції мережі Інтернеті, забезпечення державних структур та відомств компетентними та освіченими співробітниками [38], із досвідом роботи в сфері інформаційних технологій та розуміються в питаннях забезпечення кібербезпеки. Головною метою програми прописано – налагодження дієвого кіберзахисту, запобігання поширенню ризиків, пов'язаних із кібербезпекою, забезпечення безпеки національних інформаційних систем та мереж.

Відповідно до базових положень Стратегії кібербезпеки США, цитата: «кібербезпека – це комплекс заходів, спрямованих на захист комп'ютерних систем (включаючи апаратні засоби, програмне забезпечення та дані) від несанкціонованого доступу або атак через мережу Інтернет» [138]. Документ також зазначає інформацію про те, що Міністерство оборони США визнає комуністичний Китай та путінську Росію головними загрозами для світу у

кіберпросторі. Відзначається, що дій Китаю та його спецслужб, що задіяні у кіберпросторі несуть у собі деструктивну функцію, зокрема через присвоєння конфіденційної інформації, вони шкодять військовій та економічній безпеці та потужності США у світовому вимірі. Російська Федерацію, авторами стратегії описана як та, що проводить інформаційні операції, які мають на меті маніпуляцію свідомістю іноземних громадян, при цьому посягаючи на демократичні цінності та права людини в мережі Інтернет. Щоб протидіяти своїм ворогам, Сполучені Штати планують збільшити свій наступальний потенціал, а у разі війни – «боротися з супротивником за допомогою повітряних, сухопутних, морських і космічних сил». Документом також передбачено систему врегулювання ринку систем і засобів захисту інформації, йдеться уніфікацію устаткування та жорсткий відбір постачальників. Стратегія прописує і механізм відшкодування жертвам компенсації від замовників та виконувачів у разі кібератак.

Адміністрація США при цьому бере на себе зобов'язання застосувати усі можливі заходи для екстрадиції та притягнення до відповідальності обвинувачених у хакерських атаках громадян іноземних держав, а заразом і посилити кримінальну відповідальність за вчинені ними злочини. Тому ця стратегія націлена на те, що урядові структури США передаватимуть виробникам мережевого обладнання інформацію щодо можливості ймовірних ризиків та загроз. Як наслідок, виробникам необхідно буде виробляти обладнання окремо для користування всередині США, а також для іноземних покупців. А отже, ворожі системи обчислення та комп'ютерне обладнання, що використовують американські комплектуючі, не зможуть стримувати потенційні атаки. Наразі, за статистикою, найбільш вразливими місцями для США у питанні забезпечення кібербезпеки є космічна та транспортна галузі. Тут мова йдеться про безпеку морських вантажні перевезень, в головну чергу, газу і нафтопродуктів [58].

Серед перспективних напрямів у покращенні кіберзахисту, зокрема акцентується увага стратегії на:

- розробці міжнародної політики кіберстримування;
- спрощення регулюючих правил, які виступають регламентацією наступальних операцій у всесвітній мережі;
- відчутні та негативні наслідки для держав-супротивників, у разі якщо вони відбуватимуться у складі коаліції та будуть спрямовані проти безпеки США;
- здійснення наступальних кібер- та військових дій США в рамках реагування на кібератаку [77].

Нинішня стратегія кібербезпеки США є першим за останні 15 років чітко та детально сформульованим, і що найголовніше – робочим документом у цій сфері. Як відзначив тодішній радник президента США з національної безпеки Джон Болтон, подібна стратегія має на меті «розв'язати руки» керівництву США, зокрема в питанні проведення, як він зазначив, «наступальних» операцій у відповідь на кібератаки, тим самим полишивши політику оборони та замінивши її на активні дії у відповідь.

Саме тому, усвідомлюючи необхідність забезпечення кібербезпеки, Уряд США виділив на цей напрямок у 2021 році близько 5,4 млрд доларів. За словами Шемчука В., головними донорами цих коштів, відповідно до інформації опублікованої на сайті Міністерства оборони США, мають стати проекти забезпечення кібербезпеки, наступальні операцій у кіберпросторі, розробки у сфері штучного інтелекту та хмарні технології. Також відзначається необхідність покращення системи шифрування даних, що на думку посадовців, має допомогти у питанні зниження ризиків кібератак на урядові мережі [77].

Наприкінці березня 2021 року вже Адміністрація Джо Байдена заявила про те, що готується новий указ Президента США мета якого, як зазначалося,

це посилення кібербезпеки в сучасних реаліях. Було визначено 12 стратегічних кроків, за допомогою яких планувалося знизити кількість потенційних кіберінцидентів, а також відзначено можливі напрямки покращення захисту усіх об'єктів критичної інфраструктури. А вже у квітні 2021 року Сполучені Штати оголосили про створення 100-денного плану, основною ціллю якого є поліпшення кібербезпеки електроенергетичної інфраструктури країни. Документ пропонує кроки співпраці між федеральними органами США, зокрема міністерства енергетики та Агентства з кібербезпеки та інфраструктурної безпеки з приватними компаніями. Послужили подібному кроку останні події, що показали слабкі місця у захисті об'єктів енергосистеми США, яких не один раз спіткали хакерські атаки. Білий Дім зазначав, що не просто не виключає, а навіть впевнений, що за цими атаками стоять хакери з РФ. І саме тоді, як відповідь на подібне злісне порушення кібербезпеки США, американський уряд наклав санкції на шість російських технологічних компаній, пов'язаних з кібератакою на IT-компанію "SolarWinds" та зламом безпеки федеральних відомств, зокрема Міністерства енергетики США [138].

Як знову ж таки відзначив у своїй роботі Шемчук В., останні роки стали знаковими для США у питанні розуміння загрози з боку КНР, зокрема і у питаннях кібербезпеки. Отож, зважившись на це, Сенат США зайнявся розробкою та впровадження законопроєкту про державну підтримку для національних виробників мікро-чипів, щоб таким чином знизити залежність американських структур від іноземного імпорту. Підсумовуючи, зазначимо, що питання кібербезпеки для Сполучених Штатів з кожним роком набуває все більшої актуальності, зважаючи на збільшення кількості кібератак та чисельних випадків витоків та викрадення конфіденційної інформації яка напряму стосується національної безпеки. Нині існує тенденція того, що саме кіберпростір стає основною ареною бойових дій між державами, чим дуже актуалізується питання забезпечення та утримання власних позицій на

кіберфронті. І видно трансформацію поглядів американського керівництва від захисту до активної оборони та контратаки [77].

Європейський Союз також не відстає від своїх американських колег, та активно приділяє увагу безпеці кіберпростору. Ще у 2001 р. Європейська комісія підготувала свій перший документ регламентуючий кібербезпеку, який носив назву «Мережева та інформаційна безпека: європейський політичний підхід» (Network and Information Security: Proposal for A European Policy Approach). В цьому документі було запропоновано підхід до проблеми інформаційної безпеки саме з точки зору Європи. І тут ми бачимо, що тут поняття кібербезпеки трактується терміном «мережева та інформаційна безпека» [139].

Владні структури ЄС у своїх судженнях зауважують, що мережева та інформаційна безпека являє собою суттєвий та важливий фактор сучасного інформаційного суспільства, як у Європі, так і у світі. Відзначається також загроза витоку та крадіжки даних, що несуть пряму загрозу економічному добробуту громадян країн союзу. А хакерські атаки на інформаційні системи загрожують безпеці у національних масштабах країн-членів. Мова йде про ймовірні порушення систем комунікацій, витік конфіденційної інформації і т.д..

Щоб запобігти цьому, 10 березня 2004 р. було створено Європейське агентство з питань мережевої та інформаційної безпеки (European Union Agency for Network and Information Security - ENISA). ENISA – єдине з агентств ЄС, яке мало конкретний термін завершення її дії – 2020 р. Агентство функціонувало з 1 вересня 2005 р., і розташовувалося у місті Іракліон, Крит, (Греція) [149].

Основним стрижнем ENISA стало покращення мережевої та інформаційної безпеки у Європейському Союзі. На агентство покладалося завдання розвитку культури мережевої та інформаційної безпеки, щоб та

служила на користь громадян, споживачів, підприємств та громадських організацій Євросоюзу, надаючи безперебійну роботу внутрішнього ринку ЄС.

ENISA надавала поміч Єврокомісії, а також країнам-членам ЄС та приватному сектору економіки у питанні виконання вимог мережевої та інформаційної безпеки, згідно з чинним на той момент, та майбутнє законодавством ЄС. ENISA являла собою центр надання експертизи і для країн-членів, і основоположних структур ЄС з питань, що зачіпали отримання консультацій з питань, напряму пов'язаних із мережевою та інформаційною безпекою [82].

Агентство також має тісні зв'язки з Європейським поліцейським офісом (Europol) та Європейським центром боротьби з кіберзлочинністю (European Cyber Crime Centre). Кооперація присутня і з іншими установами ЄС, зокрема:

- Європейським агентством з питань правоохоронної підготовки (European Union Agency for Law Enforcement Training, CEPOL);
- Органом європейських регуляторів електронних комунікацій (Body of the European Regulators of Electronic Communications, BEREC);
- Європейським агентством оперативного управління великомасштабними IT-системами у сферах свободи, безпеки та юстиції (European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, eu-LISA);
- Європейським агентством з авіаційної безпеки (European Aviation Safety Agency, EASA).

ENISA керує і іншими програмами із забезпечення безпеки, зокрема загальноєвропейською програмою «Cyber Europe». Навчання по ній здійснюється на прикладах кіберінцидентів та має в собі кейси з управління кризовими ситуаціями на рівні Євросоюзу, що мають на меті сприяння у таких ситуаціях для державних та приватних секторів країн-членів [82].

По суті, вправи у «Cyber Europe» являють собою симуляції масштабних інцидентів, що безпосередньо зачіпають питання забезпечення кібербезпеки, для того, щоб вони не переросли у повноцінні загрози. Вправи служать для випробування новітніх дій з кібербезпеки, а заразом, вирішення проблем, що можуть виникнути у наслідок незаконних хакерських дій. «Cyber Europe» пропонують можливі послідовності дій, які беруть за основу реальний досвід та події, що вже відбулися. Вони розробляються досвідченими європейськими експертами з кібербезпеки, і при цьому така практика дає навчальний досвід для учасників, щоб вони могли застосувати набуті знання у майбутньому [101].

За час своєї роботи, Агентство ENISA покладалося на сформовані різні програми, що мали перелік головних пріоритетів та цілей для запланованих заходів. Зокрема, у програмах Агентства були визначені такі пріоритети:

- підвищення здатності європейських електронних мереж протистояти зовнішнім впливам;
- розвиток співробітництва між країнами-членами ЄС у сфері мережевої та інформаційної безпеки;
- ідентифікація нових ризиків у сфері інформаційної безпеки і формування взаємної довіри [137].

24 лютого 2005 р. було прийняте Рамкове рішення Ради ЄС 2005/222/JHA відносно нападу на інформаційні системи, яким було установлено мінімальні правила відносно визначення кримінальних злочинів та санкцій у сфері нападів на інформаційні системи, що було спрямоване на поліпшення співробітництва між судовими відомствами та уповноваженими органами, до яких входила поліція та спеціалізовані правоохоронні органи країн-членів ЄС у сфері захисту інформаційних систем [99].

Зазначалося, що будь-яке порушення системи захисту інформаційних систем є очевидними, що неабияк підриває спокій країн-членів ЄС, і несе у

собі загрозу порядку, а отже викликає очевидне стурбування. Отож, мають бути передбачені необхідні дії, які будуть направлені на кооперацію між країнами ЄС задля притягнення винних до відповідальності та справедливого покарання злочинців.

Пізніше, у травні 2007 р. членам ЄС було презентовано документ, який мав назву «На шляху до загальної політики в сфері боротьби з кіберзлочинністю» (Towards a general policy on the fight against cyber crime). Європейська комісія, що була її автором зазначила в ньому термінологічну базу, зокрема і дефініцію поняття «кіберзлочинність». До того ж, у цьому документі також було представлено напрямки підтримки безпеки інформаційного простору, які мають отримати безпосередню увагу владних органів [163].

Отож, документ подає наступне визначення, цитата: «кіберзлочинність – це кримінальні дії, скоєні з використанням електронних комунікаційних мереж та інформаційних систем або проти таких мереж та систем». В свою чергу їх можна розділити на три категорії:

- *традиційні форми злочину* (шахрайство та підробки в електронних комунікаційних мережах та інформаційних системах);
- *публікація протизаконного контенту в електронних медіа* (дитяча порнографія, матеріали із закликами до расової ненависті і т.п.);
- *специфічні злочини в електронних мережах* (атаки на інформаційні системи, хакерство тощо).

Основними же шляхами реалізації Єврокомісією забезпечення безпеки кіберпростору є:

- участь у нормотворчому процесі (що включає в себе розробку та прийняття міжнародно-правових документів у сфері протидії кіберзлочинності);

- заохочення міжнародного співробітництва правоохоронних органів країн членів ЄС (організація науково-практичних конференцій, семінарів, тренінгів з питань протидії кіберзлочинності, створення цілодобових контактних пунктів у країнах членах ЄС, розвиток платформи для навчання експертів у сфері протидії кіберзлочинністю та ін.);
- розвиток співробітництва між державним і приватним секторами у сфері протидії кіберзлочинності, зокрема, співпраця між правоохоронними органами та приватними компаніями;
- заохочення підписання державами-членами ЄС та іншими країнами Конвенції про кіберзлочинність 2001 р. та ін. [22, с.39].

Наступним кроком ЄС до покращення кібербезпеки став документ під назвою «Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості» (Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience), який було опубліковано Європейською комісією у березні 2009 року. І знову відзначалися головні проблеми та питання у забезпеченні кібербезпеки, зокрема саме об'єктів критичної інфраструктури [96].

Документ наводив наступний перелік основних викликів для ЄС:

- слабка координація між державними органами у питанні протидії кібератакам, що призводить до хаосу на національному рівні;
- відсутність у країнах ЄС достатнього рівня партнерства та довіри між державним та приватним секторами;
- обмеженість співпраці між державами-членами ЄС у питаннях протидії кіберзлочинам, нерівномірний розвиток систем захисту у різних державах;
- відсутність міжнародного консенсусу щодо пріоритетів у реалізації політики захисту критичної інформаційної інфраструктури.

З розвитком технологій та діджиталізацією суспільства, поставали все більші загрози для кібербезпеки країн ЄС, тому 7 лютого 2013 р. Європейською комісією була ухвалена нова Стратегія кібербезпеки «Відкритий, надійний та безпечний кіберпростір» (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace) [102]. Тут представлений досить детальний план відносно безпеки у кіберпросторі. Як і раніше відзначалося, що загрози та шкода від них зростають, а отже потрібно посилення зусиль країн-членів у цих питаннях. Відзначалося, що відсутність достатньої координації досі сприяла тому, що заходи безпеки були на незадовільному рівні, і необхідно посилити співпрацю заради захисту європейських цінностей та демократії.

Виділяється п'ять основних напрямів роботи:

1. Досягнення кіберстійкості всередині ЄС.
2. Суттєве скорочення кіберзлочинності.
3. Розробка політики кібероборони, пов'язаної зі Спільною політикою безпеки і оборони.
4. Розвиток виробничих і технологічних ресурсів для кібербезпеки.
5. Створення узгодженої міжнародної політики кіберпростору для ЄС і просування основних цінностей ЄС.

Стратегія прописує також чіткі механізми регулювання та покарання для порушників кібербезпеки, що має сприяти тому, що кара настигне кожного хто спробує скоїти подібні дії по відношенню до європейського кіберпростору [103].

Стратегія та Порядок денний, які розроблялися паралельно, побачили світ навесні 2015 р. та в липні 2016 р. відповідно. Європейська комісія вжила «Додаткові заходи по сприянню розвитку індустрії кіберзахисту», а вже у липні 2016 р. була ухвалена Директива ЄС щодо заходів по забезпеченню високого загального рівня безпеки мережевих та інформаційних систем у

всьому Союзі (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) [97].

Ця Директива надає єдині правила та вимоги в сфері кібербезпеки для всіх країн ЄС, проте, відзначає, що кожна держава-член ЄС має право вжити власних заходів щодо впровадження норм цієї Директиви у власне національне законодавство.

Також, у Директиві прописано положення, що маю бути виконані державами, зокрема:

- Покращення національних систем захисту, задля поліпшення ситуації у кіберпросторі;
- Поліпшення зв'язків між державами та спільні дії;
- Вчасне інформування провайдерів та дистриб'юторів мережевого обладнання відносно вчинених кіберінцидентів та реакції на них правоохоронних органів.

Задля досягнення вищенаведених завдань, країнам-членам необхідно розробити комплексну національну стратегію захисту кіберпростору, що має включати в себе певні заходи, а саме: координація між правоохоронними відомствами, програми протидії кібератакам, тренувальні та освітні комплекси для залучення нових кадрів, міжнародна співпраця з іншими державами ЄС, задля поліпшення їхньої роботи.

Основними же загрозами кіберпростору ЄС нині були визначені:

- Кібершпигунство та військові дії, що проводяться за відома чи за сприяння певної держави. При цьому, у документі відзначається, що розвинені держави, а також їхні промислові об'єкти по суті стають основними цілями для іноземних хакерів.

- Використання всесвітньої мережі у терористичних цілях. Говориться про те, що за допомогою Інтернету злодії здійснюють хакерські атаки заради отримання матеріальної вигоди, пропаганди, а також вербування спільників.
- Кіберзлочинність, що виражається у викраденні персональних даних та відмивання коштів, отриманих незаконним шляхом [97].

13 вересня 2017 р. було сформовано новий документ, що мав назву «Стійкість, стримування та захист: створення сильної кібербезпеки для ЄС» (Resilience, Deterrence and Defence: Building strong cybersecurity for the EU) [109]. Європейська комісія відзначала в ньому, що кібербезпека грає найважливішу роль у сучасному достатку для країн ЄС. Тому для покращення міжнародної кооперації мали бути створені спеціальні мережі та «Група співробітництва», що мають забезпечувати планування, керування, обмін інформацією та підготовку звітів відносно стану кібербезпеки в ЄС.

В першу чергу це стосується наступних секторів:

- енергетика: електроенергія, нафта, газ;
- транспорт: повітряний, залізничний, водний, автодорожній;
- банки, кредитні установи;
- інфраструктура фінансового ринку: біржі, центральні контрагенти;
- заклади охорони здоров'я;
- постачання питної води;
- цифрова інфраструктура: точки обміну Інтернет-трафіком, провайдери системи доменних імен, сервіс-провайдери, реєстратури доменних імен верхнього рівня [150, 157].

Світ вступив у новий етап свого існування, і країни ЄС так само. Після розв'язаної РФ у 2014 році війні проти України, а також посилення гібридного протистояння через інтернет ресурси та медіа, країни Європи зіткнулися просто з лавиною кібератак та зливів керованих Москвою. А від так, необхідно

було посилити співпрацю не просто між собою, але й з провідними країнами світу та міжнародними організаціями. Зокрема, не стосувалося кооперації всередині Організації Північноатлантичного договору (НАТО), також велася активна співпраця з країнами Асоціації держав Південно-Східної Азії (АСЕАН), всередині ж Європи спільні дії у кіберпросторі узгоджувалися з Організацією з безпеки і співробітництва в Європі (ОБСЄ), Радою Європи (РЄ) та Організацією економічного співробітництва та розвитку (ОЕСР) [20, с.9-10]. ЄС вів співпрацю з США, Японією, Індією, Південною Кореєю. За часів правління у Німеччині Ангели Меркель, за ініціативи її уряду, було пожвавлено співпрацю з комуністичним Китаєм (КНР), що було вкрай спірною тенденцією, оскільки США, а особливо за каденції Дональда Трампа вели з комуністичним Китаєм торговельну війну. Це неабияк ускладнювало співпрацю між США та ЄС, оскільки в доктрині кібербезпеки перших було заявлено про загрозу з боку КНР [80, 166].

Щороку Європейським центром боротьби з кіберзлочинністю надається детальний звіт про кіберзагрози організованої злочинності (IOCTA). Звіт несе у собі при цьому основні висновки, які було зроблено після річної роботи, нові загрози безпеки. Через IOCTA Євросоюз складає поради правоохоронним органам, державним органам, задля того, щоб реакція на кіберзлочини була своєчасна та відповідна [12, 123].

Європейський Союз покладається на просування навчань (тренінгів) з питань кібербезпеки та проведення досліджень у цій галузі, як одним із передових методів покращення кібербезпекової ситуації, чим дуже співпадають у своїх намірах та способах досягнення мети зі США. До цих заходів входить створення певного переліку вимог до спеціалістів у сфері кібербезпеки, підвищення їхньої кваліфікації та підготовка їх до кризових ситуацій. Для цього в Естонії під егідою НАТО навіть було започатковано Центр експертизи з питань кооперативної кібероборони - CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence) [13].

Робота Центру CCDCOE являє по суті співпрацю між країнами НАТО у сфері покращення заходів кіберзахисту через навчання, підготовку наукових досліджень, проведення міжнародних консультацій, а також відточування майстерності, здобутої під час навчання [73].

Європейська Комісія вклала понад 63,5 млн. євро в проєкти, що мали закласти фундамент для посилення кібербезпеки ЄС, а також надавати свої консультації приводу можливих загроз та методів як їм протидіяти. Чотири таких проекти: CONCORDIA, ECHO, SPARTA та CyberSec4Europe, були покликані на те, щоб стати планом дій для Європейських держав після 2020 року у сфері забезпечення безпеки у кіберпросторі. До того ж, одним із завдань цих проектів є формування системи навчання та підготовки спеціалістів, так звана «європейська модель» для забезпечення кібербезпеки.

Нова ж глобальна стратегічна програма Євросоюзу, що має назву «Порядок денний на 2019-2024 рр.», яка замінила наразі своїх попередників у сфері кіберзахисту, має наступні пріоритети:

- захист європейських громадян, їхніх прав та свобод;
- протидія кіберзлочинності, а також сучасним гібридним загрозам та дезінформації у мережі та медіа;
- розвиток економічного добробуту країн ЄС;
- створення «кліматично зеленої», справедливої й соціальної Європи;
- пропагування європейських цінностей та інтересів у міжнародних відносинах.

Цей документ поклав кінець дискусії між країнами-членами ЄС після виходу з його складу Великої Британії, що дало поштовх європейським політикам до того, щоб задуматися над причинами подібного ходу з боку острів'ян та наслідків подібного для Союзу загалом. У заключній частині дискусії наголошується на тому, що ЄС, як ніколи, потребує єдності та консолідації всередині організації. Відзначалася пріоритетність соціальної

політики для громадян ЄС та покращення їхнього становища через впровадження інновацій. І також, до основних тем питань денних ЄС було віднесено – бурхливу міграцію всередину Європи, безпеку та економічну стабільність [110, 141].

Нова стратегія наголошує на тому, що сучасний світ стає все більш складним, особливо з точки зору забезпечення безпеки у кіберпросторі. Злочинці, що проводять свою діяльність у всесвітній мережі не знають кордонів, і їхні дії несуть іноді навіть більшу загрозу ніж звичайна конвенційна зброю. Відзначається, що проблеми спільної безпеки посилюються через нестабільну ситуацію у країнах сусідах, а також радикалізацією терористичних груп. Постають все більші загрози, які зачіпають одразу кілька секторів держави та несуть вкрай деструктивних характер для європейської спільноти. Проте, на відміну від попередніх стратегій, нова стратегія наділяє правоохоронні органи більшими інструментами впливу на безпосередні загрози кібербезпеці.

2.2 Доктрини Китаю, Росії та Індії у питанні захисту кіберпростору

Комуністичний Китай, як одна з країн з найбільшим у світі населенням, по-суті являє собою чудову мішень для різного роду хакерів та кібершахраїв. І якщо ми звернемося до Інформаційного центру Інтернет-мережі Китаю (CNNIC), то на кінець грудня 2020 року, у Китаї нараховувалося приблизно 989 мільйонів інтернет-користувачів. І саме тому китайське керівництво за останні роки приділяє безпеці кіберпростору досить суттєву увагу, зважаючи на те, наскільки швидко змінюються методи злочинців із отримання доступу до секретних даних.

Загалом, дослідники теми кібербезпеки Китаю, як наприклад Мікк Рауд та Скотт Малкольмсон у своїх роботах неодноразово відзначали, що їхня політика формується на засадах сильного суверенітету від іноземних

технологій, а також формування закритої нормативно-правової системи з сильним утиском та контролем усієї інформації, що знаходиться у всесвітній мережі, щоб таким чином ізолювати населення своєї держави від невгодної владі даних та джерел [148, 132]. У цьому комуністичному Китаю допомагає високий рівень самозабезпеченості в таких напрямках, як космічна розвідка, моніторинг, а також військова контррозвідка. І так як комуністичний Китай являє собою високо бюрократизовану та авторитарну структуру, то подібні методи та жорстка цензура знаходять своє відображення у всіх владних структурах. Потужним кулаком влада КНР прокладає та створює систему кібербезпеки, підкріплюючи стратегію партії на законодавчому рівні [90]. Заявлена стратегія уряду вже багаторічно незмінного лідера комуністичного Китаю Сі Цзіньпіна «Made in China 2025» [111] несе у собі головний принцип – КНР має стати на шлях зміцнення своїх позицій у світі, і кібербезпека розглядалася як одна з важливих складових цього процесу. І тому, урядом було прокладено шлях до модернізації та покращення технологічного рівня держави. Проте, іронічно, що попри усі зусилля партії, КНР досі залишається вкрай залежною від іноземних комплектуючих та програмного забезпечення зокрема США, ЄС та – найбільш принизливе для китайської влади – Республіки Тайвань, що є світовим лідером з виробництва мікро чіпів. До того ж, китайські IT-спеціалісти досі не запропонували достойної конкуренції американським Windows чи macOS. А репресивна машина партії придушує силою будь-які спроби населення обійти жорсткі рестрикції влади.

Але поглянемо трохи в історію розвитку кібербезпеки КНР. До 2013 року інфраструктура кібербезпеки комуністичного Китаю, а також його правова система знаходилися у вкрай слабкому порівняно з іншими державами стані. В деякому сенсі це пов’язують з тим, що більшість мережевого обладнання та забезпечення було Західним, що і робило його вразливим до кібератак з того боку. Тоді, керівництво держави забажало посилення своєї безпеки, а також партія жадала стати лідером у інтернет-засобах та

забезпеченні безпеки. Тому, у військовій стратегії, опублікованій у 2015 році та додатково описаній у першій офіційній національній стратегії кібербезпеки у 2016 році, йшлося про те, що поставлені КНР амбітні цілі посилення свого кіберзахисту, а також зміцнення свого мережевого суверенітету мають бути виконані до 2030 року [130].

Повертаючись до нормативно-правової бази, а також контролюючих органів КНР, то зазначимо, що важливим кроком до Китаю стало прийняття Закону про кібербезпеку в 2017 році. Він заклав правовий фундамент законодавства КНР, а також регулював питання поширення інформації. Потім у 2021 році було прийнято Закон про безпеку даних і Закон про захист особистої інформації. При цьому органом, що має регулювати діяльність користувачів Інтернет-ресурсів, є Адміністрація кіберпростору Китаю (АКК). Адміністрація кіберпростору Китаю по суті являє собою центр усіх питань, що стосується цивільного кіберпростору, хоча, окрім нього подібну роботу також виконують Міністерство громадської безпеки (MPS), Міністерство державної безпеки (MSS) і Міністерство промисловості та інформаційних технологій. Хоча по суті своїй усі ці відомства являють собою одну єдину структуру, що має на меті одне – повний контроль. У свою чергу регулювання військової сфери підпадає під юрисдикцію Сил стратегічної підтримки, які було започатковано у 2015 році. І на відміну від Адміністрація кіберпростору Китаю вони являють собою чітко регламентовану та єдину структуру. Даний орган підпорядковується безпосередньо Центральній військовій комісії КНР та здійснює операції, що направлені на забезпечення кібербезпеки китайської мережі [148].

Але не тільки питання захисту власного кіберпростору турбують комуністичний Китай. Його представники також беруть участь у таких міжнародних проектах як Група урядових експертів з інформаційної безпеки в рамках ООН, Міжнародний союз електрозв'язку, Всесвітній саміт з питань інформаційного суспільства. Китай хитро займає позицію борців з

пережитками холодної війни, звинувачуючи Захід у надмірній концентрації влади над інтернет-ресурсами у своїх руках, та виступають з тим, щоб світ звернувся до моделі розподілення цифрових ресурсів та контрою над ними. Міжнародна стратегія співпраці в кіберпросторі, видана Міністерством закордонних справ та Адміністрацією кіберпростору Китаю в 2017 році, як ніщо інше є уособленням подібної думки [168]. Зокрема, Розділ 2 містить по суті прямий заклик відмови від зосередження влади в руках одної групи країн, мається на увазі в першу чергу США, та недопущення перетворення кіберпростору на місце бойових дій держав. Проте, вкрай лицемірно з боку комуністичної партії Китаю заявляти подібне, оскільки саме посилення кібератак на державні органи США з боку КНР, а також спроби викрадення секретної інформації призвели до того, що США у своїй сучасній доктрині кібербезпеки відзначили особливу небезпеку з боку комуністичного Китаю та відповідають їм взаємністю [169].

Саме через зростання побоювань китайського керівництва у тому, що Сполучені Штати посилюють свою могутність та контроль у мережі, так сильно посилюється зацікавленість КНР у власній безпеці, зокрема у питанні їх наступальних можливостей. Після того як американський перебіжчик Е. Сноуден розповів про те, наскільки сильний захист діє у США в питанні кібербезпеки [89], навіть попри реформи проведені у 2013 році, китайська система захисту все ще залишалася на неприпустимо низькому рівні. Контррозвідка США, особливо після подій 2001 року, вкрай болісно реагує на питання можливих терористичних атак, особливо в питанні кіберпростору. Нерідко подібні дії можуть послаблювати кордони між такими поняттями як безпека держави та суспільні права. Дослідження, проведене Національною технічною групою реагування на надзвичайні ситуації у КНР, визначало Сполучені Штати, Канаду та Росію головними джерелами ворожих кібератак на китайські мережі [122].

Як вже відзначалося, китайські теоретики безпеки відзначають той факт, що питання кібербезпеки світової мережі Інтернет по більшій мірі тримає на своєму особистому контролі саме США, що потенційно може призвести до того, що недостатня комунікація між державами та посилення потенціалу кібернетичних сил обох призведе до колапсу у системі міжнародного захисту. Проте певно у КНР більше переймаються питанням того, що таким чином США зможуть отримати доступ до їхніх даних, а також умів населення, через що і намагаються досягти перерозподілу ресурсів контролю. При цьому, інтереси обох держав категорично не сходяться в п'яти головних областях: ідеологічній, безпековій, дипломатичній, міжнародній торгівлі та дослідницькій сфері. Китайськими експертами зокрема відзначається, що у США вони вбачають навіть загрозу світовому порядку [81].

Китайський уряд приділяє велику увагу посилення та вдосконалення своєї військової могутності, і кіберпростору це також стосується. У Білій книзі, на яку орієнтується керівництво держави, написано наступне: КНР є вкрай зацікавленою у впроваджені сучасних технологій у військовій сфері, при цьому включаючи штучний інтелект, хмарні та квантові обчислення. Реакція Вашингтону на подібні дії та заяви при цьому носили, звичайно, різко негативний характер, що дуже посилило ізоляцію КНР від світових систем. Комуністичний Китай при цьому виставляв себе жертвою дій США. А програма технічної незалежності Китаю тим часом набирала оберти. І починаючи з 2015 року, китайськими фірмами зокрема було запроваджено систему переформатування американських операційних систем китайськими [144].

Також, у контексті Китаю, варто також відзначити його дії у напрямку певного наслідування прикладу інших світових держав, які впроваджують власні системи захисту свого кіберпростору. Такі дії наштовхують китайське керівництва до створення та впровадження подібних заходів і на своїй батьківщині. Наприклад, стратегія ЄС запропонована Єврокомісією під

назвою Загального регламенту захисту даних (GDPR), лягла в основу того, що Китай впровадив у себе ще більш жорстку політику відносно захисту персональних даних, а також послужив створенню власного механізму захисту даних. Відповіддю Китаю стало прийняття у 2017 році закону про кібербезпеку [160]. Він як і його європейське першоджерело, визначає права об'єктів даних, визначає обов'язки контролерів даних і підтримує принципи безпеки даних, згоди користувача, мінімізації збору даних, анонімності даних та інших заходів захисту. А вже 1 листопада 2021 року урядом Китаю було прийнято Закон про захист персональних даних, який покликаний регулювати зберігання, передачу та обробку персональних даних [122]. Китайські та європейські документи настільки схожі, що навіть містять схожі норми та, майже ідентичні, фрази.

Як зазначалося вище, Китай у своїй політиці демонструє бажання до мультиполяризації Інтернету та недопущення одноосібного панування, та поширення міжнародної кооперації у створенні багатодоменного, багаторівневого та багатосуб'єктного Інтернету. При цьому, одночасно у інформаційному полі Китаю панують два бачення цієї концепції, а саме: створення міжнародного співтовариства держав, розвантаження системи контролю; або ж, варіант посилення національного контролю та жорстке регламентування мережі через правила та закони, що надаватимуть національним органам можливість контролювати мережу. Зокрема, друга концепція дуже підтримується керівництвом КНР та РФ [132]. Позиція Китаю, як можна побачити базується на забезпеченні кіберсуверенітету, та підганянні міжнародних стандартів, зокрема і статуту ООН, до реалій кібербезпеки. Для цього як КНР, так і її сателітом Росією створюються спеціальні комісії та робочі групи, що мають на меті створення системи безпеки кіберпростору, яка дозволить обом режимам, в обхід країн Заходу впроваджувати у свій інформаційний сегмент ті меседжі, що вигідні їм з точки зору їхнього ідеологічного вектору.

Будапештська конвенція про кіберзлочинність, яка була підписана ще в 2001 році, є основним наразі міжнародним документом, що регулює міжнародний контроль кібербезпеки, до якої приєдналося 65 краї світу [25]. Та попри це, Китай так і не підписав дану конвенцію. Натомість, Китай, особливо у період 2014 року поставив дуже велику ставку на зміцнення військової могутності. Саме тоді була затверджена нова концепція бачення кіберзахисту, а також впроваджено реформу органів її здійснення. А зважаючи, що зобов'язань, які б обмежували його діяльність, у цьому напрямку майже немає, КНР, на противагу Заходу, прагнуть до створення власної законодавчої бази регулювання цих питань. На погляд компартії, нинішні домовленості та угоди носять вкрай розрізнений та нечіткий характер, що вкрай обмежує можливості регуляції.

У китайському розумінні система контролю над кіберпростором має здійснюватися за принципом «згори до низу», підтримуючи чітку ієрархію та жорстку модель контролю. Провідна роль у цій моделі відводиться національним урядам, а форум ООН має виступати в якості органу обговорення нагальних проблем та концепцій на майбутнє. Такі ж принципи були викладені в Міжнародній стратегії співпраці в кіберпросторі, опублікованій Міністерством закордонних справ Китаю та Адміністрацією кіберпростору Китаю в 2017 році [160]. І таку модель китайські очільники просувають не тільки на рівні ООН, а і більш локально. Зокрема і на форумах Шанхайської організації співробітництва, де знаходять значну підтримку з боку РФ та її поплічників. Подібні наміря навіть вилилися у спільну угоду між цими режимами, яку вони підписали у 2015 році, де віталося бажання обох сторін до зміцнення безпеки інформаційного простору [122].

Резюмуючи, відзначимо наступне, комуністичний Китай, як і РФ явно невдоволені нинішньою системою світопорядку та нормативного регулювання міжнародного співіснування, що зокрема виливається і у питанні кібербезпеки. У своєму прагненні створити законодавчу базу для регулювання

кіберпростору, КНР прагне не до диверсифікації інформаційного простору, а до концентрації влади та відгородженні свого інтернет-простору від можливих впливів з боку інших держав та блоків. У їхньому розумінні – хоча вони декларують протилежне – всесвітня мережа являє собою поле битви держав за вплив на маси та забезпеченість інформаційної гігієни та безпеки державних секретів. Саме тому, у їхніх ініціативах мова йде про створення власного, «стерильного» від іноземного впливу, кіберпростору, задля того, щоб мати змогу самостійно визначати межі свого впливу та розмивати кордони між захистом своїх інтересів і безпеки держави, та втручанням у життя суспільства. Поширюючи потрібні меседжі, і навпаки, приглушуючи можливі невдоволення та ідеологічно протилежні погляди [131].

Держава-агресор, Російська Федерація, у своїй парадигмі бачення «безпеки», дечим схожа у більшості позиціях з комуністичним Китаєм. Бачення агресора зазвичай зводиться до декількох постулатів, а саме: звинувачення Заходу у надмірній узурпації влади на міжнародній арені, «демонізація» ворога; та просування наративів про необхідність перегляду нинішніх міжнародних документів із регулювання безпеки.

У міжнародному полі, російський істеблішмент намагається нав’язати, зокрема країнам ООН, власну «Конвенцію про забезпечення міжнародної інформаційної безпеки». Вміло підміняючи поняття, Росія подає свою програму, як альтернативу баченню США, які, як зазначалося у попередньому підрозділі, бачать кіберпростір як зону бойових дій між державами за вплив. РФ же натомість пропонує концепцію обмеження будь-яких кіберзасобів, якими держави можуть потенційно завдавати одне одному шкоди [32]. Хоча, зрештою, всі договори з Росією зводяться до того, що РФ намагається, як і комуністичний Китай, поставити себе у роль жертви агресії, а коли доходить справа до взаємності у виконанні підписаних домовленостей, одразу намагається викрутитися від їхнього виконання затягуючи, чи навіть зриваючи процес.

Росія у своєму маніакальному баченні «збереження» безпеки, надає перевагу не так формуванню ієрархії органів та підрозділів у боротьбі з кіберзлочинністю, як введення всередині держави жорстких методів та нормативно-правового регулювання будь-якої діяльності у кіберпросторі. Російське керівництво приділяє вкрай велику увагу формування в своєму інфопросторі системи контролю та обмежень, що у першу чергу стосується її державних інтересів. І, як будь-яка авторитарна держава з диктатом однієї владної групи – РФ не бажає того, щоб у її медіапростір потрапляла будь-яка інформація, яка у їхньому баченні несе деструктивний характер для їхнього правління [55].

Отже, починаючи з 2013 року, у владних кабінетах Кремля розпочалася робота над реорганізацією підходу до захисту безпеки. Під час засідання ради безпеки, президент В. Путін заявив про те, що треба віднині розглядати кіберпростір як один із найважливіших напрямків удосконалення безпеки. Ця заява була підтримана і тодішнім заступником голови уряду Д. Рогозіним, який відзначив те, що кібербезпека має стати пріоритетом номер один [32].

Після цього було здійснено ряд важливих заходів, які і сформували сучасну модель бачення РФ кіберзахисту. Зокрема, Міністерством Оборони РФ, було навіть сформовано «Концепцію діяльності Збройних сил в інформаційному просторі», де було прописано методи та дії країни-агресорки в кіберпросторі [27]. Вона містила у собі чотирнадцять сторінок тексту, де було також викладено і основні терміни, якими оперуватиме держава у правому полі. Якщо коротко відобразити сутність цього документу, то все зводиться до того, що РФ має сприяти стримуванню, запобіганню та подоланню кіберзлочинності. При цьому, документ акуратно обходив та відмовлявся від ведення наступальних дій у кіберпросторі.

І хоча документ було сформовано у дусі радше оборони, тим не менше у російському безпековому осередку можна також прослідкувати і можливість

відповіді на можливі дії держави у кіберпросторі по відношенню до іншої. Про це говорить пункт 3.2.5 документа, де відзначається наступне, цитата: «в умовах ескалації конфлікту в інформаційному просторі та переходу його в кризову фазу скористатися правом на індивідуальну чи колективну самооборону із застосуванням будь-яких обраних способів та засобів, що не суперечать загальновизнаним нормам та принципам міжнародного прав» [27]. Що, в принципі, може означати наступне: якщо ми вважатимемо за необхідне, ми матимемо право застосувати будь-які засоби задля «забезпечення безпеки». Вкрай схоже на типову російську політику.

Наступним знаковим документом в області кібербезпеки РФ є Указ В. Путіна від 15 січня 2013 р. «Про створення державної системи виявлення, попередження та ліквідації наслідків комп'ютерних атак на інформаційні ресурси РФ». Якщо коротко викласти його суть, то документ торкається питання створення захищеної бази даних, розробка та впровадження власних методів у боротьбі з кіберзлочинністю, обмін інформацією між державними органами, яка стосується кіберінцидентів, а також оцінка ступеню захищеності критичної інформаційної інфраструктури. І це завдання Путін покладав саме на Федеральну службу безпеки РФ (ФСБ РФ), що дуже чітко ілюструє, що дії їхні носитимуть цілком каральну функцію [70].

А на продовження теми повноважень у сфері кібербезпеки, варто згадати, що ще 12 грудня 2013 року Держдума РФ ухвалила закон, який по-суті надавав ФБС можливість проведення оперативно-розшукових заходів для протидії загрозам інформаційної безпеки. Контроль за діяльність у кіберпросторі має здійснюватися зокрема у питаннях, які стосуються державної, військової, економічної чи екологічної безпеки РФ [32].

На додачу до вже зазначеного вище, у Росії також діє Доктрина інформаційної безпеки Російської Федерації та Стратегія розвитку інформаційного суспільства на Російської Федерації [28]. Одначе, у їхньому

тексті не відображаються повною мірою усі аспекти життєдіяльності держави у сфері кіберпростору, а також її взаємодія з іншими державами в цьому плані. Проте, РФ з 2013 року проводила постійні зустрічі з представниками інших держав з питання забезпечення кіберзахисту, і США за президентства Барака Обами, зокрема.

У цьому плані керівництвом РФ відзначалися наступні заходи у забезпеченні партнерських відносин, а також покращення взаємодії між країнами-партнерами: держави мають зберігати контакт одна з одною з метою інформування кожної зі сторін відносно ведення своїх дій у кіберпросторі, щоб їхні дії не були сприйняті за агресію; а так підтримувати обмін інформацією про діяльність хакерських груп, кібер-терористів та фахівців з безпеки країн, які є по відношенню до країн-партнерів недружніми. У разі кризових ситуацій також відзначалася необхідність безпосереднього прямого зв'язку між державами [32].

Останні роки у медіапросторі Росії, зокрема на її пропагандистських медіа («Интерфакс» та РИА «Новости») лунали розмови про те, що у Збройних силах РФ з 2014 року функціонує спеціальний підрозділ, основною метою якого є проведення операцій у кіберпросторі.

Міністерству Оборони РФ було доручено розробити детальний план з розробки та впровадження органу, який має захищати російські комп'ютерні мережі та стратегічні об'єкти від кіберзагроз. У деякому сенсі подібний план являє собою копію американської системи United States Cyber Command (USCYBERCOM). Ця структура заразом із космічною та протиракетною обороною підпорядковується безпосередньо військово-стратегічному командуванню [32].

Якщо торкатися питання саме навчання кадрів у питанні захисту кібербезпеки РФ, то тут система також дуже схожа на американську. В Росії також впроваджують систему навчання спеціалістів у вищих навчальних

закладах, але окрім цього діють ще й державні програми та конкурси з відбору гідних претендентів, які мають до цього ремесла хист. Але є одне «але», будь-яка діяльність у цій сфері проходить під пильним наглядом ФСБ і саме вони формують ті професійні стандарти, які потім лягають в основу навчання.

Нинішню ж політику Індії у сфері впровадження сучасних технологій можна пояснити як і у багатьох інших країн – бажанням покращити внутрішньодержавний добробут власних громадян, а також створити безпечну основу для їхньої життєдіяльності. Оскільки, Індія є вкрай населеною державою, необхідно було забезпечити власне населення доступом до сучасних технологій. І хоча на 2014 рік, лише 20 відсотків від усього населення (близько 1,2 млрд. осіб) на той час мали доступ до всесвітньої мережі, супроводжувалося повільними темпами впровадження технологій, а також висока вартість послуг та державний бюрократизм, тим не менше уже у 2018 р. Індія за кількістю користувачів Інтернет мала понад 500 млн осіб [147].

Копнувши глибше у процес формування Індією власної системи та правил відносно захисту свого кіберпростору, можна взяти за відправну точку 2000 рік, коли було ухвалено «Закон про інформаційні технології для формування нормативної бази стратегії кібербезпеки держави». Він і нині являє собою основний документ, яким регламентується кіберзахист держави, а також визначає основні пріоритети держави у власному захисті [135; 136]. Також документ надає можливість урядові Індії, у зв'язку зі зростанням кіберзагроз впроваджувати всередині цензуру та регуляторні заходи. А вже у 2004 р., було створено підрозділ «Індійська команда реагування на надзвичайні ситуації в Інтернеті (CERTIn). Саме він являється національним агентством і має контролювати діяльність держави та її громадян у кіберпросторі [135].

Під час Мюнхенської конференції з кібербезпеки у 2012 році, індійські представники заявили про те, що будуть впроваджувати розробку та

застосування чисто вітчизняних технологій, щоб знизити залежність від імпорту із інших держав. Проте глобальним поштовхом у планах уряду Індії став скандал зі вже згаданим у попередніх розділах Сноуденом, через якого світова громадськість дізналася про те, що США активно впроваджували спостереження не тільки по відношенню до ворогів, але й своїх союзників. Це зачіпало і Індію також. Тому, у владних колах почало каталізуватися бажання до створення власної мережі захисту та методичної бази. Тоді ж була представлена «Національна політика у галузі кібербезпеки», що заклала собою основу індійської доктрини кібербезпеки, у якому зазначався те, як має розвиватися їхня безпека на всіх рівнях та верствах, а також механізми узгодження їхньої роботи. Але цей документ торкався більше питання саме внутрішньої безпеки, в той час, як саме регулювання міжнародної кооперації відводилося до інших документів [120].

Стратегія індійського уряду полягала у наступному:

- впровадити робочу систему захисту персональної інформації громадян, фінансової і банківської інформації та дані, що мають значення для державного управління і безпеки, від можливого несанкціонованого доступу та кібератак;
- високий рівень інформаційно-комунікаційних технологій, та застосування їх у всіх секторах держави;
- створити базу професійних кадрів протягом наступних 5 років [134].

Однак, ще починаючи з 2011 року, Індія намагалася донести до світової спільноти ідею, що дуже схожа з тою, що намагаються популяризувати Росія та комуністичний Китай, а саме дерегуляція нинішньої системи контролю за Інтернетом, який по більшій мірі здійснює США, та запровадження міжнародної системи контролю з розподіленням повноважень. І хоча, як вже відзначалося, такі ідеї по більшій мірі просувають авторитарні РФ та КНР, Індія намагається не сильно схилятися саме до їхніх методів, описаних вище,

намагаючись балансувати між м'яким, Західним, методом та жорстким автократичним [158].

Відносно світових організацій, то Індія також просуває своє бачення системи кібербезпеки. Зокрема, підчас засідань Генеральної Асамблеї ООН «Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки» у 2016 р. та 2018 р. [164; 165]. У ній індійськими представниками було відзначено визначну роль сучасних технологій та впровадження їх у всі сфери суспільства , однак поряд із цим відзначалося і досить велике засилля в останні роки інцидентів з кібератак та шпигунства, що є вкрай неприпустимо. Отож, відзначалася необхідність створення певного міжнародного контролю з цього приводу [164].

Дуже важливим кроком для Індії стало прийняття у 2015 році програми «Цифрова Індія», яка має на меті покращити комунікацію між державою та громадянами, а також покращити доступ до технологій [127]. Пріоритет отримали такі завдання: надання швидкого доступу до всесвітньої мережі, сприяння поширенню мобільних технологій, упровадження системи надання цифрових послуг державними органами, а також запровадження нової системи економічної стабільності держави, шляхом покращення якості освіти в пріоритетних напрямках [105]. Програма по своїй суті побудована на тому, щоб покращити інформаційну інфраструктуру в державі та покращити доступ громадян до сучасних технологій [127]. До того ж, за останні роки програма досягнула значних успіхів у питаннях надання онлайн-послуг держави, а також медичній та освітній галузях [153].

Але із приходом інформатизації суспільства, наступає і необхідність підтримання гідного рівня безпеки держави, що на жаль уряду Індії вдається вкрай скрутно. І навіть попри високий рівень саме забезпечення правового регулювання кіберзлочинності, все ще існує досить високий рівень загроз від найнижчих рівнів, і аж до критичних об'єктів. Це стосується зокрема

шкідливого програмного забезпечення, атак на фінансові установи, банківські структури і т.д. [154].

Необхідно було створити орган, який не просто буде протистояти атакам, але й зможе давати відповідь. Тому, у 2018 році в Індії було створено військову агенцію з питань кібербезпеки, яка мала назву «Оборонна кіберагенція». Вона має співпрацювати з апаратом національного радника з питань безпеки. У планах на це відомство – створення бази спеціалістів, які зможуть забезпечити безпеки, особливо, військового сектору, тобто військово-морські та військово-повітряні сили, а також космічні програми Індії. У планах переформатування цього органу у повноцінне структурне командування. Нині апарат агенції займається розробкою доктрини здійснення операцій у кіберпросторі. Здобутки також наразі є і у питаннях кіберрозвідки. Так за підтримки поліції та прикордонної служби, було впроваджено обробку великих масивів бази даних та розпізнавання обличь [120].

Багато індійських експертів відзначають те, що головними загрозами для безпеки кіберпростору Індії складають такі країни як Пакистан та комуністичний Китай. КНР до прикладу постійно проводить проти Індії масштабні кібератаки, що тамтешніми урядовцями фактично класифікується як повноцінна війна. Ось у 2016 було здійснену масштабну атаку китайської групою кібершпигунів Suckfly. Об'єктами нападу тоді стали інформаційні системи уряду і великих фінансових інституцій держави. Протягом двох попередніх років, починаючи з 2014 і впродовж усього 2015 року, китайці несанкціоновано отримували доступ до секретної інформації. Головною метою цієї атаки на думку експертів було підірвати економіку Індії [119]. Тому протистояння все ще триває, і воно набуває форм як просто злам систем, так і повноцінних атак та терористичних актів. Втім, обидві країни при цьому намагаються не афішувати подібні протиборства, натужно показуючи свою прихильність одна до одної та проводячи політику зміцнення відносин між державами.

А тепер, від неоголошеного ворога Індії, перейдемо до ворога явного, а саме до Пакистану, з яким у Індії відносини знаходяться у постійному стані конфронтації та ненависті. І хоча потенціал Пакистану та Індії у питанні ведення повноцінних кібервоїн знаходиться не на такому високому рівні як у КНР, США чи РФ, тим не менше, обидві вони не гребують застосуванням будь-яких методів, задля досягнення своїх політичних цілей. Наприклад, зі сторони Пакистану не раз проводилися активні спроби зламу державних відомств чи пов'язаних з ними компаній, або намагання завербувати індійських держслужбовців у якості агентів всередині. Також, активно в цьому плані використовуються соціальні мережі, які стають по-суті джерелом дезінформації та підживлення конфлікту [121, 171]. При цьому програми написані спеціалістами Пакистану можуть через блоги та новинні сайти отримувати доступ до пошти, акаунтів та навіть веб-камер користувачів. Індія у протидію цьому створила спеціальне програмне забезпечення, яке має на меті мінімізувати можливість подібних атак [119]. Проте на жаль, через величезний ріст популярності соціальних мереж, особливо Facebook та WhatsApp у обох країнах, стає важко забезпечити безпеку кожного громадянина від потенційних атак [125].

І звичайно, з точки зору розвитку економіки та ринку послуг, інформатизація суспільства є позитивним аспектом, проте все ще залишається головна проблема – захист користувачів. Не так давно Індії навіть довелося обмежити доступ своїх громадян до мережі WhatsApp. Це сталося внаслідок хвилі масових вбивств у 2018 році, через засилля фейкової інформації всередині додатку [116].

2.3 Український досвід у боротьбі з кіберзлочинністю. Сучасний стан кібербезпеки України в умовах відкритої війни, а також перспективи

Хотілося б знову повернутися до пункту 5 частини 1 статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII, де закладаються основи сучасного кіберзахисту України: «кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [52].

Огляд положень Закону України «Про основи національної безпеки України», а також Доктрини інформаційної безпеки України, дає перелік об'єктів кібернетичної безпеки, які є пріоритетними для нашої держави:

- особу – її права і свободи на збирання, зберігання, використання та поширення інформації, що реалізуються за допомогою ІТС;
- суспільство – та частина його духовних, морально-етичних, культурних, історичних, інтелектуальних і матеріальних цінностей, що формуються з використанням ІТС;
- державу – її суверенітет і недоторканність у кіберпросторі, спроможність виконувати свої функції за допомогою ІТС [4, 53].

Основними суб'єктами, що мають відповідати за забезпечення безпеки при цьому є: Президент України; Верховна Рада України; Рада національної безпеки і оборони України; Кабінет Міністрів України; Збройні Сили України; Служба безпеки України; Служба зовнішньої розвідки України; Національний банк України; інші міністерства та центральні органи виконавчої влади; місцеві державні адміністрації та органи місцевого самоврядування; суб'єкти

підприємницької діяльності різних форм власності у сфері виробництва інформаційних продуктів та надання інформаційних послуг [67].

Спеціальними суб’єктами є органи, наділені можливістю безпосередньої протидії кіберзлочинцям, а також відбиття кібератак. До таких суб’єктів належать: Міністерство внутрішніх справ України; Служба безпеки України; Державна служба спеціального зв’язку та захисту інформації України; Міністерство юстиції України; Генеральна прокуратура України [14, 34].

Відповідно до українського законодавства, всі вищеперелічені органи мають у кооперації та співпраці один з один здійснювати захист нашої держави у кіберпросторі, а також вести розслідування та притягувати до відповідальності усіх винних у порушенні кібербезпеки України. При цьому від них вимагається належний зв’язок та забезпеченість інформацією кожного спеціалізованого органу, та відповідне розподілення повноважень [1, 76].

Окрім структур описаних вище, в Україні також діє спеціальний структурний підрозділ Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України під назвою Команда реагування на комп'ютерні надзвичайні події України (більш поширена назва - Computer Emergency Response Team of Ukraine, або просто CERT-UA) [71]. Його робота підкріплюється зокрема такими нормативно-правовими актам, як: Закон України «Про Державну службу спеціального зв'язку та захисту інформації», Закон України «Про телекомунікації», та Закон України «Про основні засади забезпечення кібербезпеки України» [66, 68].

Головною метою цього підрозділу є забезпечення захисту державних інформаційних ресурсів та інформаційних і телекомунікаційних систем від несанкціонованого доступу, неправомірного використання, а також порушень їх конфіденційності, цілісності та доступності даних. При цьому підрозділ CERT-UA займається збором та обробкою інформації відносно спроб порушення кібербезпеки, аналізом цих інцидентів, формуванням

рекомендацій на майбутнє, а також проводить взаємодію з державними правоохоронними органами та міжнародними партнерами України [31].

І хоча історія цього підрозділу бере свій початок ще з 2007 року, головним чином те, те яким він є зараз ми завдячуємо Революції Гідності 2013-2014 років, після якої країна-агресорка Росія розпочала свою війну проти України не тільки на землі, повітрі та морі, але й кіберпросторі. Саме тоді, на Україну було здійснено масовану інформаційну та кібератаку на державні органи та суспільство, що підштовхнуло тодішніх керманичів до створення сильного кіберщита для нашої держави [41, 76].

Зокрема, після атак під час виборів президента у 2014 році [51], а також масштабних атак на енергетичну інфраструктуру у грудні 2015 року [24], коли російські хакери намагалися отримати доступ до секретних даних та поширити дезінформацію серед населення України, було прослідковано методи та способи, якими користувалися ці групи. Це в подальшому лягло в основу створення вітчизняної методології виявлення та знешкодження кіберінцидентів, а також подальшого розслідування цих злочинів та дослідження причин їх виникнення [67].

Кібервійна тим часом продовжувалася, і на противагу хакерським атакам та спробам несанкціонованого доступу, посилювалися і інші методи досягнення мети, а саме дія так званих «ботів» та «интернет-тролів» у соціальних мережах. Активна боротьба проти цієї загрози розпочалася ще з 2014 року, і досі задишається досить актуальною. Проте на момент 2016 року, боротьба з ними сягнула свого піку [54, 63]. Саме тоді пройшов неймовірний сплеск поширення фейків та дезінформації населення, посилення терористичних груп, зокрема через підконтрольні Москві сайти «Одноклассники», «ВКонтакте», браузер «Яндекс» та пропагандистські ЗМІ. Проте тим не менше, будь-які спекуляції та загрози безпеці були відкинуті кібербезпековими органами України в кооперації з вітчизняними хакерськими

групами FalconsFlame, Trinity, Рух8 та КиберХунта. Завдяки їхнім спільним діям було отримано доступ до інформації деяких російських пропагандистів та терористичних груп, що дало спецслужбам України доступ до імен замовників та безпосередньо російських шпигунів та бойовиків, як всередині нашої держави, так і за її межами [23].

Оскільки нам вже відомий досвід Індії у кібервійні з Пакистаном, то можна згадати той факт, що частіше всього зараження шкідливими програмами, а також несанкціонований злам стаються саме через ворожі додатки та програмне забезпечення. А так як довгий час Україна та її громадяни користувалися саме російськими сервісами та соціальними мережами (особливо тими, що згадувалися у попередньому абзаці), через них російські спецслужби, зокрема ФСБ (які, як вже згадувалося у попередньому підрозділі, згідно чинного законодавства РФ мають доступ до будь-яких додатків чи сервісів розроблених російськими компаніями), отримували доступ до персональних даних населення та мали змогу відслідковувати усе що відбувається інсайдером. Тому, наказом № 133/2017 від 15 травня 2017 року Президент України Петро Порошенко ввів у дію рішення РНБО України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» до низки російських інтернет-ресурсів, а також компаній їх розробки [50]. За заявами тодішніх державних посадовців та аналітиків, цей крок став досить суттєвим у зміцненні кібербезпеки України, так як таким чином, особливо на рівні особистостей, зменшилася можливість доступу російських спецслужб до конфіденційної інформації.

Проте, того ж року, 27 червня, Україна пережила одну із наймасованіших кібератак з боку Росії за всі попередні роки. Того дня вірусом під назвою “Petya” [133] було уражено більшість державних структур та підприємств, зокрема обласні держадміністрації, енергетичні об’єкти та банківську систему. Збої спостерігалися в роботі об’єктів

«Запоріжжяобленерго», «Дніпроенерго» та Дніпровської електроенергетичної системи, повідомлялося також про проблеми в системі роботи "Ощадбанку", а також "Нової Пошти", "Укрпошти", "Укртелекому", "Укрзалізниці" та деяких найбільших радіостанцій та телеканалів країни. ЗМІ також повідомляли про проблеми на Чорнобильській атомній електростанції та роботі міжнародного аеропорту Бориспіль. І хоча вже на наступний день керівництво держави вийшло з заявою про те, що кризу було подолано, і державні сайти відновили роботу, скандал спричинений цією атакою тільки набирав оберти.

Такий розмах та сила атаки пояснювалася пізніше, зокрема представниками Департаменту кіберполіції Національної поліції України, тим, що система передачі даних M.E.Doc, яку широко використовували на той момент державні органи була заражена вірусом, і саме через неї зловмисники змогли дістатися до своєї цілі. Розробників програми, як дізналися правоохоронні органи, неодноразово попереджали про небезпеку можливої атаки, але тим не менше, ними це було проігноровано, а спеціалізовані установи, які мали це перевіряти також не діяли [9]. Таке нехлюйство з боку органів контролю та розробників свідчило про слабкість у системі контролю нашої держави, і вкрай підривало її авторитет та компетентність. Бо слідом за Україною, атакою сімейства вірусів "Petya" було уражено і інші держави. Велику Британію, США, Австралію, Нову Зеландію, Канаду та Данію. Вашингтон тоді назвав цю атаку - найбільшою в історії.

Ця атака стала поштовхом для України, а також країн ЄС та НАТО до перегляду своїх тодішніх підходів до забезпечення кібербезпеки, що в свою чергу вимагало від їхніх урядів дій відносно покращення правової бази, а також системи методів боротьби з кіберзлочинцями. І оскільки Україна проголошувала стратегію на євроінтеграцію та поглиблення співпраці з цими країнами, необхідно було створити нормативно-правове підґрунтя, особливо в області термінології та розподілення повноважень органів контролю та

створення механізмів захисту. Тому, 5 жовтня 2017 року було ухвалено Закон № 2163-VIII «Про основні засади забезпечення кібербезпеки України» та прийнято Національну стратегію кібербезпеки України. Завдяки прийняттю цих актів, Україна домоглася підтримки з боку ЄС та НАТО, о надто США. А фінансова допомога у сфері кібербезпеки та її зміцнення стали фактично щорічною статтею витрат у їхніх бюджетах [61, 69].

Тим не менше, кібератаки держави-агресора не обмежувалися виключно зараженням шкідливими вірусами та збором конфіденційної інформації. У 2018 і по 2019 роки особливої популярності серед російських хакерів набули дзвінки та повідомлення про замінування. Це стосувалося державних підприємств, об'єктів критичної інфраструктури, як то залізниця, метро, аеропорти, енергетичні об'єкти, та транспортні магістралі, урядових установ, навчальних закладів, лікарень, а також торгових центрів.

Розслідування поліції показало, що більшість із подібних повідомлень були надіслані з території Російської Федерації та окупованих нею територій Донецької і Луганської областей, а також Криму. Більшість зловмисників тоді ховалися за фальшивими документами та здійснювали дзвінки через тимчасові електронні скриньки та мережу інтернет [19].

У період підготовки до повномасштабного вторгнення Росії в Україну у 2022 році, російськими хакерами велася активна підготовка до проведення масованої атаки на українські державні сайти та інституції. 14 січня, атаки зазнали 22 державні органи та 70 українських веб-сайтів. Російські хакери тоді намагалися проштовхнути у маси думку, що кібератака була скоєна Польщею заради того, щоб викликати всередині України хвилю обурення та розбрату. Тоді, органи кібербезпеки повідомили, що ця атака – ніщо інше як провокація Росії [9].

А вже 15 лютого того ж року, представниками російських хакерских груп під кураторством ФСБ РФ було здійснено атаку на державні сайти, а

також банківські установи. Тоді зазнали атаки 15 банків, серед яких “Приват Банк” та “Ощадбанк”. Державні сайти не працювали близько п’яти годин. Постраждали такі відомства як Міністерство оборони України, Збройні сили України та Міністерство з питань реінтеграції тимчасово окупованих територій. Це стало першими ластівками у підготовці Росії до повноцінної атаки під час повномасштабного вторгнення.

За день до вторгнення 23 лютого 2022 року, ввечері, було атаковано сайти Верховної Ради, Кабінету Міністрів України, Міністерства закордонних справ, Служби Безпеки України та інших державних відомств. А вже вранці 24 лютого, коли російські війська перетнули кордон України, було вчинено атаку на Київську Обласну Державну Адміністрацію [56], найбільші електронні портали, якими користуються українці були використані для розповсюдження дезінформації, а також фішингових операцій з метою дестабілізації роботи військових [108]. Це стосувалося різного роду дзвінків та повідомлень на мобільні телефони солдатів та їхніх родин з погрозами чи закликами не чинити опір окупантам. Основними джерелами поширення дезінформації за словами представників СБУ стали такі платформи як Telegram, WhatsApp та Viber [57].

Разом із початком повноцінної війни на полі бою, не припинив своєї роботи і кібер-фронт. Найбільші хакерські групи України об'єдналися на захист своєї батьківщини та почали проводити власні контрзаходи по відношенню до Росії [46, 79]. Зокрема, було проведено атаки на критичні відомства РФ. Це стосувалося і сайту Президента РФ, і Міністерства оборони, і ФСБ. Також, українськими хакерами було проведено злам федеральних пропагандистських каналів РФ, під час яких росіянам було продемонстровано реальну інформацію відносно “успіхів” їхньої армії в Україні, а також надано можливість послухати українські патріотичні пісні [47]. 25 лютого 2022 року також було знищено систему управління Федерального казначейства РФ разом з резервними копіями. Більшість цих атак дуже сильно вдарили по агресору,

що позитивно вплинуло на хід бойових дій, та моральному духу російської армії в перші дні війни. А у лютому та березні 2022 року хакерами було зламано систему документообігу РФ між нею та окупованими територіями Донецької, Луганської області та Криму, що допомогли виявити списки тих, хто зрадив Україну та перейшов на сторону ворога [48].

Боротьба за кіберпростір триває і нині, бо країна-агресор використовує будь-які заходи задля втілення своїх планів по розчленуванню українського суспільства. Досі триває масштабна кампанія з дезінформації та розповсюдження фейків у соціальних мережах, досі існує система шпигунів та корисних ідіотів, які продовжують надавати агресорові конфіденційні дані, а також інформацію відносно локацій військових об'єктів. Тому, боротьба за безпеку у кіберпросторі продовжується, і за підтримки Західних партнерів України – зміцнюється.

Висновки до розділу 2

Отож, підсумовуючи зазначене у другому розділі, хотілося ще раз відзначити, що методи забезпечення інформаційної безпеки кіберпростору набувають досить різноманітних форм в залежності від підходу держави. Так, особливо в «Західному» підході до забезпечення безпеки, ми можемо спостерігати метод, за якого система регулювання кібербезпеки є досить м'якою, а також вітається розвантаження державних органів та передача повноважень місцевим осередкам, а також приватному сегменту та інтернет-провайдерам. Але за цього підходу, країни делегують частину повноважень відносно контролю всесвітньої мережі Інтернет саме Сполученим Штатам Америки, на території яких і знаходяться компанії-регулятори. За такого підходу, існує небезпека, а також сум'яття світових лідерів, відносно доброчесності самих США та захищеністю основних хабів Інтернету. Особливо після скандалу зі Сноуденом у 2013 році, коли в публічному просторі було опубліковано інформацію про те, що американські спецслужби ведуть цілодобове стеження та шпигують за своїми союзниками й ворогами, авторитет США у цьому питанні притерпів значних збитків. В свою чергу, цим скористалися геополітичні вороги Заходу, проголошуючи на міжнародному рівні намір послабити роль США в процесі забезпечення світової кібербезпеки.

З іншого ж боку, ми маємо підхід протилежний до політики Європи та Америки. Блок країн на чолі, зокрема з Росією та комуністичним Китаєм, формують свою інтерпретацію захисту кіберпростору. В цьому плані вони перш за все стоять на тому, щоб позбавити США визначного положення на світовій арені та добитися від американського уряду передачі важелів впливу на інтернет-середовище на рівень держав, щоб кожна держава сама по собі формувала свій кіберпростір, а також отримувала повний контроль над потоком інформації всередині своєї країни. І тут легко прослідковується головна мета подібних красномовних заяв – отримання тотального контролю

за населенням. За таких умов, свобода слова та обмін інформації віддається на відкуп місцевому керівництву, які на свій розсуд можуть обмежувати доступ, отримувати конфіденційну інформацію, а також слідкувати за власними громадянами. Для авторитарних держав така практика є не новою, а особливо для таких країн як Росія та КНР. У цих державах побудована жорстка вертикаль органів контролю, а інформація, отримувана їхніми громадянами проходить жорсткий контроль та цензуру. І саме їхні спецслужби формують кістяк органів безпеки кіберпростору. Тому, шлях який пропонують вони є по-суті легке прикриття для недемократичних режимів, які прагнуть до повного контролю свого інформаційного простору. І хоча Індія не дуже намагається схилятися до подібних методів, тим не менше також виступає за подібний сценарій, хоч і зі своїми особливостями.

Україна ж в цьому плані намагається слідувати саме Західній парадигмі кібербезпеки, закріплюючи нормативні положення країн ЄС та НАТО у своїх законодавчих структурах. Демократичний та євроатлантичний шлях нашої держави вписано у Конституції, а отже і пропагувати ми маємо саме ці цінності. Адаптувавши свої органи під норми та стандарти Заходу – ми створюємо власний плацдарм для захисту своєї держави від кібернетичних загроз, особливо з боку Росії. Послідовно впроваджуючи інновації та за підтримки наших партнерів, ми створили власну базу спеціалістів, які неухильно борються за нашу безпеку на інформаційного фронту, підлаштовуючись під реалії сучасної війни.

РОЗДІЛ 3: СУЧАСНИЙ СТАН КІБЕРБЕЗПЕКИ СВІТУ, НОВІ ВИКЛИКИ

3.1 Кібертероризм, як глобальна проблема

Розвиток інформаційних технологій, які заполонили майже всі сфери життєдіяльності, несе з собою не тільки позитивні, а й негативні тенденції та явища. Використання інформаційних технологій викликало новий вид злочинів, які загально можна окреслити як кіберзлочини. Серед них окремо можна виділити такий вид злочинів як «кібертероризм» – «умисна атака на інформацію, яка обробляється комп'ютером, комп'ютерну систему чи комп'ютерні мережі, що створює небезпеку для життя і здоров'я людей або призводить до інших тяжких наслідків» [113].

Деталі кібертероризму та залучені сторони в даному випадку розглядають по-різному. Федеральне бюро розслідувань США (ФБР) визначає кібертероризм як певну «навмисну, політично мотивовану атаку на інформацію, комп'ютерні системи, комп'ютерні програми та дані, що призводить до насильства проти некомбатантів з боку субнаціональних груп або таємних агентів» [142].

На відміну від шкідливого вірусу або комп'ютерної атаки, що призводить до порушень роботи систем безпеки, ФБР розрізняє кібертерористичні атаки як тип кіберзлочинів, явно спрямованих на заподіяння фізичної шкоди. Однак наразі немає консенсусу між різними урядами та спільнотами інформаційної безпеки щодо того, що кваліфікується як акт кібертероризму.

Інші організації та експерти припускають, що менш шкідливі атаки також можна вважати актами кібертероризму, якщо атаки мають на меті бути руйнівними або підвищити політичну позицію зловмисників. У деяких випадках кібертерористичні атаки відрізняються від звичайної кіберзлочинної

діяльності; основна мотивація кібертерористичних атак полягає в тому, щоб порушити або завдати шкоди жертвам, навіть якщо атаки не призводять до фізичної чи фінансової шкоди.

В інших випадках диференціація пов'язана з результатом кібератаки. Гордон Лоуренс, Леб Мартін та Чжу Лей, дослідники теми кібербезпеки, вважають, що інцидент слід вважати кібертероризмом, якщо він призведе до фізичної шкоди або втрати життя, прямо чи опосередковано через пошкодження або порушення роботи критичної інфраструктури. Однак інші вважають, що фізичне пошкодження не є передумовою для класифікації кібератаки як терористичної події. Організація Північноатлантичного договору, наприклад, визначила кібертероризм як «кібератаку з використанням або експлуатацією комп'ютерних або комунікаційних мереж, щоб викликати достатні руйнування або зриви, щоб викликати страх або залякати суспільство для досягнення ідеологічної мети» [117].

За даними Комісії США із захисту критичної інфраструктури, можливими об'єктами кібертероризму є банківська галузь, військові об'єкти, електростанції, центри управління повітряним рухом та системи водопостачання. На нашу думку, кібертероризм є транснаціональним діянням, яке вчиняється окремими індивідами чи організаціями осіб. Мотивами вчинення можуть бути як і політичні аспекти, так і аспекти помсти або прагнення до самоствердження. Цілі, при цьому, можуть переслідуватися найрізноманітніші, як підрив, так і демонстративність. Кібертерористи можуть використовувати як матеріальні засоби, зокрема інформаційні – демагогію, пропаганду помилкових ідей, залякування за допомогою ЗМІ, так і нематеріальні, наприклад хибні повідомлення про вибухи та інше [140].

Доктор Пол Корніш з Королівського інституту міжнародних відносин, що є незалежним політичним інститутом у Лондоні, у своєму звіті

підготовленому для Європарламенту виокремив наступні категорії кібертерористичних актів [98].

За *способами* вчинення вони поділяється на:

1. провокування збройного заколоту, повстання чи військового перевороту для захоплення або зміни влади;
2. порушення системи державного управління за допомогою вбивств політичних лідерів, шантажу, навіювання жаху, відчаю, психологічної пригніченості;
3. руйнування основ конституційного ладу, цивілізованого життя і створення хаосу у функціонуванні систем зв'язку та життєзабезпечення, транспортних засобів, роботі організацій та установ сучасного суспільства.

За *об'єктом* спрямованості:

1. акти тероризму, що вчиняються проти безпеки держави;
2. акти тероризму, що вчиняються проти безпеки осіб;
3. акти тероризму, що вчиняються щодо майна або окремих фізичних чи юридичних осіб.

За *змістом* діяльності: діяльність терористської групи (особи, організації), спрямовану на зміни у зовнішньому (навколишньому) світі, та внутрішню діяльність терористських груп, спрямовану на забезпечення власного існування.

За *характером наслідків* поділяються на такі, що спричиняють:

1. шкоду здоров'ю;
2. створення загрози чи заподіяння шкоди життю людей або їх здоров'ю, матеріальної, моральної чи всіх видів у сукупності;
3. людські жертви, які можуть бути груповими, а також одиничними;

4. матеріальну шкоду [98].

Варто також відзначити не добру тенденцію, яка спіткала сучасний світ, бо як показують дані агентства Purplesec, за час пандемії COVID-19 статистика кібератак та кібертерористичних актів у світі зросла у 600% [146]. Такі дані просто шокуючі. Згідно ж зі статистикою сформованою тим самим агентством, у період з 2006 по 2020 рр найбільш постраждалими від дій кібертерористичних атак виявилися такі держави як Сполучені Штати Америки, відповідно 156 випадків, Велика Британія – це 47 випадків, Індія – 23 випадки, Федеративна Республіка Німеччина – 21 випадок, та Південна Корея – 18 випадків [87].

Проте, автор також хоче відзначити, що приведена вище статистика відображає тільки ті дані, які були офіційно озвучені, а також торкаються питань шкоди завданої державним органам, об'єктам критичної інфраструктури, оборонним підприємствам чи економічними атаками, які коштували компаніям більше мільйона доларів США. Що може означати, що цифра злочинів може бути набагато вище від приведених агентством.

Тому, відзначимо, що кібертероризм стає дедалі більшою проблемою з кожним днем. В контексті війни України з Росією, остання проводить постійні атаки не тільки через збройні сили, а також і завдає атак на інформаційну систему України. За свідченням голови Державної служби спеціального зв'язку та захисту інформації Юрія Щиголя, тільки за 2022 рік наша країна пережила 2194 хакерські атаки з боку держави-агресора [47].

Основні проблеми протистояння подібного роду атакам полягають у тому, що спрогнозувати їх дуже важко, і держави не завжди мають змогу діяти на випередження. При цьому сам хакер чи хакерська група можуть знаходитися як всередині держави, так і за її межами. У цьому випадку досить важко визначити де саме вони знаходяться та хто їх підтримує. Саме на це

найбільше намагаються давити іноземні спецслужби чи замовники, коли їх обвинувачують у скоєнні злочину.

І знову ж таки, камінь спотикання сучасної системи, притягнення до відповідальності зловмисників, які знаходяться за межами держави – в цьому випадку, якщо держава на території якої перебуває зловмисник, відмовляє державі позивачу у екстрадиції та затриманні хакера – остання не може його отримати для суду. Отож зловмисники залишають безкарними. Проте, як ми вже згадували у попередньому розділі, ті самі Сполучені Штати Америки та Європейський Союз можуть накласти санкції на держави, які переховують терористів, чи компанії спонсори кібертеактів, як то було з Росією. Та такі ситуації радше – окремі моменти, аніж константа. Зрештою, міжнародне законодавство по контролю кібербезпеки і досі досить скупе на реальні механізми боротьби з подібного роду злочинцями, спираючись більше на двосторонні договори чи роботу власних спецслужб [138].

3.2 Кібершпигунство, як засіб роботи світових спецслужб

Сучасний світ потребує і сучасних засобів для спецслужб різних країн світу у отриманні доступу до інформації, яка є строго конфіденційною. Розвиток кіберпростору, а також впровадження новітніх технологій у життя суспільства відкрили нову сторінку для держав у питанні розвідки та контррозвідки. Нині кожен пристрій, будь то телефон, ноутбук, комп'ютер чи планшет являє собою засіб як для стеження і збору інформації. І, таким чином він стає джерелом усіх даних відносно їхнього власника та його життя.

Ера цифровізації та діджиталізації принесла у наш світ можливості легкого пошуку будь-якої інформації, і таким чином заклало основу певної «прозорості» індивіда. Викладаючи фотографії у соціальних мережах, пишучи

статті та пости в Інтернеті ми ділимося частинкою себе з усім світом. А, оскільки кожна програма чи технологічний продукт мають конкретного власника, ми стаємо видимими і для них. Отож, перед виробниками стоїть завдання адекватного збору інформації та моніторингу ситуацію всередині власних продуктів задля усунення можливості скоєння кібератак [17].

Зазвичай такий контроль здійснюється через аналіз даних отриманих з таких ресурсів як антивіруси, Data Leak Prevention (програми призначені для запобігання витоків конфіденційної інформації), Intrusion Detection System (програми які виявляють вторгнення сторонніх осіб та програм), маршрутизатори, міжмережеві екрани, операційні системи серверів. Коли система виявляє будь-яке відхилення від норми – вона реагує, і таким чином генерується так званий кіберінцидент.

По суті робота цих систем являє собою світову практику відстеження кіберзлочинів, оскільки кожен із них залишає по собі слід, який вноситься у журнал даних, і вони опрацьовуються системою задля унеможливлення потенційної атаки. У цьому випадку надходить інформація не тільки про час, але й причину чому цей інцидент мав місце. У такому випадку відповідні органи аналізують інформацію надану системою, виявляють в системі слабкі місця та проводять тренування по відбиттю атаки базуючись на отриманому досвіді [17].

Держава також слідкує за тим, що відбувається в її інформаційному просторі, і спецслужби також. Нерідко вони вдаються навіть до того, що проводять повний моніторинг того, що пишуть та чим займаються їхні громадяни, як то наприклад наш східний сусід Російська Федерація, де навіть існує нормативна база, яка регулює питання того, які теми вважається дозволеним до демонстрації у Інтернеті, а за що призначається навіть адміністративне чи кримінальне покарання. З початку повномасштабного

вторгнення там навіть введено директиву про покарання тих, хто на думку влади «дискредитує їхні збройні сили» [70].

Але, повернемося до теми. Як вже відзначалося, законодавства певних країн дозволяють їхнім правоохоронним органам отримувати доступ до особистої інформації їхніх громадян у кіберпросторі, проте, залишається запитання їхнього доступу і до даних іноземних громадян, урядів чи підприємств. Подібна діяльність характеризується як кібершпигунство, або, як частіше зустрічається в термінологічних джерелах – кіберрозвідка. У Законі України «Про основні засади забезпечення кібербезпеки України», цей термін характеризується як: «діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням»[52, 59].

Проблеми організації протидії потенційним атакам з боку кіберзлочинців спонукало світові держави відповідальніше поставитися до цієї проблеми і з точки зору внутрішньої політики, і з точки зовнішньої. Тому, як вже відзначалося нами у попередньому розділі, вже на кінець 2013 року можливі стратегії було прописано більшістю країн ЄС (мова йде як про національне законодавство, так і європейське загалом), США, Канадою, Японією, Російською Федерацією, комуністичним Китаєм та багатьма іншими державами [21].

Проте, як показала практика, як у США так і у КНР були свої підходи до трактування забезпечення безпеки. Зокрема, саме в стратегії США прописано необхідність створення «наступальних військ» кіберзахисту, що свідчить про існування спец призначенців, в чию компетенцію входить кібершпіонаж. Дані ж про потенціал, чисельність і завдання китайських кібервійськ, на жаль, практично відсутні. Проте, у китайських офіційних документах, як наприклад вже у згаданій нами Білій Книзі, починаючи з 2000-х років неодноразово відзначалося прагнення КНР до створення власного інформаційного

потенціалу для забезпечення безпеки китайських інтересів у світі та створення адекватної системи захисту, яка має відповідати сучасним стандартам [148].

У 2010 році Міністерство оборони США опублікувало доповідь у якій говорилося про військову міць Китаю. І попри те, що даних про чисельність китайських кібершпигунів там не було зазначено, посадовці стверджували, що припускають причетність китайського уряду та китайських військ до атак на державні об'єкти Сполучених Штатів [86].

За даними опублікованими The Daily Beast, урядові США було представлено секретний звіт Федерального бюро розслідувань, у якому говорилося про потенціал та розвиток військової кібермережі КНР. Висвітлені у звіті дані говорили про те, що КНР та її кібершпигуни володіють достатнім потенціалом, щоб знищувати критичну інфраструктуру США, отримувати доступ до банківських, комерційних, військових та оборонних баз даних. Звіт ФБР також включав інформацію про 180 тис. китайських кібершпигунів, які щоденно атакували кібермережі США, і лише 2009 рік ними було вчинено 90 тисяч атак проти системи Міністерства оборони США. До того ж, ФБР відзначали, що 30 тисяч із них були працівниками невійськової сфери, а були приватними особами, чиїми послугами користувався уряд КНР. Мета цих атак була у тому, щоб дістатися до секретної інформації державних відомств США, та внесення хаосу у функціонування цих органів [132].

Проте, одним із найбільших скандалів у питанні кібершпигунства, який заслуговує, на нашу думку, згадки в цій роботі, є скандал із Едвардом Сноуденом, що розгорівся у 2013 році, коли цей працівник Агентства національної безпеки Сполучених Штатів Америки втік спочатку до комуністичного Китаю, а потім і до Росії, попутно виказавши світовій громадськості через газети The Guardian та The Washington Post, яким він дав інтерв'ю, секретну інформацію про те, що Сполучені Штати ведуть стеження за власними громадянами та керівництвами іноземних держав [60].

Історія цього воістину неймовірного випадку розпочалася десять років тому, коли Едвард працював у Гавайському відділі Агентства національної безпеки США, де займався адмініструванням комп'ютерних систем. Там, він отримав доступ до секретної американської програми безпеки PRISM (англ. Planning Tool for Resource Integration, Synchronization, and Management), яка являла собою засіб АНБ для стеження та збору інформації користувачів як на території США, так і за його межами. Агентство, за словами Сноудена отримувало доступ до: електронної пошти, відео- та голосових повідомлень, відео, фотографій, VoIP (англ. voice over IP – технологія передачі медіа-даних у реальному часі), передачі файлів, повідомлень про логіни та деталі із сайтів соціальних мереж.

З матеріалів, які були оприлюднені Сноуденом у газеті New York Times зазначалося, що система прослуховування дозволяла зводити дані про телефонні дзвінки в єдину схему з інформацією з відкритих, комерційних та інших джерел, а також інформацією страхових ідентифікаторів, банківських кодів, профілів у Facebook, пасажирських списків на транспорті, списків виборчих дільниць тощо. З початку передбачалося, що систему будуть використовувати відносно іноземних держав та їхніх урядів, проте і американці були під стеженням. Інформація, наприклад, про номери щойно набраного телефону або місця перебування того, хто телефонує по мобільному дозволяє виявити, що у людини на думці. По-суті, у кримінальному процесі це можна порівняти зі стеженням за підозрюваним [89].

Сноуден встиг завантажити тисячі секретних документів, які стосувалися роботи зазначеної системи, а також містили інформацію відносно інших операцій Сполучених Штатів за межами власної держави, перед тим як покинути їх назавжди. 20 травня 2013 року, Едвард ніби бере відпустку, та негайно вилітає до Гонконгу, де вже й оприлюднює пресі секретну інформацію відносно програми PRISM, а також інші важливі дані Агентства національної безпеки США. Такі дії свідчать про те, що він заздалегідь готувався до втечі, а

також певно посвітив керівництво КНР та Росії у свої плани відносно інформації яку він мав у своєму розпорядженні.

Проте, окрім інформації яка стосувалася його власної батьківщини, Сноуден також розповів про співпрацю США з іншими державами та їхніми спецслужбами. Зокрема, у інтерв'ю Дейлі Телеграф ним було заявлено про те, що британське агентство електронної безпеки Центр урядового зв'язку також проводив політику стеження за власними громадянами. Журналісти отримали інформацію про те, що GCHQ (спецслужба Великої Британії, відповідальна за ведення радіоелектронної розвідки і за забезпечення захисту інформації органів уряду і армії) прослідковувала міжнародний телефонний та інтернет-трафік, отримавши доступ до відповідних мереж [115].

Публікація у засобах масової інформації цих даних викликала гучний скандал у світі по відношенню до США, і хоча американські спецслужби виправдовувалися застосуванням програми виключно у правовому полі США та оперували тим, що вона допомагала у розслідуваннях кібезлочинної діяльності, а також дозволяла владі запобігати терористичним актам на своїй території, все ж необхідний для Сноудена та його покровителів скандал набрав обертів, і подібні заяви виглядали радше виправданням, аніж реальними аргументами для світової громадськості.

З секретних документів випливало те, що американці проводили стеження за дипломатичними установами іноземних держав та структурами ООН, і що найболючіше врізалося клином у відносинах США зі країнами Європи, їхніми найбільшими партнерами, – то це те, що стеження велося і за органами Європейського союзу. Тодішній голова Європейського парламенту Мартин Шульц навіть вимагав від американського керівництва відповіді за подібні дії.

Для Німеччини обнародування цієї інформації призвело до того, що у владних колах почали лунати заклики про необхідність притягнення

Сполучених Штатів та Великої Британії до відповіді за подібні дії. Сноуден спровокував поглиблення іще більшого розколу у відносинах між провідними членами ЄС, які за часів правління Ангели Меркель просували ідею відходу від орієнтації на США та залежності від них. Тому, після цього скандалу, 2 серпня 2013 року Федеративна республіка Німеччина скасувала угоди з США та Великою Британією, які дозволяли західним союзникам ФРН вести стеження на їх території. Вони формально дозволяють розвідслужбам США і Великобританії користуватися інформацією, отриманою в результаті прослуховування німецьким відомством щодо захисту конституції і федеральною розвідслужбою Німеччини, а також самим відслідковувати листи і з'єднання, якщо викликає загрозу для безпеки військових підрозділів з цих країн, дислокованих на території ФРН.

Звичайно, після возз'єднання Німеччини у 1990 році ці угоди не застосовувалися, тим не менше, заважаючи на отриману інформацію від перебіжчика Сноудена: «Скасування адміністративних угод, на якій ми наполягали в останні тижні, є необхідним і правильним наслідком останніх дебатів про захист особистої сфери», - відзначив тодішній глава МЗС ФРН Гідо Вестервелле у інтерв'ю російському пропагандистському виданню «РИА «Новости»» [39].

Після зчиненого скандалу, Сноуден запросив політичного притулку у Російській Федерації, де він і до нині переховується від кримінальної відповідальності у США, яке пред'явило йому звинувачення у шпигунстві та розголошенні державних таємниць [18].

Дії Сноудена дали карт-бланш таким державам як Росія та КНР у тому, щоб дискредитувати Сполучені Штати перед міжнародною спільнотою та вимагати, зокрема на платформі ООН, зменшення можливостей контролю американськими органами Інтернет-простору та передачі контролю над ними національним державам, просуваючи власні концепції бачення кібербезпеки

В цей же час Європейські держави починають займати позицію диверсифікації свого напрямку співпраці у кібербезпеці з іншими державами, не беручи до уваги тільки США. Посилюється китайський чинник на європейському просторі, поглиблюючи свою економічну співпрацю з провідними європейськими державами, як то Німеччина та Франція.

3.3 Світові тенденції у питанні посилення безпеки кіберпростору

Конвенція про кіберзлочинність, також відома як Будапештська конвенція про кіберзлочинність або Будапештська конвенція, є першим міжнародним договором, спрямованим на боротьбу з інтернет-злочинністю та комп'ютерною злочинністю (кіберзлочинністю) шляхом гармонізації національних законів, удосконалення методів розслідування та розширення співпраці між державами [25]. Він був розроблений Радою Європи в Страсбурзі, Франція, за активної участі держав-спостерігачів Ради Європи: Канади, Японії, Філіппін, Південної Африки та Сполучених Штатів.

Текст документу та Пояснювальна доповідь були прийняті Комітетом міністрів Ради Європи на його 109-й сесії 8 листопада 2001 року. Вона була відкрита для підписання в Будапешті 23 листопада 2001 року та набула чинності 1 липня 2004 року. Станом на квітень 2023 року 68 держав ратифікували конвенцію, тоді як ще дві держави (Ірландія та Південна Африка) підписали конвенцію, але не ратифікували її [112].

1 березня 2006 року набув чинності Додатковий протокол до Конвенції про кіберзлочинність. Ті держави, які ратифікували додатковий протокол, зобов'язані криміналізувати поширення расистських і ксенофобських матеріалів через комп'ютерні системи, а також погрози та образи на ґрунті расизму чи ксенофобії [114].

Конвенція була підписана Канадою, Японією, США та Південною Африкою 23 листопада 2001 року в Будапешті. Станом на квітень 2023 року державами, які не входять до Ради Європи, які ратифікували договір, є Аргентина, Австралія, Бразилія, Кабо-Верде, Канада, Чилі, Колумбія, Коста-Ріка, Домініканська Республіка, Гана, Ізраїль, Японія, Маврикій, Марокко, Нігерія, Панама, Парагвай, Перу, Філіппіни, Сенегал, Шрі-Ланка, Тонга та Сполучені Штати [139].

Конвенція є першим міжнародним договором про злочини, вчинені через Інтернет та інші комп'ютерні мережі, зокрема щодо порушень авторського права, комп'ютерного шахрайства, дитячої порнографії, злочинів на ґрунті ненависті та порушень безпеки мережі [25]. Він також містить низку повноважень і процедур, таких як пошук комп'ютерних мереж і законне перехоплення.

Його основною метою, викладеною в преамбулі, є проведення спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, особливо шляхом прийняття відповідного законодавства та сприяння.

Конвенція спрямована головним чином на:

- Узгодження національних кримінально-правових норм матеріального права та пов'язаних з ними положень у сфері кіберзлочинності
- Надання національним кримінально-процесуальним законодавством повноважень, необхідних для розслідування та судового переслідування таких правопорушень, а також інших правопорушень, вчинених за допомогою комп'ютерної системи, або докази щодо яких знаходяться в електронній формі
- Налагодження швидкого та ефективного режиму міжнародного співробітництва

Конвенція визначає наступні правопорушення: незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему, неправомірне використання пристроїв, комп'ютерна підробка, комп'ютерне шахрайство, злочини, пов'язані з дитячою порнографією, а також злочини, пов'язані з авторським правом і суміжними правами.

Він також визначає такі питання процесуального права, як прискорене збереження збережених даних, прискорене збереження та часткове розкриття даних трафіку, порядок виробництва, обшук і конфіскація комп'ютерних даних, збір даних трафіку в реальному часі та перехоплення даних контенту. Крім того, Конвенція містить положення про особливий тип транскордонного доступу до збережених комп'ютерних даних, який не потребує взаємної допомоги (за згодою або у відкритому доступі) і передбачає створення цілодобової мережі для забезпечення швидкого допомоги між Сторонами, що підписали. Крім того, як умови та гарантії, Конвенція вимагає забезпечення належного захисту прав і свобод людини, включаючи права, що виникають відповідно до зобов'язань за Європейською конвенцією з прав людини, Міжнародним пактом про громадянські та політичні права та іншими застосовними міжнародними документами з прав людини, і має включати принцип пропорційності [118].

Конвенція є результатом плідної роботи європейських та міжнародних експертів. Нещодавно, вона була доповнена Додатковим протоколом, який торкався питання розпалювання ксенофобії та расизму в мережі. Тому, нині подібні дії будуть прирівнюватися до кримінального злочину та розглядатиметься як умисний наклеп. До того ж, у рамках Конвенції опрацьовується питання регуляції кібертероризму, як ще одного пункту, який має бути висвітлений та врегульований.

Проте, не зважаючи на успіх європейських правових кіл та поширення парадигми вільного Інтернету, як вже зазначалося у розділі 2, є держави, що у

своїй політиці притримуються закритості та тотального контролю мережі. Вони продовжують проштовхувати свою ідею введення регулювання мережі національними державами, та передачі їм відповідних повноважень. І так, у грудні 2019 року на Генеральній Асамблеї ООН, представники держав мали розглянути запропоновану Росією резолюцію відносно кібербезпеки, що зачіпає питання розслідування цих злочинів, а також співпраці держав у цьому питанні. Навіть попри жорсткі заяви з боку західних держав, таких як США, Франція, Німеччина, Канада та Велика Британія, а також світових правозахисних організацій, РФ та її союзникам, зокрема, в обличчі центральноазійських країн пострадянського простору, Білорусі та комуністичного Китаю таки вдалося схилити більшість держав на свій бік під час остаточного голосування 27 грудня 2019 року. Російська резолюція була прийнята остаточним голосуванням 79 проти 60 при 33 утрималися [151].

Як нами вже зазначалося протягом даної роботи, у світі вже давно існує досить сильна розбіжність відносно поглядів на кібербезпеку та методи її забезпечення. А отже і на полях Організації Об'єднаних Націй ця повістка залишається актуальною, і боротьба між прихильниками вільної мережі (країнами глобального Заходу) та авторитарної моделі контролю (КНР, РФ та їхні найближчі союзники) набирає обертів.

Підготовка до Резолюції 2019 року почалася ще під час засідання Генеральної асамблеї у 2018 році, коли була прийнята резолюція щодо кіберзлочинності, яку проштовхувала Росія, яка вимагала від Генерального секретаря ООН збирати думки країн щодо кіберзлочинності та успішно включила обговорення можливого договору про кіберзлочинність у порядок денний ООН [165].

І як говориться у тексті Резолюції, має бути створена консультаційна рада ООН у Нью-Йорку задля проведення переговорів відносно впровадження нового міжнародного правового документу який має регламентувати питання

безпеки кіберпростору. Мета Росії очевидна – вона бажає замінити Будапештську конвенцію Ради Європи, яка наразі є єдиним міжнародним документом, що безпосередньо стосується цього питання. Не один раз до цього РФ намагалася проштовхнути в інформаційний простір ООН ідею про заміну Будапештської конвенції, наголошуючи на тому, що вона застаріла, а характер її суто регіональний та не має жодного імперативу, і натомість порушує суверенітет держав-членів [25]. Хоча, як ми відзначили у другому підрозділі розділу другого, Росія не була підписантом угоди, і носила виключно статус спостерігача.

І попри те, що автор погоджується з думкою про необхідність посилення переговорного процесу відносно питання регулювання ІКТ на глобальному рівні, тим не менше, вважає неприпустимим можливість узурпації влади над інформаційним простором, оскільки це може призвести до зменшення свободи слова, яке є одним з базових принципів сучасного суспільства. А в даному випадку, як висловився директор відділу правозахисної Організація Human Rights Watch з проблематики ООН Луїс Шарбонно, через досить розпливчасті формулювання тексту резолюції, світова громадськість може зіткнутися з тотальною цензурою інтернету національними урядами, та можливим переслідуванням владою своїх політичних опонентів, та незгодних з позицією влади громадян, прикриваючись боротьбою з кіберзлочинністю [165].

До того ж, окрім змістового наповнення та безпосередньо питання регулювання, постає і інша проблема – забезпечення продовження міжнародної співпраці в умовах нової нормативної бази, якщо вона звичайно буде прийнята. Так як Будапештську конвенцію вже ратифікували або приєдналися до неї шістдесят чотири країни з різних регіонів, і попри свій дійсно солідний вік по мірках розвитку технологічного процесу та засобів контролю ІКТ, тим не менше вона все ще залишається базою основних критеріїв, якім мають відповідати держави. В деяких випадках навіть держави, що не є підписантами цього документу, брали за основу свого законодавства у

питанні регулювання кіберпростору саме цю конвенцію. Новий договір, який пропонує Росія та її союзники може нашкодити міжнародній співпраці у цьому питанні та внести хаос у нормотворчий процес, особливо коли питання кібербезпеки як ніколи є актуальним.

Проте, виходячи з резолюції представленої у Генасамблеї ООН у січні 2021 року, а також подальших документах ООН, поки російська Резолюція 2019 залишається документом суто декларативним та дискусійним, оскільки комітети з питань її обговорення так і не змогли прийти до спільного знаменника, а враховуючи російську агресію у 2022 році, можливість продовження переговорів по цій резолюції у потрібному Москві ключі носить вкрай примарний характер. Цим в свою чергу, можуть скористатися прихильники відкритого Інтернету [152].

Наразі ж основними слабкими місцями міжнародної спільноти яка підтримує вільне використання ІКТ є два моменти, а саме питання кваліфікованості та обізнаності представників держав у відповідних комітетах, а також забезпечення підтримки існуючої системи контролю кіберпростору. У першому випадку, як відзначає сама ООН, проблема криється у тому, що питанням забезпечення нормативної бази регулювання ІКТ та кіберзлочинів розглядається окремо одразу у трьох різних органах, що створює проблеми комунікації між ними. Тому, маємо сміливість припустити, що в даному випадку необхідно зосередитися саме на тому, щоб забезпечити просування необхідних наративів через перемовини з представниками різних держав, щоб вони були краще обізнані, а також краще розуміли про що саме йде мова. Це звичайно довгий процес, оскільки, як автор вже відзначив, деякі делегати та їхня обізнаність у цих процесах вкрай низька, і дається взнаки відсутність досвіду, проте саме так можна подолати їхнє нерозуміння та отримати потрібний результат.

Другий момент має бути вирішений радше не через протидію новим нормотворчим тенденціям, а як підкреслення позитивних сторін діючих документів. У цьому ключі необхідно продовжувати сприяння поширенню основних цінностей, прописаних у Будапештській конвенції. Саме її доповнення та адаптація до сьогоднішніх реалій має стати головною метою західних держав на міжнародній арені. Зрештою, саме Будапештська конвенція вже багато років залишається основною збіркою норм та правил, за якими здійснюється контроль та співпраця у кіберпросторі. Демонстрація важливості та переваг Будапештської конвенції та цього можливого протоколу для держав, що ще не приєдналися до даної конвенції, чи для держав, які знаходяться за межами основних дебатів має вирішальне значення для отримання їхньої підтримки. Все ж таки, незважаючи на свої обмеження, Будапештська конвенція вже понад десять років діє як механізм зміцнення довіри між країнами, які до неї приєдналися. У такій сфері, як кіберзлочинність, це дуже важливо [151].

Загроза кіберзлочинності продовжує зростати, і уряди здебільшого не притягують винних до відповідальності, що потребує поглиблення співпраці між державами. Запропонована Росією та її союзниками Резолюція 2019 року, стала викликом для світу та сигналом про те, що фрагментація міжнародного суспільства набиває все більше обертів. В умовах відкритого протистояння російській та китайській автократії демократичним державам необхідно сформувати чітку позицію на міжнародній арені, щоб не допустити просування наративів про впровадження тотального контролю національних урядів над інформаційним простором, як шлях до вирішення проблем кібербезпеки, а також запобіганню кіберзлочинів.

Висновки до розділу 3

Як свідчать результати проведеного нами аналізу у вищезазначеному розділі: реалії сучасного світу вимагають від держав конкретних та цілеспрямованих дій відносно регуляції кіберпросттору. Унормування міжнародного права відносно безпеки кіберпростору зможе допомогти правоохоронним органам по всьому світу розкривати потенційні злочини та діяти на випередження. Проте, одночасно з цим, все ще існує загроза того, що методи, якими будуть діяти ці органи та держави носитимуть характер порушення особистих прав людину на свободу слова, а також конфіденційності її особистого життя. Скандал спровокований Сноуденом у 2013 році, а також інші не менш важливі викриття відносно роботи спецслужб у сфері кібербезпеки говорять про те, що попереднє припущення є об'єктивною реальністю. Нині усе що відбувається у цифровому просторі являє собою величезний жорсткий диск з компроматом на кожного з нас. До того ж, камери на вулицях та дорогах, WI-FI точки та маршрутизатори, GPS-навігатори, фотографії у соціальних мережах, коментарі та перегляди на YouTube завжди залишають по собі слід, яким зрештою можуть скористатися зловмисники. Інтернет пам'ятає усе. І саме тому, навіть до найзахищеніших місць на землі, де б вони не знаходилися, зрештою можна дістатися.

Тому, оскільки кожна держава має безпосередній вплив на власний інформаційний простір – усе що відбувається всередині неї так чи інакше проходить через відповідні органи. Питання лише в тому, чи мають вони відповідні повноваження в державі відносно цього, і чи не є подібні дії порушенням прав людини. Прикриваючись словами про державну безпеку та піклування про добробут громадян, так чи інакше, правоохоронні органи намагаються виправдати свої дії перед власною громадськістю.

У питанні створення єдиної правової системи регулювання злочинних дій в кіберпросторі на жаль також спостерігається криза. Особливо вона

виникає у площині того якими методами має проводитися протидія таким злочинам, а також притягнення винних до відповідальності. Бо можна зламати систему захисту знаходячись при цьому на іншому кінці планети, і навряд правоохоронні органи тієї конкретної держави зможуть дістатися до хакера. До того ж, як і у внутрішньодержавній політиці, світові лідери схильні притримуватися подібних стратегій і у кібербезпеці. І таким чином авторитарні держави нав'язують свою систему бачення, яка виливається у жорсткому контролі інтернет-середовища, в той час як демократичні держави схильні до м'якших засобів безпеки. І саме розрив між цими поглядами на проблему зумовлює слабкість саме міжнародної системи контролю кіберпростору. На разі, у більшості своїй, ця сфера регулюється саме національними законодавствами держав, а також договорами локального та регіонального значень. Спроби ж якось вплинути на нормотворчий процес через глобальні організації, так як ООН – поки не принесли відчутних зрушень в цьому напрямку.

ВИСНОВКИ

Сучасна система кібербезпеки, а також її трактування науковим співтовариством, напряму випливає з того, в яких політичних умовах вона формується. Країни Заходу, а також країни світу, які являють собою демократичні режими, у своїй політиці спираються на сучасні тенденції, в яких громадянин та його безпека у кіберпросторі являють собою найбільшу цінність для держави. Це стосується не просто захисту особистих даних, але й нерозповсюдження потенційно образливого контенту для певних груп населення (булінг та обрáзи расистського, ксенофобського, релігійного та шовіністського характеру). Натомість у державах, в яких панує або ідеологічна, або релігійна, або націоналістична складова, ми спостерігаємо діаметрально протилежну картину, в якій вже саме держава та її цінності є найбільшим приорітетом. У цій ситстемі громадянин виступає як об'єкт, що потрібно опікати, слідкувати за ним, а також контролювати інформацію, що поступає до нього. Саме з цього й випливає формування нормативно-правової бази в зазначених державах.

До того ж, виходячи з проведених вище досліджень, можна стверджувати, що наразі спостерігається тенденція, яка, з одного боку намагається впровадити у загальне користування єдину термінологічну систему відносно кіберпростору та ІКТ, і навіть такі держави, як комуністичний Китай (КНР) беруть собі у законодавчу базу досвід європейських держав цьому питанні. А з іншого боку ми спостерігаємо те, що деякі держави, як наприклад РФ, намагаються сформувати свою власну термінологічно-правову базу, яка б відповідала саме їхнім внутрішньо-політичним інтересам. Тож можна стверджувати, що і у питанні уніфікації термінів відносно кіберпростору та кіберзлочинності існує вплив саме політичного поля держави, коли уряди кожної країни вносять щось своє.

Стан нинішньої кіберзлочинності у світі є надзвичайно високим. Нині в умовах розвитку ІКТ та ІТС, політичне протистояння держав перейшло й у кіберпростір. Цифровізація світу призвела до того, що більшість критичної інформації більше не знаходиться на аналогових носіях чи папері, а зберігається у хмарних сховищах, до яких мають можливість дістатись професійні хакери. Що в свою чергу породжує можливість витоку інформації та шпигунство. Єдине чим обмежуються хакери – це технології та методи зламу, і тому те, що зараз здається неприступним захистом - вже завтра стає застарілим та відсталим.

А виходячи з досвіду України у відбитті кіберінцедентів за останні 10 років можна зробити висновок, що навіть захищені урядові канали можуть стати жертвами кібератресії. До того ж існують загрози витоку зсередини. Інцидент з Е. Сноуденом тому гарний приклад, коли людина, що має доступ до секретної інформації, зливає її ворогам держави, що, в свою чергу, провокує міжнародні конфлікти та дипломатичні скандали. Також, не менш важливою деталлю, є те, що всіма використовувані соціальні мережі служать спецслужбам, як база для збору особистої інформації про користувачів. Тому, знову ж таки, чудовий приклад історія з блокування таких російських соціальних мереж, як «Одноклассники» та «ВКонтакте», як цілодобово моніторяться російським ФСБ.

Повертаючись до питання законодавчих основ, якими користуються провідні держави світу, в тому числі й Україна, можна зробити висновок, що умовно їх можна поділити на два табори.

До першого табору відносяться держави, які у своїй політиці дотримуються принципу демократизації, що означає залучення у процес кібербезпеки не тільки державних органів, а й приватних підприємств та компаній, які займаються відслідковуванням трафіку всесвітньої мережі Інтернет. Сюди входять і виробники оптоволоконних кабелів, а також мобільни

оператори, які надають користувачам доступ до Інтернету. Їм надається можливість контролю трафіку заради мінімізації кіберінцедентів на побутовому рівні (нерозповсюдження забороненого контенту, обмеження доступу до шкідливих сайтів). При цьому законодавства держав є досить гнучкими щодо питань кіберпростору та його безпеки.

До другого табору належать держави, що притримуються ідеї тотального контролю, в тому числі й Інтернету. Більшість цих країн по суті являють собою авторитарні режими із жорсткою вертикаллю влади та зневагою до прав людини. Саме тому вони прагнуть до підпорядкування всесвітньої мережі через свої спецслужби, яким надається повна свобода дії відносно тих, кого держава вважає порушниками. Йде жорстка цензура того, що відображається у мережі на території цієї держави для пересічних громадян. А їхня діяльність у мережі є повністю контрольованою спецслужбами. І якщо на думку спецслужб людина є порушником законів, вони мають повноваження до затримання та покарання такого індивіда. Для прикладу можна привести ту ж саму РФ, де ФСБ має повноваження карати усіх, хто незгоден з нинішньою політикою керівництва держави.

У цьому плані Україна дотримується ідеї саме демократичного блоку, вдосконалюючи та адаптуючи власне законодавство до європейського. Російська агресія з 2014 року показала світові початок нової віхи в історії війн, ведучи її не тільки на полі бою, але й у медіапросторі. Тому на захисті інформаційного простору держави нині працюють не тільки державні органи, але й залучаються приватні кампанії та групи професійних хакерів, які не тільки захищають наше інфополе, але й проводять наступальні дії на кіберпростір агресора.

Щодо ситуації у міжнародному правовому регулюванні кіберпростору та протистояння кіберзлочинності, нажаль усе не так однозначно. Потуги світових держав на початку 2000-х років щодо впровадження у світове

користування Будапештської конвенції не призвело до відчутних результатів. У державах все ще спостерігається скептицизм відносно міжнародного регулювання, так як найбільші держави мають у своєму розпорядженні суттєвіші важелі впливу на інформаційний простір у світі, й таким чином держави поменше опиняються у прямій залежності від їхнього медійного простору. До того ж, після згаданого вище інциденту зі Сноуденом, довіра у співпраці між країнами у питанні кіберзахисту ослабла, що негативно вплинуло на міжнародний простір, посилюючи відцентрові тенденції у світі.

В останні роки спостерігалося посилення авторитету держав недемократичного блоку (КНР та РФ), які проводили політику економічного впливу на держави середньої Азії та Африки, що в свою чергу призвело до падіння Західного лобі на міжнародній арені, а також внесло в ці держави моделі жорсткого правління, коли існує внутрішньо-державне свавілля при якому відсутній контроль з боку міжнародної спільноти.

Прямий напад на Україну 24 лютого 2022 року довів світові недієздатність міжнародних організацій у питанні збереження миру та безпеки у глобальному вимірі, тому ми можемо припустити, що в майбутньому нас очікує переформатування та адаптація міжнародних структур до сучасних реалій, а також посилення поляризації світу на зразок холодної війни. Питання кіберпростору також буде одним з головних. Бо технологічний прогрес – це неминуча та неупинна річ і в умовах потенційної глобальної міжнародної конфронтації – ще й зброя масового ураження, як вже ми наголошували раніше.

СПИСОК ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1 Безпека у глобальному світі / В. Ю. Констатинов, І. С. Мінгазутдінов, М. Г. Капітоненко, С. П. Галака, Р. А. Кривонос // Міжнародні системи та глобальний розвиток : підручник / кер. авт. колективу О. А. Коппель ; за ред. Л. В. Губерського, В. А. Манжоли. – Київ : «Київський університет», 2008. – С. 389-468.

2. Бабич Є. Ю. Забезпечення кібербезпеки в Україні / Є. Ю. Бабич // Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23–25 листоп. 2016 р. – Кропивницький : КНТУ, 2016. – С. 77–78.

3 Баранов О.А. Інформаційне право України: стан, проблеми, перспективи / О.А. Баранов. – К. : Видавничий дім "СофтПрес", 2005. – 316 с.

4. Безуглий Д., "Інформаційна безпека України: огляд останніх тенденцій", Фізико-математична освіта, вип. 2(16), с. 13–17, 2018.

5 Болгов В. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій: наук.-практ. посіб. Київ: Національна академія прокуратури України, 2015. 202 с.

6 Бурячок В. Л. Характерні ознаки та проблемні аспекти забезпечення кібернетичної безпеки / В. Л. Бурячок, С. О. Гнатюк, О. Г. Корченко // Інформаційна безпека: виклики і загрози сучасності : зб. Матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

7 Вдовенко С.Г., Даник Ю.Г. Концептуальні напрямки комплексного вирішення проблеми захисту від несанкціонованого доступу в складних системах спеціального призначення. URL: http://epsi.vntu.edu.ua/uploads/2017/61-fls0m4m1jhvk8ix2vjd81nyxuzb1i3q9.pdf

8 Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / [М.В. Гребенюк, Г.В. Попов, В.Д. Гавловський,

М.В. Гуцалюк, В. Г. Хахановський та ін.] ; за заг. ред. М.В. Гребенюка. – К. : НДЦ при РНБО України, 2017. – 76 с.

9. Від кібератаки 14 січня постраждали 22 державних органи. cip.gov.ua. 24 січня 2022. URL: https://web.archive.org/web/20220201013127/https://cip.gov.ua/ua/news/vid-kiberataki-14-sichnya-postrazhdali-22-derzhavnikh-organi

10. Вірус Petya: компанії M.E.Doc загрожує кримінальна справа. Факти.ICTV. 4 липня 2017. 4 липня 2017. URL: https://web.archive.org/web/20170704115628/http://fakty.ictv.ua/ua/ukraine/20170704-virus-petya-kompaniyi-m-e-doc-zagrozhuye-kryminalna-sprava/

11. Войціховський А. В. Міжнародне співробітництво у боротьбі з кіберзлочинністю. Портал: Національна бібліотека імені В. І. Вернадського. URL: http ://www.archive.nbuv.gov.ua/portal/.../PB-4_26.pdf.

12. Впровадження європейської кібербезпеки: загальний огляд. ISACA. URL: https://www.isaca.org/Knowledge-Center/Research/Documents/European-CybersecurityImplementation-Overview/ res_Ukr_1215.pdf.

13. Гассельбах К., Завгородня І. Європейський центр боротьби з кіберзлочинністю починає роботу // DW. Made for minds. URL: http://p.dw.com/p/17HRW

14. Геращенко С.В. Державна політика у сфері кібербезпеки в Україні. Вчені записки ТНУ імені В.І. Вернадського. Серія: «Державне управління». 2019. Т. 30 (69). С. 140-145.

15. Головкін Б.М. Як стають жертвами злочинів. Проблеми законності : зб. наук. праць. Харків : Нац. юрид. ун-т імені Ярослава Мудрого, 2017. Вип. 136. С. 161–172.

16. Діордіца І. В. Поняття та зміст національної системи кібербезпеки / І. В. Діордіца. – URL: http://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/

17. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 2014. 328 с. URL: http://www.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf

18. Едвард Сноуден отримав притулок у Росії. 3 серпня 2013. URL: https://web.archive.org/web/20130803213614/http://dt.ua/WORLD/edvard-snouden-otrimav-pritulok-u-rosiyi-126056_.html

19. Єдиний звіт про кримінальні правопорушення по державі за жовтень 2021 року / Статистична інформація Генеральної прокуратури України URL: https://old.gp.gov.ua/ua/stst2011.html?dir_id=114140&libid=100820&c=edit&_c=fo#

20. Забара І.М. Формування сучасних правових засад кібернетичної безпеки Європейського Союзу в умовах поширення нових інноваційних технологій. Журнал європейського і порівняльного права. 2017. Вип. 3. С. 2-13.

21. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших. Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит народного депутата України. Київ: Інфоцентр, Європейський інформаційно-дослідницький центр, Лабораторія законодавчих ініціатив, 2016. 37 с.

22. Запорожець О.Ю. Політика Європейського Союзу в сфері інформаційної безпеки. Актуальні проблеми міжнародних відносин. 2009. Вип. 87, ч. II. С. 36-45.

23. Зламана схема координації російських пропагандистів: завдання, оплата, звіти. Інформнапалм. 8 липня 2016. URL: https://web.archive.org/web/20160921084211/https://informnapalm.org/ua/shema-koordynatsiyi-rosijskyh-propagandystiv/

24. Кім Зеттер, Wired (17 березня 2016). Хакерська атака Росії на українську енергосистему: як це було. ТЕКСТИ. Архів оригіналу за 25 лютого 2022. URL: https://web.archive.org/web/20220225152407/https://texty.org.ua/articles/66125/Hakerska_ataka_Rosiji_na_ukrajinsku_jenergosystemu_jak-66125/

25. Конвенція про кіберзлочинність: Конвенція Ради Європи від 23.11.2001 / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/994_575

26. Константинов В. Шанхайська організація співробітництва // Політична енциклопедія. Редкол.: Ю. Левенець (голова), Ю. Шаповал (заст. голови) та ін. — К. : Парламентське видавництво, 2011. — с. 778.

27. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве URL: http://ens.mil.ru/science/publications/ more.htm?id=10845074@cmsArticle

28. Концепция стратегии кибербезопасности Российской Федерации. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

29. Лидин А. Кибершит Америки URL: http://vpk-news.ru/ articles/6388

30. Ліпкан В. А. Національна і міжнародна безпека у визначеннях та поняттях / В. А. Ліпкан, О. С. Ліпкан. – 2-ге вид., доп. і перероб. – К.: Текст, 2008. – 400 с.

31. Лук'янчук Р.В. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції. Вісник НАДУ: зб. наук. праць. 2015. Вип. 3. С. 110–116.

32. Максименко Е., Жилин А., Государственная и кадровая политика соединенных штатов америки и российской федерации в области кибербезопасности, Институт специальной связи и защиты информации НТУУ «КПІ», Україна, 2014 р.

33. Марущак А.І. Інформаційно-правові аспекти протидії кіберзлочинності. Інформація і право. 2018. №1 (24). С. 127-132.

34. Марущак А.І. Пріоритети розвитку інформаційного права України // Інформація і право. – № 1(1)/2011. – С. 20-24.

35. Международная стратегия кибер-безопасности URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

36. Мельник С. В. Актуальні напрями попередження правопорушень у кіберпросторі як складова стратегії кібернетичної безпеки держави Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ / С. В. Мельник, В. І. Кащук. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

37. Мельник С.В., Тихомиров О.О., Лєсков О.С. До проблеми формування понятійно-термінологічного апарату кібербезпеки / зб. матер. наук.-практ. конф. [Актуальні проблеми управління інформаційною безпекою держави], (Київ, 22 березня 2011 р.). – К. : Вид-во НА СБ України, 2011. – Ч. 2. – С. 43-48.

38. Национальная стратегия кибербезопасности (NCSS). От понимания к возможности. – Holland, Den Haag. National Coordinator for Security and Counterterrorism, 2013. – URL: //www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie

39. Німеччина скасувала угоди про прослуховування з США і Великою Британією 5 серпня 2013. URL: https://web.archive.org/web/20130805190228/http://www.pravda.com.ua/news/2013/08/2/6995409/

40. Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза. Криминология: вчера, сегодня, завтра. 2012. №24. С. 45-55.

41. Офіційний сайт кіберполіції України: про підрозділ. URL: https://cyberpolice.gov.ua/contacts/.

42. Офіційний сайт Ліги арабських держав. Статут організації. URL: http://www.lasportal.org/ar/Pages/default.aspx

43. Офіційний сайт НАТО. Статут організації. URL: https://www.nato.int/nato-welcome/index_uk.html

44. Офіційний сайт ОБСЄ. Статут організації. URL: https://www.osce.org/whatistheosce/factsheet

45. Офіційний сайт ОДКБ. Статут організації. URL: https://odkb-csto.org/

46. Павлюк О. (26 лютого 2022). Україна створює ІТ-армію — Федоров. Суспільне | Новини (укр.). 28 лютого 2022. URL: https://web.archive.org/web/20220228140721/https://suspilne.media/211480-ukraina-stvorue-it-armiu-fedorov/

47. Павлюк О. (26 лютого 2022). Хакери атакували російські сайти і, ймовірно, зламали російські телеканали. Суспільне | Новини (укр.). URL: https://web.archive.org/web/20220226180853/https://suspilne.media/211432-hakeri-atakuvali-sajti-kremla-roskomnadzora-i-jmovirno-zlamali-rosijski-telekanali/

48. Петров В. В. Щодо формування національної системи кібербезпеки України / В. В. Петров // Стратегічні пріоритети. – Київ: НІСД, 2013. – No 4(29). – С.127-130.

49. Поняття та зміст системи забезпечення кібербезпеки URL: http://goal-int.org

50. Порошенко підписав наказ про заборону "Яндекс", "Вконтакте" и "Одноклассники". День. 16 травня, 2017. Архів оригіналу за 19 травня 2017. URL: https://web.archive.org/web/20170519123405/http://day.kyiv.ua/uk/news/160517-poroshenko-pidpysav-nakaz-pro-vvedennya-sanktsiy-protyv-yandeks-vkontakte-y-odnoklassnyky

51. Прес-служба Держспецзв'язку (23 травня 2014). Коментар Держспецзв'язку щодо інциденту в ЦВК. URL: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=114116&cat_id=112509

52. Про основні засади забезпечення кібербезпеки України : Закон України від 17.08.2022 No 2470-IX/ Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

53. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.07. № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.

54. Про рішення Ради національної безпеки і оборони України від 29.12.16 р. "Про загрози кібербезпеки держави та невідкладні заходи щодо їх нейтралізації" : Указ Президента України від 13.02.17 р. № 32. – URL: http://zakon3.rada.gov.ua

55. Распоряжение Правительства РФ от 3 ноября 2011 г. N 1944-р URL: http://www.garant.ru/products/ipo/prime/doc/55072466/

56. Сайт Київської ОДА атакують хакери. www.ukrinform.ua (укр.). 25 лютого 2022. URL: https://web.archive.org/web/20220225222318/https://www.ukrinform.ua/rubric-technology/3411812-sajt-kiivskoi-oda-atakuut-hakeri.html

57. СБУ заявляє, що викрила російську «ботоферму війни». Радіо Свобода (укр.). 26 лютого 2022. URL: https://web.archive.org/web/20220226175329/https://www.radiosvoboda.org/a/news-sbu-boty-rf/31725112.html

58. Североатлантический договор URL: http://www.nato.int/cps/ru/natolive/official_texts_17120.htm

59. Словник термінів з кібербезпеки / за заг. ред. О. Копатіна, Є. Скулишина. Київ : АванпостПрим, 2012. 214 с.

60. Сноуден розповів, як йому вдалося завантажувати дані і залишатися непоміченим. 22 лютого 2014. URL: https://web.archive.org/web/20140222171551/http://dt.ua/WORLD/snouden-rozpoviv-yak-yomu-vdalosya-zavantazhuvati-dani-i-zalishatisya-nepomichenim-137112_.html

61. Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері. Київ, 28 с., 2019. URL: https://geostrategy.org.ua/ua/analitika/item/1565-cooperation-ukraine-nato.

62. Статут ООН. URL: http://zakon3.rada.gov.ua/laws/show/995_010.

63. Стратегія кібербезпеки України від 15.03.2016 URL: http://zakon3.rada.gov.ua/laws/show/96/2016

64. Таволжанський О.В. Кримінологічні аспекти кіберзлочинності у сучасних умовах. Журнал східно-європейського права. 2016. No 31. С. 80–86. URL: http://dspace.nlu.edu.ua/bitstream/123456789/17724/1/Tavolzhanskyi_80-86.pdf

65. Таволжанський О.В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності. Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія Право. 2018. Вип. 6(18). С. 154–163.

66. Тімкін І. Ф. Структурно-функціональна характеристика системи забезпечення національної безпеки України/ І. Ф. Тімкін, Н. Є. Новікова. – URL: er.nau.edu.ua

67. Трофименко О., "Моніторинг стану кібербезпеки в Україні", Правове життя сучасної України: матер. міжнар. наук.-практ. конф., 17 травня 2019 р., Т. 1, Одеса: Видавничий дім «Гельветика», с. 642–646, 2019.

68. Трофименко О.Г. Законодавча база забезпечення кібербезпеки держави. Кібербезпека в Україні: правові та організаційні питання: матер. II всеукр. наук.-практ. конф., 17 листопада 2017 р., Одеса: ОДУВС, С. 55–56.

69. Угода між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво: міжнародний договір від 14.12.2016 // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/984_001-16/paran2#n2

70. Указ Президента Российской Федерации от 15.01.2013 № 31с (выписка) «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» URL: http://publication.pravo.gov.ru/Document/View/0001201301210012

71. Указ Президента України №242/2016. Про Національний координаційний центр кібербезпеки. URL: https://web.archive.org/web/20160828184044/http://www.president.gov.ua/documents/2422016-20141

72. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності // Інформація і право. – 2012. – № 2. – С. 162-169.

73. Центр експертизи з питань кооперативної кібер-оборони (CCDCOE) / North Atlantic Treaty Organization. URL: https://www.nato.int/docu/other/ukr/pdf/CCD%20COE%20presentation%20ukr.pdf

74. Чернега О. Б., Іваненко І. А. НАТО та система міжнародної безпеки [Текст] : навч. посіб. для студ. вищ. навч. закл. / О. Б. Чернега, І. А. Іваненко ; Донецький національний ун-т економіки і торгівлі ім. Михайла Туган-Барановського. – Донецьк : [б.в.], 2009. – 228 с.

75. Шеломенцев В. П. Формування законодавчих основ забезпечення кібербезпеки України / В. П. Шеломенцев // Інформаційна безпека: виклики і загрози сучасності : зб. матеріалів наук.-практ. конф., 5 квітня 2013 року, м. Київ. – К. : Наук.-вид. центр НА СБ України, 2013. – 416 с.

76. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – № 1. – С. 312-320.

77. Шемчук В. Національна стратегія кібербезпеки США: досвід для України. Науковий вісник Національної академії внутрішніх справ. 2020. № 4. С. 119-124.

78. Шепелєв М.А. Теорія міжнародних відносин: підручник / М.А. Шепелєв; передм. Д.В. Табачника. – К.: Вища школа, 2004. – 622 с.

79. Як борються українські кібервійська, УП, 1 березня 2022 URL: https://www.pravda.com.ua/columns/2022/03/1/7327173/

80. A new strategic agenda for the EU URL: https://www.tiaformazione.org/new-strategic-agenda-forthe-eu/

81. Aaronson, Susan Ariel, 2016, 'The Great Moderation? China and the US in Cyberspace', URL: http://www.chinausfocus.com/peace-security/the-great-moderation-china-and-the-us-incyberspace

82. About ENISA - European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/about-enisa

83. About the networking and information technology research and development (NITRD) program. URL: https://www.nitrd.gov/about/

84. Amoroso, E. 2006. Cyber Security. New Jersey: Silicon Press.

85. An official website of the European Union. URL: https://european-union.europa.eu/principles-countries-history/principles-and-values_uk

86. ANNUAL REPORT TO CONGRESS. Military and Security Developments. Involving the People's Republic of China, 2010. URL: https://dod.defense.gov/Portals/1/Documents/pubs/2010_CMPR_Final.pdf

87. Australia among countries most targeted by 'significant' cyber attacks, as cyber crime costs global economy US$6 trillion. URL: https://itwire.com/business-it-news/security/australia-among-countries-most-targeted-by-%e2%80%98significant%e2%80%99-cyber-attacks,-with-cybercrime-to-cost-global-economy-us$6-trillion.html

88. Baldwin, D. A. 1997. The Concept of Security. Review of International Studies, 23(1): 5-26.

89. Barbara Star, (10 червня 2013 р.). Man behind NSA leaks says he did it to safeguard privacy, liberty. CNN. 15 червня 2013. URL: https://web.archive.org/web/20130615001329/http://www.cnn.com/2013/06/10/politics/edward-snowden-profile/index.html?hpt=hp_c2

90. Burgman, Paul Jr., 2016 "Securing Cyberspace: China Leading the Way in Cyber Sovereignty", 18.05.2016. URL: http://thediplomat.com/2016/05/securing-cyberspace-china-leading-the-way-incyber-sovereignty/.

91. Buzan, B., Wæver, O., & De Wilde, J. 1998. Security: A New Framework for Analysis. Boulder, CO: Lynne Rienner Publishers.

92. Canongia, C., & Mandarino, R. 2014. Cybersecurity: The New Challenge of the Information Society. In Crisis Management: Concepts, Methodologies, Tools and Applications: 60-80. Hershey, PA: IGI Global. URL: http://dx.doi.org/10.4018/978-1-4666-4707-7.ch003

93. Cavelty, M. D. 2010. Cyber-Security. In: P. Burgess (Ed.), The Routledge Handbook of New Security Studies: 154-162. London: Routledge.

94. Center of Academic Excellence – Cyber Operations Program URL: http://www.nsa.gov/academia/_files/CAE_Cyber_Ops_Application33_distributed.pdf

95. CNSS. 2010. National Information Assurance Glossary. Committee on National Security Systems (CNSS) Instruction No. 4009: URL: http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf

96. Communication from the Commission on Critical Information Infrastructure Protection «Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience»: adopted by the European Commission on 30 March 2009 / European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0149

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

98. Cornish, P. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks/ P. Cornish; Directorate-General for External Policies of the Union, Policy Department. – Brussels : European Parliament, 2009. – 34 p.

99. Council framework decision 2005/222/JHA on attacks against information systems: adopted by the Council of the European Union on 24 February 2005 / European Union. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:32005F0222

100. Craigen D., Diakun-Thibault N., Purse R., Defining Cybersecurity, Technology Innovation Management Review, 2014, p. 13 - 21. URL: https://www.timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf

101. Cyber Europe / European Union Agency for Network and Information Security. URL: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme

102. Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace. URL: https://edps.europa.eu/data-protection/our-work/publications/opinions/cyber-security-strategy-european-union-open-safe-and_en

103. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace: adopted by the European Commission on 7 February 2013 / European Union. URL: https://ec.europa.eu/digital-singlemarket/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cybersecurity

104. DHS. 2014. A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. October 1, 2014. URL: http://niccs.us-cert.gov/glossary#letter_c

105. Digital India, 2015. - [online]. Available at: https://www.digitalindia.gov.in

106. 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. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L1148

107. Elman, C. (2008). Realism. Security Studies:and Introduction. P. D. William. New York, Routledge.

108. Email-адреси українських військових атакують хакери. www.ukrinform.ua (укр.) 25 лютого 2022. URL: https://web.archive.org/web/20220225222318/https://www.ukrinform.ua/rubric-technology/3412829-emailadresi-ukrainskih-vijskovih-atakuut-hakeri.html

109. EU cybersecurity initiatives working towards a more secure online environment / European Union. URL: http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf (дата звернення 04.06.2018).

110. EU strategic agenda for 2019–2024 URL: https://eu2019.fi/en/priorities-and-programme/strategicagenda

111. Financial Times, 2016. 'Xi's China: Smothering Dissent', 27.07.2016. URL: https://www.ft.com/content/ccd94b46-4db5-11e6-88c5-db83e98a590a

112. For a stronger European security and defence URL: https://euagenda.eu/publications/for-a-strongereuropean-security-and-defence

113. Franscella J. Cybersecurity vs. Cyber Security: When, Why and How to Use the Term /J. Franscella. – URL: //www.infosecisland.com/blogview/23287-Cybersecurity-vs-CyberSecurity-When-Why-and-How-to-Use-the-Term.html

114. Frequently Asked Questions and Answers About the Council of Europe Convention on Cybercrime (Draft 24REV2) (December 1, 2000). URL: web.archive.org.

115. GCHQ is a greater problem than American spies, claims intelligence whistleblower // The Daily Telegraph, 22-6-2013 URL: http://www.telegraph.co.uk/news/uknews/defence/10135919/GCHQ-is-a-greater-problem-than-American-spies-claims-intelligence-whistleblower.html

116. Goel, V., Raj, S. and RavichandranJuly, P., 2018. How WhatsApp Leads Mobs to Murder in India. - [online]. URL: https://www.nytimes.com/interactive/2018/07/18/technology/whatsapp-indiakillings.html

117. Gordon, Lawrence A; Loeb, Martin; Zhou, Lei (January 1, 2020). "Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model". Journal of Cybersecurity.

118. Home Ministry pitches for Budapest Convention on cyber security. The Indian Express (англ.). 18 січня 2018. URL: https://indianexpress.com/article/india/home-ministry-pitches-for-budapest-convention-on-cyber-security-rajnath-singh-5029314/

119. India is quietly preparing a cyber warfare unit to fight a new kind of enemy - [online]. URL: https://economictimes.indiatimes.com/news/defence/india-is-quietly-preparing-acyber-warfare-unit-to-fight-a-new-kind-ofenemy/articleshow/61141277.cms?from=mdr

120. India saw world's largest data breach in 2018 due to lax cyber security: WEF report - [online]. URL: https://www.thenewsminute.com/article/indiasaw-world-s-largest-online-data-breach-2018-due-lax-cyber-security-wef-95141

121. India set to have 530 million smartphone users in 2018: Study [online]. URL: https://indianexpress.com/article/technology/india-set-to-have-530-million-smartphone-users-in-2018-study-4893159/

122. Inkster, Nigel, 2016. China's Cyber Power. London: Routledge/IISS.

Lindsay, Jon R. 2015. 'The Impact of China on Cybersecurity, Fiction and Friction', URL: http://belfercenter.ksg.harvard.edu/files/183903_pp007-047.pdf Accessed, 13.01.2017

123. Internet Organised Crime Threat Assessment (IOCTA) / Europol. URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threatassessment

124. ITU. 2009. Overview of Cybersecurity. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). URL: http://www.itu.int/rec/T-REC-X.1205-200804-I/en

125. Jamal Abdul Nasir & Aaisha Khatoon & Shubhangi Bharadwaj. Social Media users in India: A Futuristic Approach. - [online]. URL: http://ijrar.com/upload_issue/ijrar_issue_20542638.pdf

126. Kemmerer, R. A. 2003. Cybersecurity. Proceedings of the 25th IEEE International Conference on Software Engineering: 705-715. URL: http://dx.doi.org/10.1109/ICSE.2003.1201257

127. Kimberly Enger. A Digital Revolution in India. URL: https://www.icann.org/en/ blogs/details/a-digital-revolution-in-india-7-11-2016-en

128. Kramer F., Starr S., and Wentz L., Cyberpower and National Security Washington, USA:Potomac Books,2009.[3]J.B.Sheldon,"Deciphering cyberpower strategic purpose in peace and war",Strategic Studies Quarterly, vol. 5, no. 2, pp. 95-112, 2011.

129. Lewis, J. A. 2006. Cybersecurity and Critical Infrastructure Protection. Washington, DC: Center for Strategic and International Studies. URL: http://csis.org/publication/cybersecurity-and-criticalinfrastructure-protection

130. Lindsay Jon R., Tai Ming Cheung and Derek S. Reveron, 2015. China and Cybersecurity. Oxford: Oxford University Press.

131. Lu Wei, 2014. 'Cyber Sovereignty Must Rule Global Internet', Huffington Post, 15.12.2014. URL: http://www.huffingtonpost.com/lu-wei/china-cyber-sovereignty_b_6324060.html Accessed 10.01.2017

132. Malcolmson, Scott, 2016.'How Russia and China are Cooperating to Dismantle America's Dominance of the Internet', Huffington Post, 05.05.2016. URL: http://www.huffingtonpost.com/scott-malcomson/russia-china-internet_b_9841670.html

133. McEvatt Paul (30 червня 2017). Petya, Medoc and the delivery of malicious software. Fujitsu Information Security. 3 липня 2017. URL: https://web.archive.org/web/20170703182432/http://blog.uk.fujitsu.com/information-security/petya-medoc-and-the-delivery-of-malicious-software/#.WVu4cSdgHq4

134. Ministry of Electronics & Information Technology, Government of India, 2013. National Cyber Security Policy-2013. - [online] URL: https://meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf

135. Ministry of Law And Justice, 2008. The Information Technology Act (Amendment). - [online] URL: https://meity.gov.in/writereaddata/files/it_amendment_act2008%20%281%29_0.pdf

136. Ministry of Law, Justice and Company Affairs (Legislative Department), 2000. The Information Technology Act. - [online]. URL: https://meity.gov.in/writereaddata/files/itbill2000.pdf

137. National Cyber Security Strategies. Practical Guide on Development and Execution. – ENISA, 2012. – URL: //www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

138. National Cyber Strategy of the United States of America (2018) (n.d.). URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

139. Network and information security: proposal for a european policy approach: adopted by the European Commission on 6 June 2001 / European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298

140. NIST Cybersecurity Framework. URL: https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

141. Origins of the 2019-24 EU Strategic Agenda: The Future of Europe debate and the Sibiu European Council URL: https://epthinktank.eu/2019/10/11/origins-of-the-2019-24-eu-strategic-agenda-the-future-of-europe-debate-and-the-sibiueuropean-council/

142. Ostrom, E., & Hess, C. 2007. Private and Common Property Rights. In B. Bouckaert (Ed.), Encyclopedia of Law & Economics. Northampton, MA: Edward Elgar.

143. Oxford University Press. 2014. Oxford Online Dictionary. Oxford: Oxford University Press. October 1, 2014: URL: http://www.oxforddictionaries.com/definition/english/Cybersecurity

144. Perritt, Henry H. 1998. 'The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance', Global Legal Studies Journal, 5(2): 423–42

145. Public Safety Canada. 2014. Terminology Bulletin 281: Emergency Management Vocabulary. Ottawa: Translation Bureau, Government of Canada. URL: http://www.bt-tb.tpsgc-pwgsc.gc.ca/publications/documents/urgence-emergency.pdf

146. PurpleSec. Recent Cyber Attacks & Data Breaches In 2023. URL: https://purplesec.us/security-insights/data-breaches/

147. Ranjani Ayyar. Number of Indian internet users will reach 500 million by June 2018, IAMAI says. [online]. URL: https://timesofindia.indiatimes.com/business/india-business/number-indianinternet-users-will-reach-500-million-by-june-2018-iamai-says/articleshow/62998642.cms

148. Raud, Mikk. 2016. 'China and Cyber: Attitudes, Strategies, Organisation', URL: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf

149. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance) // Official Journal L 077, 13/03/2004 P. 0001-0011. – URL: //www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

150. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. adopted by the European Commission on 13 September 2017 / European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:0450:FIN

151. Resolution adopted by the General Assembly on 27 December 2019. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/N1944028.pdf?OpenElement

152. Resolution adopted by the General Assembly on 31 December 2021. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/25/PDF/N2100025.pdf?OpenElement

153. Rijksdienst voor Ondernemend Nederland, 2018. Cyber Security in India. Opportunities for Dutch companies - [online]. URL: https://www.thehaguesecuritydelta.com/media/com_hsd/report/218/document/Cyber-Security-in-India.pdf

154. Samaya Dharmaraj The current state of cyber security in India. - [online]. URL: https://opengovasia.com/the-current-state-of-cyber-security-in-india/

155. Shiraev, Eric B. (2014). International Relations. New York: Oxford University Presses. p. 78.

156. Shiraev, Eric B., Vladislav M. Zubok. 2014. International Relations. New York, NY: Oxford University Press.

157. State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyberattacks: European Commission - Press release, 19 September 2017 / European Union. URL: http://europa.eu/rapid/press-release_IP-17-3193_en.htm

158. Strategy for New India - [online]. URL: https://niti.gov.in/writereaddata/files/Strategy_for_New_India.pdf

159. Stubley D. What is Cyber Security? - URL: //www.7elements.co.uk/resources/blog/what-is-cyber-security

160. Tech sell-off pushes Hong Kong stocks into bear market. URL: https://www.ft.com/content/c5372f5a-d086-4ca2-995a-7b559f4e1e32

161. The Comprehensive National Cybersecurity Initiative – URL: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

162. The national strategy to secure cyberspace. – Washington, 2003. – 60 с. – URL: //www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

163. Towards a general policy on the fight against cyber crime: adopted by the European Commission on 22 May 2007 / European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14560

164. United Nations, 2016. Developments in the field of information and telecommunications in the context of international security. Report of the Secretary-General - [online]. URL: https://undocs.org/A/71/172

165. United Nations, 2018. Current developments in science and technology and their potential impact on international security and disarmament efforts. Report of the Secretary-General - [online]. URL: https://undocs.org/A773/177

166. Why a new European Agenda on Security? URL: https://ec.europa.eu/home-affairs/what-wedo/policies/european-agenda-security_en

167. Wohlforth, W. C. (2010). Realism and Security Studies. The Routledge Handbook of Security Studies. M. D. Cavelty and V. Mauer. New York, Routledge.

168. Xi Jinping, 2015. Speech to World Internet Conference. URL: http://www.bbc.com/news/world-asia-china-35109453 and https://www.youtube.com/watch?v=GNR3MV9C2-Q Accessed 10.01.2017

169. Xinhua Net, 2014. 'Chinese President Calls for Greater Democracy in Int'l Relations', 28.06.2014, URL: http://news.xinhuanet.com/english/china/2014-06/28/c_133445551.htm accessed 08.03.2017

170. 2009 Cyberspace Policy Review URL: http://www.dhs.gov/publication/2009-cyberspace-policy-review

171. 2018 Top 50 Countries – Smartphone Users By Countries. [online]. URL: https://rlist.io/l/2018-top-50-countries-by-smartphone-users