НАЦІОНАЛЬНИЙ УНІВЕРСТИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Гуманітарно-педагогічний факультет

УДК 070.431.5

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан гуманітарно-педагогічного факультету	**В.о. завідувача кафедри журналістики та мовної комунікації**
_____ Інна САВИЦЬКА	_____ Марина НАВАЛЬНА
“ ” _____ 2023 р.	“ ” _____ 2023 р.

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ПРОБЛЕМИ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Спеціальність 061 Журналістика

Освітня програма Журналістика

Орієнтація освітньої програми освітньо-професійна

Гарант освітньої програми

доктор філол. наук, професор _____ Марина НАВАЛЬНА

Керівник магістерської кваліфікаційної роботи

доктор філол. наук, професор _____ Тетяна СЕМАШКО

Виконав_____Снігур Олег

КИЇВ – 2023

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Розвиток інформаційних технологій став невід'ємною частиною життя сучасного суспільства, а оскільки інформація є одним із найцінніших та найважливіших ресурсів будь-якого процесу, інформаційна безпека стала найважливішим аспектом безпеки. Інформаційна безпека включає комплекс заходів, спрямованих на запобігання та усунення несанкціонованого доступу, обробки, спотворення, форматування, аналізу, неузгодженого оновлення, виправлення та знищення даних. Простіше кажучи, це набір заходів, стандартів та технологій, необхідних для захисту конфіденційних даних.

Проблема захисту інформації від несанкціонованого доступу та небажаних впливів існує давно, з розвитком людського суспільства, появою приватної власності, державного устрою, а з подальшим розширенням людської діяльності інформація набуває все більшого значення. Інформація стає цінною, і її володіння дозволить нинішнім та потенційним власникам отримувати певні виграші.

Перехід на інформатизовані системи торкнувся органів державної влади. Важливу роль у діяльності щодо захисту інформації та інформаційних систем займають заходи щодо створення комплексного захисту. Потрібно проаналізувати особливості та стан міжнародної інформаційної безпеки. Таким чином, тема є актуальною в сучасних умовах.

Мета роботи полягає у висвітленні проблем міжнародної інформаційної безпеки.

Завдання:

1. Висвітлити теоретичні засади формування та забезпечення міжнародної інформаційної безпеки;
2. Охарактеризувати специфіку організації інформаційної безпеки органів державного управління;

3. Дослідити політику міжнародних організацій з питань інформаційної безпеки;
4. Проаналізувати глобальні військово-політичні проблеми міжнародної інформаційної безпеки;
5. Виявити роль і місце інформаційної безпеки у контексті викликів і загроз національній безпеці.

Об'єкт дослідження – це відносини, що виникають між суб'єктами міжнародного права щодо забезпечення інформаційної безпеки.

Предмет дослідження – це проблеми міжнародної інформаційної безпеки.

Стан наукової розробки з теми дослідження. Проблемами дослідження міжнародної інформаційної безпеки займалися такі науковці, як О. Архипов, В. Богуш, М. Вавринчук, В. Василюк, А. Войціховський, С. Глобенко, О. Гончаренко, І. Громико, В. Дереко, К. Захаренко, В. Копанчук, Б. Кормич, В. Лужецький, Є. Макаренко, А. Марущак, А. Нашинець-Наумова, В. Остроухов, В. Пилипчук, О. Резнікова, О. Степко, Є. Тихомирова, В. Торічний, О. Юдін та ін. У своїх працях науковці розглядають проблеми безпеки шляхом комплексного підходу до міжнародного та вітчизняного досвіду її забезпечення, надають рекомендації зі зміцнення інформаційної безпеки країни.

Методи дослідження склали загальнонаукові (діалектичний, формально-логічний, структурно-функціональний, аналізу, синтезу, дедукції, індукції) та спеціальні (історико-правовий, порівняльно-правовий) методи пізнання. Також використовувався метод моделювання та наукового прогнозування.

Наукове значення теми дослідження обумовлене її важливістю дослідження та вивчення, оскільки проблема формування інформаційної безпеки в нашій країні, розробка новітніх методів реалізації цієї проблеми є сьогодні найважливішим завданням для фахівців у галузі світової політики, політології та соціології, а також у сфері бізнесу та підприємництва.

Теоретичне значення дослідження полягає у збільшенні фактологічного матеріалу, що становить основу сучасних теорій міжнародних відносин, що сприяє їхньому подальшому розвитку. Дослідження також має значення для вироблення підходів до вирішення питань протидії використанню ІКТ у військово-політичних цілях, створення системи міжнародної інформаційної безпеки, теоретичного осмислення використання ІКТ у військово-політичних цілях у сучасних міжнародних відносинах та оцінки впливу цього фактору на міжнародну та національну безпеку.

Практичне значення дослідження полягає у можливості його використання у діяльності уповноважених органів влади при формуванні зовнішньополітичного курсу, національної політики в галузі інформаційної безпеки та міжнародної інформаційної безпеки, а також під час підготовки відповідних документів. Матеріали та висновки роботи можуть бути використані при підготовці навчальних посібників з міжнародної інформаційної безпеки, теорії міжнародних відносин на користь різних цивільних та військових навчальних закладів та розробці відповідних навчальних курсів.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел, додатків.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ ТА ЗАБЕЗПЕЧЕННЯ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Поняття інформаційної безпеки

Розвиток сучасних міжнародних відносин відбувається в умовах інформаційно-технологічної революції, що впливає на всі сторони життя людського суспільства. Ступінь цього впливу така, що фахівці відзначають зростаючу залежність людства загалом від інформаційних та комунікаційних технологій (ІКТ).

Глибоке проникнення ІКТ спостерігається не тільки у технологічній, економічній та соціальній сферах життя сучасних держав, побоювання викликає поширення ІКТ у військовій сфері, їх використання у ворожих цілях в умовах сучасних кризових та конфліктних ситуацій. Як зазначив у 2014 р. генеральний секретар ООН у доповіді «Про роботу Організації», «геополітична напруженість позначилася також на спорах щодо кіберпростору» [60, с. 356].

Подібну тенденцію розвитку та розширення сфер застосування ІКТ враховують у своїх стратегіях держави. Насамперед вони прагнуть не допустити використання ІКТ для заподіяння шкоди національній безпеці. Поряд із цим держави звертають увагу і на необхідність розробки концепції міжнародної інформаційної безпеки, яка має бути прийнята та реалізована міжнародною спільнотою держав. Для досягнення цієї мети окремі держави приймають власні стратегії, спрямовані на створення сприятливих умов для розробки наукових основ такого документа.

Перш ніж розпочати міжнародно-правовий аналіз даних термінів і понять, слід уточнити, що вони широко застосовуються у двох суміжних галузях сучасного міжнародного права: права міжнародної безпеки та міжнародного гуманітарного права, що застосовується в умовах збройних конфліктів [2, с. 185].

Слід зазначити, що й значення зазначених галузей у системі міжнародного права неоднакове зважаючи на відмінності цілей, а в ширшому плані та функцій цих галузей, і навіть їх неоднакового сприйняття у міжнародній правосвідомості. Справді, підтримка міжнародного миру та безпеки – одна з головних цілей ООН та основний зміст міжнародного права.

Усі інші галузі міжнародного права роблять внесок у вирішення важливого завдання – зберегти та уберегти світ та міжнародне співтовариство від військових загроз, не допустити розв'язання воєн та збройних конфліктів [6, с. 282].

Міжнародне гуманітарне право, навпаки, у цьому контексті виглядає певним парадоксом, оскільки прагне врегулювати відносини між воюючими в ході воєн та збройних конфліктів, зробити все можливе для мінімізації негативних наслідків для людської особистості в ході застосування збройної сили. Звідси пріоритетне значення, яке надається праву міжнародної безпеки у правосвідомості людства, а в ширшому плані і в світовій громадській думці.

Зважаючи на те, що в документах та науковій літературі відзначається можливість використання ІКТ як зброї, очевидно, що це відбуватиметься в умовах воєн чи збройних конфліктів. В даний час в науковий і публіцистичний оборот введений термін «інформаційна війна», що спонукає нас розширити діапазон аналізу і ввести терміни, що цікавлять нас, у ширший дослідницький контекст [39].

Сучасне право міжнародної безпеки спирається на положення Статуту ООН та прийняті у період після Другої світової війни міжнародні договори як універсального, так і регіонального, а також двостороннього характеру. Статут ООН як вихідна категорія для побудови сучасних міжнародно-правових рамок універсальної безпеки використовує поняття «сила», застосування якої згідно з п. 4 ст. 2 названого документа у міжнародних відносинах заборонено.

Система безпеки, сформована ООН, включає низку найважливіших компонентів, одним з яких є можливість застосування «ефективних колективних заходів», які мають як превентивний (запобігання та усунення

загрози миру), так і примусовий характер (придушення актів агресії та інших порушень світу). Як бачимо, у Статуті ООН не використовується поняття «війна» як об'єкт міжнародно-правового регулювання та відповідної категорії, на відміну від міжнародно-правових актів початку XX ст. [49].

Аналізу концепції «ворожа дія» або «агресивний акт» з використанням ІКТ, як нам видається, має передувати з'ясування ключового терміна, що має ширше значення, – «інформаційна атака (напад)», або «кібератака». Цей термін є новим для сучасного міжнародного права і ще не отримав загальновизнаного визначення у діючих міжнародно-правових документах.

Однак у міжнародно-правовій літературі та офіційних документах робляться спроби визначення комп'ютерних мережевих атак. Зокрема, у словнику військових термінів, випущеному Міністерством оборони США, дається таке визначення: «Комп'ютерні мережеві атаки – це дії, які вживаються з використанням комп'ютерних мереж для того, щоб зіпсувати або знищити інформацію, що знаходиться в комп'ютерах та комп'ютерних мережах або комп'ютери та самі мережі» [38].

Об'єктом інформаційної атаки (кібератаки) є інформація, тому термін є ключовим у визначенні. Інформація з погляду інформатики – це будь-які дані, які знижують невизначеність у стані системи; вона включає набагато більше, ніж традиційне визначення фактів і знань, необхідних для людини, щоб змінити або сформувати думку. У військовій науці зустрічаються близькі визначення терміна «інформація» – це факти, дані або інструкції в будь-якому середовищі або у будь-якій формі [38].

Термін «комп'ютерна мережна атака», або «кібератака», таким чином, охоплює широкий спектр ворожих способів впливу на комп'ютерні мережі, що включають комп'ютерний код. Таке шкідливе програмне забезпечення (шкідливі програми) може призвести до серйозних порушень, як і у випадку з атаками, що спровокували відмову в обслуговуванні, зафіксовану в Естонії в 2007 р., або фізичне знищення об'єкта, як це було в Ірані.

На сьогоднішній день інформаційна безпека вважається одним із найважливіших компонентів національної безпеки. Значимість останньої поступово зростає у всіх сферах життя, зокрема й у політичній. У цьому відношенні постає очевидним, що у інформаційному суспільстві інформація представлена, з одного боку, предметом масового споживання, а з другого – потужним економічним ресурсом. При цьому створення ідеальної системи інформаційної безпеки може залежати від того, хто і як нею управлятиме [34, с. 212].

Сьогодні все частіше висловлюються побоювання, що ключовим стримуючим фактором впровадження міжнародної інформаційної безпеки є нерівномірний розвиток інформаційної сфери. Звідси випливає, що розвиток інформаційного суспільства є одним із найважливіших завдань підвищення ефективності управління інформаційною безпекою. При цьому важливо наголосити на тому, що інформаційне суспільство пов'язане з високим рівнем розвитку телекомунікаційних та інформаційних технологій, а також їх інтенсивним використанням бізнесом, громадянами та органами державної влади.

Крім того, міжнародний досвід свідчить про те, що інформаційні та телекомунікаційні технології вже є локомотивом соціально-економічного розвитку більшості країн світу, а забезпечення гарантованого вільного доступу громадян до інформації є одним із найважливіших завдань держави.

У сучасних умовах інформаційна сфера життя міжнародного співтовариства представлена у вигляді системи самоорганізації різних соціальних інститутів, що динамічно розвивається, яку не можна підкорити виключно позитивному праву однієї держави [3, с. 34].

Соціальні комунікативні системи та інстигути ставлять собі за мету виробити моральні установки і сформувати уявлення людей про необхідні моделі поведінки в суспільстві; внаслідок соціальної комунікації виникають нові аспекти модернізації соціальної організації нашого суспільства та розвитку права [5, с. 65].

Проблема інформаційної безпеки тісно пов'язана з поняттями «міжнародна безпека» та «економічна глобалізація». Так, ключовою потребою системи держави є необхідність забезпечення умов, які необхідні для її функціонування та розвитку.

Стрімке поширення зброї масового знищення ставлять світове співтовариство перед необхідністю збереження та забезпечення миру. Система міжнародного права при цьому нормативно закріпила потребу у світі як глобальний основний інтерес та поклала юридичний обов'язок щодо підтримки ідеї миру між різними державами.

У науковому та правовому середовищі міжнародна безпека представлена у вигляді такого стану міждержавних відносин, який здатний відповідати об'єктивному інтересу кожної держави, та, крім того, не суперечити глобальному інтересу, який нормативно закріплений у сучасному міжнародному праві [7, с. 196].

Водночас необхідність забезпечення виконання державами покладених на них юридичних обов'язків щодо підтримання миру, заснованих на неухильному дотриманні ними основоположних принципів та норм міжнародного права, має на меті захист та реалізацію суб'єктивних внутрішньодержавних прав на їх індивідуальну безпеку, включаючи право на існування, рівноправне функціонування та розвиток у міждержавних відносинах [10, с. 17].

Під міжнародною інформаційною безпекою, згідно з термінологією ООН, розуміється захищеність глобальної інформаційної системи від терористичних, злочинних та військово-політичних загроз. Міжнародними загрозами позначено небезпеку втручання у внутрішні справи суверенної держави за допомогою інформаційно-комунікаційних технологій (ІКТ). Такий тип загроз небезпечний можливістю порушення суспільної стабільності, а також розпалювання міжетнічної та міжнаціональної ворожнечі.

Крім цього, слід зазначити, що щодо термінології немає єдності думок у розумінні терміна «міжнародна інформаційна безпека». Найчастіше вона

сприймається як зіткнення національних інтересів держав, проте загалом питання термінології залишається дискусійним. Науковці дотримуються широкого розуміння терміну «міжнародна інформаційна безпека», що є сукупністю різних технічних аспектів, включаючи безпеку інформаційних мереж та систем, а також маніпулювання інформацією, її поширення шляхом глобальних інформаційних мереж та інформаційного впливу. При цьому країни Заходу і насамперед США є прихильниками вузького підходу, розуміючи під міжнародною інформаційною безпекою лише технічні аспекти та кібербезпеку [9].

У світі серйозну загрозу національній безпеці становлять різні форми тероризму. Міжнародним тероризмом створено відкриту кампанію з метою дестабілізації ситуації вже не лише в окремих країнах, а й групах країн і в усьому світі загалом.

Розібравшись із поняттям та правовою основою міжнародної інформаційної безпеки, варто звернути особливу увагу також на сучасні теоретичні підходи до міжнародних аспектів інформаційної безпеки з позиції політологічних та міжнародно-політичних досліджень. Так, ліберальна методологія ґрунтується на підходах до змісту поняття «інформаційна безпека», а також емпіричних даних, що відстоюють нігілістичний вектор, у рамках якого ігнорується сутність цієї проблематики, а також допускається її упереджена інтерпретація. Деякі дослідники пов'язують проблематику забезпечення інформаційної безпеки держави з необхідністю повернення до практики цензури ЗМІ та запровадження деяких обмежень на свободу інформації [8, с. 43].

При цьому етап становлення концепції інформаційної безпеки є логічним відображенням накопиченого політичного досвіду, що зумовлює пошук засобів захисту від загроз національній безпеці. Позитивний аспект дискусії про смислові характеристики концепції інформаційної безпеки полягає у формуванні наукових уявлень про сутність інформаційних загроз, які характерні для реалій інформаційного суспільства, пов'язаних із

уявленнями практиків холодної війни та ідеологічним протиборством двох систем.

У цьому контексті плідність змін політичного дискурсу у політології проявляється у процесі ефективної розробки концепції інформаційної безпеки, і навіть збагаченні понятійного апарату теорії міжнародних відносин. Особливо наочно це проявляється у тому, що похідним від концепції інформаційної безпеки стає поняття «міжнародна інформаційна безпека», що міцно утвердилося у робочій мові сучасної дипломатії та теорії міжнародних відносин [11, с. 110].

Таким чином, концептуальні підходи, що сформували поняття «міжнародна інформаційна безпека», знаходять своє відображення у тексті Спільної заяви про загальні виклики безпеки на початку XXI ст. від 2 вересня 1998 р. Ця заява сприяла конституюванню питань міжнародної інформаційної безпеки як об'єкт теорії міжнародних відносин. Велике значення для формування системи міжнародної інформаційної безпеки та закріплення інформаційної безпеки як частини системи міжнародної безпеки має стандартизація вимог та характеристик захищених інформаційних комплексів, що знайшла відображення у Системі міжнародних та національних стандартів безпеки інформації, що включає понад сотню різних документів.

1.2. Специфіка та складники інформаційної безпеки

Інформаційна безпека передбачає комплекс організаційних, правових та технічних заходів щодо запобігання загрозам та усунення їх наслідків. Ці заходи полягають у виявленні, усуненні або нейтралізації негативних джерел, причин та умов впливу на інформацію, що становлять загрозу безпеці. Інформаційна безпека спрямована:

- на запобігання загрозам як превентивним заходам щодо забезпечення інформаційної безпеки в інтересах запобігання можливості їх виникнення;

- на виявлення загроз, що виражається в систематичному аналізі та контролі можливості появи реальних чи потенційних загроз та своєчасних заходів щодо їх попередження;
- виявлення загроз, метою якого є визначення реальних загроз і конкретних злочинних дій;
- на локалізацію злочинних дій та вжиття заходів щодо ліквідації загрози чи конкретних злочинних дій;
- на ліквідацію наслідків загроз та злочинних дій та відновлення статус-кво [18, с. 20].

Важливим є облік шляхів отримання інформації про підготовчі протиправні акти, заплановані розкрадання, підготовчі дії та інші елементи злочинних діянь. Виявлення має на меті проведення заходів щодо збирання, накопичення та аналітичної обробки відомостей про можливу підготовку злочинних дій інформаційних та інших з боку кримінальних структур чи конкурентів на ринку [15, с. 76].

Виявлення загроз – це дії щодо визначення конкретних загроз та їх джерел, які завдають той чи інший вид шкоди. До таких дій можна віднести виявлення фактів розкрадання чи шахрайства, а також фактів розголошення конфіденційної інформації або випадків несанкціонованого доступу до джерел комерційних секретів.

Припинення чи локалізація загроз – це дії, спрямовані на усунення чинної загрози та конкретних злочинних дій. Наприклад, припинення підслуховування конфіденційних переговорів за рахунок акустичного або електронного каналу витоку інформації.

Ліквідація наслідків має на меті відновлення стану, що передував настанню загрози. Наприклад, відновлення інформації, очищення комп'ютерів від вірусів тощо. Захищена інформація включає відомості, що становлять державну, комерційну, службову та інші таємниці, що охороняються законом. Кожен вид інформації має свої особливості в галузі регламентації, організації та здійснення цього захисту [17, с. 132].

Найбільш загальними ознаками захисту будь-якого виду інформації, що охороняється, є наступні:

- захист інформації організує та проводить власник або власник інформації або уповноважені ним на те особи (юридичні чи фізичні);
- захистом інформації власник охороняє свої права на володіння та розпорядження інформацією, прагне захистити її від незаконного заволодіння та використання на шкоду його інтересам;
- захист інформації здійснюється шляхом проведення комплексу заходів щодо обмеження доступу до інформації, що захищається, та створення умов, що виключають або суттєво ускладнюють несанкціонований, незаконний доступ до інформації, що захищається, та її носіїв. Захищена інформація, що є державною або комерційною таємницею, як і будь-який інший вид інформації, необхідний для управлінської, науково-виробничої та іншої діяльності [14, с. 76].

Нині перед захистом інформації ставляться ширші завдання, ніж забезпечення безпеки інформації. Це зумовлено рядом обставин, і в першу чергу тим, що все ширше поширення в накопиченні та обробці інформації, що захищається, отримують ЕОМ, в яких може відбуватися не тільки витік інформації, але і її руйнування, спотворення, підробка, блокування та інші втручання в інформацію та інформаційні системи [12, с. 64].

З аналізу загроз безпеки інформації випливає, що досягти максимального (необхідного) рівня захищеності можна лише за рахунок комплексного використання існуючих методів та засобів захисту. Комплексність є одним із принципів, які мають бути покладені в основу розробки як концепції захисту інформації, так і конкретних систем захисту.

Цілі захисту інформації на об'єктах захисту можуть бути досягнуті під час проведення робіт за такими напрямами:

- визначення охоронюваних відомостей про об'єкти захисту;
- виявлення та усунення (ослаблення) демаскуючих ознак, що розкривають відомості, що охороняються;

- оцінки можливостей та ступеня небезпеки технічних засобів розвідки;
- виявлення можливих технічних каналів витоку інформації;
- аналізу можливостей та небезпеки несанкціонованого доступу до інформаційних об'єктів;
- аналізу небезпеки знищення чи спотворення інформації за допомогою програмно-технічних впливів на об'єкти захисту;
- розроблення та реалізації організаційних, технічних, програмних та інших засобів та методів захисту інформації від усіх можливих загроз;
- створення комплексної системи захисту;
- організації та проведення контролю стану та ефективності системи захисту інформації;
- забезпечення сталого управління процесом функціонування системи захисту інформації [20, с. 136].

Інформаційна безпека здебільшого пов'язана з комплексним вирішенням трьох завдань:

1. Забезпечення доступності інформації.
2. Забезпечення цілісності інформації.
3. Забезпечення конфіденційності інформації [22, с. 54].

Доступність інформації. Інформаційні системи створюються, щоб одержати певні інформаційні послуги. Якщо з тих чи інших причин надати ці послуги користувачам стає неможливо, це, очевидно, завдає шкоди всім користувачам.

Доступність – це гарантія отримання необхідної інформації або інформаційної послуги за певний час. Фактор часу у визначенні доступності інформації у ряді випадків є дуже важливим, оскільки деякі види інформації та інформаційних послуг мають сенс лише у певний проміжок часу [31, с. 91].

Цілісність є найважливішим аспектом інформаційної безпеки у випадках, коли інформація використовується, щоб керувати різними процесами, наприклад технічними, соціальними тощо. Цілісність – гарантія

того, що інформація зараз існує у її вихідному вигляді, тобто при її зберіганні чи передачі не було зроблено несанкціонованих змін [32, с. 175].

Конфіденційність – гарантія доступності конкретної інформації лише тому колу осіб, кому вона призначена. Порушення кожної із трьох категорій призводить до порушення інформаційної безпеки загалом. Наприклад, розкрадання пароля для доступу до комп'ютера (порушення конфіденційності) може призвести до його блокування, знищення даних (порушення доступності інформації) або фальсифікації інформації, що міститься в пам'яті комп'ютера (порушення цілісності інформації).

Значення кожної з перерахованих складових інформаційної безпеки для різних категорій суб'єктів інформаційних відносин по-різному. У разі державних організацій на чільне місце ставиться конфіденційність. Для державних структур також особливе значення набуває цілісність інформації [31, с. 91].

Для комерційних організацій провідну роль відіграє доступність інформації, що забезпечує інформування клієнтів та партнерів, виконання робіт із продажу, надання банківських послуг. Цілісність також є найважливішим аспектом інформаційної безпеки комерційних структур. Набір і характеристики комплектуючих виробів, хід технологічного процесу – це приклади інформації, порушення цілісності якої може бути буквально смертельним. У той самий час конфіденційність в такому разі комерційної інформації відіграє у конкуренції [32, с. 175].

Ступінь захисту інформаційних ресурсів та досягнутий рівень інформаційної безпеки можна оцінити, аналізуючи політику безпеки – набір законів, правил і норм, що визначають, як воно обробляє, захищає та поширює інформацію. Залежно від сформульованої політики можна вибирати конкретні механізми, що забезпечують безпеку системи. Політика безпеки – це активний компонент захисту, що включає аналіз можливих загроз і вибір заходів протидії.

Основні елементи політики інформаційної безпеки:

1) довільне керування доступом до інформаційних ресурсів;

2) безпека повторного використання інформаційних ресурсів;

3) безпека інформаційних ресурсів;

4) примусове управління доступом до інформаційних ресурсів. Залежно від опрацьованості вищеперелічених елементів політики безпеки можна ранжувати інформаційні системи за ступенем їхньої надійності [31, с. 91].

Отже, реалізація безперервного процесу захисту інформації можлива лише на основі систем концептуального підходу та промислового виробництва засобів захисту, а створення механізмів захисту та забезпечення їх надійного функціонування та високої ефективності може бути здійснено лише фахівцями високої кваліфікації у галузі захисту інформації.

1.3. Роль та значення інформаційної безпеки

Роль інформаційної безпеки в економічних науках визначається здатністю засобів та методів інформаційної безпеки протистояти загрозам економічної цілісності держави та організацій. Інформацію без перебільшення можна віднести до одного з вирішальних ресурсів розвитку. Вона активно впливає на всі сфери життєдіяльності як окремих держав, так і всього світового співтовариства.

Однак у певних випадках інформація може бути використана не тільки на благо, а й на шкоду інтересам особи, суспільства та держави. Тому роль інформаційної безпеки у системі національної безпеки не лише суттєво зростає, а й виходить на перший план [35, с. 138].

Але в той же час необхідно враховувати про суперечливість характеру процесу глобальної інформатизації, що з одного боку відкриває нові можливості для транснаціональної соціальної взаємодії, а з іншого – веде до появи нових ризиків і загроз національній та міжнародній безпеці, а також необхідності пошуку адекватних відповідей на виклики інформаційної доби.

При цьому традиційний підхід до державної політики інформаційної безпеки, який грунтується на безпеці інформації, більше не можна вважати ефективним. У рівній мірі не можна ототожнювати зміни до національної політики у зазначеній галузі лише із захистом інформації комп'ютерних мереж та національних інформаційних систем [32, с. 175].

У сучасному світі, зі зростанням кількості інформаційних джерел та загальної ролі інформації посилюється і роль соціально-політичної задоволеності потреб громадян у отриманні інформації, а також участі в процесі створення та обміну інформації як основи політичної стабільності суспільства та держави.

Стабільний та безпечний розвиток суспільства можливий лише за наявності у громадських об'єднань та неформальних груп можливості доступу до джерел інформації. Надмірне регулювання сучасних інформаційно-комунікаційних мереж та інформаційних процесів з боку держави може значно уповільнити процеси соціально-економічного, технологічного та політичного розвитку суспільства. Водночас сьогодні не можна не звернути увагу на загрозу використання інформаційних технологій у злочинних цілях, у тому числі й екстремістськими терористичними організаціями.

Розвиток інформаційних мереж, феномен швидкісного поширення інформації у віртуальному середовищі, а також неможливість контролю над інформацією у віртуальному середовищі, що випливає з її технологічних основ та міжнародного, наддержавного становища, призводять до появи загрози масового поширення інформації, що пропагує насильство, екстремізм [35, с. 138].

Отже, основою державної політики у сфері забезпечення інформаційної безпеки має стати гнучкий підхід до проблеми інформаційної безпеки, що базується на дотриманні основних прав та свобод особистості в інформаційній сфері, при обмеженні використання інформаційних технологій у протиправних цілях. При цьому контроль з боку органів державного управління має бути мінімальним, оскільки будь-які спроби жорсткого

контролю над сучасними інформаційними мережами неминуче призведуть до загальмовування їх розвитку, що, у свою чергу, негативно позначиться як на інформаційно-технологічному потенціалі країни, так і на її міжнародному статусі. Найефективнішою, на мою думку, слід визнати політику спільного регулювання інформаційно-комунікаційних мереж, яке здійснюється органами державного управління за активної участі комерційних структур та громадських організацій.

1.4. Нормативно-правові основи гарантування міжнародної інформаційної безпеки

В даний час основними напрямками забезпечення міжнародної інформаційної безпеки є:

- протидія військово-політичним загрозам (деструктивний інформаційний вплив, включаючи питання пропаганди, кібератресія);
- протидія злочинності у сфері високих технологій (СВТ) [60, с. 356].

При цьому міжнародне співробітництво у сфері підтримки міжнародної інформаційної безпеки здійснюється в інституційній та конвенційній формі.

Слід зазначити, що проблемам міжнародної інформаційної безпеки приділяється досить пильна увага з боку багатьох міжнародних організацій, включаючи ООН, Організацію Договору про колективну безпеку (ОДКБ), НАТО, Шанхайську організацію співробітництва (ШОС) та ін. Координацію такої взаємодії здійснюють органи загальної компетенції (Генеральна Асамблея ООН, Північноатлантична рада НАТО, Рада колективної безпеки ОДКБ), органи спеціальної компетенції, для яких мандат у цій сфері є додатковим (Міжамериканський комітет проти тероризму), спеціально створені структурні одиниці (Консультаційний координаційний центр ОДКБ з питань комп'ютерні інциденти, Комітет з кібероборони НАТО, Управління

НАТО у сфері кібероборони, Агентство з комунікацій та інформації НАТО та створений у його рамках Центр з реагування на кіберзагрози, Агентство з мережевої та інформаційної безпеки Європейського Союзу, Європейський центр з кіберзлочинності, створений і т.д.).

Тим часом співпраця у сфері забезпечення міжнародної інформаційної безпеки в рамках конвенційної форми пов'язана з деякими проблемами. Так, нині відсутні комплексні міжнародні договори універсального характеру, що регулюють співпрацю держав у сфері забезпечення міжнародної інформаційної безпеки та боротьбі зі злочинністю в СВТ.

Разом з тим, у доктрині широко визнано, що кіберпростір не є середовищем «поза законом» і на нього також поширюються загальновизнані принципи міжнародного права [35, с. 102-107; 43, с. 458-459; 44, с. 9; 8]. Деякі питання забезпечення міжнародної інформаційної безпеки частково врегульовані у різних міжнародних договорах універсального характеру. Так, по-перше, вороже використання інформаційних технологій, наслідки та масштаб якого можна порівняти з реальним збройним нападом (кібератрегресія), цілком виразно забороняється чинним міжнародним правом (п. 4 ст. 2 Статуту ООН). Зазвичай правова заборона вчинення подібних актів визнавалася експертами ООН, НАТО [52; 58]. Інакше кажучи, нині заборона застосування сили чи загрози силою діє і щодо інформаційного простору.

Слід зазначити, що військове реагування на будь-які інциденти в кіберпросторі або на акти, вчинені з використанням інформаційно-комунікаційних технологій, можливе лише у повній відповідності до Статуту ООН та з повним розумінням визначальної ролі Ради Безпеки ООН у цій сфері. Інакше такі дії вважатимуться неправомірними [60, с. 356; 43, с. 473-474].

По-друге, використання потенціалу інформаційних технологій для підриву соціально-політичної обстановки, здійснення деструктивного інформаційного впливу, формування громадської думки шляхом поширення певної інформації також не є новою областю міжнародних відносин, не врегульованих міжнародним правом.

1) заборона негативного впливу на суспільно-політичну свідомість населення, наслідки якого становлять втручання у внутрішні справи держави, також випливає із чинних норм міжнародного права (п. 7 ст. 2 Статуту ООН). Неприпустимість такої діяльності неодноразово підтверджувалася в актах міжнародних організацій та конференцій, судовій практиці (п. 3 Декларації про засади міжнародного права, що стосуються дружніх відносин та співробітництва між державами відповідно до Статуту Організації Об'єднаних Націй, від 24 жовтня 1970, п. 2 Декларації про неприпустимість втручання у внутрішні справи держав, про запобігання їх незалежності та суверенітету від 21 грудня 1965 р., п. I Декларації про неприпустимість інтервенції та втручання у внутрішні справи держав від 9 грудня 1981 р., принцип VI розділу I Заключного акта Наради з безпеки та співробітництва в Європі від 1 серпня 1975 р., п. 202–209 рішення Міжнародного суду ООН у справі про військову та воєнізовану діяльність у Нікарагуа та проти Нікарагуа від 27 червня 1986 р. та ін.);

2) неприпустимість деструктивного інформаційного впливу нині на універсальному рівні випливає з положень низки міжнародних договорів (ст. 1, п. 4 ст. 2 Статуту ООН, ст. 4 Міжнародної конвенції про ліквідацію всіх форм расової дискримінації від 21 грудня 1965 р., ст. 20 Міжнародного пакту про громадянські та політичні права від 16 грудня 1966 р.), вона також знайшла відображення у значній кількості резолюцій Генеральної Асамблеї ООН (п. 1 резолюції 110 (II) від 3 листопада 1947 р., п. 1 резолюції 2625) (XXV) від 24 жовтня 1970 р., абз. 4 п. 3, 8 резолюції 67/178 від 20 грудня 2012 р., п. 20 резолюції 67/154 від 20 грудня 2012 р. та ін.);

3) поширення тієї чи іншої ідеології, формування певної громадської думки шляхом використання глобальної інформаційно-телекомунікаційної мережі не є новим видом діяльності. Такі дії тією чи іншою мірою завжди використовувалися державами у своїх цілях упродовж усієї історії [35, с. 138; 42, с. 217; 45, с. 4], і мають усталену назву – пропаганда.

У зв'язку з тим, що в даний час у науці не вироблено єдиного підходу до визначення термінів «інформаційна війна», «інформаційна зброя», у політологічних роботах деяких учених пострадянського простору поняття «пропаганда» найчастіше підмінюється новим терміном «інформаційна війна», а засоби здійснення такої пропаганди оголошуються «інформаційною зброєю», яку необхідно заборонити за допомогою міжнародного договору. Вважаємо, що ця пропозиція нереалізована. Критерії визначення таких засобів та методів впливу мають бути гранично конкретними. Наприклад, відповідно до концепції, розробленої Д. Деннінг, як інформаційна зброя можуть розглядатися шкідливі програми, розробка, поширення та використання яких фізичними та юридичними особами, як правило, кримінально карається: комп'ютерні віруси; троянські програми; мережеві черви; інструменти, що викликають відмову в обслуговуванні; програми-бекдори; фільтри системних лог-файлів для приховування залишених електронних слідів та ін. [37, с. 43-53].

Отже, з одного боку, сучасним міжнародним правом закріплюються основи забезпечення міжнародної інформаційної безпеки, з другого – поведінка держав у інформаційно-комунікаційному просторі нині докладно не регламентовано.

В даний час питання міжнародної інформаційної безпеки на універсальному рівні регулюються документами, норми яких мають морально-політичний характер і належать до м'якого права. За підсумками роботи трьох груп урядових експертів для вивчення потенційних загроз у сфері інформаційної безпеки, створених відповідно до резолюцій Генеральної Асамблеї ООН 58/32 від 8 грудня 2003 р., 63/70 від 2 грудня 2008 р., 68/243 від 27 грудня 2013 р., були представлені доповіді, останні з яких, зокрема, стосувалися норм, правил та принципів відповідальної поведінки держав у кіберпросторі, а також заходів зміцнення довіри в інформаційному просторі, підвищення потенціалу держав у даній сфері тощо. Державами-членами Шанхайської організації співробітництва на 70-ту сесію Генеральної Асамблеї

ООН було представлено проект Кодексу поведінки держав у кіберпросторі, який створюватиме політичні основи діяльності держав у цій сфері [37, с. 43-53].

На наш погляд, акти Генеральної Асамблеї ООН є базою, на основі якої може бути зроблено універсальну кодифікацію міжнародних норм, що регулюють співпрацю держав у галузі забезпечення інформаційної безпеки. Більш того, м'яке право, не створюючи юридичних обов'язків для держав, визначає цілі та завдання у сфері забезпечення міжнародної інформаційної безпеки, які на даному етапі не всі держави готові прийняти як правову норму.

Вважаємо також, що їхнє послідовне виконання здатне згодом сформувати відповідні міжнародні звичайні норми. Крім того, процес розробки та прийняття резолюцій Генеральної Асамблеї ООН простіше і швидше в порівнянні з укладенням міжнародних договорів, за рахунок чого такі акти є більш гнучким і своєчасним інструментом регулювання нових міжнародних відносин.

На регіональному рівні склалося кілька підходів до правового регулювання співробітництва у сфері забезпечення інформаційної безпеки у контексті протидії військово-політичним загрозам [37, с. 43-53].

У рамках ШОС, СНД, Африканського союзу було укладено спеціальні договори, присвячені розглянутій проблемі (Угода між урядами держав–членів Шанхайської організації співробітництва про співробітництво в галузі забезпечення міжнародної інформаційної безпеки від 16 червня 2009 р., Угода про співпрацю держав–учасниць СНД у галузі забезпечення інформаційної безпеки від 20 листопада 2013 р., Конвенція Африканського союзу про кібербезпеку та захист персональних даних від 27 червня 2014 р.) [60, с. 356].

У НАТО та ОДКБ співробітництво у сфері забезпечення інформаційної безпеки здійснюється на підставі документів, прийнятих органами цих міжнародних організацій (політика НАТО в галузі кібербезпеки, схвалена міністрами оборони країн Альянсу у 2014 р., план дій, ухвалений на Саміті НАТО в Уельсі у 2014 р.), Рішення Ради колективної безпеки ОДКБ від 10

грудня 2010 р. «Про Положення про співпрацю держав–членів ОДКБ у сфері забезпечення інформаційної безпеки», Рішення Ради колективної безпеки ОДКБ від 5 вересня 2008 р. «Про Програму спільних дій щодо формування системи інформаційної безпеки держав–членів ОДКБ» та ін.) [35, с. 138].

Таким чином, загалом слід зазначити, що питання протидії військово-політичним загрозам у сфері інформаційної безпеки регулюються сучасним міжнародним правом. Крім того, діючі міжнародно-правові норми накладають заборону на застосування інформаційно-телекомунікаційних технологій з метою поширення певної інформації (наприклад, з метою пропаганди війни, поширення расової та релігійної ворожнечі), а також втручання у внутрішні справи держави.

У зв'язку із зазначеним, вважаємо, що найбільш актуальним є питання правового регулювання міжнародного співробітництва у боротьбі зі злочинністю у СВТ. Це зумовлено тим, що взаємодія держав у цьому напрямі практично не врегульовано на універсальному рівні, а зростання кількості укладених регіональних спеціальних міжнародних договорів у цій галузі веде до вироблення різних стандартів співробітництва у боротьбі зі злочинами у СВТ, що не сприяє реалізації принципу невідворотності кримінальної відповідальності за вчинення таких протиправних діянь.

Універсальне договірно-правове співробітництво у боротьбі зі злочинністю в СВТ здійснюється на підставі міжнародних договорів, що регулюють боротьбу держав з окремими видами злочинів (Конвенція ООН проти транснаціональної організованої злочинності від 15 листопада 2000 р., Факультативний протокол до Конвенції про права дитини, дитячої проституції та порнографії від 25 травня 2000 р.) [37, с. 43-53].

Спеціальні конвенції, спрямовані на координацію міжнародної боротьби зі злочинністю в СВТ, укладені під егідою регіональних міжнародних організацій (Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 р. та додатковий протокол до неї від 21 січня 2003 р., Арабська конвенція щодо боротьби з боротьбою сфері інформаційних технологій від 21 грудня

2010 р., Угода про співпрацю держав-учасниць СНД у боротьбі зі злочинами у сфері комп'ютерної інформації від 1 червня 2001 р., Африканська конвенція про кібербезпеку та захист персональних даних від 27 червня 2014 р., Протокол про взаємодію держав – членів Організації Договору про колективну безпеку щодо протидії злочинній діяльності в інформаційній сфері від 23 грудня 2014 р.) [36, с. 430].

Регіоналізація міжнародного співробітництва у боротьбі зі злочинами у СВТ створює низку проблем практичного характеру у сфері протидії таким протиправним діянням. Наприклад, у міжнародних договорах, укладених державами на пострадянському просторі, відсутні положення, що регулюють можливість отримання транскордонного доступу до комп'ютерної інформації, невідкладного забезпечення збереження комп'ютерних даних, що зберігаються, збору даних про трафік у режимі реального часу, перехоплення даних про зміст і т.д.

Перешкоди щодо співробітництва органів держав, що належать до різних регіонів, також пов'язані з недостатньою гармонізацією норм кримінального права у сфері. Питання протидії міжнародному кібертероризму викликає особливе побоювання у світової спільноти. У міжнародних договорах, укладених на регіональному рівні, відбилися окремі аспекти співробітництва держав з метою боротьби з такими протиправними діяннями. Так, кібертероризм заборонено Арабською конвенцією щодо боротьби зі злочинами у сфері інформаційних технологій від 21 грудня 2010 р.

При цьому в цьому міжнародному договорі закріплено інструментальний підхід до змісту кібертероризму, який не враховує можливості використання інформаційно-комунікаційних технологій проти критично важливої інфраструктури держави [35, с. 138].

У рамках ОДКБ було укладено Протокол про взаємодію держав–членів ОДКБ щодо протидії злочинній діяльності в інформаційній сфері від 23 грудня 2014 р., який вперше закріпив спеціальні норми, що регулюють питання співробітництва у боротьбі з діяннями, які посягають як на основи

конституційного ладу та безпеки держав-учасників, так і на міжнародний мир та безпеку, що здійснюються за допомогою інформаційних технологій (ст. 3). Фактично міжнародне співробітництво боротьби з кібертероризмом входить у сферу регулювання цього міжнародного договору.

Водночас, цей документ не містить спеціальних норм, що регулюють оперативну співпрацю компетентних органів держав з метою протидії злочинам в інформаційній сфері. Так, відповідно до ст. 6 документа, що розглядається, співробітництво в рамках Протоколу здійснюється на підставі письмового звернення уповноваженого компетентного органу [36, с. 430].

Звернення, передане за допомогою технічних засобів зв'язку, потребує підтвердження у письмовій формі. При цьому такий екстраординарний спосіб передачі звернення можливий лише «при отриманні оперативної інформації про злочини, що готуються», перерахованих у ст. 3 Протоколу.

Отже, з цієї норми випливає, що терміновий порядок зносин компетентних органів може бути задіяний стосовно закінчених злочинів. Тим часом, розслідування транснаціональних злочинів у СВТ вимагає негайної реакції, оскільки комп'ютерні дані можуть бути швидко видалені.

Усі проблеми договірно-правового регулювання співробітництва держав у боротьбі зі злочинністю в СВТ вимагають врегулювання у міжнародному договорі універсального характеру. Слід зазначити, що питання укладання універсальної міжнародної угоди боротьби зі злочинним використанням високих технологій широко обговорюються як у науці, і лише на рівні ООН. Прихильниками укладання універсального міжнародного договору є С. Шольберг [54, с. 1], А. Софаєр, С. Гудмен [56, с. 2, 31], Р. Бродхарст [36, с. 430].

Ще на 11-му Конгресі ООН із запобігання злочинності та кримінальному правосуддю йшлося про необхідність розробки універсальної міжнародної конвенції з питань боротьби зі злочинністю у СВТ. Водночас у 2015 р. на 13-му Конгресі ООН із запобігання злочинності та кримінальному правосуддю,

що пройшов у м. Досі (Катар), консенсус з цього питання так і не був досягнутий.

Безсумнівно, як модель для розробки національного законодавства в даній сфері може служити Інструментарій для законодавства про кіберзлочинність, розроблений Міжнародним союзом електрозв'язку. Ряд рекомендацій щодо вдосконалення законодавства у цій сфері міститься в актах Генеральної Асамблеї ООН (резолюції Генеральної Асамблеї ООН 55/63 від 4 грудня 2000 р., 56/121 від 19 грудня 2001 р., спрямовані на боротьбу зі злочинним використанням інформаційних технологій), (злочини пов'язані з особистими даними (резолюції ЕКОСОС 2004/26 від 21 липня 2004 р., 2007/20 від 26 липня 2007 р., 2011/35 від 28 липня 2011 р., 2009/22 від 30 липня), продаж психотропних ліків через Інтернет (резолюція ЕКОСОС 2004/42 від 21 липня 2004 р.), зловживання новими інформаційними технологіями щодо дітей (резолюція ЕКОСОС 2011/33 від 26 липня 2007 р.) [36, с. 430].

Водночас таких заходів нині недостатньо, оскільки модельне законодавство та рекомендації, які містяться в резолюціях органів міжнародних організацій, не створюють юридичних зобов'язань для держав, а отже, не можуть врегулювати відносини, пов'язані як із гармонізацією кримінального законодавства, так і зі створенням дієвої системи міжнародної взаємодії органів, які ведуть кримінальний процес. Це обумовлює необхідність укладання міжнародного договору про співробітництво держав у боротьбі зі злочинами у СВТ у рамках ООН.

Таким чином, відсутність комплексного міжнародного договору універсального характеру, що регулює співробітництво держав у сфері забезпечення міжнародної інформаційної безпеки, не свідчить про відсутність міжнародно-правового регулювання у досліджуваній галузі загалом. Основи міжнародно-правового регулювання міжнародної інформаційної безпеки містяться в чинних міжнародних договорах універсального характеру.

Висновки до першого розділу

У першому розділі ви виявили, що з практичної точки зору, під інформаційною безпекою розуміємо захищеність інформації та інфраструктури, що її підтримує, від випадкових або навмисних впливів природного або штучного характеру, що загрожують заподіянням шкоди власникам або користувачам цієї інформації та інфраструктури. Захист інформації – це комплекс заходів, спрямованих на забезпечення інформаційної безпеки. На практиці під цим розуміється підтримка цілісності, доступності та, якщо потрібно, конфіденційності інформації та ресурсів, що використовуються для введення, зберігання, обробки та передачі даних.

Питання відповідальної поведінки держав у кіберпросторі нині доцільно врегулювати за допомогою норм м'якого права (зокрема резолюцій Генеральної Асамблеї ООН). Зазначені норми створюють орієнтири для поведінки держав у інформаційному просторі, сприяють формуванню норм міжнародного права у аналізованої області. Міжнародно-правове регулювання співробітництва держав у боротьбі зі злочинністю у сфері високих технологій на універсальному рівні в даний час не є достатнім. Практичні проблеми взаємодії компетентних органів з метою припинення, розкриття та розслідування таких злочинів можуть бути вирішені виключно укладанням міжнародного договору, який має закласти основи співробітництва в галузі надання міжнародно-правової допомоги у таких кримінальних справах, здійснення екстрадиції, а також гармонізації кримінального законодавства держав.

РОЗДІЛ 2. ІНСТРУМЕНТИ УПРАВЛІННЯ ТА СПОСОБИ ЗАБЕЗПЕЧЕННЯ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Специфіка організації інформаційної безпеки органів державного управління

Сучасні інформаційні технології не тільки відкривають безмежні можливості, а й породжують нові проблеми розвитку українського суспільства, несуть нові небезпеки, виклики та загрози його безпеці, однією з найважливіших складових якої є інформаційна безпека. Національна безпека істотно залежить від забезпечення інформаційної безпеки, і під час розвитку технічного прогресу, швидкими темпами зростання використання сучасних інформаційних технологій ця залежність неминуче зростає. Значимість інформаційної безпеки обумовлена тим, що інформаційна сфера забезпечує функціонування решти сфер життя нашого суспільства та держави.

Безпека, у тому числі національна, в залежності від сфери включає різні види безпеки, до яких прийнято відносити зовнішню, внутрішню, міжнародну, військову, економічну, політичну, соціальну, інформаційну, екологічну, суспільну та ін. Таким чином, безпека як така характеризується комплексністю, а інформаційна безпека є її складовою [32, с. 175].

Забезпечення інформаційної безпеки передбачає насамперед правильне визначення загроз безпеки відповідного суб'єкта, зокрема загроз державним органам виконавчої влади в інформаційній сфері, а також адекватний вибір та застосування адекватних засобів захисту від цих загроз, що може бути досягнуто лише комплексним використанням засобів захисту по кожному виду загроз у рамках єдиної державної політики [60, с. 356].

Інформаційне забезпечення діяльності державних органів виконавчої влади – це неодмінна умова ефективності державного управління, прийняття обґрунтованих рішень на основі повної, своєчасної та достовірної інформації. Рівень інформаційного забезпечення діяльності органів виконавчої істотно

впливає на всі процеси соціально-економічного розвитку суспільства, є одним із стратегічних напрямів підвищення ефективності діяльності на всіх рівнях:

- необхідна оцінка та забезпечення інформаційних потреб у межах кожної функції управління конкретного органу виконавчої влади;
- організація документообігу та обміну інформацією;
- оптимізація потоків інформації та процедур обміну тощо [32, с. 175].

Обсягу компетенції кожного органу виконавчої влади повинен відповідати необхідний для її реалізації обсяг інформаційного забезпечення, при цьому на інформаційну безпеку негативно впливатиме як брак інформації, так і її надлишок. Видається доцільним визначати обсяг інформаційного забезпечення конкретного органу виконавчої влади у положенні про цей орган, іншими словами, встановлювати його інформаційний статус на основі поставлених перед ним завдань та обсягів наданих повноважень.

На підвищення інформаційної безпеки органів виконавчої впливає створення на основі інформаційно-комунікаційних технологій електронного уряду, внаслідок чого забезпечується сучасна інформаційна основа для прийняття управлінських рішень, підвищується рівень інформаційного забезпечення, достовірність, швидкість отримання та повнота інформації. При цьому не можна зводити електронний уряд лише до його технічної складової; його завдання – підвищення ефективності діяльності держави загалом, формування нового рівня відносин громадян зі своєю державою [60, с. 356].

Цілями формування електронного уряду є підвищення якості адміністративно-управлінських процесів, удосконалення системи інформаційно-аналітичного забезпечення прийнятих рішень на всіх рівнях державного управління.

Безпека інформації як складова інформаційної безпеки органів виконавчої влади включає захист інформації та інформаційних ресурсів від несанкціонованого доступу, спотворення, знищення, встановлення режиму інформації залежно від її змісту, забезпечення захисту відомостей, що становлять державну таємницю, іншої інформації обмеженого доступу.

Безпека інформації, що циркулює у органах виконавчої, забезпечується різними заходами: організаційними, технічними, правовими. Зазначені заходи щодо захисту інформації спрямовані на:

- забезпечення захисту інформації від неправомірного доступу, знищення, модифікування, блокування, копіювання, надання, розповсюдження, а також від інших неправомірних дій щодо такої інформації;
- дотримання конфіденційності інформації обмеженого доступу;
- реалізацію права доступу до інформації [2, с. 185].

Перелічені заходи, по суті, є встановленням щодо конкретних видів інформації правового режиму та забезпечення його дотримання. Їхнє виконання покладено на власника інформації, оператора інформаційної системи у випадках, встановлених законодавством. Щодо інформації, що циркулює у сфері державного управління, володарями інформації, операторами державних інформаційних систем за загальним правилом є органи виконавчої влади. З метою забезпечення інформаційної безпеки органи виконавчої зобов'язані виконувати вимоги захисту інформації у державних інформаційних системах, які встановлюються уповноваженими органами виконавчої влади.

Найбільш повно врегульовані питання захисту інформації, що становить державну таємницю, а найпроблемнішими є питання встановлення правового режиму службової таємниці, у зв'язку з чим необхідне зупинитися на цьому питанні докладніше [60, с. 356].

Обмеження доступу до інформації, що знаходиться в органів виконавчої влади, встановлюються в тому випадку, коли інші заходи регулювання не можуть забезпечити належний правовий порядок, насамперед безпеку. Це досягається за допомогою таких засобів, як:

- встановлення додаткових заборон та зобов'язань, обмеження певних дій;
- вжиття спеціальних заходів, спрямованих на встановлення та підтримання правил;
- дозвільний спосіб і тип реалізації права і свободи;

- система контролю та нагляду за виконанням вимог;
- встановлення відповідальності порушення спеціального правового режима [6, с. 282].

Основна частина заборон та обмежень знаходить регламентацію у законах шляхом запровадження спеціальних правових режимів певних видів інформації, і насамперед шляхом встановлення режиму таємниці.

Одним із питань, що довго не вирішуються щодо інформації, яке циркулює в системі органів виконавчої влади, є питання про службову таємницю. До службової інформації обмеженого поширення належить несекретна інформація, що стосується діяльності організацій, обмеження поширення якої диктуються службовою необхідністю. Перелік відомостей, які стосуються інформації обмеженого доступу, а також порядок віднесення зазначених відомостей до інформації обмеженого доступу відповідно до тієї ж статті мають бути встановлені законом [2, с. 185].

Підстави для обмежень доступу до інформації можуть встановлюватися законом лише як виняток із загального дозволу і повинні бути пов'язані саме зі змістом інформації, оскільки інакше вони не були б адекватні конституційно визнаним цілям.

Безпека телекомунікацій та інформаційного обміну — це одна із складових інформаційної безпеки органів виконавчої влади. Інформаційні технології знайшли широке застосування в управлінні найважливішими об'єктами життєзабезпечення, які стають більш уразливими перед випадковими та навмисними впливами. Підвищення вразливості пов'язане з низкою факторів, основними з яких є зниження рівня міжнародної безпеки; розвиток міжнародного тероризму; збільшення кількості потенційно небезпечних об'єктів, багато з яких розташовані у великих містах [6, с. 282].

Один із принципових чинників – суттєва залежність інфраструктур від зарубіжних технологій, що зумовило виникнення нових загроз, пов'язаних насамперед із можливістю використання інформаційно-комунікаційних технологій з метою, несумісною з національними інтересами.

З метою забезпечення інформаційної безпеки при здійсненні міжнародного інформаційного обміну через інформаційні системи, інформаційні мережі та мережі зв'язку, включаючи міжнародну комп'ютерну мережу Інтернет, суб'єктам міжнародного інформаційного обміну наказано не здійснювати включення інформаційних систем, мереж зв'язку та автономних персональних комп'ютерів, в яких обробляється інформація, що містить відомості, що становлять державну таємницю, службову таємницю, до складу засобів міжнародного інформаційного обміну, у тому числі до міжнародної комп'ютерної мережі Інтернет [2, с. 185].

Оскільки така інформація перебуває, обробляється у державних і муніципальних структурах, ці вимоги поширюються усім, хто її отримує, обробляє чи передає, незалежно від підпорядкованості і форми власності. Власникам відкритих та загальнодоступних державних інформаційних ресурсів наказано здійснювати їх включення до складу об'єктів міжнародного інформаційного обміну лише за умови використання сертифікованих засобів захисту інформації, що забезпечують її цілісність та доступність, у тому числі криптографічних засобів для підтвердження достовірності інформації. Обов'язок використання лише сертифікованих засобів захисту в цьому випадку істотно підвищує ступінь інформаційної безпеки.

Однак наведені вище заходи, безумовно, є необхідними, але недостатніми. На думку аналітиків, фактори вразливості в інформаційній сфері визначаються наявністю таких серйозних проблем, як її технологічна залежність від іноземних держав у сфері інформатики, недостатній рівень захищеності критично важливих сегментів інформаційної інфраструктури та низький рівень державного контролю її внутрішнього інформаційного простору [6, с. 282].

З метою забезпечення інформаційної безпеки передбачено створення державної системи виявлення, попередження та ліквідації наслідків комп'ютерних атак на інформаційні ресурси – інформаційні системи та

інформаційно-телекомунікаційні мережі, що знаходяться на території України та у дипломатичних представництвах та консульських установах за кордоном.

Основними завданнями державної системи виявлення, попередження та ліквідації наслідків комп'ютерних атак на інформаційні ресурси встановлено:

- прогнозування ситуації у сфері забезпечення інформаційної безпеки України;
- забезпечення взаємодії власників інформаційних ресурсів, операторів зв'язку, інших суб'єктів, які здійснюють ліцензовану діяльність у галузі захисту інформації, при вирішенні завдань, що стосуються виявлення, попередження та ліквідації наслідків комп'ютерних атак;
- здійснення контролю за ступенем захищеності критичної інформаційної інфраструктури від комп'ютерних атак;
- встановлення причин комп'ютерних інцидентів, пов'язаних із функціонуванням інформаційних ресурсів країни [6, с. 282].

Таким чином, проблеми, що розглядаються, належать до тих, які потребують постійної уваги держави та пріоритетного рішення, підвищення ступеня державного контролю за дотриманням вимог безпеки в інформаційному просторі. Істотний внесок у забезпечення інформаційної безпеки може зробити формування сучасного законодавства у цій сфері.

2.2. Політика міжнародних організацій з питань інформаційної безпеки

Міжнародне співробітництво у сфері інформаційної безпеки зумовлює необхідність пошуку спільних рішень у рамках міжнародних організацій з протидії інформаційним та кіберзагрозам, вироблення спільної стратегії інформаційної безпеки для протидії кібервійнам, інформаційному тероризму

та інформаційній злочинності. можливо вирішити проблеми у політичній, економічній безпеці та інших сферах життєдіяльності суспільства [34, с. 212].

Організація Об'єднаних Націй як інститут глобального управління здатна забезпечити комплексне вирішення політичної проблеми інформаційної безпеки при широкому представництві та максимальному обліку позицій та інтересів усіх країн світу. Діяльність ООН у сфері інформаційної безпеки спрямована на розробку міжнародно-правової бази та вироблення документів для протидії протиправному використанню науково-технічного та технологічного прогресу терористичними угрупованнями та організованою злочинністю. Проблема інформаційної безпеки у контексті формування глобального інформаційного суспільства стала актуальною для діяльності спеціалізованих установ ООН, зокрема ЮНЕСКО, враховуючи гуманітарні та технічні програми та проекти організацій.

Однією з перших зустрічей на міжнародному рівні з розвитку інформаційного суспільства та забезпечення безпеки стала конференція «Інформаційна спільнота та розвиток», що відбулася в Мідранді (ПАР) 13-15 травня 1996 р. [6, с. 282].

30 липня 1996 р. в Парижі відбулася нарада на рівні міністрів закордонних справ та міністрів з проблем тероризму. Було проведено глибокий аналіз нових тенденцій, пов'язаних із тероризмом у всьому світі. За результатами роботи міжнародної конференції було прийнято заключний документ, де містився заклик до країн вживати заходів, які за поваги до основних свобод і верховенства права були б спрямовані на ефективну боротьбу з тероризмом. У документі містився заклик розглянути питання про небезпеки, пов'язані з використанням терористами мереж та систем передачі інформації з метою злочинної діяльності, та необхідність знаходження коштів для запобігання таким діям [34, с. 212].

Конференції у Мідранді та Парижі стали історичною основою та провісниками прийняття у 1998 р. на 53 сесії Генеральної Асамблеї ООН Резолюції A/RES/53/70 «Досягнення в сфері інформатизації та

телекомунікацій у контексті міжнародної безпеки». Саме в резолюції 53/70 вперше на найвищому рівні зазначається, що нові технології та засоби потенційно можуть бути використані з метою, несумісною із завданнями забезпечення міжнародної стабільності та безпеки, і можуть негативно впливати на безпеку держав [34, с. 212].

Резолюція містить заклик до держав-членів ООН сприяти розгляду на міжнародному рівні існуючих та потенційних угод у сфері інформаційної безпеки, розробити міжнародні принципи, спрямовані на зміцнення глобальних інформаційних та телекомунікаційних систем та на боротьбу з інформаційним тероризмом та криміналом.

Доповідь Генерального секретаря була опублікована в 1999 р. (A/54/213) [49]. Він складався з оцінок Австралії, Білорусії, Брунея, Великобританії, Катару, Куби, Оману, Росії, Саудівської Аравії та США. Об'єднуючим чинником цих оцінок було визнання наявності проблеми, але виявилися суттєві розбіжності у розстановці акцентів (військова, правова, гуманітарна чи інші складові), у методиці її розгляду та шляхах рішення.

Резолюція 53/70 започаткувала широке обговорення питань міжнародної інформаційної безпеки та пошуку стратегій забезпечення безпеки суб'єктів міжнародних відносин від нових загроз. Генеральний секретар щорічно надає Генеральній Асамблеї доповідь, яка містить позиції держав-членів Організації Об'єднаних Націй на цю тему.

Ще одним важливим етапом для розгляду питання міжнародної інформаційної безпеки стала Всесвітня зустріч на найвищому рівні з питань інформаційного суспільства (перший етап – 2003 р., Женева, другий етап – 2005 р., Туніс) та Всесвітня зустріч на найвищому рівні з питань інформаційного суспільства ВВСІО +10 2015 р., що проходила під егідою ООН. Конференція запропонувала світовій спільноті розглянути існуючі та потенційні загрози безпеці інформаційних та комунікаційних мереж, об'єднати зусилля держав-членів ООН, спрямованих на оцінку стану інформаційної

безпеки, а також на перспективну розробку міжнародної конвенції з інформаційної безпеки [6, с. 282].

Основою для такого рішення стали відповідні положення підсумкових документів регіональних конференцій щодо підготовки Всесвітньої зустрічі, а саме загальноєвропейської, азіатсько-тихоокеанської, африканської, західноазійської та латиноамериканської, в яких було закладено основу для подальшого обговорення проблематики міжнародної інформаційної безпеки.

Проблематика міжнародної інформаційної безпеки увійшла до підсумкових документів женевської зустрічі ВСІС – Декларації принципів «Побудова інформаційного суспільства – глобальне завдання нового тисячоліття». Зокрема, у Декларації принципів (розділ «Зміцнення довіри та безпеки при використанні ІКТ») наголошується, що міжнародна інформаційна безпека та безпека інформаційної інфраструктури є необхідною передумовою становлення глобального інформаційного суспільства та подолання асиметрії інформаційного розвитку [34, с. 212].

Необхідно відзначити, що підвищення довіри та безпеки при використанні інформаційно-комунікаційних технологій, враховуючи їх подвійну природу, визначається в документі як стратегія глобальної культури кібербезпеки, яка має забезпечуватися за допомогою міжнародного співробітництва всіма зацікавленими сторонами та компетентними міжнародними організаціями [3, с. 34].

Подальший розвиток міжнародного співробітництва у сфері інформаційної безпеки знайшов своє втілення в політичних дискусіях та документах туніської зустрічі щодо інформаційного суспільства, під час якої виявилися гострі протиріччя між підходами ООН та більшості держав-членів організації та США, оскільки саме позиція найбільш потужної інформаційної держави стосувалася лише визнання проблеми глобальної культури кібербезпеки та протидії розгляду високих технологій як технологій подвійного призначення та зброї масового ураження. У Туніському зобов'язанні 2005 р. було підтверджено позицію ООН щодо потенціалу ІКТ як

фактора запобігання конфліктам, а також сприяння їх мирному врегулюванню, з підтримки гуманітарних акцій, включаючи захист цивільних осіб у збройних конфліктах, діяльність місій з підтримки миру та надання допомоги у миробудуванні [34, с. 212]. Держави-члени ООН та учасники всесвітнього форуму в Тунісі наголосили на важливості боротьби з тероризмом у всіх його формах та проявах в Інтернеті поряд з дотриманням прав людини та закликали уряди всіх країн та світову спільноту підтвердити право кожної людини на доступ до інформації відповідно до Женевської Декларації за принципами та іншими міжнародними документами [3, с. 34].

На 71-й сесії ГА ООН 19 липня 2016 р. було прийнято доповідь Генерального секретаря «Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки». У доповіді подано офіційні звіти урядів 19 держав для зміцнення міжнародної безпеки та сприяння міжнародному співробітництву у цій сфері.

На 72-й сесії ГА ООН 11 серпня 2017 р. було прийнято доповідь Генерального секретаря «Досягнення в сфері інформатизації та телекомунікацій у контексті міжнародної безпеки» як виконання рекомендацій резолюції A/RES/71/28 від 5 грудня 2016 р. щодо інформування країн про свою точку зору з питань загальної оцінки міжнародної інформаційної безпеки та зусиль, які докладають держави. Резолюцію підтримала 181 країна [5, с. 65].

Багато країн і територій зміцнили свої стратегічні плани щодо захисту від інтернет-загроз. З 2016 р. багато країн опублікували або оновили свої стратегії захисту від інтернет-загроз. Вони опублікували правила та закони, заснували спеціальні агентства, удосконалили робочі механізми, запустили просвітницькі та освітні ініціативи в галузі інтернет-безпеки, сприяли поширенню культури безпеки в Інтернеті та наростили свій потенціал та зміцнили міжнародне співробітництво [7, с. 196].

Більшість країн приділяє велику увагу питанням інформаційної безпеки, регулюванню мережі Інтернет, формуванню загальноприйнятих міжнародних

правил та норм визнаючи потребу у співпраці та взаємній згоді, заснованих на Статуті ООН, міжнародному законодавстві та базових засадах міжнародних відносин. Прагнення досягти сталого, стабільного та безпарного суспільства об'єднало міжнародне співтовариство, підштовхнуло до партнерства, співробітництва та взаєморозуміння.

Таким чином, можна зробити висновок, що тема міжнародного співробітництва у питаннях забезпечення міжнародної безпеки взагалі та інформаційної безпеки зокрема стала гострою та актуальною в сучасному світі. Міжнародна спільнота в рамках міжнародних організацій та завдяки механізмам ООН демонструє прагнення до масштабної співпраці, об'єднання зусиль, взаємодії, спільної участі, відкритості та прозорості, відповідальності та інноваційності у вирішенні спільної проблеми безпечного миру.

У рамках сучасності, доповненої збільшенням ризиків та конфліктів у просторі суспільної та політичної взаємодії, особливо гостро постає проблема забезпечення міжнародної інформаційної безпеки. Це пов'язано також з тим фактом, що глобальні актори, будь то держави, ТНК, чи неурядові об'єднання здатні використовувати аспекти ІКТ у своїх політичних та інших цілях. Неконтрольоване використання комунікаційних технологій загрожує проблемами маніпулювання та підтасовуванням інформації в глобальному масштабі [3, с. 34].

Що ж до методів протидії щодо кібератак, то дослідники, наприклад, відзначають метод стримування геополітичних суперників, його втіленням виявляється здатність держав у здійсненні заходів у відповідь військового штибу. Тим не менш, видається також очевидною проблема того, що подібний сценарій розвитку подій загрожує підвищенням напруги міжнародної взаємодії. Цей аспект знайшов своє відображення і в роботі ООН щодо досягнень у галузі інформатизації та комунікації, де наголошено на тому, що феномен швидкого розвитку ІКТ охоплює один із сегментів міжнародних відносин [5, с. 65].

Специфіка інформаційної галузі взаємодії суспільства в рамках різних способів комунікації полягає в тому, що вона відрізняється від інших форм

взаємодії людей, які регулюються міжнародним та національним законодавством. Наслідком появи глобальних форм комунікації стає той факт, що інформація, що тиражується і створювана, порушує територіально-часову обумовленість. У зв'язку з чим однією з форм геополітичної сили виявляється досягнення геополітичних конкурентних переваг, які полягають у наявності першості у розвитку передових інформаційних технологій.

Міжнародний політичний контекст наголосив на важливості загроз міжнародній інформаційній безпеці. Наприклад, у 2010 р. вірус Stuxnet атакував ядерну інфраструктуру Ірану. А у 2011 р. у Північній Африці та на Близькому Сході пройшли масові протести, які у ЗМІ назвали «революціями Facebook». Ці події наголосили на важливості загроз ІКТ для глобальної безпеки та необхідності гармонізації правил та безпарного використання ІКТ [41].

У той же час особливості технологій (їх глобальний характер, можливість збереження анонімності при їх використанні, загальна доступність, неможливість чіткої ідентифікації суб'єкта, відповідального за кібератаку тощо) означають, що міжнародно-правова база, що діє, залишається недостатньою. У зв'язку з цим, документ передбачав можливість розробки в майбутньому додаткових норм для регулювання відносин в інформаційній сфері.

Наступний етап співробітництва в рамках групи урядових експертів відноситься до грудня 2013 р., коли 68 сесія Генеральної Асамблеї ООН ухвалила проект резолюції «Досягнення в галузі інформатизації та телекомунікацій у контексті міжнародної безпеки» [51]. У документі віталася ефективна робота попередньої групи урядових експертів та містилося прохання про те, щоб четверта група урядових експертів розпочала свою роботу у 2014 р. у розширеному складі за участю представників 20 країн. На відміну від попередньої групи, завдання нової групи урядових експертів були більш конкретними: ключовим пунктом порядку денного було не вивчення всього спектру загроз у галузі міжнародної інформаційної безпеки, а скоріше

вивчення проблем використання ІКТ у конфліктах та застосування міжнародного права до інформаційної сфери.

Незважаючи на гострі розбіжності, що супроводжували обговорення у рамках четвертої групи урядових експертів, учасники групи подали підсумковий звіт 26 червня 2015 р. Доповідь включала інформацію, що декларує ідею розвитку форм і засобів боротьби з кібератаками і необхідність регулювання конфліктів в інформаційному просторі. Для держав, наприклад, у зв'язку з цим орієнтиром для врегулювання конфліктів виявилися загальновизнані принципи міжнародного права при використанні ІКТ [7, с. 196].

Щодо цього держави були гарантами безпеки свого інформаційного простору та несли відповідальність за запобігання його використанню іншими суб'єктами з метою вчинення протиправних дій. У документі відображено елемент підходу до проблем міжнародної інформаційної безпеки, а саме необхідність обґрунтування будь-яких обвинувачень, які висуваються проти держави у вчиненні незаконних дій у сфері ІКТ. Щодо загальних питань застосування міжнародного права до інформаційного простору, експерти групи урядових експертів підтвердили можливість розробки нових правових норм з урахуванням специфіки технологій.

Крім того, у підсумковій доповіді було намічено перспективні галузі для подальшої роботи, які включали колективну та індивідуальну розробку державами концепцій забезпечення міжнародного миру та безпеки при використанні ІКТ на правовому, технічному та політичному рівнях, а також розширення співробітництва на регіональному та багатосторонньому рівнях для сприяння загальній згоді у питаннях у сфері ІКТ.

Таким чином, держави потребують розробки концептуальних програм інформаційної безпеки, певної угоди на регіональному рівні. Тим не менш, країни намагаються проектувати власне бачення у вирішенні питань інформаційної безпеки на інтеграційні об'єднання більш високого порядку,

такі як Організація Об'єднаних Націй, для пропозиції нових моделей міжнародного законодавства в цифровій сфері.

Сучасний стан міждержавної системи називають політичною нестабільністю. Характерними рисами такого стану вважають відсутність з часів Холодної війни будь-якого всеосяжного міжнародного договору, який закріплює новий світовий правопорядок. За цей період не було створено жодного нового міжнародного інституту для його підтримки. Існуючі міжнародні інституції, такі як ООН, НАТО, СОТ у нових умовах поступово втрачають свою ефективність [7, с. 196].

Поступово формуються певні тенденції розвитку сучасних міжнародних відносин, які безпосередньо впливають на стан міжнародної безпеки. По-перше, посилюється фактор дестабілізації в останні 15-20 років через перерозподіл сил у світі. По-друге, Азія зазнає небувалого піднесення, наслідком якого є розморожування старих або поява нових конфліктів: Японії – з сусідами, Китаю – з Індією, сунітських монархій – з Іраном тощо.

По-третє, складається тривожна ситуація в системі міжнародної безпеки, пов'язана з формуванням зворотних відцентрових напрямків розвитку у військово-технічній сфері, обумовлена виходом США з Договору з протиракетної оборони (2003 р.), а потім – з ДРСМД (2019 р.). Згодом балістична ракета середньої дальності та наземного базування, випробувана 12 грудня 2019 р. у США, пролетіла понад 500 км. В результаті починає руйнуватися основа колишнього режиму нерозповсюдження такої зброї [7, с. 197].

Ще одним проявом кризи міжнародних відносин стає втрата свого впливу і значущості багатьма глобальними і регіональними міжнародними інститутами як у сфері економіки, так і безпеки. Усі названі вище проблеми та протиріччя викликають загострення відносин та протистояння в ідеологічній сфері, посилення ціннісних розбіжностей, інформаційні війни.

Тим не менше, поки існує зазначений перелік проблем, кількість злочинів в інформаційній сфері невпинно зростає, набуваючи нових форм

свого прояву. Поодинокі злочини можуть носити системний характер. Яскравим прикладом цього є глобальна атака на SolarWinds, що сталася 13 грудня 2020 р. Її результатами виявились системні проблеми в інформаційному забезпеченні як міністерств Сполучених Штатів Америки, так і великих компаній приватного сектору. Було зламано понад 16 тисяч комп'ютерних систем. Все, що сталося, є результатом кібератаки на SolarWinds. Серед таких подій діагностують проблему того, що міжнародне співтовариство не здатне до регулювання подібних проблем [10, с. 17].

Аналізуючи міжнародні документи, статті, статистику та конкретні події, варто виділити ключові проблеми, пов'язані зі специфікою міжнародної інформаційної безпеки:

1. Проблема ситуації, коли інформаційні ресурси опиняються залежно друг від друга. Подібне становище дуже точно описує технологія «блокчейну». У разі виникнення проблем у певному секторі інформаційних ресурсів, під загрозу можуть потрапити суміжні йому. Цей аспект сигналізує про необхідність поліпшення рівня кібербезпеки як з боку державних структур, так і сектора НУО.

2. Збільшення числа кібератак та неможливість держави у їх врегулюванні. Наприклад, цей аспект досить докладно посилаються дослідники, які брали участь у створенні доповіді Всесвітнього економічного форуму, присвяченого проблемам глобального характеру. Крім іншого, в ньому постулюється ідея відсутності досвіду у державних структур у регулюванні питань кібератак, а як наслідок питань переслідування відповідальних за них людей.

3. Аспекти, пов'язані зі слабким вивченням з боку наукового співтовариства, 5-G зв'язку. Відсутність якісних досліджень, пов'язаних з уразливістю нових технологій, призводять до того, що зловмисники, користуючись цими вразливістю, застосовують їх у власних інтересах.

4. Як було з'ясовано нами раніше, питання доступності технологій інформаційного штибу різним країнам. Менш підготовлені до різних форм

кібератак держави стають ключовими цілями із боку злочинців. Відсутність солідарного погляду держав щодо питань забезпечення інформаційної безпеки пов'язані з відсутністю закріплених нормативних правил і дій щодо такого роду явищ. Як наслідок, проблеми інформаційної кіберзлочинності набувають спекулятивного характеру на міжнародному рівні [10, с. 17].

Для вирішення нагальних проблем, що визначають міжнародно-правове регулювання та співробітництво держав на глобальному рівні в інформаційній сфері, слід уважно ставитися до здійснення таких дій, як:

1. Сприяння у співпраці держав, національних структур, організацій комерційного спрямування та наукових об'єднань у питаннях забезпечення кібербезпеки.

2. Розробка та дотримання міжнародних інститутів у єдиному напрямку у питаннях визначення ключових проблем в інформаційній сфері.

3. Створення єдиного міжнародно-правового акта, що є свого роду згодою думок різних сторін за принципами поваги державного суверенітету, що включає концептуальний апарат, цілі, завдання, види загроз, а також положення про відповідальність держав у міжнародному інформаційному просторі.

4. Здійснення спільних ініціатив у галузі наукового вивчення питань інформаційної безпеки та обмін досвідом різними державами.

5. Створення ефективного механізму протидії інформаційним загрозам з урахуванням єдиного документа. Створення єдиних правил, визнання більшістю держав, створить ефективний механізм забезпечення міжнародної інформаційної безпеки [10, с. 18].

Дотримуючись ключових положень даних нормативно-правових актів, важливо зазначити, що вони визначають заборону використання комунікаційних структур та технологій в екстремістських та злочинних цілях. При цьому на глобальному рівні це питання потребує більш ретельної та переконливої артикуляції.

Виходячи з досвіду взаємодії держав у сфері забезпечення глобальної інформаційної безпеки, ми можемо виділити перелік можливих рішень, здатних сприяти подоланню зазначеної глобальної проблеми, серед них:

1. Закріплення єдиного акта, що закріплює міжнародні норми для врегулювання міжнародних ситуацій, та створення єдиної концепції міжнародної інформаційної безпеки.

2. Нарощування досвіду у кіберпросторі. Профілактичні заходи для програм-кібератак, а саме: визначення відсотка загроз, резервне копіювання ІТ-ресурсів та даних, забезпечення безперервності операцій при збоях у роботі комп'ютерних систем, а також навчання організацій реалістичним кібер-відповідям. Навчання дипломованих фахівців у галузі кібер-злочинів, які зможуть у розумні терміни виявляти злочинців, а також захищати дані міжнародних організацій та своїх країн.

3. Співробітництво у сфері доказів та переслідування кібер-злочинців, щоб зменшити розрив між державами. Таким чином, дотримуючись правильного курсу у питанні міжнародної інформаційної безпеки, ми зможемо зміцнити безпеку міжнародних організацій, самих країн і, звичайно, громадян, оскільки в нашому світі все взаємопов'язане [10, с. 18].

Глобальний і регіональний підхід у зв'язку з цим передбачає або прийняття єдиної системи вирішення проблем інформаційної безпеки на міжнародному рівні, або вдосконалення систем на національному рівні. Зважаючи на те, що інформаційний простір має глобальний характер, виникає явна необхідність вжиття міжнародних заходів щодо забезпечення його безпеки, одночасно й удосконалення механізмів правового регулювання на міжнародному рівні.

На регулювання питань міжнародної інформаційної безпеки спрямована увага багатьох міжнародних організацій, серед яких: Організація Об'єднаних Націй, Організація Договору про колективну безпеку, НАТО, а також Шанхайська організація співробітництва та інші. Діяльність міжнародних організацій надає консультативні механізми, а також дозволяє об'єднати

зусилля країн-членів міжнародного співтовариства у справі протидії глобальним та універсальним інформаційним загрозам [16, с. 43].

Отже, в означених умовах та обставинах дуже важливо розробити з урахуванням успішного досвіду країн-лідерів цілісний кодифікаційний нормативно-правовий акт, який би повноцінно охопив різні аспекти формування державної політики у сфері національної безпеки з урахуванням сучасного розвитку міжнародних відносин та міжнародного права в даній сфері, а також визначив конкретний інструментарій її реалізації. Глобальний підхід, у зв'язку з цим виявляється більш релевантним по відношенню до регіонального в силу того, що такий документ дозволить підвести нормативно-правову основу діяльності різних суб'єктів, у тому числі держави, але в першу чергу людини і громадянина, у сфері забезпечення різних рівнів інформаційної безпеки суспільства.

Висновки до другого розділу

У другому розділі ми виявили, що забезпечення інформаційної безпеки передбачає насамперед правильне визначення загроз безпеки відповідного суб'єкта, зокрема загроз державним органам виконавчої влади в інформаційній сфері, а також адекватний вибір та застосування адекватних засобів захисту від цих загроз, що може бути досягнуто лише комплексним використанням засобів захисту по кожному виду. загроз у рамках єдиної державної політики.

На регулювання питань міжнародної інформаційної безпеки спрямована увага багатьох міжнародних організацій, серед яких: Організація Об'єднаних Націй, Організація Договору про колективну безпеку, НАТО, а також Шанхайська організація співробітництва та інші. Діяльність міжнародних організацій надає консультативні механізми, а також дозволяє об'єднати зусилля країн-членів міжнародного співтовариства у протидії глобальним та універсальним інформаційним загрозам.

РОЗДІЛ 3. АКТУАЛЬНИЙ СТАН МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Глобальні військово-політичні проблеми міжнародної інформаційної безпеки

Зміни в політичній, економічній та соціально-культурній сферах у XXI ст. все більше залежать від прискореного розвитку нових інформаційно-комунікаційних технологій (ІКТ), під якими розуміються процеси та методи взаємодії з інформацією, що здійснюються із застосуванням пристроїв обчислювальної техніки та засобів телекомунікації.

В умовах сучасної четвертої індустріальної революції, що поєднує можливості промислового виробництва, інформаційних технологій, а також інтернету речей та послуг, індекс конкурентоспроможності економіки держав має високий рівень кореляції з індексом розвитку ІКТ [55]. А за оцінками Бостонської консалтингової групи (The Boston Consulting Group), однією з лідерів у галузі аналітики економіки та управлінського консалтингу, вплив Інтернету на ефективність діяльності компаній вищий, ніж будь-яких інших технологій з часів попередньої промислової революції .

Таким чином, розвиток ІКТ-засобів веде до проривних результатів не лише у віртуальному, а й у реальному, фізичному просторі. Ймовірно, тому сьогодні точиться жорстка боротьба за ролі в цій революції. Однак разом із унікальними можливостями ІКТ несуть і глобальні загрози. Інформаційні диверсії у ІКТ просторі стали новим знаряддям недержавних колективних та індивідуальних суб'єктів.

Крім того, інформаційні методи перетворюються на важливий елемент військового потенціалу держав, що доповнює, а іноді й замінює звичайні військові засоби. ІКТ можуть стати детонатором розв'язання міждержавного військового конфлікту, а кібервійни одних держав проти інших можуть виявитися не менш руйнівними, ніж традиційні [59].

Жодна країна у світі не може вважати себе захищеною від транскордонних інформаційних загроз і не в змозі вирішити проблеми інформаційної безпеки самотужки. Незважаючи на розбіжності між державами в ІКТ сфері, стрімке наростання загроз робить інформаційний простір не лише плацдармом для конфлікту, а й територією необхідної та неминучої співпраці.

Проте процес вироблення режиму забезпечення міжнародної інформаційної безпеки іде повільніше наростання загроз. Пошук компромісу під час переговорів на багатосторонній основі – єдиний спосіб мінімізувати загрози у цій сфері. А для цього треба прийти до спільного розуміння існуючих глобальних проблем [39].

Таким чином, необхідність класифікації ІКТ-загроз, що є ознаками наявності цих проблем, є одним із найважливіших, зазначених у документах ООН, але поки що не реалізованих завдань. Нині існують різні варіанти класифікації, які означено у національних нормативно-правових базах країн і організацій. Однак жоден із них поки що не став загальноприйнятим та задовольняючим інтереси усіх зацікавлених країн. Тому значимість постійного моніторингу та дослідження шкідливих інформаційних технологій неухильно зростає.

Однією з найнебезпечніших загроз міжнародній інформаційній безпеці є застосування інформаційної зброї у військово-політичних цілях для здійснення ворожих дій та актів агресії. Важливими також є загрози деструктивного впливу ІКТ на елементи критично важливих об'єктів державної інфраструктури; втручання у внутрішні справи суверенної держави, порушення суспільної стабільності, розпалювання міжетнічної, міжнаціональної ворожнечі за допомогою ІКТ.

Наявність цих небезпек становить загрозу міжнародному порядку, а отже вимагає негайного пошуку додаткових механізмів міжнародного управління. Одним із перших таких механізмів можуть стати Правила поведінки держав при забезпеченні міжнародної інформаційної безпеки.

Інформаційні операції у світі надають унікальні можливості створення деструктивного ефекту. Військові засоби, що сприяють проведенню цих операцій, включають стратегічні комунікації, міжвідомчі координаційні групи, дії у кіберпросторі та у космосі, підтримку інформації, розвідку, спеціальні технічні процедури тощо [46, с. 13].

Безперечним світовим лідером у цій сфері протягом багатьох років є США. За висловом відомого американського політолога Дж. Ная, «та країна, яка очолить інформаційну революцію, і матиме більшу силу порівняно з усіма іншими країнами» [50].

У цьому стратегія досягнення інформаційної переваги, під якою у США розуміється здатність збирати, обробляти та поширювати безперервний потік інформації, позбавляючи супротивника можливості здійснювати подібні дії, удосконалюється вже кілька десятиліть, що знайшло відображення у доктринальних документах та у практиці застосування інформаційних операцій. Така ситуація несе додаткові ризики, вона пов'язана з проблемою забезпечення стратегічної стабільності. А тому потребує особливої уваги фахівців.

Одна з найважливіших актуальних тенденцій пов'язана з тим, що захищеність ІКТ-систем має стратегічне значення для більшості країн світу. Ці системи стали важливим чинником забезпечення суверенітету, обороноздатності та безпеки держави. При цьому йдеться сьогодні про розвиток так званих інформаційних озброєнь.

За деякими оцінками, вже більше 30 держав мають наступальну кібернетичну зброю (кіберзброю). ІКТ можуть спровокувати розв'язання міждержавного військового конфлікту насамперед через можливість невідповідного використання методів реагування на загрози та атаки: постраждала сторона може застосувати у відповідь реальну зброю. З іншого боку, конфлікт може виникнути помилково, адже нині відсутня універсальна методологія ідентифікації порушників, не вироблено критерії віднесення

кібератак до збройного нападу, не сформовано універсальних принципів розслідування інцидентів.

На сьогоднішній день створено широкий спектр ІКТ-засобів для застосування у військовій галузі. Зокрема, серед таких:

- боротьба із системами управління та контролю – військова стратегія із застосуванням інформаційного середовища на полі бою для фізичної руйнації командної структури супротивника;
- розвідувальне протистояння – наступальні та оборонні операції за допомогою автоматизованих систем, які, у свою чергу, є потенційними об'єктами кібератак;
- електронне протиборство – військові дії з використанням електромагнітної та спрямованої енергії для контролю противника, які складаються з трьох підрозділів: електронна атака, електронний захист та підтримка електронного протиборства;
- військові засоби, що сприяють проведенню інформаційних операцій, зокрема, включають стратегічні комунікації, втручання у кіберпросторі та космосі, військову підтримку інформації, розвідку, спільні операції електромагнітного спектру тощо [47].

Пов'язані з цими можливостями проблеми можна зарахувати до різних елементів військової організації та інфраструктури. Але найважливішим, безумовно, є блок ІКТ-загроз у сфері ядерної зброї (табл. 3.1).

Таблиця 3.1.

Стратегічні ядерні озброєння: деякі ІКТ-уразливості та потенційні наслідки

ІКТ-уразливості та потенційні наслідки		
Точка вразливості	**Результат атаки**	**Наслідки**
Радари і супутники	Імітація ядерної атаки	Ядерний удар

Система бойового управління і зв’язку	Вплив на різні канали зв’язку: порушення чи відключення	Ядерний удар або збій/втрата управління ядерною зброєю
Інформаційно-ударна техносфера	Шкідливі програми у різних елементах системи	Збій або втрата управління
Системи безпеки і розвідки	Відключення або фізична шкода	Викрадення руйнування, модифікація даних

Сьогодні існують різні думки щодо ймовірності та наслідків шкідливого впливу ІКТ-засобів на систему командування, управління та контролю над ядерною зброєю: від повного заперечення до доказів різкого збільшення такої ймовірності.

Однак, і в науці взагалі, і у військовій стратегії, зокрема, необхідно сходити з найгірших варіантів розвитку подій. Отже, ця проблема має перебувати у фокусі уваги вчених та практиків, насамперед із держав – власників ядерної зброї. При цьому не йдеться про необхідність докорінно змінювати основні принципи управління. ІКТ-загрози загострюють, ускладнюють, поглиблюють, посилюють та видозмінюють ті проблеми, які завжди існували у забезпеченні безпеки ядерного озброєння [46, с. 15].

Загрози, що створюють проблему застосування ІКТ у військово-політичних цілях для здійснення ворожих дій та актів агресії, ознаки наявності та можливості здійснення цих загроз представлені у Додатку А.

До критично важливих об'єктів інфраструктури держави (КІ) відносять системи та засоби, які настільки життєво важливі для країни, що порушення їхньої роботи або знищення надає незворотний негативний вплив на національну та економічну безпеку, охорону здоров'я, правопорядок тощо. При цьому під безпекою КІ розуміється захищеність від загроз, що

реалізуються через застосування спеціальних інформаційних технологій для руйнування або для неприпустимого використання цих об'єктів.

Навіть якщо ці об'єкти не підключені безпосередньо до Інтернету, пристрої автоматизованої системи управління технологічним процесом (АСУ ТП), які використовуються для дистанційного контролю за захищеними комунікаційними лініями, можуть бути зламані в результаті атаки на інші об'єкти, де функціонують АСУ ТП. Ізоляція мережі від зовнішніх систем, яка вважалася непорушною вимогою 10-15 років тому, більше не розглядається як ефективний захисний захід, адже стала невигідною економічно та важко реалізованою на практиці. Тому загроза великомасштабної комплексної атаки на критично важливу інфраструктуру більш ніж реальна та прискорено зростає [39].

Сьогодні вже понад 30 країн мають програмне забезпечення (ПЗ) для нападу на об'єкти КІ. У цьому показник небезпеки для АСУ ТП нині оцінюється фахівцями як критичний чи високий. Шкідливі програми розробляються нині у багатьох країнах, проте 83% всіх майданчиків, що використовують їх поширення, розташовані лише у 10 державах.

Лідером цього рейтингу є США, де знаходиться чверть джерел зараження. Цілями таких «шкідливих даних» можуть бути органи державної влади, банки, супутникові, нафтогазові та транспортні системи, електро- та атомні станції, комунікаційні системи, порти, аеропорти, військові об'єкти, що може призвести до страшних наслідків як на державному, так і на глобальному рівні.

Таким чином, подібні шкідливі програми являють собою перспективну стратегічну зброю, а складність обладнання, що зростає, веде до зростання ймовірності помилок і вразливостей, що може бути використане противником.

Зазначимо деякі загальносвітові тенденції, які збільшують загрози для таких об'єктів:

- використання особистих мобільних пристроїв на критично важливих об'єктах;

- перехід на цифрові системи управління виробничими та технологічними процесами на таких об'єктах;
- підключення офісних та промислових корпоративних мереж об'єктів інфраструктури до Інтернету;
- складність трансконтинентальних ланцюжків постачання програмного забезпечення систем управління виробничими та технологічними процесами [1, с. 63].

Ці тенденції стосуються всіх об'єктів КІ. Але найбільше занепокоєння викликають загрози системі командування та управління ядерною зброєю. Однією з найсерйозніших загроз у військовій ядерній сфері є можливість впливу ІКТ на зростання ймовірності несанкціонованого запуску балістичних ракет (БР), а також прийняття рішення про застосування ядерної зброї [53, с. 17].

Завдання захисту БР від несанкціонованих пусків виникло з створення перших ракет. Вона щоразу вирішується заново при створенні нових БР, постановці їх на чергування, підготовці та проведенні випробувальних, навчально-бойових та контрольно-бойових пусків.

Незважаючи на те, що країни завжди приділяють цьому велику увагу, за десятиліття існування ядерної зброї були випадки технічних збоїв та людських помилок, які могли б спровокувати ядерний запуск. Уникнути такої ситуації у майбутньому буде складніше, адже проблема зниження ймовірності випадкового запуску стоятиме гостро в міру переходу військ стратегічного призначення в різних країнах на цифрові технології передачі інформації.

Ця загроза продиктована можливістю отримання неправдивої інформації від систем попередження про ракетний напад (СПРН) про запуск БР з боку супротивника. У зв'язку з тим, що кібератаки стають все більш витонченими, зростає ймовірність обходу хакерами існуючої системи захисту для надсилання сигналу про запуск ракет.

Крім того, можуть пошкоджені або зруйновані канали комунікацій, створені перешкоди в системі управління збройними, в тому числі, ядерними,

силами, а також знижена впевненість військових, які приймають рішення, у працездатності систем управління, командування та контролю. Таким чином, у кризовій ситуації ІКТ-напади можуть негативно вплинути на ухвалення рішення про дії у відповідь [4, с. 38].

Загрози, що створюють проблему забезпечення ІКТ безпеки об'єктів військово-промислового комплексу (ВПК), ознаки наявності та можливості здійснення цих загроз представлені у Додатку Б.

Відмова від продовження діалогу з проблем міжнародної інформаційної безпеки може призвести до тяжких наслідків. З урахуванням наростання загроз у сфері міжнародної інформаційної безпеки для того, щоб зробити інформаційний простір більш стійким і безпечним, необхідно вирішити цілий комплекс дуже складних завдань.

Вважаємо доцільними такі кроки:

1. Продовжувати багатосторонні переговори щодо обмеження та скорочення стратегічних ядерних озброєнь;

2. Включати найважливіші спеціальні питання інформаційної безпеки у переговори щодо ядерних озброєнь та стратегічної стабільності на двосторонній та багатосторонній основі;

3. Розробляти конкретні заходи щодо зміцнення довіри (зокрема, обмін даними про інформаційні загрози, практичне міждержавне співробітництво);

4. Державам – власникам ядерної зброї:

- удосконалювати інформаційну безпеку критично важливої державної інфраструктури, зокрема військових об'єктів;
- підвищувати ефективність підготовки персоналу (забезпечувати уніфікацію фахівців, їхнє правильне територіальне розосередження, дублювання обробки даних, вузьку спеціалізацію програмного забезпечення тощо);
- зміцнювати бойову стійкість збройних сил (стратегічних сил стримування) в умовах можливого виходу з ладу об'єктів критично важливої державної інфраструктури.

5. Розширювати спільні міжнародні дослідницькі проекти за участю науково-експертної спільноти для обговорення проблем організації партнерства у галузі міжнародної інформаційної безпеки;

6. Активізувати наукові дослідження щодо розробки теоретичних, методологічних та практичних підходів до вирішення проблеми стратегічної стабільності;

7. Вдосконалювати ефективність системи сертифікації імпортних програмних засобів та елементної бази, що плануються для застосування на критично важливих для оборони та безпеки країни об'єктах, а також систему забезпечення інформаційної безпеки сучасних комп'ютерних технологій, що розробляються, в умовах розширення імпортозаміщення програмно-апаратних компонентів програмного забезпечення та обладнання з метою переходу в доступній для огляду перспективі на повністю вітчизняну елементну базу.

8. Створювати під егідою ООН міжнародний режим контролю за шкідливим ІКТ:

- прийняття правил відповідальної поведінки держав у галузі забезпечення міжнародної інформаційної безпеки;
- розробка міжнародних норм щодо засобів та методів запобігання та усунення кібер-конфліктів;
- обмеження та/або відмова від наступальних ІКТ можливостей;
- заборона на ІКТ-атаки на конкретні об'єкти;
- контроль за поширенням ІКТ-озброєнь.

3.2. Роль і місце інформаційної безпеки у контексті викликів і загроз національній безпеці

Із розвитком інформаційних технологій і інформаційного суспільства за умов глобалізації постала низка невирішених питань та проблем, суттєво

змінилася характеристика викликів та загроз цивілізації. Національна безпека держави суттєво залежить від забезпечення інформаційної безпеки, і під час технічного прогресу така залежність лише посилюється.

За Законом України «Про Концепцію Національної програми інформатизації» інформаційна безпека є невід'ємною частиною оборонної, економічної, політичної та інших складників національної безпеки [25]. Вона забезпечує захищеність життєво важливих інтересів особи, суспільства й держави від внутрішніх та зовнішніх загроз. Таким чином, національна безпека залежить від змісту національно-державних інтересів і характеризує стан країни, за якого їй не загрожує небезпека війни чи інших посягань на суверенний розвиток.

Національна безпека України – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу й інших національних інтересів України від реальних і потенційних загроз [26].

Серед основних компонентів національної безпеки виділяють військову, економічну, соціальну, екологічну, інформаційну безпеку. Сама по собі національна безпека є геополітичним аспектом безпеки загалом, цілий комплекс питань фізичного виживання держави, захисту й збереження його суверенітету та територіальної цілісності.

Наразі проблема інформаційної безпеки є досить важливою, адже суттєво зросла роль збирання, обробки й поширення інформації, передусім збільшилася кількість суб'єктів інформаційних відносин та споживачів інформації. Інформації все більш вагома роль в процесі життєдіяльності людини.

Інформаційна безпека суспільства й держави визначається мірою їх захищеності, а тому й стійкістю основних сфер життєдіяльності до небезпечних, дестабілізуючих, деструктивних інформаційних дій, що притискають інтереси країни [19, с. 65].

Зазначимо, що на сьогодні немає чітко вираженої організованої системи вироблення і реалізації єдиної державної політики в галузі забезпечення інформаційної безпеки, що визначає пріоритети розвитку єдиного інформаційного простору. Серед причин, які зумовлюють незадовільний стан в галузі забезпечення інформаційної безпеки такі:

- безсистемний розвиток законодавства, який регулює інформаційну сферу;
- низький рівень правової й інформаційної культури громадян та суспільства загалом;
- незадовільне фінансування діяльності з забезпечення інформаційної безпеки;
- недостатній розвиток інформаційних і комунікаційних технологій в сфері державного управління, неготовність органів державної влади застосовувати ефективні технології управління та організацію взаємодії із громадянами й господарськими суб'єктами;
- недостатній рівень підготовки кадрів в сфері утворення й застосування інформаційних та комунікаційних технологій [19, с. 67].

Погоджуємося зі словами В. Торічного стосовно того, що інформаційна безпека в сфері державно-управлінських відносин повинна розглядатись як сукупність взаємодіючих та взаємопов'язаних компонентів, передусім:

- загрози життєво важливим інтересам суспільства в сфері інформаційної безпеки, а також небезпеки, виклики і ризики;
- життєво важливі інтереси суспільства, держави і особистості, які підлягають інформаційному захисту;
- основні заходи, які проводяться суб'єктами механізму держави, представниками громадянського суспільства із нейтралізації загроз, небезпек та ризиків в сфері інформаційної безпеки [33, с. 114].

Оглядаючись на це слід зважати на те, що глобальний інформаційний простір формується та розвивається доволі стрімко, у інформаційній сфері

людства відбуваються революційні зміни й трансформації, що сприяють активізації нових глобальних викликів і загроз, які становлять реальну небезпеку для людства і міжнародного правопорядку, а наслідки застосування сучасної інформаційної зброї можуть зіставитися з використанням зброї масового ураження [21, с. 150].

В. Копанчук виділяє такі загрози національній безпеці на рівні інформаційної сфери, властиві Україні:

- недосконалість нормативно-правової бази, якою унормовано сферу інформаційної безпеки на галузевому рівні;
- недостатній рівень розвиненості інформаційно-телекомунікаційної інфраструктури національного масштабу;
- непослідовність державної політики із забезпечення інформаційної безпеки, побудованої на принципах системності, комплексності та ефективності, перевантажена і неефективна система державного управління та регулювання у зазначеній сфері;
- відсутність дієвих механізмів реалізації операцій інформаційно-психологічного типу, системи, яка забезпечує активний кіберзахист інформаційного простору країни, та надає асиметричну відповідь агресору;
- інформаційна війна інших держав проти України;
- зосередження ЗМІ загальнодержавного рівня у руках окремих груп стейкхолдерів;
- дезінформація громадян України і використання проти них технологій інформаційно-психологічного маніпулятивного характеру [13, с. 196-197].

За таких обставин досягнути оптимального функціонування національного інформаційного простору видається реальним завданням. Так, наразів Україні розробка загальнодержавних документів стратегічного

значення, дотичних до сфери забезпечення безпеки держави має орієнтуватися на таких трьох альтернативах, запропонованих О. Резніковою:

- зменшення негативних впливів загроз будь-якого характеру чи забезпечення швидкого відновлення системи публічного управління після надзвичайних й кризових явищ;
- пріоритетність превентивних чи реактивних заходів реагування держави на загрозу;
- пріоритетність заходів із забезпечення готовності та прогнозування загроз, ефективний кризовий менеджмент, нарощування безпекових спроможностей [30, с. 113].

Основні принципи та зміст діяльності з забезпечення безпеки наведено у Законі України «Про національну безпеку». Тут визначено і розмежовано повноваження державних органів в сфері національної безпеки та оборони, створено основу для інтеграції політики і процедур органів державної влади, інших державних органів, функції яких зачіпають національну безпеку та оборону, сили безпеки та сили оборони, визначено систему командування, контролю і координації операцій сил безпеки й сил оборони, запроваджено всеосяжний підхід до планування в сферах національної безпеки та оборони, забезпечуючи таким способом демократичний цивільний контроль за органами і утворенням сектору безпеки і оборони [26].

Головними принципами забезпечення безпеки є: дотримання та захист прав і свобод людини й громадянина; законність; системність та комплексність застосування публічними органами влади політичних, організаційних, соціально-економічних, інформаційних, правових й інших заходів забезпечення безпеки; пріоритет запобіжних заходів для забезпечення безпеки; взаємодія органів державної влади із громадськими об'єднаннями, міжнародними організаціями та громадянами для забезпечення безпеки.

Діяльність держави із забезпечення безпеки включає:

- прогнозування, виявлення, аналіз та оцінювання загроз безпеки;

- визначення головних напрямів державної політики та стратегічне планування в сфері забезпечення безпеки;
- правове регулювання в сфері забезпечення безпеки;
- розробка та застосування комплексу оперативних та довготривалих заходів із виявлення, попередження та усунення загроз безпеки, локалізації та нейтралізації наслідків їх прояву;
- застосування спеціальних економічних заходів задля забезпечення безпеки;
- розробку, виробництво й запровадження сучасного вигляду озброєння, військової та спеціальної техніки, техніки подвійного і цивільного призначення для забезпечення безпеки;
- організація наукової діяльності в сфері забезпечення безпеки;
- координація діяльності регіональних органів державної влади, органів державної влади суб'єктів України, органів місцевого самоврядування в сфері забезпечення безпеки;
- фінансування витрат на забезпечення безпеки, контроль за цільовим витрачанням виділених засобів;
- міжнародна співпраця в сфері забезпечення безпеки;
- здійснення інших заходів в сфері забезпечення безпеки за законодавством України.

Так, в Законі України «Про Національну програму інформатизації» визначається, що основною метою Національної програми інформатизації є створення необхідних умов задля забезпечення громадян і суспільства своєчасною, достовірною і повною інформацією завдяки широкому використанню інформаційних технологій, забезпеченню інформаційної безпеки держави [27].

Отже, категорія «безпека» розглядається як поняття, що відображає стан об'єкта у системі його зв'язків із точки зору здатності до самовиживання за умов внутрішніх і зовнішніх загроз, а також за умов дій непередбачених і

складно прогнозованих факторів. Національна безпека України складається з сукупності складників, що мають забезпечувати збалансовані інтереси особи, суспільства й держави.

До таких складників належить безпека у міжнародній економічній, військовій, внутрішньополітичній, інформаційній, соціальній, екологічній й інших сферах. Водночас, одна із ключових ролей в системі забезпечення національної безпеки відведено економічному й інформаційному складникам.

Базовим документом де визначено зміст національних інтересів України у інформаційній сфері, є Доктрина інформаційної безпеки України [28]. Правовою основою доктрини є Конституція України [19], закони України, Стратегія національної безпеки України, затверджена Указом Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 р. «Про Стратегію національної безпеки України» [29], а також міжнародні договори, згода на обов'язковість яких надано Верховною Радою України.

Стратегія національної безпеки України є документом, обов'язковим для виконання, та основою для розробки конкретних програм відповідно до державної політики національної безпеки [28]. В доктрині інформаційної безпеки закріплено актуальні загрози національним інтересам і національній безпеці України у інформаційній сфері.

Отже, національна безпека нерозривно пов'язана із діяльністю держави. Тільки вона спираючись на свій апарат, владні органи, діяльність яких є жорстко обмеженою та підкріпленою належними правовими актами, може забезпечити спокій громадян, утворити сприятливі умови для їх життя та діяльності.

Жодні інші соціальні сили не зможуть виконати це завдання. Забезпечення власної безпеки і своїх громадян є одним із головних завдань держави. Успішний розвиток України як суверенної держави неможливий без забезпечення її національної інформаційної безпеки.

Зазначимо основні завдання із забезпечення інформаційної безпеки як складника національної безпеки держави, що вимагають розв'язання:

1. Необхідність нормативно-правового регулювання із протидії використання інформаційних технологій, що загрожують інтересам держави.

2. Необхідність утворення економічних передумов задля розвитку національних інформаційних ресурсів й інфраструктури, впровадження новітніх технологій у інформаційну сферу.

3. Необхідність вдосконалення виробництва вітчизняних інформаційних технологій, що розробляються, запровадження вітчизняних розробок, підвищення ефективності наукових досліджень і якості освіти в секторі інформаційних технологій.

Одним з показників ефективності національного законодавства у зазначеній сфері є рейтингування країн за критеріями оцінювання їх спроможностей в відповідній галузі. Провідними та загальновизнаними рейтингами сфери інформаційної і кібернетичної безпеки є Global Cybersecurity Index [40] і National Cyber Security Index [48].

Глобальний індекс кібербезпеки (Global Cybersecurity Index – GCI), перша редакція якого була опублікована в 2015 р., спрямовується на визначення сфер та напрямків кібербезпеки, які потребують подальшого вдосконалення державами, залученими до цієї ініціативи.

Отже, розробляються практичні рекомендації національного рівня із врахуванням регіональної і галузевої специфіки, що у сукупності справляють вплив на підвищення загальносвітового рівня кібербезпеки, поширення і запровадження передового досвіду, формування глобальної культури кібербезпеки та ін.

Сфера охоплення і структура GCI нормовані Резолюцією 130 [57], що нормативно закріплює посилення ролі та значущості Міжнародного союзу електрозв'язку (ITU) – спеціалізованої агенції ООН щодо ІКТ із питань зміцнення довіри і забезпечення належного рівня безпеки в застосуванні інформаційно-телекомунікаційних технологій за п'ятьма основними сферами:

правовою, технічною, організаційною, розвитком потенціалу, співробітництвом.

За даними GCI 2020 р. [40], Україна посіла 78 місце серед 194 країн, залучених до анкетування загалом, і 39 місце з 46 держав, що входять до європейського регіону (Додаток В).

Національний індекс кібербезпеки (National Cyber Security Index – NCSI) – це глобальний індекс, що у режимі реального часу вимірює готовність країн запобігати кіберзагрозам і управляти кіберінцидентами. Цей індекс сфокусовано на окремих аспектах кібербезпеки, які впроваджуються урядами на національних рівнях за чотирма сферами – чинного законодавства, сформованих інституцій, форматами співпраці, результатами.

Так, задля розробки оновленої редакції N08 було загалом вивчено стан кібербезпеки 163 країн світу за показниками ефективності законодавства в сфері кібербезпеки, управління кіберінцидентами, інформаційної безпеки, довірчих послуг, захисту персональних даних, боротьби з кіберзлочинністю тощо. За підсумками дослідження Україна посіла 24 місце із 163 проаналізованих країн (Додаток Г).

Крім того, в контексті викладеного вважаємо за необхідне навести дані про видатки Державного бюджету України 2022 р. на сферу захисту інформаційного простору (див. табл. 3.2), головний фокус якого спрямовано на підтримання економіки нашої держави за умов надзвичайних та кризових явищ.

Таблиця 3.2.

Видатки Державного бюджету України 2022 р. на сферу захисту інформаційного простору [24]

№	Показник	Сума (грн)
1	Інформаційно-аналітичне забезпечення координаційної діяльності в сфері національної безпеки й оборони	335126,3
2	Інформаційно-аналітичне забезпечення діяльності в сфері інформаційної безпеки України	53006,2
3	Модернізація цифрових інформаційно-аналітичних систем	50000
4	Електронне урядування	651524
5	Розвиток пріоритетних проектів у сфері інформаційних технологій	450000
6	Національна програма інформатизації	2205274,6
7	Збирання, обробка та розповсюдження офіційної інформаційної продукції	268543,9
8	Здійснення заходів в сфері захисту національного інформаційного простору	50000
	Усього	**4 063 475**

Показовим є той факт, що показник «здійснення заходів в сфері захисту національного інформаційного простору» для Міністерства культури й інформаційної політики України у розрізі видатків Державного бюджету України виник тільки в 2018 р., а за результатами аналізу їх розподілу впродовж п’ятирічного періоду встановлено, що він тяжіє до скорочення.

Проте інші показники, дотичні до сфери захисту інформаційного простору держави та відповідного організаційно-функціонального забезпечення публічного управління, що загалом сприяють зміцненню національної стійкості, залишаються сталими з невним збільшенням видатків на сферу національної безпеки й оборони.

Науковці говорять, що для імплементації будь-яких стратегічних планів і відповідних заходів із питань забезпечення безпеки у інформаційній сфері дуже важливим є налагодження тісного співробітництва і взаємодії між державою і суспільством. Такий формат здатний мати значні позитивні ефекти, а саме:

- для суспільства загалом – його активізація у аспекті забезпечення власної безпеки, підвищення рівня кібербезпеки, розвиток інститутів громадянського суспільства;
- для окремих індивідів – навички протидії інформаційним загрозам, медіаграмотність, цифрова компетентність;
- для приватного сектора – підвищення спроможностей в подоланні інформаційних загроз, корпоративної безпеки, налагодження ефективної комунікації;
- для інститутів громадянського суспільства – інструментарій долучення до процесів та процедур формування і реалізації державної політики в безпековій сфері, громадські ініціативи із впровадження інноваційних підходів до відповідної сфери державної політики;
- для органів публічної влади – одержання додаткових експертних консультацій, вивчення досвіду громадського сектора та міжнародних організацій, залучення інститутів громадянського суспільства безпосередньо до реалізації державної політики, моніторингу і аналізу її ефективності та ін. [23, с. 197-199].

Основоположними чинниками формування державної системи інформаційної безпеки повинні бути:

- законність;

- чітке розмежування повноважень;
- добровільність залучення стейкхолдерів;
- колегіальність управління системою;
- стабільність ядра системи;
- адаптивність до змін та умов функціонування;
- раціональне поєднання універсальності й диференціації механізмів забезпечення інформаційної безпеки;
- поетапність впровадження і забезпечення сталості як цієї підсистеми, так і усієї системи забезпечення національної безпеки держави, оскільки новітня дійсність суттєвою мірою актуалізує потребу й нагальність відповідної державної політики [33, с. 246-247].

Отже, проведене дослідження дає можливість зробити певні узагальнення і систематизувати основні підходи із забезпечення захисту інформаційного простору держави в Україні. Так, пріоритетними є:

- забезпечення спроможностей держави в сфері безпеки й оборони, передусім стосовно нейтралізації негативних інформаційних впливів, дестабілізуючих й деструктивних явищ, відповідної рішучої протидії;
- посилення здатності суб'єктів механізму держави щодо реалізації проактивного підходу, зокрема у аспекті імплементації превентивних заходів стосовно безпосередніх, опосередкованих, ймовірнісних загроз та належного на них реагування;
- проведення інформаційно-роз'яснювальної роботи серед різноманітних суспільних груп і окремих індивідів, представників суб'єктів механізму держави із питань надзвичайних і кризових ситуацій у контексті потенційних ризиків та загроз для національної безпеки держави загалом і її окремих компонентів.

Висновки до третього розділу

У третьому розділі встановлено, що відмова від продовження діалогу з проблем міжнародної інформаційної безпеки може призвести до тяжких наслідків. З урахуванням наростання загроз у сфері міжнародної інформаційної безпеки для того, щоб зробити інформаційний простір більш стійким і безпечним, необхідно вирішити цілий комплекс дуже складних завдань.

На сьогодні немає чітко вираженої організованої системи вироблення і реалізації єдиної державної політики в галузі забезпечення інформаційної безпеки, що визначає пріоритети розвитку єдиного інформаційного простору.

Національна безпека нерозривно пов'язана із діяльністю держави. Тільки вона спираючись на свій апарат, владні органи, діяльність яких є жорстко обмеженою та підкріпленою належними правовими актами, може забезпечити спокій громадян, утворити сприятливі умови для їх життя та діяльності. Україні варто приділяти особливу увагу національній інформаційній безпеці, адже вона є основою визначення найважливіших напрямків та принципів державної політики країни, життєво важливих інтересів особи, держави та суспільства.

ВИСНОВКИ

Нами висвітлено теоретичні засади формування та забезпечення міжнародної інформаційної безпеки. Під інформаційною безпекою розуміємо захищеність інформації та інфраструктури, що її підтримує, від випадкових або навмисних впливів природного або штучного характеру, що загрожують заподіянням шкоди власникам або користувачам цієї інформації та інфраструктури. Захист інформації – це комплекс заходів, спрямованих на забезпечення інформаційної безпеки. На практиці під цим розуміється підтримка цілісності, доступності та, якщо потрібно, конфіденційності інформації та ресурсів, що використовуються для введення, зберігання, обробки та передачі даних. Питання відповідальної поведінки держав у кіберпросторі нині доцільно врегулювати за допомогою норм м'якого права (зокрема резолюцій Генеральної Асамблеї ООН). Зазначені норми створюють орієнтири для поведінки держав у інформаційному просторі, сприяють формуванню норм міжнародного права у аналізованої області. Міжнародно-правове регулювання співробітництва держав у боротьбі зі злочинністю у сфері високих технологій на універсальному рівні в даний час не є достатнім. Практичні проблеми взаємодії компетентних органів з метою припинення, розкриття та розслідування таких злочинів можуть бути вирішені виключно укладанням міжнародного договору, який має закласти основи співробітництва в галузі надання міжнародно-правової допомоги у таких кримінальних справах, здійснення екстрадиції, а також гармонізації кримінального законодавства держав.

Охарактеризовано специфіку організації інформаційної безпеки органів державного управління. Безпека інформації як складова інформаційної безпеки органів виконавчої влади включає захист інформації та інформаційних ресурсів від несанкціонованого доступу, спотворення, знищення, встановлення режиму інформації залежно від її змісту, забезпечення захисту відомостей, що становлять державну таємницю, іншої

інформації обмеженого доступу. Забезпечення інформаційної безпеки передбачає насамперед правильне визначення загроз безпеки відповідного суб'єкта, зокрема загроз державним органам виконавчої влади в інформаційній сфері, а також адекватний вибір та застосування адекватних засобів захисту від цих загроз, що може бути досягнуто лише комплексним використанням засобів захисту по кожному виду загроз у рамках єдиної державної політики.

Досліджено політику міжнародних організацій з питань інформаційної безпеки. На регулювання питань міжнародної інформаційної безпеки спрямована увага багатьох міжнародних організацій, серед яких: Організація Об'єднаних Націй, Організація Договору про колективну безпеку, НАТО, а також Шанхайська організація співробітництва та інші. Діяльність міжнародних організацій надає консультативні механізми, а також дозволяє об'єднати зусилля країн-членів міжнародного співтовариства у протидії глобальним та універсальним інформаційним загрозам.

Проаналізовано глобальні військово-політичні проблеми міжнародної інформаційної безпеки. Однією з найнебезпечніших загроз міжнародній інформаційній безпеці є застосування інформаційної зброї у військово-політичних цілях для здійснення ворожих дій та актів агресії. Важливими також є загрози деструктивного впливу ІКТ на елементи критично важливих об'єктів державної інфраструктури; втручання у внутрішні справи суверенної держави, порушення суспільної стабільності, розпалювання міжетнічної, міжнаціональної ворожнечі за допомогою ІКТ. Наявність цих небезпек становить загрозу міжнародному порядку, а отже вимагає негайного пошуку додаткових механізмів міжнародного управління.

Виявлено роль і місце інформаційної безпеки у контексті викликів і загроз національній безпеці. Національна безпека нерозривно пов’язана із діяльністю держави. Тільки вона спираючись на свій апарат, владні органи, діяльність яких є жорстко обмеженою та підкріпленою належними правовими актами, може забезпечити спокій громадян, утворити сприятливі умови для їх життя та діяльності. Україні варто приділяти особливу увагу національній

інформаційній безпеці, адже вона є основою визначення найважливіших напрямків та принципів державної політики країни, життєво важливих інтересів особи, держави та суспільства. Однак, на сьогодні немає чітко вираженої організованої системи вироблення і реалізації єдиної державної політики в галузі забезпечення інформаційної безпеки, що визначає пріоритети розвитку єдиного інформаційного простору.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Архипов О.Є., Архипова Є.О. Положення про інформаційну безпеку в міжнародних стандартах. *Інформаційна безпека людини, суспільства, держави. науково-практ.журнал. Національна академія Служби безпеки України*. 2010. №2(4). С.62-65.
2. Архипов О.Є., Муратов О.Є. Про зміст та взаємозв'язок понять "інформаційна безпека" та "безпека інформації". *Актуальні проблеми управління інформаційною безпекою держави*: зб. матер. наук.-практ. конф., 17 березня 2010 р., м. Київ. К.: Наук.-вид. Відділ НА СБ України, 2010. С.185-187.
3. Богуш В.М., Юдін О.К. Інформаційна безпека держави. К.: МК-Пресс, 2005. 432 с.
4. Вавринчук М.П. Інформаційна безпека держави. *Правові засади організації та здійснення публічної влади* : зб. тез II Всеукр. наук.-практ. інтернет-конф. (м. Хмельницький, 2-8 трав. 2019 р.). Хмельницький : ХУУП, 2019. С. 37-40.
5. Василюк В.Я., Климчик С.О. Інформаційна безпека держави. К.: КНТ, Видавничий дім "Скіф", 2008. 136 с.
6. Войціховський А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В.Н. Каразіна. Сер.: Право*. 2020. Вип. 29. С. 281-288
7. Глобенко С. Інформаційний простір держави та проблеми забезпечення його захисту в Україні. *Науковий вісник: Державне управління*. 2023. №1 (13). С. 195–210.
8. Гончаренко О.М., Методологічні засади розробки нової редакції концепції національної безпеки України. *Національний інститут стратегічних досліджень Серія «Національна безпека»*. 2001. № 4. 56 с.
9. Громико І., Державна домінантність визначення інформаційної безпеки України в умовах протидії загрозам. *Право України*. 2008. № 8.

10. Дереко В. Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави*. 2015. № 2. С. 16-22.
11. Захаренко К. Теоретичні засади дослідження інформаційної безпеки. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2018. № 2(4). С. 107-116.
12. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. К.: КНТ, 2006. 280 с.
13. Копанчук В. О. Державна політика у сфері національної безпеки та охорони громадського порядку : дис. ... докт. держ. упр. : спец. 25.00.05. «Держ. упр. у сфері держ. безпеки та охорони гром. порядку» / НУЦЗУ. Харків, 2020. 375 с.
14. Кормич Б.А. Інформаційна безпека: організаційно-правові основи : Навч. посібник. К.: Кондор, 2008. 384 с.
15. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України: монографія. Одеса: Юридична література, 2003. 472 с.
16. Лужецький В.А., Войнович О.П., Дудатьєв А.В. Інформаційна безпека : Навч.посібник. Вінниця: УНІВЕРСУМ-Вінниця, 2009. 240 с.
17. Макаренко Є. А., Рижиков М. М., Ожеван М. А., Головченко В. І., Гондюл В. П. Міжнародна інформаційна безпека: Сучасні виклики та загрози. К.: Центр вільної преси. 2006. 916 с.
18. Марущак А.І. Концептуальні засади забезпечення безпеки інформаційного простору та інформаційних ресурсів держави. *Актуальні проблеми забезпечення інформаційної безпеки держави:* Зб. Матеріалів наук.-практ.конференції, Київ, 20 березня 2009 р. НА СБ України, Ін-т ЗізОД. К.: Наук.-вид. Відділ НА СБУ, 2009. С.19-24.
19. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Гельветика, 2017. 168 с.

20. Остроухов В. До проблеми забезпечення інформаційної безпеки України. *Політичний менеджмент*. 2008. № 4. С.135-141.

21. Пилипчук В. Г. Розвиток правової науки в інформаційній сфері : системні проблеми та пріоритети. *Право України*. 2013. No 9. С. 146-1б1

22. Правові засади інформаційної безпеки України [Текст] : монографія / Біленчук П.Д. [та ін.] ; за ред. П.Д. Біленчука. Харків, 2018. 289 с.

23. Прав Р. Ю. Механізми формування і реалізації політики державної безпеки в інформаційній сфері : дис. ... канд. держ. упр. : спец. 25.00.05 «Держ. упр. у сфері держ. безпеки та охорони гром. порядку» / МАУП. Київ, 2020. 263 с.

24. Про Державний бюджет України на 2022 рік : Закон України від 02.12.2021 р. № 1928-IX. Офіційний веб-портал парламенту України. URL : https://zakon.rada.gov.ua/laws/show/1928-20#Text

25. Про Концепцію Національної програми інформатизації: Закон України від 4 лют. 1998 р. № 75/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80.

26. Про національну безпеку України: Закон України від 21 черв. 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19.

27. Про Національну програму інформатизації: Закон України від 4 лют. 1998 р. № 74/ 98-ВР. URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.

28. Про рішення Ради національної безпеки і оборони України від 29 груд. 2016 р. «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лют. 2017 р. № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374.

29. Про рішення Ради національної безпеки і оборони України від 6 трав. 2015 р. «Про Стратегію національної безпеки України»: Указ Президента України від 26 трав. 2015 р. № 287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015.

30. Резнікова О. Національна стійкість в умовах мінливого безпекового середовища : монографія. Київ : НІСД, 2022. 456 с.
31. Степко О.М. Аналіз головних складових інформаційної безпеки держави. *Науковий вісник Інституту міжнародних відносин НАУ. Сер. : Економіка, право, політологія, туризм*. К. : Вид-во Нац. авіац. ун-ту "НАУ-друк", 2011. Вип. 1(3). С. 90-99.
32. Тихомирова Є. Б. Міжнародна інформаційна безпека як складова міжнародної системи підтримання миру і стабільності. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2017. № 2. С. 175-177.
33. Торічний В. О. Інформаційне забезпечення безпеки держави в умовах інформаційного суспільства : державно-управлінський аспект : монографія. Харків : НУЦЗУ, 2020. 274 с.
34. Юдін О.К. Інформаційна безпека держави: Навчальний посібник. Х.: Консум. 2005. 576 с.
35. Beard J.M. Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law. *Vanderbilt Journal of Transn. Law*. 2014. Vol. 47, № 1. P. 67–144.
36. Broadhurst R. Developments in the global law enforcement of cyber-crime. An Int. *Journal of Police Strat. a. Management*. 2006. Vol. 29, № 3. P. 408–433.
37. Denning D. Reflections on Cyberweapons Controls. *Computer Security Journal*. 2000. Vol. XVI, № 4. P. 43–53.
38. Dictionary of Military and Associated Terms. US Department of Defense. URL: http:// www.dtic.mil/doctrine/dod_dictionary/data/c/10082.html.
39. Dinnis H. H. Cyber Warfare and the Laws of War. Cambridge, 2012.
40. Global Cybersecurity Index 2020. ITU Publications : websit. URL : https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E
41. Group of Governmental Experts on Advances in Informatization and Telecommunications in the Context of International Security. Note of the

Secretary General. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=R.

42. Hutchinson W. Information Warfare and Deception. *Informing Science*. 2006. Vol. 9

43. Kondoch B. Jus ad Bellum and Cyber Warfare in Northeast Asia. *Journal of East Asia and Int. Law*. 2013. Vol. 6. P. 473–474.

44. Lawrence T. Greenberg. Information warfare and international law / T. Lawrence, S.E. Goodman, K.J. Soo Hoo. Washington : Nat. Defense Univ. Press, 1998. 53 p.

45. Macdonald S. Propaganda and Information Warfare in the Twenty-first Century. Altered Images and Deception Operations. Abington : Routledge, 2006. 224 p.

46. Molander R., Riddile A., Wilson P. Strategic information warfare: a new face of war. Library of Congress Cataloging in Publication Data, RAND (Firm), 1996. 33 p.

47. Molander R., Wilson P., Mussington D., Mesic R. Strategic information warfare rising war. Library of Congress Cataloging in Publication Data, RAND (Firm), 1998. URL: https://www.rand.org/pubs/monograph_reports/MR964.html.

48. National Cyber Security Index. URL : https://ncsi.ega.ee/

49. Neff S. C. War and the Law of Nations. A Generall History. Cambridge, 2006. P. 1.

50. Nye J. S. Controlling Cyber Conflic. Project Syndicate. Aug. 8, 2017. URL: https://www.project-syndicate.org/commentary/new-norms-to-prevent-cyber-conflict-by-joseph-s--nye-2017-08/russian

51. Resolution adopted by the General Assembly on December 27, 2013 [on the report of the First Committee (A / 68/406)]. URL: https://undocs.org/ru/A/RES/68/243.

52. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Seventieth session Item 93 of the General Assembly provisional agenda. The United Nations. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

53. Sherman F. Aborting Unauthorized Launches of Nuclear-Armed Ballistic Missiles through Postlaunch Destructio. *Science and Global Security*, 1990, Volume 2, No. 1.

54. Schjolberg S. The history of global harmonization on cybercrime legislation: the road to Geneva. Journal of Int. Com. *Law and Technology*. 2008. Vol. 1, №12. P. 1–23.

55. Schwab K. The fourth industrial revolution What It Means and How to Respond? Foreign Affairs. December 12, 2015. URL: https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.

56. Sofaer A.D. Transnational dimension of cybercrime and terrorism. Stanford: Hoover Institution Press, 2001. 292 p.

57. Strengthening the role of ITU in building confidence and security in the use of information and communication technologies : Resolution 130 Rev. Dubai, 2018. URL : https://www.itu.int/en/ITU-D/Cybersecurity/Documents/RES_130_rev_Dubai.pdf.

58. Tallinn Manual on the international law applicable to cyber warfare. Nuclearenergy.ir. URL: http://nuclearenergy.ir/wp-content/uploads/2013/11/tallinn_manual.pdf.

59. U.S. Cyberattacks Target ISIS in a New Line of Combat The New York Times. April 24, 2016 URL: https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

60. Weissbrodt, D. Cyber-Conflict, Cyber-Crime, and Cyber-Espionage. *Minnesota Journal of Int. Law*. 2013. Vol. 22 P. 347–387.

ДОДАТКИ

Додаток А

Проблема застосування ІКТ у військово-політичних цілях для здійснення ворожих дій та актів агресії

Загроза	Ознаки наявності загрози	Можливості здійснення загрози
Розвиток ІКТ-озброєнь	Прискорена мілітаризація ІКТ-простору.	**ІКТ-засоби для застосування у військовій галузі:** ● боротьба із системами управління та контролю; ● розвідувальне протистояння; ● електронне протиборство; ● військові засоби, що сприяють проведенню інформаційних операцій.
	Включення ІКТ-сфери до інтегрованого поля бойових дій у стратегіях деяких країн.	
	Наявність наступальної кіберзброї та кібервійськ у 30 держав.	
	Нарощування можливостей наступальних та оборонних інформаційних та кібероперацій країнами НАТО.	
	Плани створення коштів кібервійни мають 140 країн.	
	Складність виявлення автора ІКТ-атаки, можливість	

	використання «неправдивого прапора», що веде до відсутності відповідальності.	
Використання «м'якої сили» із застосуванням ІКТ у ворожих військово-політичних цілях, для втручання у внутрішні справи держав	**Зростання кількості фактів втручання у внутрішні справи держав із застосуванням ІКТ:** Революція «Солідарності», Польща, 1980-1990	**Альтернативні військовому тиску методи та засоби впливу на противника:** ● **економічні** (ІКТ-вплив на промислові та фінансові об'єкти); ● **інформаційні** (пропагандистське іномовлення, Інтернет (пошукові системи, соціальні мережі, мережеві «дзеркала»), мобільні додатки, смс) для підготовки та проведення масових заворушень, антиурядових демонстрацій, політичних акцій, державних переворотів.
	«Оксамитова революція», Чехословаччина, 1989	
	«Бульдозерна революція», Югославія, 2000	
	підготовка вторгнення із застосуванням ІКТ, Афганістан, 2001	
	«Революція троянд», Грузія, 2003	
	вторгнення із застосуванням ІКТ, Ірак, 2003	

«Помаранчева революція», Україна, 2004
«Революція тюльпанів», Киргизстан, 2005
«Жасминова революція», Туніс, 2011
«Твіттерна революція» («Революції лотоса»), Єгипет, 2011
громадянська війна, Лівія, 2011
«Революція розеток», Вірменія, 2015
громадянська війна, Сирія, 2011 – наші дні
підготовка державного перевороту, Венесуела, 2019

Додаток Б

Проблема забезпечення інформаційної безпеки військових об'єктів як частини критично важливої інфраструктури держави

Загроза	Ознаки наявності загрози	Можливості здійснення загрози
Розвиток ІКТ-засобів для шкідливого на об'єкти ВПК	Наявність ІКТ-загроз для різних елементів військової організації та інфраструктури. Найважливіші: стратегічні озброєння, система попередження про ракетний напад (СПРН), система командування та контролю за ядерною зброєю, ІПО. Зростання масштабів застосування ударних роботизованих засобів з дистанційним управлінням, штучного інтелекту у військових цілях, автоматизованих систем прийняття рішень тощо, які можуть зазнавати кібератаки.	● кібернапади на об'єкти військової або пов'язаної з нею цивільної інфраструктури; ● фізична шкода ПЗ, елементної бази, лініях зв'язку та мереж військового об'єкта; ● дистанційну «логічну» шкоду за допомогою ВП, «логічних бомб» тощо; ● умисну або ненавмисну віддалену шкоду через комп'ютерні мережі (в т.ч. Інтернет) або внаслідок контакту з комп'ютером;
	Переклад військ стратегічного призначення в різних країнах на цифрові технології передачі	

	інформації, що зробить їх більш уразливими для технічних помилок та навмисних кібератак.	● кібершпигунство та створення кіберагентурних мереж;
Зниження рівня стратегічної стабільності	Вплив розвитку ІКТ на зростання ймовірності: ● несанкціонованого запуску балістичних ракет (БР) на ухвалення рішення про застосування ядерної зброї; ● отримання хибної інформації від СПРН про запуск БР з боку супротивника через зростаючу витонченість кібератак; ● пошкодження або руйнування каналів комунікацій, створення перешкод у системі управління збройними, у тому числі ядерними силами; ● зниження впевненості військових, які приймають рішення, у працездатності систем управління,	● кіберсаботаж; ● створення невпевненості командування та персоналу у безперебійній та ефективній роботі систем.

	командування та контролю ЗС.
	Вплив зростання ймовірності виведення з ладу або знищення ядерної зброї через ІКТ на майбутнє процесів ядерного роззброєння та нерозповсюдження.
	Вплив ІКТ-чинників на рівень стратегічної стабільності

Додаток В

Рейтинг країн за Глобальним індексом кібербезпеки (GCI) [global]

Рейтинг	Країна	Оцінка	Рейтинг	Країна	Оцінка
1	США	100	1	Сполучене Королівство	99,54
2	Сполучене Королівство	99,54	2	Естонія	99,48
2	Саудівська Аравія	99,54	3	Іспанія	98,52
3	Естонія	99,48	4	Литва	97,93
4	Корея	98,52	5	Франція	97,6
4	Сінгапур	98,52	6	Туреччина	97,5
4	Іспанія	98,52	7	Люксембург	97,41
5	ОАЕ	98,06	7	Німеччина	97,41
5	Малайзія	98,06	8	Португалія	97,32
6	Литва	97,93	9	Латвія	97,28
7	Японія	97,82	10	Нідерланди	97,05
8	Канада	97,67	30	Грузія	81,07
9	Франція	97,6	31	Ісландія	79,81
10	Індія	97,5	32	Румунія	76,29
70	Узбекистан	71,11	33	Молдова	75,78
71	Йорданія	70,96	34	Словенія	74,93
72	Уганда	69,98	35	Чеська Республіка	74,37
73	Замбія	68,88	36	Монако	72,57
77	Болгарія	67,38	37	Болгарія	67,38
78	**Україна**	**65,93**	**39**	**Україна**	**65,93**
79	Пакистан	64,88	40	Албанія	64,32

80	Албанія	64,32	41	Чорногорія	53,23
180	Екваторіальна Гвінея	1,46	42	Ліхтенштейн	35,15
181	КНДР	1,35	43	Боснія і Герцеговина	29,44
182	Мікронезія	0	44	Андорра	26,38
182	Ватикан	0	45	Сан-Марино	13,83
182	Ємен	0	46	Ватикан	0

Додаток Г

Рейтинг країн за Національним індексом кібербезпеки (NCSI) [natio]

Рейтинг	Країна	Національний індекс кібербезпеки	Рівень цифрового розвитку	Різниця
1	Греція	96,10	64,02	32,08
2	Бельгія	94,81	74,07	20,74
3	Литва	93,51	67,34	26,17
4	Естонія	93,51	75,59	17,92
5	Чеська Республіка	92,21	69,21	23,00
6	Німеччина	90,91	80,01	10,90
7	Румунія	89,61	59,84	29,77
8	Португалія	89,61	68,46	21,15
9	Іспанія	88,31	72,21	16,10
10	Польща	87,01	65,03	21,98
20	Малайзія	79,22	62,19	17,03
21	Італія	79,22	67,26	11,96
22	Сполучене Королівство	77,92	79,96	-2,04
23	Швейцарія	76,62	82,93	-6,31
24	**Україна**	**75,32**	**55,96**	**19,36**
25	Латвія	75,32	66,23	9,09
160	Домініка	3,90	56,90	-53,00
161	Соломонові острови	2,60	21,10	-18,50
162	Тувалу	2,60		
163	Південний Судан	1,30		

НУБіП України

НУБіП України

НУБіП України

НУБіП України

НУБіП України

НУБіП України

НУБіП України