МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
Кафедра міжнародного права та порівняльного правознавства

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ О. В.Стрєльцова
«____»_____2021 р.

ДИПЛОМНА РОБОТА
ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
«МАГІСТР»
спеціальності 293 «Міжнародне право»

Тема: **Міжнародно-правове регулювання в сфері забезпечення інформаційної безпеки**

Виконавець: Блайда Максим Анатолійович
Науковий керівник: к.ю.н., доцент кафедри міжнародного права та порівняльного правознавстваЗамула Аліна Юріївна
Нормоконтролер: Головатенко Марина Юріївна

Київ 2021

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Сучасний етап науково-технологічного розвитку пов'язаний із впровадженням передових технологій. Нині у нашій країні є всі передумови для формування суспільства нової формації, що базується на інформаційних і телекомунікаційних технологіях, проривних технологіях, наскрізній цифровізації виробництва, які забезпечують актуальність, достовірність інформації, – суспільство знаннями.

Особливість сучасних інформаційних технологій полягає у можливості їх використання незалежно від рівня технічної грамотності та підготовленості суб'єктів. Найбільш «дружні» інтерфейси, доступність комп'ютерних програм та обладнання сприяють активізації широкого кола осіб в інформаційній сфері. Проте внаслідок того, що державне регулювання, створення та використання інформаційних технологій та інфраструктур відстає від темпів їх розвитку, ускладнення та вдосконалення, учасники відносин у сфері використання інформаційних інфраструктур виявляються недостатньо захищеними від інформаційних техногенних факторів, що впливають на них.

Стратегія розвитку інформаційного суспільства в Україні визначає як мету розвиток інформаційної та комунікаційної інфраструктури України шляхом забезпечення вільного доступу громадян та організацій, органів державної влади, органів місцевого самоврядування до інформації на всіх етапах її створення та розповсюдження. Для цього передбачається створення ефективної системи забезпечення інформаційної безпеки на рівні програмного забезпечення та сервісів, що надаються за допомогою Інтернету; інформаційних систем та центрів обробки даних; мереж зв'язку; криптоалгоритмів і засобів шифрування при електронній взаємодії органів виконавчої влади, органів державної влади, суб'єктів країни, державних

позабюджетних фондів, органів місцевого самоврядування між собою, і навіть з громадянами та організаціями та інших.

Основними цифровими технологіями, важливість використання яких відзначається більшістю розвинених країн, є технології розподілених обчислень. В основі промислового інтернету речей лежать технології, програмне забезпечення та їх апаратна реалізація, створення та використання яких у суспільстві має бути забезпечено нормативним правовим регулюванням.

Без правового забезпечення інформаційної безпеки, взаємодії учасників суспільних відносин, подальший розвиток та використання перерахованих вище технологій буде ускладнено. У зв'язку із застосуванням сучасних інформаційних технологій потрібна зміна підходу до правового регулювання інформаційних відносин в умовах використання технологій, що ґрунтуються на принципах розподіленої обробки інформації, запровадження інститутів «цифрових прав», «цифрових реквізитів» електронного документа, «цифрових доказів».

Теоретичним та організаційно-правовим питанням розвитку та використання інформаційної інфраструктури присвячено значну кількість зарубіжних робіт, але в Україні теоретико-правових досліджень у цій галузі недостатньо. Процеси пошуку, збору, зберігання, обробки, надання, розповсюдження інформації, методи та способи здійснення таких процесів, що ускладнюються, дозволяють позначити вектори державної політики в галузі створення та використання інформаційної інфраструктури. Все більший вплив технологій на суспільні відносини послужив поштовхом для затвердження в нашій країні за останні чотири роки цілого ряду стратегічних документів, що стосуються створення, розвитку та обліку соціальних змін, що вносяться інформаційними системами та сервісами у суспільні відносини. Однак для створення та подальшого цифрового державного управління необхідно вирішити сукупність правових, нормативно-технічних та організаційних проблем та завдань. Зокрема йдеться про подолання

відставання нормативного правового регулювання; розроблення стандартів обов'язкових вимог, методологій моделювання апаратно-програмного комплексу з позиції забезпечення: інформаційної безпеки, включаючи безпеку даних; визначення перспектив розвитку суспільних відносин у сфері інформаційних систем та можливостей їх правового регулювання. Активне використання у суспільних відносинах технології обробки великих обсягів даних виявляє проблему визначення надійності даної технології та забезпечення безпеки інформації, що збирається та обробляється за її допомогою, у тому числі забезпечення безпеки інформації обмеженого доступу, що розміщується в інформаційній системі.

Вказані проблеми актуальні не лише для України. 25 травня 2018 р. у Євросоюзі набув чинності Регламент ЄС 2016/679 (General Data Protection Regulation), що передбачає посилення вимог обробки персональних даних резидентів Євросоюзу, нові підходи та концепцію обробки персональних даних. По-новому, з урахуванням специфіки обробки інформації великими даними, у Європі формується склад учасників таких відносин.

На особливу увагу заслуговує проблема можливого негативного впливу сетецентричних технологій на учасників інформаційних відносин, що завдає шкоди як особистості та суспільству, так і державі.

Розвиток цифрового середовища спонукає до життя перспективні наскрізні цифрові платформи та технології та створює умови для виникнення нових відносин. Правове регулювання відносин, що формуються в даному середовищі без розуміння технологічних процесів, що відбуваються в них, породжує проблему використання неефективних правових методів регулювання даних відносин і забезпечення інформаційної безпеки.

Необхідні теоретичні правові дослідження, створені задля розробку теоретичної концепції та методологічної основи забезпечення реалізації регулятивних та охоронних функцій держави з урахуванням рівня розвитку інформаційних технологій та виявлення закономірностей розвитку

цифрового державного управління. Цим визначається і авторська мотивація вибору напряму дослідження, відображеного у дипломній роботі.

В українській науковій літературі проблемі правового забезпечення інформаційної безпеки посвячені роботи низки науковців, серед яких В.Ю. Богданович, В.Ф.Загурська-Антонюк, Р.А. Калюжний, В.А. Ліпкан,О.В. Левченко, А.І. Марущак , І.М. Сопілко та інші. Серед зарубіжних можна виділити : Боукер Г.К. , Чак Істтом, Джефф Тейлор, Джефф Хендельсман та інші.

Основна **мета** дослідження – проведення порівняльного дослідження вітчизняних та зарубіжних підходів до правового регулювання інформаційних відносин. У даній роботі проведено аналіз законодавчої бази, практики нормативного правового регулювання в розвинених державах, міжнародної практики нормативного правового регулювання, спрямованої на формування, розвиток та побудову безпечної інформаційної інфраструктури, забезпечення цифрової взаємодії суб'єктів, використання технологічних платформ та умов їх застосування для формування ефективного державного регулювання.

Вищевказана мета зумовила постановку таких основних **завдань**:

- обґрунтувати теоретико-правову природу правового регулювання суспільних відносин, що виникають під час створення та використання інформаційної інфраструктури;
- розкрити зміст основних понять, правової природи інформаційних відносин, що виникають у процесі створення та використання інформаційної інфраструктури;
- дослідити закордонні правові та технологічні підходи в галузі створення та використання інформаційної безпеки з метою організації та розвитку ефективного державного управління;
- дослідити підходи, що застосовуються міжнародними організаціями;
- визначити та систематизувати виклики, загрози та ризики, що виникають при створенні та використанні інформаційної безпеки;

– визначити основні напрямки розвитку правового регулювання у сфері забезпечення інформаційної безпеки.

Об'єктом дослідження є суспільні відносини у сфері створення та використання інформаційної безпеки.

Предмет дослідження – міжнародно-правове регулювання в сфері забезпечення інформаційної безпеки.

Методологічну основу роботи склали філософські, загальнонаукові та спеціальні методи, які у своєму органічному поєднанні допомогли досягти виконання поставлених завдань.

В основу дослідження покладено метод порівняно-правового аналізу, який має своїм об'єктом аналогічні або подібні інститути права та метод порівняння, що включає наступні етапи: 1) вивчення порівнюваних норм окремо; 2) порівняння виявлених ознак з позиції їх подібності та відмінності; 3) оцінка результатів, що дозволяють простежити загальні риси та виявити найбільш вдалі правові рішення. Аналіз нормативних правових актів у цій сфері дозволив виявити державні підходи до регулювання інформаційних відносин у сфері створення та використання інформаційної інфраструктури.

Використано історико-правовий метод з метою вивчення динаміки розвитку та змін законодавства, що відбуваються під впливом інформаційних технологій.

Апробація результатів дослідження. Окремі наукові результати дослідження були апробовані та опубліковані у межах наступних науково-практичних конференцій та юридичних видань:

Структура роботи обумовлена її метою, завданнями та предметом дослідження. Дипломна робота складається із вступу, трьох розділів, якими охоплюються вісім підрозділів, висновків та списку використаних джерел (95 найменувань). Загальний обсяг дипломної роботи – 86 сторінок, у тому числі список використаних джерел – 13 сторінок.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІБ	Інформаційна безпека
ІТ	Інформаційні технології
ІКТ	Інформаційно-комунікаційні технології

РОЗДІЛ 1

МІЖНАРОДНИЙ ДОСВІД ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Інформаційна безпека: поняття, види, роль інформаційних операцій

Масове впровадження нових технічних засобів, на основі яких здійснюється інформатизація у всьому світі, робить прозорими державні кордони і формує нові геополітичні парадигми у розумінні глобальних соціотехнічних систем. Міжнародна інформаційна сфера стає не тільки однією з важливих сфер співробітництва, а й середовищем конкуренції між окремими особами, державами, міждержавними політичними та економічними угруповуваннями. Електронно-комунікаційна інфраструктура, як і інші інформаційні ресурси, стає об'єктом міждержавної боротьби за світове лідерство або об'єктом недобросовісної конкуренції у підприємницькій діяльності чи інших суспільних інформаційних відносин.

Все це зумовлює необхідність формування такого аспекту інформаційної культури, як культура інформаційної безпеки, культура організації інформаційної безпеки. Зазначений аспект розвитку інформаційної культури набуває відображення у такій прикладній науковій дисципліні, як теорія організації (тектологія) інформаційної безпеки.

Існує досить багато варіантів визначення поняття інформаційної безпеки в науковій літературі, а також закріплено на рівні національного законодавства. Розглянемо основні з них:

1. Інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання й розвиток в інтересах громадян, організацій, держави[59, с.23].

Під інформаційним середовищем розуміють сферу діяльності суб'єктів, пов'язану із створенням, обробленням й споживанням інформації.

2. Інформаційна безпека – це стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та

прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Стан інформованості визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і як наслідок – обґрунтованість рішень і дій, що приймаються[56,с.124].

3. Інформаційна безпека – складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується:

- інформаційний суверенітет України;

- вдосконалення державного регулювання розвитку інформаційної сфери, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

- активне залучення засобів масової інформації до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці України;

- неухильне дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;

- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України[53].

4. В інформаційному праві інформаційна безпека – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позиції захисту життєво важливих інтересів особистості, суспільства, держави і акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами[75,с.126].

Інформаційна безпека виступає як характеристика стабільного, стійкого стану системи, яка при впливі внутрішніх та зовнішніх загроз та небезпек зберігає суттєво важливі характеристики для власного існування.

Основні характеристики інформаційної безпеки:

1) доступність — це ознака, що дозволяє користувачам у певних випадках безперешкодно отримати інформацію, що їх цікавить. Винятком є дані, приховані від загального огляду, розголошення яких може завдати серйозної шкоди суб'єктам та інформації. Наприклад, доступними є матеріали, які може одержати кожна людина: купівля квитків, послуги у банках, оплата комунальних платежів.;

2) цілісність — один із елементів інформації, що гарантує її стабільність при навмисному (ненавмисному) перетворенні або знищенні певних даних. Вона буває статичною (стабільність основних об'єктів від початкового стану) та динамічною (точна реалізація послідовних дій). Якщо буде порушено єдність інформації, це може призвести до серйозних негативних наслідків. Ця характеристика є основною та актуальною в інформаційному просторі.;

3) конфіденційність — захист від несанкціонованого ознайомлення[77].

Сутність і зміст інформаційної безпеки проявляються по-особливому на кожному з рівнів державного управління, зокрема на:

1) стратегічному — Кабінет Міністрів України;

2) тактичному — центральні органи виконавчої влади;

3) оперативному — місцеві органи виконавчої влади, провідне місце серед яких посідають місцеві державні адміністрації[65,с.167].

Інформаційна безпека є невід'ємною частиною загальної безпеки, чи то національної, чи то регіональної, чи то міжнародної. Аналіз інформаційної безпеки передбачає розгляд сукупності таких об'єктивних чинників:

• потреб громадян, суспільства і держави і світового співтовариства;

• уразливість індивідів, суспільства і держави від цифрових технологій;

• наявність широкого кола загроз і небезпек, якими має управляти система забезпечення інформаційної безпеки[37].

Інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення людини, держави і суспільства. Вона орієнтована на захист значимих або вже згаданих суб'єктів інформаційних ресурсів, законних інтересів.

Рівні інформаційної безпеки:

- нормативно-правововий — включає в себе сукупність заходів, спрямованих на формування та підтримку в суспільстві негативного ставлення до кіберзлочинців та порушників ІБ. Більшість громадян не роблять кіберзлочинних дій через засудження та покарання за подібні дії, а не тому, що немає такої технічної можливості. Держава реалізує механізм, який забезпечує узгодження процедури створення законопроектів із розвитком сфери ІТ. Вкрай важливий процес – актуальність чинних законів рівнем розвитку ІТ.;

- адміністративний — дії загального характеру, які вживаються органами державного управління;

- процедурний — конкретні процедури забезпечення інформаційної безпеки;

- програмно-технічний — конкретні технічні заходи забезпечення інформаційної безпеки.Відповідно до актуальних трендів, у рамках інформаційної системи необхідне забезпечення доступності кількох основних механізмів безпеки:

- криптографія;
- екранування;
- забезпечення максимальної доступності;

- протоколювання, аудит;
- керування доступом;
- ідентифікація, автентифікація користувачів[34,с.46].

Інформаційна безпека як одна з характеристик стійкого розвитку виступає в якості базової цінності держави. Водночас, ціннісні орієнтації, що ґрунтуються на уявленнях про інформаційну безпеку у різних суспільних груп і окремих осіб, почасти не співпадають. Саме у цьому знаходить свій безпосередній вираз вплив держави, яка за допомогою системи методів виражає загальні цінності у сфері інформаційної безпеки.

Види інформаційної безпеки:

1) Інформаційна безпека особистості – це захищеність психіки й свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до образ, самогубства тощо.

2) Інформаційна безпека держави характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи тощо) відносно небезпечних (дестабілізуючих) інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека держави визначається здатністю нейтралізувати такі впливи[34,с.47].

Інформаційна операція – використання можливостей електронної зброї, комп’ютерних мережевих операцій, психологічних операцій, операцій з військової дезінформації і дезорганізації та операцій безпеки для використання можливостей впливу на людську свідомість з метою руйнування, розкладання або й взагалі перехоплення впливу на прийняття рішень противника, і захисту свого власного рішення.

О.В. Левченко запропонував класифікацію інформаційної зброї за засобами інформаційної війни. Автор приходить до висновку, що інформаційна зброя становить особливу небезпеку для інформаційних ресурсів, комп’ютерних систем і мереж державних органів, фінансових і банківських установ, систем управління військами і зброєю, а також для

психіки, свідомості та підсвідомості. населення та особового складу збройних сил. За ефективністю та результатами застосування інформаційна зброя прирівнюється до зброї масового ураження [64, с. 145].

Слід зазначити, що в більшості досліджень, у тому числі російськомовних та україномовних, ефективність інформаційних (психологічних) операцій (ПСО) розглядається на прикладі переважно за межами України та Росії.

Так, зазначається, що перша масштабна операція, названа психологічною, була проведена Збройними силами США на підтримку військ ООН у Корейській війні (1950-1953). У 1951 р. при міністерстві армії було створено кафедру психологічних операцій, яка в 1955 р. була реформована в кафедру спеціальних методів ведення війни. Тоді ж розпочалася підготовка спеціального персоналу. Сили USAR широко застосовувалися в Панамі та в Перській затоці, де американські фахівці проводили інформаційні операції проти режиму Саддама Хусейна, спрямовані на захист курдського населення, а також мусульман-шиїтів від політики Багдада. Масштабні місії USAR також проводилися в рамках операції «Риба-ангели» та підтримки демократії (Гаїті, 1991, 1994), «Відродження надії та спільного щита» (Сомалі, 1992-1995), «Спільні зусилля» (Боснія, 1996). Майже всі миротворчі компанії, в яких беруть участь США, супроводжуються психологічними операціями. Зазначається, що якщо в Першій світовій війні на 20 тис. військовослужбовців припадав один журналіст, то під час операції в Боснії – на 500 військовослужбовців [63, с. 30].

Водночас Україна має свій «сумний досвід» інформаційних атак на себе.

Як зазначав Ю.О. Горбань [41, с. 140], в інформаційній війні проти України Російська Федерація використовує майже весь арсенал впливу на

свідомість людей. Зокрема, спостерігачі зазначають, що, наприклад, протягом усіх 23 років незалежності України на кримському телебаченні велася антиукраїнська пропаганда. Г. Почепцов [82] зазначає, що до подій 2013-2014рр. 60% дорослого населення України отримувало суспільно-політичну інформацію через телебачення. 54,5% населення віддали перевагу новинно-аналітичним програмам російського телебачення.

Агресивно-військовий характер інформаційних впливів знайшов відображення у термінології, яка використовується під час опису явищ інформаційної війни. Ця термінологія сама по собі надає чітке враження по цілі і засоби, що ставить перед собою ворожа інформаційна діяльність, зокрема: зовнішня інформаційна агресія, інформаційна війна, психологічна війна, стратегічна інформаційна війна, інформаційна операція, спеціальна інформаційна операція (СІО), психологічна операція тощо.

Концепція інформаційної безпеки держави – це систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення. В рамках цієї концепції проводиться системна класифікація дестабілізуючих факторів та інформаційних загроз безпеці особистості, суспільства, держави; обґрунтовуються основні положення з організації забезпечення інформаційної безпеки держави; розробляються пропозиції щодо способів і форм забезпечення інформаційної безпеки.

1.2. Міжнародні норми щодо регулювання інформаційної безпеки

Найважливішою ознакою глобального розвитку є інформаційне суспільство, фундамент якого становлять новітні технології та засоби комунікації. Будучи «специфічною формою соціальної організації, в якій нові технології генерування, обробки та передачі інформації стали фундаментальними джерелами продуктивності та влади», інформаційне суспільство схильне до особливо складних загроз, оскільки широкий спектр можливостей впливу ІКТ дуже різноманітний і характеризується високим

ступенем небезпеки для всіх сфер життєдіяльності соціуму та функціонування держави. У цьому контексті проблема вдосконалення системи державних гарантій конституційних прав людини та громадянина в інформаційній сфері набуває особливої актуальності[50,с.117].

Рівень розвитку інформаційно-комунікаційних технологій держави є визнаним у міжнародному співтоваристві важливим індикатором оцінки військово-політичного та соціально-економічного потенціалу держави загалом. Україна у цьому сенсі не є винятком.

Міжнародне право встановлює, що забезпечення права адекватну інформацію є умовою ефективної реалізації всіх інших права і свободи громадян. На основі дотримання конституційних норм щодо недоторканності приватного життя та конфіденційності кореспонденції має будуватися вся система нормативного правового забезпечення безпеки в інформаційній сфері, оскільки права та свободи людини та громадянина мають найвищий пріоритет.

Закономірно, що концептуальні засади та принципи правового регулювання безпеки в інформаційній сфері, розроблені на міжнародному рівні, відповідно до пункту 49 Резолюції 2200А (XXI) Генеральної Асамблеї ООН знаходять більшою чи меншою мірою відображення, як вважає комісія Європейського Союзу з кібербезпеки, законодавстві всіх економічно розвинених країн. Найважливішим стратегічним завданням забезпечення інформаційної безпеки є стан інформаційного простору, в якому виключені можливості порушення прав особистості, суспільства і держави. Конституційно-правова база має створювати підстави для реалізації політики інформаційної безпеки всіх трьох об'єктів: держави, суспільства, особистості «з урахуванням специфіки вимог кожного об'єкта до захисту своїх ресурсів»[91,с.76].

Експоненційний розвиток інформаційно-комунікаційних технологій стає викликом для національної безпеки в контексті захисту тріади інтересів особистості, суспільства та держави в інформаційній сфері. Неконтрольовані

процеси у глобальних мережах та специфіка політичної боротьби у віртуальній сфері прямо та опосередковано впливають на забезпечення захисту національних інтересів. Цей виклик національної безпеки вкрай актуальний у зв'язку зі стихійним створенням відкритих інформаційних мереж загального призначення, їх підключенням до міжнародних телекомунікаційних мереж». Про загрозу національній безпеці будь-якої держави свідчить той факт, що розробка віртуальної міжнародної мережі, забезпечення працездатності та вдосконалення актуальних технологій контролюється Міністерством оборони США[93].

Динаміка та характер розвитку інформаційних технологій інтенсифікують новітні виклики та загрози, спрямовані на особистість як уразливий суб'єкт інформаційних відносин, оскільки досягає потенційно-глобальної аудиторії за допомогою піринговых мереж та підключення до мережі Інтернет. Окінавська хартія глобального інформаційного суспільства декларує: «інформаційно-комунікаційні технології є одним із найважливіших факторів, що впливають на формування суспільства двадцять першого століття. Їх революційний вплив стосується способу життя людей, їхньої освіти та роботи, а також взаємодії уряду та громадянського суспільства. Інформаційно-комунікаційні технології швидко стають життєво важливим стимулом для розвитку світової економіки. Перед усім світом відкриваються великі можливості».

1.3. Специфіка міжнародно-правового регулювання інформаційної безпеки

Розвиток Інтернету та розширення його сфери впливу на території практично всіх країн світу послужило розвитку інформаційних інфраструктур у міжнародному масштабі. Нині Інтернет одна із найпоширеніших інформаційних інфраструктур, що з інформаційних систем більшості розвинених країн. У цій транснаціональній інформаційній

інфраструктурі представлений весь комплекс існуючих суспільних відносин, які не підпадають під правове регулювання будь-якої держави.

Інформаційні інфраструктури створюються та формуються за допомогою об'єднання та взаємодії різних інформаційних технологій, у тому числі комп'ютерних технологій, які дозволяють здійснювати транскордонне звернення інформації. Як зазначають автори підручника з міжнародного права, інформація та інформаційні технології справили революційний вплив на економічні та соціальні процеси. Розвиток інформаційно-телекомунікаційних технологій вплинуло на лексичний склад мов світу, з'явилися слова-неологізми з приставкою «кібер-»: «кібератакам», «кіберпростір», «кіберзлочинність», «кібертероризм», «кіберзброя», «кібербезпека», «кіберспівпраця» , "кібервійська", які вже включені в нормативні правові акти, документи міжнародних організацій та інші документи правового характеру[47,с.32].

Така різноманітність термінів, що використовуються, ставить завдання про одноманітність застосовуваних термінів і понять, правової кваліфікації використовуваних понять, а також адекватності перекладів цих понять іншими мовами, включаючи українську.

Прийнято вважати, що технологічний прогрес сприятливо позначається на еволюції суспільства, наприклад, завдяки комп'ютерним технологіям стало можливим створювати нові інформаційні ресурси, отримувати безперешкодний доступ до віддаленої інформації, формувати нові державні послуги та ін. Проте сучасні концепції розвитку суспільства та правового регулювання відносин, що формуються завдяки використанню інформаційно-комунікаційних технологій, передбачають існування шкідливої інформації та інформаційних технологій. Звернення шкідливої інформації в інформаційній інфраструктурі може завдати непоправної шкоди державі. Шкідливі інформаційні технології створюють передумови для формування традиційної та інформаційної злочинності, наприклад, програмне забезпечення, що містить віруси та «закладки», дозволяє

отримувати доступ до інформації про третіх осіб без інформування цих осіб або до іншої інформації обмеженого доступу, здійснювати інтернет-шахрайства, зламування інформаційних систем та поширення шкідливої інформації. Останні двадцять років більшість країн світу активно розробляють національне законодавство у сфері створення та використання інформаційної інфраструктури[51,с.52].

Однак питання про вплив інформаційних технологій та освічених інформаційних інфраструктур ставився на міжнародному рівні ще у 2003 р. Цього року було зібрано саміт з питань Інформаційно-комунікаційних технологій та інформаційного суспільства, що проходив у Женеві, де МСЕ організував Всесвітню зустріч на найвищому рівні з питань інформаційного суспільства. Перший етап саміту закінчився прийняттям Женевської декларації принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті»[48]. Ця декларація містить положення, спрямовані на використання потенціалу інформаційних та комунікаційних технологій та на вирішення проблем, що виникають у зв'язку з нерівномірністю поширення та розподілу інформаційних технологій між розвиненими та країнами, що розвиваються, а також усередині країн.

У 2005 р. у Тунісі пройшов другий етап зустрічі на найвищому рівні, який ознаменувався прийняттям Туніського зобов'язання та Туніської програми для інформаційного суспільства. У рамках цієї зустрічі було порушено таку важливу проблему як управління Інтернетом. Нині Інтернетом управляє фактично єдина держава – США.

У Туніському зобов'язанні зазначається, що ІКТ «є ефективним інструментом сприяння справі миру, безпеки та стабільності, посилення демократії, соціальної згуртованості, належного управління та верховенства права на національному, регіональному та міжнародному рівнях»[45,с.89].

Крім прийнятих документів, підсумком другого етапу стало рішення країн про початок процесу інтернаціоналізації управління Інтернетом, реалізацією якого є перше засідання Форуму з питань управління Інтернетом

(ФУІ), що пройшло у жовтні – листопаді 2006 р. в Афінах. На цій зустрічі найбільш жорстко на інтернаціоналізації управління Інтернетом та його ресурсами наполягали країни, що розвиваються, які підтримав Євросоюз.

У Женеві у травні 2010 р. на Всесвітній зустрічі, оголошено, що кожна держава пов'язує свій соціально-економічний розвиток з інформаційними технологіями та розробляє власну національну стратегію в ІКТ. У Посланні Генерального секретаря ООН з нагоди всесвітнього дня телекомунікації та інформаційного суспільства №10-30082(R) 17 травня 2010 р. вказується, що в сучасному світі телекомунікація є чимось більшим, ніж просто базова послуга: вона є засобом, що сприяє розвитку, покращенню суспільства та порятунку життя людей[45,с.93].

Використання ІКТ пов'язані з розширенням міжнародного співробітництва у цій сфері. У зв'язку із чим держави беруть участь у профільних міжнародних організаціях.

Основною організацією в галузі міжнародно-правового регулювання інтернет-відносин та управління Інтернетом є ООН.

Перерахування основних спеціалізованих організацій ООН у галузі ІКТ дозволить уявити широту охоплення проблем, які вона вирішує. Наприклад, підрозділ Департаменту ООН з Економічних та соціальних питань (DESA) є відділом державних установ та цифрового уряду (DPIDG) та забезпечує підтримку Секретаріату для Програми розвитку ООН у галузі державного управління[19].

Основною функцією вищезазначеного Департаменту є надання допомоги державам у сфері використання інновацій у державному управлінні інформаційними інфраструктурами.

Економічна та соціальна рада ООН подає звіти для формування статистичної інформації про застосовувані ІКТ у світі та державах.

ЮНЕСКО є спеціалізованою організацією ООН з питань освіти, науки та культури, що здійснює діяльність у сфері зміцнення миру та безпеки за рахунок розширення співробітництва у галузі освіти, науки та культури. У

сфері комунікації діяльність ЮНЕСКО спрямовано скорочення розриву між розвиненими країнами, що розвиваються, через забезпечення безперешкодного доступу до інформації у всіх країнах світу. Як ключовий напрям ЮНЕСКО визначило перехід до суспільства знання через реалізацію принципу свободи слова та доступу до інформації, знань та освіти. Крім того, ЮНЕСКО реалізує низку програм інформаційного та комунікаційного спрямування: Пам'ять світу; Інформація для всіх; Міжнародна програма розвитку комунікацій; Програма захисту цифрової спадщини[22].

До структури ВОІВ включений Постійний комітет з інформаційних технологій, який формує політики та рекомендації в галузі використання глобальної інформаційної мережі, ВОІВ представляє рекомендації та політику на затвердження Генеральної Асамблеї, а також є спеціалізованим майданчиком, створеним спеціально для обговорення питань, що виникають у зв'язку з наданням мережевих інформаційних послуг у галузі інтелектуальної власності.

З 1947 р. МСЕ розробляє рекомендації у сфері телекомунікацій та радіо, розраховує показник розвитку ІКТ, регулює питання міжнародного використання радіочастот. Основною метою МСЕ є забезпечення легкого доступу до інформації та надання зв'язку кожній людині з метою забезпечення соціально-економічного розвитку.

Більшість держав сходиться у необхідності забезпечення безпеки інформації, інформаційних інфраструктур, захисту соціальних систем від шкідливого інформаційного впливу та критичної інформаційної інфраструктури, що поєднує інформаційні системи та технології, пов'язані з особливо важливими сферами функціонування держави[20,с.344].

У сфері правового регулювання інтернет-відносин сформувалися дві протилежні концепції. Перша концепція визначає анархію правового регулювання відносин у Мережі. Ідея формування цієї концепції пов'язані з початком етапу розвитку Інтернет – воно здійснювалося без правового регулювання. Відповідно, подальший її розвиток має залишатися таким. Дж.

Барлоу, є основоположником цієї концепції, ідеї якого було покладено в «Декларацію незалежності кіберпростору» [23]. Декларація була написана у відповідь на прийняття в 1996 р. Урядом США Білля про пристойність комунікацій та введення цензури в Інтернет.

Друга концепція визначає необхідність правового регулювання інтернет-відносин та подальшого розвитку Інтернету, оскільки інтернет-анархія знижує рівень захисту прав і дозволяє здійснювати різні правопорушення як у реальному, так і у віртуальному середовищі[21]. Ітернет-правопорушення мають особливість, оскільки ідентифікувати порушника в Мережі досить складно. Принцип саморегулювання в Мережі в даному випадку не є ефективним інструментом регламентації відносин, у зв'язку з чим прихильники другої концепції доводять необхідність застосування правових норм для врегулювання інтернет-відносин.

Існування двох концепцій зумовлює необхідність дотримання балансу інтересів всіх суб'єктів, але оскільки інтернет відносини є динамічними зробити це досить складно. Однак незважаючи на існуючі складнощі, держави роблять спроби знайти вихід із ситуації.

В даний час основними напрямками міжнародного правового регулювання у галузі створення та використання інформаційної інфраструктури є розробка та розвиток національного законодавства у галузі забезпечення безпеки мережевих та інформаційних систем.

У зв'язку із чим створюються міждержавні інформаційні інфраструктури для спрощення міждержавного інформаційного обміну та взаємодії громадян. Це виражається в прийнятих стратегічних документах у галузі кібербезпеки та інформаційної безпеки, в яких особлива увага приділяється стандартизації вимог,що забезпечують кібербезпеку та інформаційну безпеку[1].

Кібербезпека стає невід'ємною частиною забезпечення національної оборони держави.

Однак у сфері безпеки передачі даних та розвитку транскордонної комунікації державами відзначаються проблеми забезпечення захисту даних у контексті потоків даних, які вимагають розробки та прийняття ефективних методів забезпечення безпеки транскордонної передачі даних. Проблемою правового регулювання є різниця у рівнях забезпечення захисту даних та конфіденційності, прийняті у різних країнах. Для усунення даних проблем пропонуються правові методи, що дозволяють стандартизувати положення транскордонної передачі[4].

Система правового регулювання у сфері інформаційних відносин включає як норми інформаційного міжнародного права, так і механізми їх реалізації у вигляді міжнародних стандартів інформаційної безпеки.

І цей висновок цілком вірний, оскільки будь-які інформаційні інфраструктури складаються із сукупності інформаційних технологій та інформаційних систем. Відповідно, дані технологічні компоненти підпадають під численні національні та державні юрисдикції. Держави у межах свого суверенітету визначають політику у сфері регулювання інтернет-відносин та формуванні міжнародно-правових методів управління Інтернет мережею.

Про цю специфіку правового регулювання пишуть автори підручника з міжнародного права. Так, вони вважають, що «технічний» рівень функціонування Інтернету регулюється не лише правовими актами, а й нормами технічного регулювання у сфері телекомунікацій. До яких автори відносять стандарти та технологічні правила функціонування Інтернету, що розробляються недержавними інженерними організаціями[47,с.164].

На прикладному рівні, об'єктами регулювання стають порядок зберігання та розповсюдження інформаційних ресурсів, пошукові системи, мережеві послуги, у тому числі соціальні мережі, а об'єктами правовідносин – розробка та стандартизація правил передачі інформації, процедури ідентифікації, використання адресних посилань, створення та адміністрування доменних зон. Відповідно, прикладний рівень Мережі регулюється внутрішньодержавним інформаційним та цивільним

законодавством та нормативними технічними актами в галузі телекомунікацій[26,с.151].

У питаннях створення та використання інформаційних інфраструктур роль та обов'язки держав пов'язані зі здійсненням діяльності у таких напрямках:

– створення та використання інформаційної інфраструктури та технологій;

– розробка міжнародних договорів та узагальнення найкращих практик правового регулювання;

– розробка та прийняття правових та норм технічного регулювання;

- створення сприятливих економічних умов з метою розвитку ІКТ;

- боротьба з кіберзлочинністю;

– розробка державної політики на національному, регіональному та міжнародному рівнях, її реалізація та координація;

– забезпечення вільного доступу до послуг у сфері ІКТ;

– сприяння міжнародному та регіональному співробітництву[55].

Необхідно також зазначити, що в рамках міжнародного правового регулювання держави для забезпечення інформаційної безпеки під час використання інформаційної інфраструктури розробляють національні стандарти, а також ухвалюють міжнародні стандарти інформаційної безпеки. Крім того, розробляються міжнародні принципи транскордонної передачі даних та надання комп'ютеризованих інформаційних послуг, забезпечення безпеки транскордонних потоків даних.

Наприклад, у країнах Євросоюзу розроблено та постійно вдосконалюються процедури реагування на інциденти. У зв'язку з чим створюються групи швидкого реагування усунення наслідків кібератак або комп'ютерних збоїв[5].

Слід зазначити, що єдиного правового регулювання функціонування Інтернет немає. Держава регулює відносини, виходячи зі своїх норм, що ґрунтуються на моральних, моральних принципах та традиціях. Ці принципи

і традиції у державах різні та зобов'язання держав контролювати зміст інформації, розміщеної в комп'ютерних мережах, узгоджуючи у своїй як із нормами міжнародного права, і національного законодавства, який завжди виконуються.

У числі значних проблем правового регулювання створення та використання інформаційних інфраструктур можна виділити такі:

– встановлення міжнародно-правових засад функціонування Інтернету та управління Інтернетом;

- визначення правового статусу суб'єктів правових відносин, пов'язаних з використанням Інтернету;

- визначення правового режиму об'єктів, що відносяться до різних рівнів інфраструктури, засобів адресації та ідентифікації;

– міжнародно-правові методи запобігання здійснення протиправних дій в Інтернеті[7,с.512].

Виникають складнощі з регламентацією відносин, які впливають на узгодження у міжнародно-правовому плані громадських інтересів держав у сфері створення міжнародної міжурядової організації або укладання міжнародного договору.

Порушена проблема управління мережею не є новою. Однак, незважаючи на те, що дана проблема відзначалася ще в 2005 р. у Туніському зобов'язанні, до цього часу держави не дійшли однозначного рішення. Крім того, теоретичні підходи, представлені в наукових джерелах, вирішення цієї проблеми також різноманітні. Однак більшість дослідників сходиться на думці, що для забезпечення функціонування інтернету необхідно поряд із правовими нормами застосовувати та норми організаційно-технічного характеру.

Таким чином, в основі міжнародно-правового регулювання в галузі використання та створення інформаційних технологій та інфраструктур лежать нормативні акти міжнародного публічного права, викладені в

документах ООН, її галузевих структурах та міжнародних договорах, а також міжнародних стандартах у цій галузі.

Правові підходи, відображені у національних нормативних правових актах країн різноманітні. Однак спільними для всіх держав, які використовують глобальні інформаційні інфраструктури, є проблеми, пов'язані з управлінням інформаційною інфраструктурою, забезпеченням безпеки транскордонної передачі даних, захистом соціальних структур у державі від шкідливого інформаційного впливу, забезпеченням безпеки інформаційної інфраструктури.

РОЗДІЛ 2

ПРОБЛЕМАТИКА МІЖНАРОДНО-ПРАВОВОГО РЕГУЛЮВАННЯ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Вирішення питань інформаційної безпеки діючим міжнародним правом

Спори про інформаційну безпеку та інформаційну війну, а також про інформаційну складову державної влади, в більшості випадків наголошують на технологічних проблемах, при цьому недостатньо уваги приділяється правовому середовищу, в якому відбуваються суспільні зміни, пов'язані з розвитком інформаційних технологій.

Це може призвести до неясності в деяких реальних і неврегульованих правових питаннях, які мають бути вирішені при вирішенні проблем забезпечення інформаційної безпеки держави.

Однією з основних і найнебезпечніших дій, що стосуються інформаційної безпеки, є інформаційна війна. Практика підготовки до ведення інформаційних війн з боку окремих держав, наприклад США, є досить серйозною і реальною загрозою інформаційній безпеці. Тому розгляд того, як за допомогою чинного міжнародного права вирішуються питання інформаційної безпеки, на наш погляд, доцільно розпочати з міжнародно-правових питань, що виникають у зв'язку з інформаційними війнами[70].

Однією з постійних характерних рис в історії взаємовідносин війни і права є те, що коли б війна не поширювалася в нове середовище, наприклад під воду або повітряний простір, право завжди йшло позаду технологій. Це і не дивно, ніхто не створюватиме права для того, що ще не існує, наприклад, правила повітряної війни до винаходу літака. Зазначене властивість правового регулювання дозволяє деяким західним дослідникам стверджувати, що у час немає потреби у створенні міжнародно-правових основ, регулюючих діяльність у інформаційному просторі, включаючи

ведення інформаційних воєн, оскільки нині склалася відповідна практика держав[81,с.268].

Таким чином, міжнародно-правове регулювання залежатиме від того, які наслідки викличе технологія інформаційних воєн. Якщо наслідки будуть незначними, то міжнародно-правове регулювання буде досить вільним, у протилежному випадку можливе дуже жорстке регулювання.

Звісно ж, що така думка не цілком правильна. Інформаційні відносини нині досить розвинені, а загрози інформаційну безпеку держав вельми реальні. Відсутність міжнародно-правового регулювання з цього питання може дати можливість деяким державам здійснювати напади в рамках інформаційної війни, уникаючи відповідальності за зазначені дії. Тому, на нашу думку, забезпечення інформаційної безпеки та заборона ведення інформаційних воєн — це та сфера, де міжнародно-правове регулювання необхідне вже зараз чи найближчим часом.

Розвиток концепції інформаційних воєн викликає до життя низку міжнародно-правових питань. Ці питання особливо стосуються тих дій у межах інформаційних воєн, у яких використовуються комп'ютери, телекомунікації чи інформаційні комунікаційні мережі, оскільки зазначені кошти дуже відрізняються від цього, що було раніше. Деякі правові обмеження, що містяться в чинному міжнародному праві, можуть абсолютно безперечно застосовуватися до інформаційних війн, або тому що ці обмеження регулюють певні дії, що здійснюються в рамках інформаційних воєн, або через те, що до подібних дій можуть бути застосовані загальні принципи міжнародного права. Проте новизна певних засобів ведення інформаційних воєн може вивести застосування цих засобів зі сфери міжнародно-правового регулювання[82,с.236].

Таким чином, можна сформулювати основні проблеми міжнародно-правового регулювання:

Проблема перша: можливість передачі сигналів через міжнародні мережі, і навіть можливість на системи у віддалених країнах із

використанням інформаційних мереж третіх країн зачіпає принцип державного суверенітету.

Проблема друга: в даний час не зовсім ясно, чи складають інформаційні напади в рамках інформаційної війни застосування сили, чи вторгнення на територію держави, втручання у внутрішні справи держави чи збройний напад.

Чи залежить вирішення цього питання від наслідків, які спричинили ці напади. Чи вважатиметься правомірним для держави, яка зазнала нападу в рамках інформаційної війни, здійснити дії у відповідь, чи повинні зазначені дії у відповідь теж являти собою дії в рамках інформаційних воєн, або ж можна використовувати інші засоби силової відповіді.

Проблема третя: чи можна застосовувати до дій у рамках інформаційної війни положення міжнародного права в період збройних конфліктів або як його ще називають міжнародного гуманітарного права, і якщо так, то чи є збитки, які напади в рамках інформаційних воєн можуть спричинити, наприклад, руйнування урядових або приватних баз даних та систем, збитків, які забороняються міжнародним гуманітарним правом.

Проблема четверта: якщо напади здійснюються через міжнародні мережі, державі може знадобитися допомога інших держав у визначенні джерела нападу. У цьому випадку порушуються питання юрисдикції, правової допомоги та міжнародної відповідальності держав.

Деякі припускають, що інформаційна війна ознаменувала початок ери безкровних конфліктів, зіткнення відбуватимуться в інформаційному просторі, інформаційні війни зможуть вивести з ладу важливі інфраструктури командування та контролю або цивільні інфраструктури супротивника з невеликими втратами життя, якщо вони взагалі будуть. Інші припускають виникнення конфліктів у майбутньому, у яких кровопролиття лише збільшуватиметься завдяки використанню покращених засобів комунікації. Треті вважають, що інформаційні технології можуть бути

основою розвитку нових форм соціальної організації, а також викликають і нові форми конфліктів[80].

Очевидно, що деякі з нових форм нападів, які дозволяють інформаційні технології здійснювати, якісно відрізняються від раніше існуючих форм. Використання таких засобів, як комп'ютерне вторгнення та комп'ютерних вірусів, наприклад, переносить війну з фізичного, кінетичного світу у нематеріальне, електронне середовище, в інформаційний простір.

Напади можуть здійснюватися на відстані, з використанням радіохвиль або міжнародних комунікаційних мереж, без фізичного вторгнення до кордонів держави.

Збитки, які спричиняють напади в рамках інформаційної війни, можуть змінюватись від заподіяння смерті військовим або цивільним особам, від системних збоїв, до призупинення у виконанні важливою військовою або урядовою системою функцій, до поширення паніки, економічної кризи.

Розвиток інформаційних технологій, особливо комп'ютерів, телекомунікацій та мереж як уможливлює для противників атакувати один одного новими способами та з використанням нових форм заподіяння шкоди, так і викликає до життя виникнення нових цілей для нападу[77].

Така поява нових цілей є досить великою проблемою в оцінці правомірності здійснення нападів на них. Це пов'язано з тим, що розвиток інформаційних технологій характеризується так званим явищем конвергенції, яке можна визначити як зближення чи злиття деяких, до певного моменту різних структур, систем чи об'єктів. Стосовно дій у рамках інформаційних воєн дуже велике значення має конвергенція цивільних і військових систем. та комунікаційні мережі, що виконують, у тому числі й функції, необхідні для діяльності громадянського суспільства. Таким чином, подвійне призначення багатьох інформаційних систем та інфраструктур може розмити різницю між військовими та цивільними цілями. Це призводить до того, що в рамках інформаційної війни дуже важко визначити цілі нападів як тільки

військові (і, отже, легітимні) або лише громадянські (напад на які заборонено)[72,с.24].

Далі, вид нематеріальної шкоди, яку подібні напади можуть спричинити може істотно відрізнятися від фізичної шкоди, що викликається в результаті традиційної війни.

Через новизну більшості технологій, що використовуються при веденні інформаційної війни, у міжнародному праві відсутні норми, які певним чином однозначно забороняють або дозволяють або якимось іншим чином регламентують використання того, що ми називаємо інформаційною війною. Проте відсутність норми, проте, не є дозволом до дії, оскільки навіть якщо міжнародне право не регулює застосування будь-якого виду зброї чи технологій, можуть застосовуватись загальні принципи міжнародного права.

Розглянемо, як діюче міжнародне право відповідає питанням чи становлять інформаційні напади у межах інформаційної війни застосування сили, чи вторгнення на територію держави, втручання у внутрішні справи держави чи збройний напад.

Чи залежить вирішення цього питання від наслідків, які спричинили ці напади.

Збройний напад, у традиційному розумінні цього терміна, обов'язково включає застосування збройних сил, військового примусу і насильства. Для визначення поняття збройного нападу необхідно звернутися до Статуту ООН, а також міжнародно-правових документів, прийнятих у рамках ООН у цій сфері[78,с.148].

Стаття 2(4) Статуту ООН містить один з основних принципів міжнародного права, відповідно до якого забороняється застосування сили або загрози силою щодо територіальної цілісності або політичної незалежності іншої держави. З моменту прийняття Статуту ООН зазначений принцип застосовувався лише до фізичного застосування сили. Під час розробки Статуту ООН, коли Бразилія запропонувала включити економічні заходи на поняття використання сили, ця пропозиція була відхилена. Багато

держав ставили під питання думку, що застосування сили не включає економічний примус в період Арабського нафтового ембарго 1973 року, тоді як США та їх союзники висловлювали думку, що зазначене положення Статуту ООН не застосовується до економічного примусу.

У Резолюції Генеральної Асамблеї ООН 3314 (XXIX) «Визначення агресії», прийнятої 14 грудня 1974 року агресія визначається як застосування збройної сили державою проти суверенітету, територіальної недоторканності чи політичної незалежності іншої держави або якимось іншим чином, несумісним з Устав як це встановлено в цьому визначенні. У статті 3 зазначеної резолюції наводиться не вичерпний перелік дій, що становлять аіресспіо. Слід зазначити, що ці дії пов'язані з використанням збройних сил. Проте, відповідно до статті 4 Резолюції, Рада Безпеки може визначити, що інші акти є агресією, відповідно до положень Статуту ООН.

Відповідно до практики ООН, агресія обмежується застосуванням збройних сил.

У 1953 році Іран виступив в ООН з ініціативою про визнання того, що будь-яка дія, що безумовно служить цілям збройного нападу або використовує примус, що ставить в небезпеку незалежність держави, є агресією, але ООН не прийняла цю точку зору.

Якщо відповідно до документів ООН неможливо однозначно відповісти на питання про те чи є напад у рамках інформаційної війни збройним нападом чи агресією, то інша ситуація складається з питанням про інформаційний вплив як втручання у внутрішні справи держави.

Відповідно до Декларації про принципи міжнародного права, що стосуються дружніх відносин та співробітництва між державами відповідно до Статуту ООН (Прийнята 24.10.1970 Резолюцією 2625 (XXV) Генеральної Асамблеї ООН) жодна держава чи група держав не має права втручатися прямо чи опосередковано за якою б там не було причини у внутрішні та зовнішні справи будь-якої іншої держави. Також жодна держава не може ні застосовувати, ні заохочувати застосування економічних, політичних заходів

чи заходів будь-якого іншого характеру з метою домогтися підпорядкування собі іншої держави у здійсненні ним своїх суверенних прав та отримання від цього будь-яких переваг.

Подібні положення можна виявити і в Декларації ООН «Про неприпустимість втручання у внутрішні справи держав, про обгородження їх незалежності та суверенітету» (Прийнята 21.12.1965 Резолюцією 2131 (XX) на 20-й сесії Генеральної Асамблеї ООН): «Ніяка держава не може втручатися прямо чи опосередковано з будь-якої причини у внутрішні та зовнішні справи іншої держави. Внаслідок цього засуджуються не тільки збройне втручання, але також всі інші форми втручання та всілякі загрози, спрямовані проти правосуб'єктності держави або проти її політичних, економічних та культурних елементів»[40,с.202].

Незважаючи на те, що ні в Декларації принципів міжнародного права, ні в Декларації про неприпустимість втручання не дається чіткого поняття втручання у внутрішні справи держав, у зазначених документах зазначені заходи, що становлять таке втручання, причому перелік цих заходів є відкритим. Отже, така нова форма, як інформаційний вплив у рамках інформаційних воєн, пов'язана з першим чи з другим аспектом інформаційної безпеки, може розглядатися як втручання у внутрішні справи держави.

Таким чином, у Статуті ООН та в Резолюціях Генеральної Асамблеї з одного боку немає чітких норм, що кваліфікують напади в рамках інформаційної війни як агресію, збройний напад, але з іншого боку є підстави кваліфікувати зазначені дії як втручання у внутрішні справи.

Вище було розглянуто питання щодо другого аспекту інформаційної безпеки. Питання, що стосуються першого аспекту інформаційної безпеки, тобто питання змісту інформації, знаходять чіткішу відповідь у чинному міжнародному праві.

Відповідно до Декларації про принципи міжнародного права, держави зобов'язані утримуватися від пропаганди агресивних війн.

Дуже важливе значення для вирішення питань першого аспекту інформаційної безпеки має Декларація про неприпустимість інтервенції та втручання у внутрішні справи держав (Прийнята 09.12.1981 Резолюцією 36/103 на 36 сесії Генеральної Асамблеї Дод. ООН Л/6014 ООН) Відповідно до зазначеної декларації принцип відмови від інтервенції та невтручання у внутрішні та зовнішні справи держав включає такі права та обов'язки:

По-перше, право держав і народів мати вільний доступ до інформації та повністю розвивати без втручання свою систему інформації та засобів масової інформації та використовувати свої засоби інформації з метою сприяння своїм політичним, соціальним, економічним та культурним інтересами та сподіванням.

По-друге, обов'язок держав утримуватися від будь-яких наклепницьких кампаній, образливої чи ворожої пропаганди з метою здійснення інтервенції чи втручання у внутрішні справи інших держав.

По-третє, право та обов'язок держав боротися, в рамках своїх конституційних повноважень, проти поширення фальшивих чи спотворених повідомлень, які можуть розглядатися як втручання у внутрішні справи інших держав або як завдаючи шкоди зміцненню миру, співробітництва та дружніх відносин між державами та націями[8].

Таким чином, відповідно до зазначеної декларації, деякі форми розповсюдження фальшивих або спотворених повідомлень можуть розглядатися як втручання у внутрішні справи держави, припускаючи таким чином певні заходи відповідальності держави порушника.

Положення міжнародного права, що стосуються різних питань забезпечення інформаційної безпеки, містяться у низці міжнародно-правових актів, юридична сила яких різна. Проте необхідність наявності обов'язкових уніфікованих міжнародно-правових норм у цій сфері не викликає сумнівів.

Єдиним виходом із ситуації була б розробка та прийняття міжнародної конвенції, що регулює питання забезпечення інформаційної безпеки держав.

2.2. Питання інформаційної безпеки та інформаційних відносин і діяльність міжнародних організацій на сучасному етапі

Нормативно-правове регулювання на міжнародному рівні у сфері створення, використання та забезпечення безпеки інформаційної інфраструктури інтенсивно розвивається. Основною міжнародною організацією у сфері побудови міжнародного інформаційного суспільства є ООН. Їй належить провідна роль у забезпеченні та подальшому розвитку міжнародного співробітництва у сфері використання ІКТ.

В ООН входять структури, пов'язані з побудовою міжнародного інформаційного суспільства, серед яких ЮНЕСКО, Міжнародний союз електрозв'язку (МСЕ), який є спеціалізованою провідною установою ООН у галузі ІКТ та всесвітнім координаційним центром для урядів та приватного сектора у розвитку мереж та служб.

Ще 1996 р. ООН сформулювала принципи та підходи до побудови інформаційного суспільства. Обговорення проблеми інформаційної безпеки відбулося 1998 р., коли це питання було внесено до порядку денного ООН.

Генеральний секретар щорічно представляє Генеральній Асамблеї доповідь, що містить позиції держав — членів Організації з питань безпеки інформаційних технологій, дослідження та аналізу існуючих та потенційних загроз у цій сфері, кіберзагроз та можливих спільних заходів щодо їх нейтралізації з урахуванням оцінок та рекомендацій, створених для цієї мети трьох груп урядових експертів Перша така доповідь була представлена у 2010 році (A/65/201)486[15].

У 1999 р. ООН, посилаючись на свої резолюції, наголошувала, що досягнення науки і техніки можуть мати важливе громадянське та військове значення, і зазначила, що поширення інформаційних технологій та засобів зв'язку торкається інтересів усієї міжнародної спільноти.

Глобальна культура кібербезпеки схвалена відповідно до резолюції Генеральної Асамблеї 64/211 «Створення глобальної культури кібербезпеки

та аналіз національних зусиль із захисту найважливіших інформаційних інфраструктур» від 21 грудня 2009 р.[23].

У 2011 р. представники Російської Федерації, Китаю, Таджикистану та Узбекистану ініціювали розробку резолюції Генеральної Асамблеї щодо правил поведінки у сфері забезпечення міжнародної інформаційної безпеки. У документі висловлювалося занепокоєння у зв'язку з можливістю «використання інформації та комунікаційних технологій для цілей, несумісних із завданнями підтримки міжнародної стабільності та безпеки[47,с.224].

Виходячи з цього для запобігання спільним викликам та загрозам в інформаційному просторі необхідно розширювати та зміцнювати міжнародне співробітництво в галузі інформаційної та кібербезпеки засобів зв'язку, Інтернету, які повинні використовуватися тільки для економічного зростання, добробуту людей та підтримки міжнародної стабільності та безпеки.

Результатом зроблених вище заяв є проект держав-членів ШОС «Правила поведінки в галузі забезпечення міжнародної інформаційної безпеки (МІБ)», внесений як офіційний документ ООН.

У проекті вищезгаданих правил передбачаються такі принципи поведінки держав:

а) дотримання положень Статуту ООН та норм,що регулюють міжнародні відносини;

б) заборона використання ІКТ, у тому числі різних мереж зв'язку з ворожою метою або актами агресії, у тому числі створення загроз міжнародному миру та безпеці, а також на поширення інформаційної зброї або пов'язаних з нею технологій;

в) співробітництво у боротьбі зі злочинною та терористичною діяльністю в ІКТ-середовищі;

г) забезпечення безпеки інформації, продуктів та послуг у галузі зв'язку, інформаційних ресурсів, критичних інфраструктур, основних технологій та ін.[53].

У 2011 р. Генеральна Асамблея ООН одноголосно схвалила резолюцію A/RES/66/24, в якій містився заклик до подальших дій за результатами роботи у 2010 р. У зв'язку з чим групі урядових експертів було доручено подати доповідь на 68-й сесії Генеральної Асамблеї у вересні 2013 р., який було видано у вигляді документа A/68/98491[92,с.83].

У 2012 р. Генеральна Асамблея ООН на 48-му пленарному засіданні висловила занепокоєння можливим потенційно небезпечним застосуванням інформаційних технологій у цілях, несумісних із забезпеченням міжнародної стабільності та безпеки, та її наслідками у формі негативного впливу на цілісність інформаційної державної інфраструктури та забезпечення безпеки у громадян у військовій сферах.

У зв'язку з чим Генеральна Асамблея ООН визначила необхідність запобігання використанню інформаційних ресурсів або технологій у злочинних чи терористичних цілях .

У 2015 р. група урядових експертів з питань розвитку інформації та телекомунікацій підготувала доповідь, в якій рекомендувала державам-членам ООН заходи щодо зміцнення довіри та приєднатися до Конвенції про кіберзлочинність.

5 грудня 2016 р. Генеральна Асамблея ухвалила Резолюцію 71/28493 щодо розвитку в галузі інформації та телекомунікацій у контексті міжнародної безпеки. У ній (п. 3) пропонувалася всім державам-членам взяти до уваги оцінки та рекомендації, що містяться у зазначеній доповіді групи урядових експертів, у контексті міжнародної безпеки[28].

Крім того, державам-членам рекомендувалося відображати у своїх доповідях: a) зміст концепцій, що розробляються, що включають загальне розуміння питань інформаційної та кібербезпеки; b) потенційні та вживані заходи, спрямовані на зміцнення міжнародної інформаційної безпеки на

глобальному рівні; c) визначення національних зусиль, спрямованих на зміцнення інформаційної безпеки та сприяння міжнародному співробітництву у цій галузі.

У доповіді Комітету ООН з інформації 2017 р., підготовленій на виконання резолюції 72/90 Генеральної Асамблеї, міститься огляд основних досягнень Департаменту суспільної інформації за період з вересня 2017 р. до березня 2018 р. у сфері популяризації роботи ООН у глобальному масштабі через надання послуг у сфері стратегічних комунікацій. Відділ стратегічних комунікацій, виконуючи функції Секретаріату Групи Організації Об'єднаних Націй з питань комунікації та її цільових груп, займається координацією у сфері комунікаційної діяльності у всій системі ООН. Інформація про діяльність служби новин та служби інформаційно-просвітницької роботи міститься в доповідях Генерального секретаря (A/AC.198/2018/3 та A/AC.198/2018/4)[9].

Комітет ООН з інформації сформулював такі принципи, що дозволяють формувати глобальну культуру кібербезпеки:

a) обізнаність. Необхідність забезпечення безпеки інформаційних систем та мереж має бути доведена до учасників;

b) відповідальність. Учасники повинні регулярно аналізувати та оцінювати політику, заходи, практику та процедури на відповідність безпеці інформаційних технологій та мереж;

c) реагування. Учасники повинні обмінюватися інформацією про загрози, ризики та вразливості, вживати своєчасних та спільних заходів щодо попередження комп'ютерних інцидентів, їх виявлення та реагування на них, у тому числі забезпечувати оперативну та ефективну співпрацю для їх попередження;

d) етика. Необхідно враховувати інтереси учасників, оскільки інформаційні системи та мережі проникли в усі куточки сучасного суспільства;

e) демократія. Повинні дотримуватися цінностей демократичного суспільства, включаючи свободу слова, інформації, конфіденційність інформації, телефонних переговорів, телеграфних та інших повідомлень, повинні забезпечуватися гласність, відкритість та належний захист інформації особистого характеру;

f) оцінка ризику. Ризики повинні оцінюватися, це дозволить виявляти загрози та фактори вразливості. Необхідно: мати велику базу ризиків, які враховуватимуть внутрішні та зовнішні фактори, що впливають на фізичні та людські фактори, функціонування та стійкість технологій, застосовувану методику забезпечення стабільності функціонування інформаційної інфраструктури; визначити допустимий ступінь ризику та вибрати належні інструменти контролю, з тим, щоб регулювати ризик та заподіяння можливої шкоди інформаційним інфраструктурам з урахуванням характеру та значущості інформації, що захищається;

g) проектування та впровадження методів забезпечення інформаційної безпеки. Безпека має бути найважливішим елементом експлуатації та використання, планування та проектування інформаційних інфраструктур;

h) управління забезпеченням інформаційної безпеки. Повинен бути визначений комплексний підхід до цього управління, що ґрунтується на оцінці ризику, що охоплює аспекти діяльності всіх учасників;

i) переоцінка. Проблеми забезпечення безпеки інформаційної інфраструктури повинні піддаватися огляду та оцінки[23].

В даний час держави-члени ООН використовують різні правові механізми та практичні заходи для забезпечення захисту інформації та інформаційних систем. Тому, розвиваючи міжнародне співробітництво у сфері забезпечення інформаційної безпеки, необхідно враховувати національні відмінності у методах регулювання створення, використання та забезпечення безпеки інформаційних інфраструктур.

Держави-члени ООН розробляють законодавство з огляду на принципи міжнародної інформаційної безпеки. Так, у Хорватії у грудні 2014 р.

прийнято закон про державну інформаційну інфраструктуру Хорватії, спрямований на регулювання прав та обов'язків державних органів щодо створення, розвитку та управління державною інформаційною інфраструктурою. У ньому визначено метод створення та управління громадськими реєстрами, інформаційними технологіями, державними інформаційними службами, а також умови, яким вони мають задовольняти. Прийняття цього Закону є важливим кроком на шляху інтеграції Хорватії до європейських, а також глобальних інформаційних мереж[37].

Безсумнівно, створення державних інформаційних служб є складним завданням, враховуючи темпи розвитку інформаційних технологій, інформаційних послуг, електронних засобів масової інформації, а також питань захисту даних. Крім того, з точки зору організаційного та правового забезпечення безпеки, створення та управління публічними реєстрами та забезпечення сумісності та автентичності інформаційних технологій є складним завданням.

Закони про регулювання інформаційної інфраструктури також приймаються країнами Південно-Східної Азії. Так, держава Бруней Даруссалам визнала, що глобальні тенденції в галузі інформації та телекомунікації породили нові загрози у вигляді кіберзлочинності та кібертероризму життєво важливим інфраструктурам, мережам та наданню послуг. Їхня транснаціональна та нематеріальна природа вимагає спільних зусиль світової спільноти зі створення безпечного та надійного онлайн-середовища.

У Бруней Даруссаламі у травні 2004 р. створено Національне агентство боротьби з комп'ютерними та інтернет інцидентами. Держава співпрацює з регіональними та міжнародними партнерами та бере участь у робочій групі ADMM-Plus з кібербезпеки, до якої входять представники 18 країн у галузі захисту кіберпростору в регіоні з метою вирішення проблем кібербезпеки, подолання загроз кіберпростору, у тому числі загроз, що виникають у зв'язку з використанням хмарних обчислень та мобільних систем[61].

Сучасні умови потребують комплексного підходу до формування міжнародного законодавства у сфері створення та використання інформаційної інфраструктури. Наприклад, Уряд Куби вважає за необхідне розробити міжнародну-нормативну базу у сфері ІКТ. Усі держави мають поважати міжнародні стандарти у цій галузі.

Уряд Куби заявляє, що доступ до інформаційних або телекомунікаційних систем іншої держави має здійснюватися на основі міжнародних угод про співпрацю у цій сфері.

Можливе вороже використання телекомунікацій з явним чи прихованим наміром підриває правову та політичну систему держав і є порушенням міжнародного права, визнаних норм у цій галузі, є незаконним та безвідповідальним використанням таких засобів і може призвести до виникнення напруженості та ситуацій, які не є сприятливими для інформаційної безпеки та міжнародного світу, а також негативно впливають на цілісність державної інфраструктури та її безпеку.

Куба стурбована таємним та незаконним використанням окремими особами, організаціями та державами комп'ютерних систем інших країн для організації міжнародних конфліктів. Радіо та телепередачі проти Куби, що транслюються США, суперечать цілям та принципам Статуту ООН, міжнародного права та положенням Міжнародного союзу електрозв'язку. Куба вважає, що міжнародне співробітництво має важливе значення для боротьби з небезпеками, пов'язаними із неправильним використанням ІКТ[62].

Всесвітня асамблея зі стандартизації електрозв'язку (ВАСЕ) заснована 1865 р., – вищий орган Міжнародного союзу електрозв'язку, його членами є 193 держави, близько 700 компаній, організацій та інститутів.

Рекомендації та резолюції ВАСЕ-2016 стали основою для розробки найважливіших стратегічних напрямків у галузі стандартизації міжнародного електрозв'язку, що дозволило національним мережам зв'язку увійти до всесвітньої інфокомунікаційної інфраструктури. На засіданні учасники

ВАСЕ-16 обговорили проблему забезпечення інформаційної безпеки розвитку технологій «Інтернету речей», що дозволило ухвалити важливе рішення щодо визначення загальних принципів діяльності сектору стандартизації електрозв'язку Міжнародного союзу електрозв'язку (МСЕ-Т)[92,с.84].

В даний час МСЕ-Т складається з 11 дослідницьких комісій.

У 2017 р. акцент у роботі Міжнародного союзу електрозв'язку був зроблений на потребах країн, що розвиваються, велика увага приділена питанням, пов'язаним з розвитком широкосмугового доступу, насамперед з використанням систем рухомого радіозв'язку, зі зміцненням довіри та безпекою при використанні ІКТ, зі зростаючою роллю ІКТ в попередження та ліквідації наслідків надзвичайних ситуацій та при зміні клімату, з розвитком «розумних технологій».

Вироблення загальних підходів до використання інформаційних інфраструктур сприятиме стійкому економічному зростанню всіх країн, зниження рівня соціальної нерівності та скорочення економічного, технологічного та цифрового розриву. Його подолання необхідне для сталого розвитку інформаційної інфраструктури, підвищення рівня освіти та охорони здоров'я, нарощування потенціалу, збереження культурної спадщини у всьому її різноманітті, а також використання ІКТ для боротьби зі злиднями та наслідками зміни клімату, надання допомоги при надзвичайних ситуаціях, забезпечення цифрової трансформації та переходу до цифрової економіки[95].

Україна підтримує активну позицію Міжнародного союзу електрозв'язку не лише як спеціалізованої організації ООН у сфері телекомунікацій, а й як провідної міжнародної організації у цій галузі.

Питання інформаційної безпеки та управління критичною інфраструктурою Інтернету регулярно обговорюються на зустрічах «Великої двадцятки» ООН на зустрічах міністрів телекомунікацій та інформаційних технологій країн БРІКС.

Європейський Союз висловлює занепокоєння у зв'язку з інцидентами безпеки, що відбуваються, що становлять серйозну загрозу для функціонування мережевих та інформаційних систем, що перешкоджають економічній діяльності та спричиняють значні фінансові втрати.

Питання інформаційної безпеки неодноразово обговорювалися Радою Європи. Так, було прийнято перелік документів у цій галузі:

Рекомендація № R(87), що регламентує забезпечення безпеки персональних даних; керівний документ - Рекомендація № R (89) про комп'ютерні злочини, що визначає комп'ютерні злочини; у 1995 р. дві Рекомендації у сфері інформаційних технологій, це – Рекомендація № R (95) про захист персональних даних у сфері телекомунікаційних послуг та Рекомендація № R (95) щодо кримінального процесу, пов'язаного з інформаційними технологіями[30].

Розробка проекту конвенції про злочини у сфері комп'ютерної інформації тривала з 1996 р. по 2001 р., у якому була прийнята. У рамках виконання цієї Конвенції Європейським комітетом з проблем злочинів створено структуру, функціями якої є запобігання та боротьба з кіберзлочинами. Інформаційні технології, проникаючи у всі сфери суспільства, створюють точки напруженості та вразливості, що використовуються для скоєння кіберзлочинів. У лютому 1997 р. рішенням № CM/Del/Dec (97) Комітету міністрів Ради Європи засновано Комітет експертів зі злочинів у кіберпросторі. У 2000 р. на 50 пленарну сесію Комітету було представлено переглянутий варіант Конвенції, в якій регламентувалися обов'язкові міжнародно-правові норми у сфері інформаційної безпеки[10].

Таким чином, можна відзначити, що Рада Європи здійснює розробку та систематизацію правового регулювання з 1987 р. У 2001 р. Рада Європи схвалила Конвенцію про злочинність у сфері комп'ютерної інформації, до якої приєдналося понад 30 держав.

У ній передбачено наступний правовий механізм міжнародного співробітництва та дотримання принципів міжнародного права з метою протидії кіберзлочинності: заборона протиправного використання інформаційних технологій та комп'ютерних засобів, поширення шкідливого інформаційного змісту; взаємодія правоохоронних органів у сфері здійснення процесуальних дій; обов'язок надання допомоги у сфері судових розглядів та розслідування комп'ютерних злочинів; заборона на здійснення соціально небезпечних діянь, таких як порушення доступності та цілісності комп'ютерної інформації та систем; порушення авторських та суміжних прав. Конвенція містила пропозиції до держав-учасниць щодо включення норм матеріального кримінального права до національного законодавства, що передбачають кримінальну відповідальність за низку дій злочинного характеру[19].

Конвенція про злочини у сфері комп'ютерної інформації пропонувала об'єднати зусилля міжнародного співтовариства у боротьбі з кіберзлочинами, що мають транскордонний характер та уніфікувати законодавство у цій сфері. Як передбачалося, це має спростити боротьбу з комп'ютерними злочинами та полегшити взаємодію органів державної влади для притягнення винних осіб до відповідальності.

У Директиві ЄС 2016/1148503 наголошується, що наявних можливостей недостатньо для забезпечення високого рівня безпеки мережевих та інформаційних систем у Союзі. Держави-члени мають дуже різні технологічні рівні, що призводить до роздроблених підходів у рамках Союзу, до нерівного рівня захисту споживачів та підприємств та підриває загальний рівень безпеки мережевих та інформаційних систем. Крім того, відсутність загальних вимог до операторів основних послуг та постачальників цифрових послуг унеможливлює створення глобального та ефективного механізму міжнародного співробітництва в даній сфері[5].

2016 р. став важливою віхою у боротьбі з кіберзлочинністю. По-перше, було підписано Спільну декларацію між ЄС та НАТО, яка заклала основи

їхньої співпраці. По-друге, Європейським парламентом і Радою Європи було прийнято Директиву з безпеки мережі та інформаційних систем (NIS504 (далі – Директива NIS). У ній передбачені зобов'язання держав-учасниць ЄС розробитиконтроль за обміном інформацією в Інтернеті незалежно від кордонів повинен залишатися винятком, на 840-му засіданні заступників міністрів скасував такі документи: Конвенцію про злочинність у сфері комп'ютерної інформації, Рекомендацію Rec(2001) про саморегулювання віртуального змісту, а також Директиву 2000/31/ЄС Європарламенту та Ради ЄС від 8 червня 2000 р. щодо правових аспектів послуг в інформаційному суспільстві[17].

Мотивувавши своє рішення занепокоєнням про розширення можливостей щодо обмеження інформаційного обміну в Інтернеті з різних підстав, що суперечать демократичним принципам.

У ухваленій на цьому засіданні Декларації про свободу обміну інформацією в Інтернеті наголошувалося, що ця свобода має забезпечувати людську гідність, права людини, а не обмежувати їх основні свободи, зокрема права неповнолітніх.

З метою забезпечення свободи обміну інформації, балансу між бажанням користувачів Інтернетом залишатися анонімними та необхідністю правоохоронних органів відстежувати осіб, відповідальних за кримінальні правопорушення, Комітет міністрів Ради Європи сформулював такі принципи в галузі обміну інформацією в Інтернеті:

Принцип 1: Держави-члени не повинні обмежувати інформацію в Інтернеті більшою мірою, ніж це застосовується до інших засобів передачі інформації.

Принцип 2: Держави-члени повинні здійснювати саморегулювання або спільне регулювання щодо інформації, що розповсюджується через Інтернет.

Принцип 3: Органи державної влади не повинні обмежувати доступ до інформації та обміну інформацією в Інтернеті шляхом застосування заборонних або обмежувальних заходів загального характеру незалежно від

кордонів. Це положення не перешкоджає установці фільтрів для захисту неповнолітніх, зокрема, у місцях, доступних для них, таких як школи або бібліотеки.

За умови дотримання гарантій безпеки, передбачених § 2 ст. 10 Конвенції про захист прав людини та основних свобод 1950 року, можуть бути вжиті заходи щодо видалення чітко визначеної інформації, що розповсюджується в Інтернеті, або, як альтернатива, щодо заборони доступу до Інтернету у разі, якщо компетентні національні органи влади прийняли попереднє або остаточне рішення про її незаконність.

Принцип 4: Держави-члени повинні забезпечувати та заохочувати доступ усіх осіб до інформації, що міститься в Інтернеті та інформаційних послуг на недискримінаційній основі за прийнятними цінами. Крім того, активна участь населення, наприклад, шляхом розробки та підтримки індивідуальних веб-сайтів, не підлягає ліцензуванню чи виконанню аналогічних вимог.

Принцип 5: Положення про послуги, що надаються через Інтернет, не підпадає під дію спеціальних дозвільних схем лише у зв'язку з тим, що особами використовуються канали та засоби передачі інформації.

Держави-члени повинні стимулювати пропозиції щодо створення на своїй території різноманітних пропозицій послуг через Інтернет та їх просування. Ці послуги повинні бути орієнтовані на різні потреби користувачів та соціальних груп. Провайдеру мають бути дозволені дії в рамках нормативно-правової бази, яка гарантує їм недискримінаційний доступ до національних та міжнародних телекомунікаційних мереж.

Принцип 6: Держави-члени не повинні покладати на провайдера обов'язок здійснювати моніторинг інформації в Інтернеті, до якої він має доступ і яку він передає чи зберігає, або добувати докази та факти, що дають змогу встановлювати протиправну діяльність[18].

Держави-члени повинні визначити у своїх нормативних правових актах умову про те, що провайдери не несуть відповідальності за інформацію, що

розповсюджується в Інтернеті, якщо їх функціонування обмежене передачею інформації або наданням доступу до Інтернету відповідно до національного законодавства.

Якщо функції провайдерів розширені, і вони зберігають інформацію на своїх серверах, що виходить з інших сторін, то держави-члени можуть покласти на них відповідальність за поширення інформації в Інтернеті для випадків, коли провайдери не реагують на вимогу державних органів про блокування шкідливої інформації або інформаційного ресурсу в Інтернеті, як тільки стало відомо про це[25].

При визначенні відповідальності провайдерів відповідно до національного законодавства, належну увагу необхідно приділяти свободі вираження поглядів тих осіб, які спочатку опублікували інформацію, а також відповідному праву користувачів на інформацію.

Принцип 7: Держави-члени повинні забезпечити правову регламентацію бажання користувачів Інтернету не розкривати особистість.

Це не повинно заважати державам-членам вживати заходів та співпрацювати з питань розшуку осіб, відповідальних за вчинення кримінальних дій відповідно до національного законодавства, Конвенції про захист прав людини та основних свобод та інших міжнародних угод в галузі правосуддя та охорони порядку[18].

Конвенції про злочини у сфері комп'ютерної інформації, незважаючи на її скасування на 840-му засіданні заступників міністрів, є чинною, як зазначено на сайті Конвенції, і вона відкрита для підписання державами членами Ради Європи та державами, які не є членами Ради Європи, але які взяли участь у її складанні, а також для приєднання інших країн – не членів Ради Європи.

Крім того, у галузі правового регулювання безпеки мережевих інформаційних систем ЄС діє ст. 13а Рамкової директиви (2009/140/ЕС), запроваджена у 2009 р. для забезпечення безпеки та цілісності мережі та доступності послуг електронних комунікацій.

В галузі безпеки мобільних систем Європейське агентство мережевої та інформаційної безпеки (ENISA) – провідна організація Євросоюзу, відповідальна за проведення кіберучень, визначила мінімальні вимоги до кібербезпеки.

Заходи, що забезпечують безпеку з'єднання через встановлені точки відкритого доступу, визначені Рекомендацією № R (99) 14 про універсальні послуги щодо нових засобів зв'язку та інформаційних служб. В галузі електронних ідентифікаційних та довірчих послуг для здійснення електронних транзакцій на внутрішньому ринку (eIDAS) розроблено Регламент (ЄС) № 910/2014. У жовтні 2017 р. Європейська рада запропонувала Комісії ООН розробити пропозиції щодо забезпечення кібербезпеки[53].

У 2018 р. ЄС розробив загальну систему сертифікації інформаційних систем, що забезпечує кібербезпеку та адекватний рівень надання продуктів та послуг ІКТ. У тому ж році Європейська комісія запропонувала ухвалити закон про кібербезпеку, в якому передбачається вісім варіантів політик, що охоплюють сертифікацію ENISA та кібербезпеку ІКТ.

Для забезпечення інформаційної безпеки створюється європейська платформа сертифікації в галузі кібербезпеки продуктів та послугу сфері ІКТ, що визначає схеми сертифікації в даній галузі, що дозволяє цим продуктам та послугам бути визнаними у всіх державах-членах.

Крім того, ЄС створює єдину інформаційну інфраструктуру, яка забезпечить взаємодію таких інформаційних систем: в'їзду/виїзду (EES); візової інформаційної системи (VIS); Євродак – Шенгенської інформаційної системи (SIS) та Європейської системи збирання інформації про кримінальні злочини для громадян третіх країн (ECRIS-TCN), таким чином, щоб вони та їх дані доповнювали одне одного[88].

Для створення єдиної інформаційної інфраструктури як компоненти функціональної сумісності розробляються європейський пошуковий портал (ESP), спільно використовувана служба біометричного зіставлення (BMS),

загальне резидентне сховище (CIR) та детектор множинного ідентифікатора (MID).

Протягом чотирьох років країни-члени ЄС розробляють національне законодавство щодо регулювання інформаційної інфраструктури. Так, ФРН підтримує зусилля щодо узгодження методів застосування міжнародного законодавства при національному регулюванні використання ІКТ, у тому числі у разі розробки норм технічного регулювання, що застосовуються у добровільному порядку, правил (принципів) відповідальної поведінки держави, спрямованих на створення відкритої, безпечної, стабільної, доступної та мирної ІКТ. Особливого значення у цьому контексті має робота груп урядових експертів з питань розвитку галузі створення та використання інформації та телекомунікацій. ФРН брала активну участь у визначенні та здійсненні заходів зміцнення довіри, спрямованих на забезпечення безпеки в галузі державного використання ІКТ. Серед останніх національних заходів регулювання слід назвати прийняття у 2015 р. Закону «Про техніку безпеки», переглянутого у листопаді 2016 р., Стратегії кібербезпеки та прийняття Урядом ФРН рішення про створення інституту міжнародної кібербезпеки з метою систематизації зусиль у цій галузі. Зусилля ФРН щодо інформації та телекомунікацій у контексті міжнародної безпеки є частиною інтенсивної роботи із сприяння безпеці ІКТ[30].

Греція ратифікувала Конвенцію про злочини у сфері комп'ютерної інформації та Додатковий протокол до неї, що стосується криміналізації дій, пов'язаних з поширенням расової ворожнечі та інформації, що носить ксенофобський характер, скоєних за допомогою комп'ютерних систем.

Однак інтеграція Директиви ЄС з безпеки мережевих та інформаційних систем до національного законодавства Греції здійснювалася і до ратифікації зазначеної Конвенції. Згідно з інформацією, наданою Міністерством оборони Греції, на національному рівні були зроблені зусилля щодо зміцнення інформаційної безпеки та сприяння міжнародному співробітництву. Зокрема, розроблено Національну стратегію в галузі кібербезпеки Греції, в якій

передбачені дії щодо підтримання мінімальних вимог кібербезпеки, яка є частиною планів національної оборони. Створено Центр операцій із кібербезпеки, функціями якого передбачено розробку мережевих систем національної військової оборони країни[67].

Таким чином можна зазначити, що в країнах Євросоюзу розроблені та постійно вдосконалюються процедури реагування на інциденти (надзвичайні ситуації). Створюються групи швидкого реагування, які можуть розвернутися в найкоротші терміни для усунення наслідків кібератак, здійснених у військових чи громадських мережах. Процедури відновлення при комп'ютерних збоях або кібератаках інтегровані в комп'ютерну інформаційну безпеку та політичні документи.

Взаємодія між інформаційними системами країнами-членами Євросоюзу дозволяє узгоджувати вимоги до їх якості та забезпечення ефективного використання даних Європолу та баз даних Інтерполу шляхом полегшення доступу до них відповідних структур.

РОЗДІЛ 3

ПЕРСПЕКТИВИ МІЖНАРОДНО-ПРАВОВОГО РЕГУЛЮВАННЯ В СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ДОСВІД УКРАЇНИ

3.1. Механізми міжнародно-правового регулювання в сфері забезпечення інформаційної безпеки

Основні питання, пов'язані з інформаційною злочинністю та інформаційним тероризмом такі: уніфікація національного законодавства, що встановлює відповідальність за дії, що підпадають під визначення інформаційного тероризму та інформаційних злочинів, вирішення проблеми юрисдикції, тобто визначення того, яка держава має право залучити порушника до відповідальності загальної правової допомоги у справах про інформаційні злочини та інформаційний тероризм.

Вирішенню першої проблеми, пов'язаної з уніфікацією кримінального законодавства держав, може сприяти прийняття універсального міжнародного договору, присвяченого питанням інформаційної безпеки та, зокрема, проблемі інформаційного тероризму та інформаційної злочинності.

При розробці зазначеного договору слід враховувати позитивний досвід Ради Європи у розробці Конвенції про кіберзлочини, аналіз якої проводився у другому розділі цього дослідження.

При розробці міжнародного договору необхідно також проводити розмежування між злочинами, що посягають на перший аспект інформаційної безпеки, тобто пов'язаних із змістом інформації, та злочинами, пов'язаними з другим аспектом інформаційної безпеки, тобто з інформаційною інфраструктурою, включаючи комп'ютери та інформаційні мережі[28].

До злочинів, пов'язаних із змістом інформації, слід включати діяння, спрямовані на виробництво, розповсюдження, передачу або інші способи, що роблять доступною інформацію, заборонену до поширення міжнародним

правом або національним законодавством, а саме наступної інформації: пропаганди війни, підбурювання до війни, пропаганда насильства, расової ненависті, дискримінації, апартеїду, геноциду, дитячої порнографії[4].

До злочинів, пов'язаних з інформаційною інфраструктурою, можна віднести такі три групи злочинів:

1.Злочини, в яких комп'ютери та інформаційні системи та мережі виступають як об'єкт злочину:

- викрадення інформації (конфіденційних даних, тощо)
- шкідництво стосовно даних чи інформаційних систем, втручання в інформаційну систему чи комп'ютер
- неавторизований доступ до інформаційної системи або комп'ютера
- перехоплення інформації, що передається за допомогою інформаційної мережі, системи або комп'ютера
- використання шкідливих програм з метою порушення нормальної роботи комп'ютерної системи чи мережі.

2.Злочини, в яких комп'ютер та інформаційна система виступають як засіб скоєння звичайних злочині:

- присвоєння або розтрата майна крадіжка за допомогою комп'ютера
- шахрайство
- фальсифікації
- комп'ютерне хуліганство
- комп'ютерний вандалізм.

3. Злочини, пов'язані з порушенням авторських та суміжних прав:

- порушення авторських прав

- порушення суміжних прав

З суб'єктивної сторони всі ці злочини повинні відбуватися з прямим наміром[37].

Прийняття в рамках конвенції узгоджених ознак складів злочинів, пов'язаних з комп'ютерами та інформаційними мережами, дозволить державам більш ефективно боротися з цими загрозами інформаційній безпеці.

У Конвенції Ради Європи використовується принцип територіальної юрисдикції. Тобто держава має юрисдикцію щодо злочину, вчиненого на його території. Тим часом, як зазначалося, це не вирішує зазначеної проблеми, тому що необхідно визначити, що є місцем скоєння злочину.

Слід сказати, що територіальний принцип юрисдикції не єдиний у практиці держав. Крім територіального принципу існують такі теорії юрисдикції:

Теорія національності. Відповідно до цієї теорії держава має юрисдикцію над своїми громадянами, навіть якщо ці громадяни вчинили злочин на території іншої держави, за умови, що дії ними вчинені є злочином за законодавством держави, де вони були вчинені.

Захисна теорія. Держава має юрисдикцію щодо тих, чиї дії загрожують безпеці чи життєвим інтересам держави, навіть якщо ці особи є іноземними громадянами чи особами без громадянства.

Теорія пасивної індивідуальності. Держава має юрисдикцію щодо того, хто зазіхає або загрожує громадянам цієї держави, навіть якщо вони перебувають за кордоном.

Універсальна теорія, коли будь-яка держава має юрисдикцію над тими, хто вчинив певні універсально визнані злочини, наприклад, піратство. У практиці держав, як правило, застосовується не одна теорія юрисдикції, а кілька, які охоплюють різні ситуації.

У зв'язку з цим, є обґрунтованим встановлення у конвенції територіального принципу визначення юрисдикції, проте, слід зазначити, що цей принцип не повинен торкатися інших принципів, що містяться в національному законодавстві.

У зв'язку із встановленням принципу територіальної юрисдикції необхідно визначити, що є місцем скоєння злочину.

Як відомо, злочини бувають двох видів, а саме ті, які вважаються вчиненими з моменту здійснення всіх дій, передбачених складом злочину (у російській теорії кримінального права такі злочини називають злочинами з формальним складом), і ті, що вважаються вчиненими з моменту настання передбачених кримінальним. законом суспільно небезпечних наслідків (так звані злочини із матеріальним складом). Звісно ж, що місцем скоєння злочину слід вважати місце здійснення дій для формальних складів і місце наступу передбачених законом наслідків для матеріальних складів, у своїй, якщо дії, що спричинили наслідки, вважаються злочином з права іншої держави[5].

У разі конфлікту юрисдикції, зазначене питання дозволяється шляхом проведення консультацій між державами, які мають юрисдикцію щодо цього діяння.

Питання надання правової допомоги включають допомогу у зборі доказів, у виконанні судових доручень, а також питання екстрадиції. Як уже було показано у другому розділі цього дослідження, Конвенція Ради Європи про Кіберзлочини містить багато нових та прогресивних принципів, що стосуються питань надання правової допомоги у збиранні доказів, які можуть бути використані при розробці універсальної конвенції. Тому тут ми коротко зупинимося на питання екстрадиції.

Екстрадиція є важливим інститутом міжнародного кримінального права, який дозволяє забезпечити притягнення злочинця до кримінальної відповідальності за скоєне діяння. Цей інститут дуже тісно пов'язаний із національним законодавством кожної держави[73].

Для того щоб уникнути питань, пов'язаних з екстрадицією до конвенції, на наш погляд, необхідно передбачити положення, що наказує державам-учасницям конвенції включити злочини, передбачені конвенцією як злочини, за якими можлива видача злочинців у своє національне законодавство та у відповідні договори про надання правової допомоги або у договори. про видачу злочинців. Це положення не означає, що екстрадиція повинна здійснюватися щодо кожного злочину, воно лише передбачає можливість видачі особи, яка вчинила злочин державі, яка має відповідну юрисдикцію.

Щоб уникнути відмов у видачі злочинців лише на основі того, що між відповідними державами відсутня договір про правову допомогу або договір про видачу злочинців, на нашу думку, до конвенції необхідно включити положення, яке передбачає, що у разі відсутності між деякими державами договору про правову допомогу або договору про видачу злочинців, ця конвенція може розглядатися зазначеними сторонами як правова підстава для надання правової допомоги або для видачі злочинців[87].

Включення до конвенції зазначених вище положень дозволить уникнути питань та втрати часу при притягненні до відповідальності осіб, винних у скоєнні комп'ютерних злочинів.

Інформаційний тероризм може включати всі види комп'ютерних злочинів, зазначених вище. Найголовніший кваліфікуючий ознака тероризму - політичні цілі, політичний характер діяння, а також мета створення обстановки терору, паніки, небезпеки. Тероризм, таким чином, суттєво відрізняється від простих злочинів ступенем суспільної небезпеки.

З метою боротьби з інформаційним тероризмом доцільно включити становище, встановлює, що у разі якщо якесь із встановлених конвенцією злочинів відбуваються з політичних мотивів, з метою створення обстановки страху і паніки, зазначені злочини визнаються інформаційним тероризмом. Держави згодні встановити дії, визнані інформаційним тероризмом як суворе покарання.

Таким чином, у разі включення до конвенції зазначених вище положень вона стане ефективним міжнародним інструментом для взаємодії держав у сфері боротьби з інформаційним тероризмом та інформаційною злочинністю.

3.2. Відповідальність за дії в сфері інформаційної безпеки

Відповідальність є дуже важливим інститутом міжнародного права. Стосовно сфери забезпечення інформаційної безпеки, розробка механізму відповідальності держав за дії в інформаційній сфері є надзвичайно важливим та актуальним завданням, оскільки ефективне функціонування режиму інформаційної безпеки немислимо без передбачених міжнародним правом заходів міжнародної відповідальності держав за порушення зазначеного режиму.

Проблеми відповідальності держав в інформаційній сфері мають дуже велике значення для правового регулювання першого аспекту інформаційної безпеки, проте, враховуючи розвиток інформаційних та комунікаційних технологій, а також їхнє величезне значення для функціонування держави, є необхідним визначити основи відповідальності держав за діяльність в інформаційній сфері стосовно та до другого аспекту інформаційної безпеки держави[71,с.8].

Також має сенс уточнити деякі питання відповідальності держав, пов'язані зі змістом інформації, що розповсюджується.

Підставами міжнародної відповідальності держави є дії, що порушують звичайні або договірні норми міжнародного права, які називають міжнародними деліктами. Детально підстави відповідальності країн за міжнародні правопорушення розглядаються у роботах спеціально присвячених міжнародної відповідальності країн. У зазначених роботах у міжнародному правопорушенні виділяються різні елементи, наявність яких у діях є підставою відповідальності. Оскільки у зазначених теоретичних роботах загальні підстави відповідальності держав досліджено досить повно,

у цьому дослідженні доцільно ще раз систематизувати ті дії, вчинення яких може загрожувати інформаційної безпеки держави, будучи основою міжнародної відповідальності[68].

Перший аспект. Дії, що стосуються поширення інформації, забороненої для поширення міжнародним правом, а саме: пропаганда війни та застосування сили, пропаганда насильства, поширення інформації, що підбурює до війни, пропаганда різних форм расової дискримінації, поширення порнографічних матеріалів. Сюди також слід додати використання державою засобів та методів інформаційного впливу на населення іншої держави, тобто поширення інформації спеціальним чином сформульованої виключно з метою надання психологічного та/або ідеологічного впливу на свідомість населення або окремих осіб, включаючи поширення дезінформації, інформації образливої для релігійних та моральних. поглядів людей, інформації, що пропагує відмову від системи цінностей традиційної для цієї держави[79].

Таким чином, як підстави відповідальності держави в рамках першого аспекту є, по-перше, дії, які досить давно розглядаються як заборонені міжнародним правом, по-друге, дії поява та зростання значення яких обумовлено розвитком в інформаційних та комунікаційних технологіях.

Підставою міжнародної відповідальності держав є систематичне поширення зазначеної вище інформації, оскільки саме систематичність поширення є сильним чинником загрози інформаційної безпеки.

Другий аспект. Підставою відповідальності держави є дії у межах інформаційних війн, застосування інформаційної зброї, заохочення інформаційного тероризму. Дії в рамках інформаційних воєн це насамперед здійснення комп'ютерного вторгнення в інформаційні системи критичних структур держави, а також здійснення вторгнення в інші інфраструктури, якщо такі вторгнення спричинили значні економічні збитки.

Зазначене питання неодноразово обговорювалося в теорії міжнародного права. Негативний висновок щодо присвоєння державі дій осіб

або груп осіб не означає, що держава не може нести міжнародну відповідальність за ці дії приватних осіб. Державі, яка не виконала свій обов'язок по відношенню до іншої держави захищати її громадян від дій приватних осіб, слід нести відповідальність[66,с.38]

Західними державами і, насамперед США, дуже часто висловлюється думка, що держава немає права контролювати діяльність приватних осіб у сфері, оскільки будь-який контроль у цій сфері може торкнутися право кожного вільно поширювати, отримувати і шукати інформацію. На підставі цього робиться висновок про те, що держава у цій сфері не може відповідати за дії приватних осіб. Проте, на нашу думку, такий висновок не цілком виправданий з наступних причин.

По-перше, як уже говорилося, розвиток інформаційних технологій надає окремим особам можливості значного впливу на інформаційну інфраструктуру держави, у тому числі на критичні структури, тобто регулювання та контроль діяльності в інформаційній сфері необхідний з метою забезпечення безпеки кожної держави.

По-друге, регулювання та контроль діяльності в інформаційній сфері не є чимось новим у законодавчій та правозастосовній практиці переважної більшості держав. Практично у всіх державах прийняті та діють закони та інші нормативні правові акти, що висувають досить серйозні вимоги до суб'єктів діяльності в інформаційній сфері та насамперед до засобів масової інформації.

По-третє, міжнародним правом передбачена можливість певного обмеження прав людини, у тому числі права шукати, отримувати та поширювати інформацію з метою забезпечення державної безпеки та моральності, (ст. 19 Міжнародного пакту про громадянські та політичні права) Оскільки з розвитком інформаційних технологій одна держава не може сама забезпечити свою інформаційну безпеку, інакше вона була б просто відірвана від можливостей, що надаються інформаційними технологіями, кожна держава повинна вживати заходів для регулювання та

контролю в інформаційній сфері з метою запобігання вчиненню дій, що становлять під загрозу інформаційну безпеку[24].

Таким чином, стосовно сфери інформаційних відносин дуже важливо, щоб держава забезпечувала дотримання своїми громадянами принципів використання інформаційного простору, а також інших вимог та приписів міжнародного права. Отже, неефективне здійснення державою своїх функцій у цій сфері може бути основою міжнародної відповідальності держави.

Відповідно до теорії міжнародної відповідальності держави, всі міжнародні правопорушення діляться на міжнародні злочини та інші міжнародні правопорушення (делікти).

Основним критерієм віднесення міжнародного правопорушення до тієї чи іншої групи є зміст норми, яка порушена, а також важливість тих суспільних відносин, які були порушені. Так, за висловом Мазова В.А., наслідки порушення міжнародного зобов'язання повинні залежати як від змісту «первинних» норм, на яких це зобов'язання ґрунтувалося, так і від їхньої цінності для всього міжнародного співтовариства.

У міжнародному праві міжнародними злочинами вважаються тяжкі порушення міжнародних зобов'язань основоположних задля забезпечення життєво важливих інтересів міжнародного співтовариства. Такими зобов'язаннями насамперед є зобов'язання утримуватися від агресивної війни, як життєво важливе для забезпечення міжнародного миру та безпеки, зобов'язання забороняють рабство, геноцид, апартеїд, як життєво важливі для захисту людської особистості, зобов'язання, що забороняють масове забруднення морів або атмосфери, як життєво важливі захисту навколишнього середовища[13].

Звісно ж, що зобов'язання, внаслідок яких інформаційний простір має використовуватися у мирних цілях, для блага всіх держав, зобов'язання забороняють використання інформаційної зброї та ведення інформаційних війн, на сучасному етапі розвитку інформаційних технологій є життєво

важливими для підтримки сталого розвитку, стратегічної стабільності та міжнародної безпеки. Таким чином, дії, що порушують зазначені міжнародні зобов'язання, тобто підготовка та ведення державою інформаційних воєн, слід визнати не просто міжнародним правопорушенням, а міжнародним злочином, тобто найбільш тяжким діянням, що тягне за собою суворі заходи міжнародної відповідальності.

На мою думку, за сучасних умов слід переглянути заходи відповідальності держави за міжнародну інформаційну діяльність, яка загрожує інформаційній безпеці.

Як мовилося вище, порушення зобов'язань мирного використання інформаційного простору, ведення інформаційних війн, може розглядатися як міжнародний злочин. Таким чином, відповідальність за вчинення таких дій має бути суворішою, ніж просто політичні вимоги виконувати міжнародні зобов'язання, які не пов'язані з іншими наслідками для держави порушника.

Теоретично міжнародного права виділяють два основних види відповідальності держав: політична відповідальність і матеріальна відповідальність, у своїй до політичної відповідальності відноситимуться всі форми відповідальності держави, крім матеріальної відповідальності, від так званого морального задоволення до різних заходів, що з обмеженням суверенітету держави? Звісно ж, стосовно дій у інформаційної сфері держава порушник має нести всі види відповідальності, як політичну, і матеріальну[40,с.267].

Політична відповідальність держави може виражатися, наприклад, у таких негативних наслідках: інформаційна блокада держави порушника, контроль критично важливих структур держави порушника, контроль інформаційних ресурсів, вторгнення в інформаційну інфраструктуру і т.д.

Матеріальна відповідальність може виражатися як відшкодування матеріальної шкоди, викликаного інформаційним нападом, відновлення з допомогою держави-порушника роботи інформаційної інфраструктури тощо.

Таким чином, встановлення зазначених вище видів та форм відповідальності держави, яка порушила зобов'язання мирного використання інформаційного простору та інші зобов'язання в інформаційній сфері, сприятиме забезпеченню міжнародної безпеки загалом та інформаційної безпеки зокрема.

3.3.Тенденції та перспективи розвитку правового регулювання інформаційної безпеки в Україні

Інформаційна безпека є невід'ємною складовою національної безпеки і розглядається як пріоритетна функція держави. Інформаційна безпека, з одного боку, передбачає забезпечення якісного комплексного інформування громадян та вільний доступ до різноманітних джерел інформації, а з іншого – контроль за нерозповсюдженням дезінформації, сприяння доброчесності суспільства, збереження інформаційного суверенітету, протидії негативним інформаційно-психологічним пропагандистським впливам та захисту національної інформаційної безпеки. простори від маніпуляцій, інформаційних воєн та операцій. Вирішення комплексної проблеми інформаційної безпеки дозволить як захистити інтереси суспільства та держави, так і гарантувати права громадян на отримання вичерпної, об’єктивної та якісної інформації.

Існують два аспекти тлумачення інформаційної безпеки в контексті національної безпеки. З одного боку, інформаційна безпека розглядається як самостійний елемент національної безпеки будь-якої країни, а з іншого, як інтегрований компонент будь-якої іншої безпеки: військової, економічної, політичної тощо.

Найбільш повне визначення: інформаційна безпека — це такий стан захищеності життєво важливих інтересів особи, суспільства та держави, при якому шкода мінімізується внаслідок неповноти, несвоєчасної та недостовірної інформації, негативного інформаційного впливу, негативних наслідків функціонування інформації. технологій, а також із-за

несанкціонованого поширення інформації [50]. Таке визначення є оптимальним і відображає всі сторони взаємодії суб'єктів інформаційних відносин.

Увага до проблем забезпечення інформаційної безпеки України зумовлена антиукраїнськими впливами, які пропагують ідеї сепаратизму, насильства, міжнаціональної ворожнечі та є спробою знищити національну ідентичність України, зруйнувати міжнаціональну злагоду, посягати на конституційний лад України. Україна, територіальна цілісність держави. Проблема забезпечення інформаційної безпеки України актуалізується в умовах війни на Сході, коли відбувається інформаційна експансія з Російської Федерації, необ'єктивне і необ'єктивне висвітлення фактів і явищ, а також спрямовані технології російських інформаційно-психологічних операцій. на забезпечення домінування в українському (як і в світовому) інформаційному просторі. та зміст переваги ЗМІ. Через російські пропагандистські інформаційно-психологічні кампанії, акції, медіакамери відбувається вплив не лише на суспільну свідомість громадян України, а й на світову спільноту.

Представник Асоціації «Інформаційний опір» В. Гусаров, досліджуючи проблему інформаційної безпеки в Україні, зазначає, що Росія проводить інформаційно-психологічні атаки з метою посилення ескалації конфлікту на сході України, тиску на українське керівництво в щоб змусити його погодитися на московський сценарій. конфлікту. В. Гусаров визначає напрями інформаційно-психологічних атак проти України: 1) нав’язування думок про нездатність української влади керувати державою та приймати раціональні рішення; 2) формування негативних суджень щодо військово-політичного керівництва України та того, що хаотичні бойові дії призводять до невиправданих втрат серед сил ООС; 3) поширення поглядів, що українська армія на Сході України деморалізована і не може вести бойові дії, а також недовіра особового складу до керівництва; 4) нав'язування думки, що без російського газу Україна не обійдеться і що сторонам необхідно

повернутися до перегляду газових контрактів. Експерт зазначає, що цільовою аудиторією Кремля зараз є населення Російської Федерації, російськомовна діаспора за кордоном, населення України, зокрема, в окупованих регіонах Донбасу, громадяни західних країн, а також країни БРІКС та Митного союзу, близькі до Росії за політичними поглядами [43].

Україна стала об'єктом інформаційно-психологічних впливів, операцій, воєн, її інформаційна безпека знаходиться під загрозою. Можна констатувати, що: 1) український інформаційний простір не захищений від зовнішньої негативної пропаганди та маніпулятивних впливів і стає об’єктом інформаційної експансії; 2) у світовому медіапросторі немає українського національного інформаційного продукту, який би поширював об’єктивну, неупереджену та актуальну інформацію про події в Україні. Внаслідок цього світова спільнота відчуває брак інформації або отримує її з інших джерел, які іноді дезінформують, надають спотворену, спотворену, неповну інформацію. При цьому проти України активно використовується потужний медіа-ресурс, здійснюється експансія іноземних суб’єктів на ринку інформаційних послуг, активізуються негативні інформаційні впливи, спрямовані на спотворення реальності, заниження міжнародного іміджу держави; 3) діяльність вітчизняних ЗМІ щодо систематичного, об'єктивного висвітлення фактів, подій і явищ є недостатньою та позбавленою стратегічного планування; інформаційно-комунікаційна політика України у сфері національної безпеки потребує термінового перегляду та вдосконалення.

Рівень інформаційної безпеки держави значною мірою визначається рівнем її інформаційної інфраструктури. На жаль, як зазначає Петрик, низький загальний рівень інформаційної інфраструктури в Україні сприяє розширенню ринку інформаційних послуг іноземними компаніями, що створює сприятливі умови для перерозподілу ефірного часу на користь іноземних програм, частина з яких засмічує українську інформацію. простору зі своїм баченням подій, пропагують побут і традиції, тим самим деструктивно впливаючи на суспільство і державу, руйнуючи морально-

етичні основи генофонду української нації. Недостатній професійний, інтелектуальний та творчий рівень вітчизняного виробника інформаційного продукту та послуг, його недостатня конкурентоспроможність не лише на світовому ринку, а й в Україні, призводить до того, що українська аудиторія закономірно віддає перевагу закордонним інформаційним програмам. Недостатній контроль з боку держави за дотриманням законів України політичними силами, ЗМІ та окремими особами, які здійснюють підприємницьку діяльність в інформаційній сфері, призводить до того, що зараз часті випадки надання ефірного часу телерадіопрограм, спрямованих на руйнування моральних цінностей та української свідомості. нація [79].

Отже, національний інформаційний простір України, на жаль, переживає значні загрози, виклики, які становлять загрозу функціонуванню держави, її політичному та економічному розвитку, інтеграції в європейські та євроатлантичні структури.

Загрози національній безпеці України в інформаційній сфері — це сукупність умов і факторів, що створюють загрозу життєво важливим інтересам держави, суспільства та особистості через можливість негативного інформаційного впливу на свідомість і поведінку громадян, т.п. а також на інформаційні ресурси та інформаційно-технічну інфраструктуру [79].

Як зазначено в Законі України «Про основи національної безпеки», однією з основних загроз інформаційній безпеці є «намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної чи упередженої інформації» [86].

Доктрина інформаційної безпеки України визначає такі загрози інформаційній безпеці країни: поширення у світовому інформаційному просторі спотвореної, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; зовнішні деструктивні інформаційні впливи на суспільну свідомість через ЗМІ, а також Інтернет; деструктивні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності та недоторканності України; прояви

сепаратизму в ЗМІ, а також в Інтернеті за етнічною, мовною, релігійною та іншими ознаками [46].

Як зазначає Р. Р. Марутян, найбільш суттєвою загрозою національній безпеці України в інформаційній сфері є здійснення іноземними державами негативного інформаційно-психологічного впливу на суспільну свідомість громадян України та світової спільноти шляхом проведення інформаційних кампаній та кампаній, спец. інформаційні операції. Це відбувається через систематичне поширення необ'єктивної, неповної чи упередженої інформації про Україну та політичні процеси, що відбуваються на її території. Все це впливає на зовнішню та внутрішню політику нашої держави, знижує її міжнародний імідж, має політичну та економічну основу. Метою таких інформаційних операцій є забезпечення власних національних інтересів інших держав [73].

До загроз національній безпеці України в інформаційній сфері також слід віднести: прояви обмежень свободи слова та доступу громадян до інформації; спотворення, спотворення, блокування, придушення упередженого та тенденційного висвітлення інформації; його несанкціоноване розповсюдження; відкрита дезінформація; інформаційна експансія з інших держав та деструктивне інформаційне вторгнення в національний інформаційний простір, коли країни з потужнішим інформаційним потенціалом мають можливість розширити свій вплив через ЗМІ на населення та громадськість менш потужної держави; виникнення та функціонування неконтрольованих та інформаційних потоків у національному інформаційному просторі держави; поширення культу насильства та жорстокості засобами масової інформації; повільність входження України у світовий інформаційний простір; невизначеність державної інформаційної політики та відсутність необхідної інфраструктури в інформаційній сфері; розміщення дезінформації в Інтернеті.

Слід зазначити, що проти України ведеться інформаційна війна з боку Російської Федерації, спрямована на нав'язування певних ідеологічних

стереотипів, тієї чи іншої громадської думки за допомогою ЗМІ, зокрема за допомогою електронних видань [77]. Війни такого типу досить поширені в глобальному інформаційному просторі, і вони всебічно досліджуються вченими та фахівцями.

Зокрема, Інститут національних стратегічних досліджень США та деякі західні експерти та вчені виділяють декілька елементів інформаційної війни. Однією з них є психологічна війна. Головне завдання психологічної війни — маніпулювання масами. Метою такої маніпуляції є: впровадження ворожих ідей та поглядів у суспільну та індивідуальну свідомість; дезорієнтація та дезінформація мас; послаблення певних переконань, залякування народу образом ворога; залякування ворога власною силою [41].

У сучасному глобалізованому інформаційному суспільстві, де кіберпростір перетворюється на поле боротьби, суттєвими загрозами інформаційній безпеці держави (і України, зокрема) є комп'ютерна злочинність, кібертероризм, кібервійни, за участю протистояння національних інтересів у Інтернет-простору, використання комп'ютерних та Інтернет-технологій для завдавання шкоди ворогу. Частіше технології кібервійни та кібертероризму спрямовані на сферу державної безпеки та оборони і становлять реальну загрозу суверенітету держави.

Отже, проти України широко застосовуються сучасні технології негативного інформаційно-психологічного впливу, які стають загрозою для українського національного інформаційного простору та суверенітету держави. Гарантування інформаційної безпеки України в умовах дестабілізуючих негативних інформаційно-психологічних впливів та експансіоністської агресивної інформаційної політики Російської Федерації потребує консолідації зусиль на всіх рівнях влади та громадянського суспільства.

Як протидії широкомасштабним негативним інформаційно-психологічним впливам, операціям і війнам, пріоритетними напрямами державної інформаційної політики та важливими кроками з боку влади

України мають бути: 1) інтеграція України у світовий та регіональний європейський інформаційний простір; 2) інтеграція в міжнародні інформаційні та інформаційно-телекомунікаційні системи та організації; 3) створення власної національної моделі інформаційного простору та забезпечення розвитку інформаційного суспільства; 4) модернізація всієї системи інформаційної безпеки країни та формування та реалізація ефективної інформаційної політики; 5) удосконалення законодавства з питань інформаційної безпеки, гармонізації національного законодавства з міжнародними стандартами та ефективного правового регулювання інформаційних процесів; 6) розвиток національної інформаційної інфраструктури; 7) підвищення конкурентоспроможності вітчизняних інформаційних продуктів та інформаційних послуг; 8) впровадження сучасних інформаційно-комунікаційних технологій у процеси державного управління; 9) ефективна взаємодія органів державної влади та інститутів громадянського суспільства щодо формування, реалізації та коригування державної політики в інформаційній сфері.

З метою недопущення інформаційного розширення діяльність держави в інформаційному просторі має здійснюватися за такими напрямами: 1) реалізація превентивних стратегій і тактик (превентивних заходів); 2) реалізація стратегії реагування (оперативне реагування на інформаційні атаки противника та активний наступ); 3) захист державного інформаційного сайту. Основна мета – забезпечення домінування та переваги в інформаційному просторі.

Крім того, пріоритетними завданнями інформаційних структур органів влади мають бути: контроль за інформаційними потоками; надання об’єктивної, вичерпної інформації, надання професійних коментарів та роз’яснень щодо подій; систематичне висвітлення службової позиції чиновників і політичних лідерів.

Зазначимо, що для захисту національного інформаційного простору, створення ефективної системи інформаційної безпеки українська влада

вживає певних заходів. Зокрема, 14 січня 2015 р. Кабінет Міністрів України ухвалив постанову, згідно з якою створено Міністерство інформаційної політики України, першочерговими завданнями якого є протидія інформаційній агресії з боку Російської Федерації; розроблення ефективної стратегії інформаційної політики та Концепції інформаційної безпеки України; узгодженість та узгодженість функціонування та діяльності органів державної влади та інформації.

З метою протидії негативному впливу інформаційної пропаганди та інформаційних воєн, нейтралізації та запобігання реальним і потенційним загрозам в інформаційному просторі України РНБО України ухвалила рішення «Про заходи щодо удосконалення формування та реалізації державна політика у сфері інформаційної безпеки України». У документі зазначено, що РНБО, враховуючи необхідність удосконалення нормативно-правової бази та запобігання та нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері, прийняла рішення: розробити та внести на розгляд Верховної Ради України законопроекти про внесення змін. деякі закони України щодо протидії інформаційній агресії іноземних держав, що передбачають, зокрема, визначення механізму протидії негативному інформаційно-психологічному впливу, зокрема, заборону ретрансляції телевізійних каналів; посилити контроль за дотриманням законодавства про інформаційно-психологічну та кібербезпеку; вжити заходів для забезпечення поширення об'єктивної інформації про суспільно-політичну ситуацію в Україні у світі, зокрема шляхом створення відповідного медіа-холдингу для підготовки якісного конкурентоспроможного інформаційного продукту; розробити порядок аналізу інформаційних матеріалів іноземних ЗМІ з представництвами в Україні з метою впровадження ефективного механізму акредитації журналістів; вжити заходів щодо активізації міжнародного співробітництва для протидії негативним інформаційно-психологічним впливам та кіберзлочинності [1].

Крім зазначеного документа, основні напрями державної політики з питань національної безпеки в інформаційній сфері визначені в Законах України «Про основи національної безпеки України», «Доктрині національної безпеки» та інших нормативно-правових актах. документи.

Отже, в умовах сучасних інформаційних протистоянь, експансіоністської політики Російської Федерації національний інформаційний простір України недостатньо захищений від зовнішніх негативно-пропагандистських інформаційно-психологічних впливів і загроз. Тому пріоритетними завданнями органів державної влади та недержавних інституцій мають стати захист інформаційного суверенітету, створення потужної та ефективної системи інформаційної безпеки в Україні, розробка ефективних стратегій і тактик протидії інформаційним загрозам.

ВИСНОВКИ

Концепція інформаційної безпеки держави – це систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення. В рамках цієї концепції проводиться системна класифікація дестабілізуючих факторів та інформаційних загроз безпеці особистості, суспільства, держави; обґрунтовуються основні положення з організації забезпечення інформаційної безпеки держави; розробляються пропозиції щодо способів і форм забезпечення інформаційної безпеки.

Динаміка та характер розвитку інформаційних технологій інтенсифікують новітні виклики та загрози, спрямовані на особистість як уразливий суб'єкт інформаційних відносин, оскільки досягає потенційно-глобальної аудиторії за допомогою піринговых мереж та підключення до мережі Інтернет.

Активне використання у суспільних відносинах технологій великих даних, промислового інтернету речей породжує необхідність визначення критеріїв надійності та стійкості використовуваних інформаційних технологій; забезпечення безпеки інформації, що збирається та обробляється технологіями, у тому числі персональних даних, відомостей, що становлять комерційну таємницю, та інших видів інформації обмеженого доступу, що розміщуються в інформаційній інфраструктурі.

Використання інформаційних технологій потребує зміни підходу до правового регулювання інформаційних відносин, запровадження інститутів «цифрового права», «цифрових реквізитів» електронного документа; формування єдиних стандартів життєвого циклу інформаційних технологій.

Різноманітність методів реалізації технологічних процесів пошуку, зберігання, обробки, збору, розповсюдження та надання інформації дозволяє не лише позначити перехід до регулювання суспільних відносин, таких як «розумне» державне регулювання, а й окреслити коло питань безпеки нових

відносин, інформації та інформаційної інфраструктури, можливих інформаційних викликів та загроз.

Для забезпечення стійкості, безпеки та цілісності інформаційної інфраструктури необхідно розробити методику профілювання ризиків, систему стандартів обов'язкових вимог та методологій моделювання апаратно-програмного комплексу у рамках інформаційної безпеки; забезпечити узгодження правових та технічних норм. На забезпеченні інформаційної безпеки має бути зосереджена увага міжнародного співробітництва у сфері інформаційних технологій, оскільки більшість відносин базується на цифрових транскордонних технологіях.

Вирішення даних проблем у правовій галузі дозволяє сформувати правову систему інформаційної безпеки суб'єктів, у тому числі від деструктивної інформації, що впливає на них.Таким чином, в основі міжнародно-правового регулювання в галузі використання та створення інформаційних технологій та інфраструктур лежать нормативні акти міжнародного публічного права, викладені в документах ООН, її галузевих структурах та міжнародних договорах, а також міжнародних стандартах у цій галузі.

Правові підходи, відображені у національних нормативних правових актах країн різноманітні. Однак спільними для всіх держав, які використовують глобальні інформаційні інфраструктури, є проблеми, пов'язані з управлінням інформаційною інфраструктурою, забезпеченням безпеки транскордонної передачі даних, захистом соціальних структур у державі від шкідливого інформаційного впливу, забезпеченням безпеки інформаційної інфраструктури.

Таким чином, деякі форми розповсюдження фальшивих або спотворених повідомлень можуть розглядатися як втручання у внутрішні справи держави, припускаючи таким чином певні заходи відповідальності держави порушника.

Положення міжнародного права, що стосуються різних питань забезпечення інформаційної безпеки, містяться у низці міжнародно-правових актів, юридична сила яких різна. Проте необхідність наявності обов'язкових уніфікованих міжнародно-правових норм у цій сфері не викликає сумнівів. Єдиним виходом із ситуації була б розробка та прийняття міжнародної конвенції, що регулює питання забезпечення інформаційної безпеки держав.

В даний час держави-члени ООН використовують різні правові механізми та практичні заходи для забезпечення захисту інформації та інформаційних систем. Тому, розвиваючи міжнародне співробітництво у сфері забезпечення інформаційної безпеки, необхідно враховувати національні відмінності у методах регулювання створення, використання та забезпечення безпеки інформаційних інфраструктур.

Безсумнівно, створення державних інформаційних служб є складним завданням, враховуючи темпи розвитку інформаційних технологій, інформаційних послуг, електронних засобів масової інформації, а також питань захисту даних. Крім того, з точки зору організаційного та правового забезпечення безпеки, створення та управління публічними реєстрами та забезпечення сумісності та автентичності інформаційних технологій є складним завданням.

Також можна зазначити, що в країнах Євросоюзу розроблені та постійно вдосконалюються процедури реагування на інциденти (надзвичайні ситуації). Створюються групи швидкого реагування, які можуть розвернутися в найкоротші терміни для усунення наслідків кібератак, здійснених у військових чи громадських мережах. Процедури відновлення при комп'ютерних збоях або кібератаках інтегровані в комп'ютерну інформаційну безпеку та політичні документи.

Взаємодія між інформаційними системами країн-членів Європейського Союзу дозволяє узгоджувати вимоги до їх якості та забезпечення ефективного використання даних Європолу та баз даних Інтерполу шляхом полегшення доступу до них відповідних структур.

З метою недопущення інформаційного розширення діяльність держави в інформаційному просторі має здійснюватися за такими напрямами: 1) реалізація превентивних стратегій і тактик (превентивних заходів); 2) реалізація стратегії реагування (оперативне реагування на інформаційні атаки противника та активний наступ); 3) захист державного інформаційного сайту. Основна мета – забезпечення домінування та переваги в інформаційному просторі.

Крім того, пріоритетними завданнями інформаційних структур органів влади мають бути: контроль за інформаційними потоками; надання об'єктивної, вичерпної інформації, надання професійних коментарів та роз'яснень щодо подій; систематичне висвітлення службової позиції чиновників і політичних лідерів.

Отже, в умовах сучасних інформаційних протистоянь, експансіоністської політики Російської Федерації національний інформаційний простір України недостатньо захищений від зовнішніх негативно-пропагандистських інформаційно-психологічних впливів і загроз. Тому пріоритетними завданнями органів державної влади та недержавних інституцій мають стати захист інформаційного суверенітету, створення потужної та ефективної системи інформаційної безпеки в Україні, розробка ефективних стратегій і тактик протидії інформаційним загрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. “Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України” Рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. [Електронний ресурс]. – Режим доступу: http://www.zakon5.rada.gov.ua /laws/ show/n0004525-14.

2. Abdol Hossein Joodaki. The Ubiquitous Effect of Television and Dominant Surveillance in Ray Bradbury’s Fahrenheit 451. Rupkatha Journal on Interdisciplinary Studies in Humanities. Volume VII, Number 3, 2015 General Issue.

3. Bowker G.C. The history of information infrastructures: The case of the international classification of diseases [Електронний ресурс] / Bowker G.C. // Information Processing & Management. – 1996. – Режим доступу до ресурсу: https://doi.org/10.1016/0306.

4. Chuck Easttom, Jeff Taylor. Computer Crime, Investigation, and the Law / Chuck Easttom, Jeff Taylor. // International Cannel Center. Boston. – 2018.

5. Cybersecurity Strategy of the European Union:An Open, Safe and Secure Cyberspace [Електронний ресурс] – Режим доступу до ресурсу: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/.

6. Freedom of Information [Електронний ресурс] – Режим доступу до ресурсу: https://www.un.org/ruleoflaw/thematic-areas/governance/freedom-ofinformation/.

7. Fuentes-Camacho. T. The International Dimensions of Cyberspace Law / Fuentes-Camacho. T.. // American Journal of International Law. – 2002. – №96. – С. 510–514.

8. Global Threat Intelligence Report [Електронний ресурс] // NTT DATA Services. – 2017. – Режим доступу до ресурсу: Serviceshttps://us.nttdata.com/en/- /media/nttdataamerica/files/americasd.

9. Information Security Indicators [Електронний ресурс] – Режим доступу до ресурсу: /www.etsi.org/technologiesclusters/.

10. Janssen M., Jeroen van den Hoven, Yan Z., Zhang P., Vasilakos A. A survey on trust management for Internet of Things // Journal of Network and Computer Applications. № 42. 2014.

11. Jeff Handelsman and Eby Kalantar. Life, Liberty, and internet Access: Is Logging on a Basic Human Rigth [Електронний ресурс] / Jeff Handelsman and Eby Kalantar – Режим доступу до ресурсу: https://ublawjil.files.wordpress.com/2014/07/.

12. Jun C., Chung J. Big data analysis of local government 3.0: Focusing on Gyeongsangbuk – do in Korea // Technological Forecasting & Social Change. November. 2015.

13. Kelsen H. Principles of Intenational Law. N. Y., 1952. P. 208 – 210.

14. Kemp R. Legal aspects of managing Big Data // Computer law & Security review (2014) pp. 482 – 491;

15. Klischewski, R., Scholl, H. Information Quality as a Common Ground for Key Players in e – Government Integration and Int. In: HICSS 2006 – 39th Hawaii International International Conference on Systems Science 4 – 7 January, 2006, Kauai, HI, USA. 2006.

16. Kovalenko K.E., Kovalenko N.E., Gribanov D.V. Improving the effectiveness of knowledge in the process of business games // Revista Conrado. 2018. T. 14. № 61. C. 141-143.

17. Kovalenko K.E., Kovalenko N.E., Gribanov D.V. The development of the information society //Universidad y Sociedad. 2018. T. 10. № 3. C. 365-368.

18. Maa Y., Wub H., Wanga L., Huang B., Ranjan R., Zomayae A., Jie W. // Future Generation Computer Systems. 2015.

19. Mark Johnson. Cyber Crime, National Security and Digital Intelligence / Mark Johnson. // Routledge. – 2013.

20. Picciotto S. Networks in International Economic Integration: Fragmented States and the Dilemmas of Neo – Liberalism // Northwestern Journal of International Law & Business. 1996/1997. Vol. 17. P. 1043.

21. Pipkin D.L. Information Security: Protecting the Global Enterprise. New York. Pearson, 2000.

22. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development [Електронний ресурс] – Режим доступу до ресурсу: www2.ohchr.org/english/bodies/hrcouncil.

23. Robinson N. et al. «Cyber – Security Threat Characterization: A Rapid Comparative Analysis». RAND Corporation, N – Y. 2013.

24. Salome Samadashvili. Strategic Defence for Russia's Undeclared Information War on Europe. [Електронний ресурс] / Salome Samadashvili // Wilfried Martens Centre for European Studies. Rue du Commerce 20. Brussels.. – 2015. – Режим доступу до ресурсу:

https://martenscentre.eu/sites/default/files/publication-files/information-warfareeurope-defence-russia_0.pdf..

25. Shcherbovich, A. Three levels of internet governance: finding a balance to ensure freedom of expression and information accessibility rights of internet users / Shcherbovich, A.. // International Journal of Multidisciplinary Thought. – 2010. – №1. – С. 173–187.

26. Sicari S., Rizzardi A., Grieco L.A., Coen – Porisini A. Security, privacy and trust in Internet of Things: The road ahead //Computer Networks № 76 (2015) pp.146 – 164.

27. Slaughter, A – M. The Real New World Order. Princeton University Press. P. 186 – 189.

28. Suprun, V.M. Information sovereignty as part of information security: theoretical and legal aspects [Електронний ресурс] / Suprun, V.M. – Режим доступу до ресурсу: http://www.nbuv.gov.ua/portal/natural/vkhnu/Pravo/2009

29. Takaaki Koyama. Security Orchestration with a Global Threat Intelligence Platfor [Електронний ресурс] / Takaaki Koyama – Режим доступу до ресурсу: www.ntt-review.jp/archive/ntttechnical..

30. Vandezande N. Virtual currencies under EU anti – money laundering law // Computer law & Security review. № 33. 2017.

31. Warren S., Brandeis L. The Right to Privacy // Harvard Law Review. Vol. 4, № 5. 1890.

32. Yarochkin, V. The security system company. Електронний ресурс. URL: http://www.nbuv.gov.ua.

33. Абакумов, В.М., 2011. Правове регулювання протидії інформаційним війнам в Україні. Кандидат наук. Автореферат. Класичний приватний університет, Запоріжжя.

34. Богданович В.Ю., Ворович Б.О., Марко Є.І. Інформаційна безпека як основа воєнної безпеки держави та суспільства./ Богданович В.Ю., Ворович Б.О., Марко Є.І.//Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. – 2018. – № 3. – С. 44–48.

35. Богданович В.Ю., Грищук Р.В., Левченко О.В. Система критеріїв та показників оцінювання ефективності функціонування системи забезпечення інформаційної безпеки./ Богданович В.Ю., Грищук Р.В., Левченко О.В.//Збірник наукових праць Національної академії Державної прикордонної служби України. Сер.: Військові та технічні науки. – 2017. – № 4. – С. 21–37.

36. Богданович В.Ю., Дудар М.С. Узагальнена модель управління інформаційно-психологічною безпекою великих груп людей в умовах низького рівня соціально-політичної стабільності в країні. /Богданович В.Ю., Дудар М.С.//Сучасний захист інформації. – 2014. – № 4. – С. 4–11.

37. Бондаренко В. О. Інформаційна безпека сучасної держави: концептуальні роздуми [Електронний ресурс] / В. О. Бондаренко, О. В. Литвиненко. – Режим доступу: http://www.crime-research.iatp.org.ua/library/strateg.htm

38. Варивода К.С. Інформаційна безпека підлітків в Інтернет мережі / К.С. Варивода // Молодий вчений. – 2016. – № 3. – С. 365-368. Електронний ресурс. URL: http://molodyvcheny.in.ua/files/journal/2017/9.1/10.pdf

39. Верголяс О.О. Спеціальні інформаційні операції в системі засобів протидії загрозам національній безпеці України./ Верголяс О.О.// Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки». – 2019. – № 4.

40. Гібридна війна і журналістика. Проблеми інформаційної безпеки: навчальний посібник / за заг. ред. В.О. Жадька; ред.-упор. О.І. Харитоненко, Ю.С. Полтавець. К., Вид-во НПУ імені М.П. Драгоманова, –2018. –С. 356

41. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення [Електронний ресурс] / Ю. О. Горбань. – Режим доступу: http://www.visnyk.academy. gov.ua/wpcontent/uploads/2015/04/20.pdf

42. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення./ Горбань Ю.О. // Вісник НАДУ. – 2015. – № 1. – С. 136–141.

43. Гусаров В. Кремль розпочав нову інформаційну операцію проти України [Електронний ресурс] / В. Гусаров. – Режим доступу: http://www.osvita. mediasapiens.ua/material/34281

44. Гуцалюк М. Інформаційна безпека України: нові загрози та організація протидії./ Гуцалюк М. // Правова інформатика. –2004. – № 3. – С. 39–43.

45. Дзьобань О.П. Інформаційне насильство та безпека: світоглядно-правові аспекти : монографія / О.П. Дзьобань, В. Г. Пилипчук ; Нац. акад. прав. наук України, НДЦ правової інформатики, Ін-т дослідження проблем держ. безпеки СБУ. - Х. : Майдан, 2011. - 244 с.

46. Доктрина інформаційної безпеки України [Електронний ресурс]. – Режим доступу: http://www.zakon3.rada.gov.ua/laws/show/514/2009

47. Егоров С. А. Международное право: Учебник / отв. ред. С.А. Егоров / С. А. Егоров. – Москва, 2015. – 417 с.

48. Женевська декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» [Електронний ресурс] – Режим доступу до ресурсу: http://www.un.org/russian/conferen/wsis/dec.pdf.

49. Загурська-Антонюк В.Ф. Політично-інформаційні безпекові механізми в українській державній системі у контексті геополітичних змін. [Електронний ресурс] Державне управління: удосконалення та розвиток. –2020. – № 2. – Режим доступу : http://www.dy.nayka.com.ua/?op=1&z=1567.

50. Захист інформаційної безпеки як функція держави [Електронний ресурс]. – Режим доступу: http://www.mego.info/матеріал/23-захист-інформаційноїбезпеки-як-функція-держави

51. Інформаційна безпека держави у контексті протидії інформаційним війнам: Навчальний посібник / за заг. ред. В. Б. Толубка. – К. : НАОУ, 2004. – 315 с.

52. Калюжний Р.А. Держава. Політика. Інформація/ Калюжний Р.А.//Юридичний вісник. Повітряне і космічне право. – 2014. – № 2. – С. 159–160.

53. Калюжний Р.А. Теоретико-методологічні підходи до розуміння інформаційної безпеки людини./ Калюжний Р.А// Юридичний вісник. Повітряне і космічне право. –2018. –№ 2. –С. 197–198.

54. Кирильчук, Є.О. Проблеми національної інформаційної безпеки України в контексті сучасних національних державотворчих процесів

та світової інтеграції / Кирильчук, Є.О. // Наукові праці МАУП. – 2013. – №1. – С. 60–63.

55. Коваленко Є.В., Плетньов О.В. Передумови загроз у сфері інформаційної безпеки та перспективи їх подолання / Коваленко Є.В., Плетньов О.В. // Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 4 квітня 2019 р.). Київ : Нац. акад. СБУ. – 2019. – С. 58–59.

56. Коваленко Ю.О. Забезпечення інформаційної безпеки на підприємстві./ Коваленко Ю.О.// Економіка промисловості. – 2010. –№ 3. – С. 123–129.

57. Коваль, З.В., 2011. Політико-правові механізми державного управління інформаційно-психологічною безпекою України. Кандидат наук. Автореферат. Одеський регіональний інститут державного управління Національної академії державного управління при Президентові України.

58. Концепція національної безпеки України [Електронний ресурс]. – Режим доступу: http://www.w1. c1.rada.gov.ua/pls/zweb2/webproc4_1

59. Кормич Б. А. Інформаційне право / Б. А. Кормич. – Харків: Бурун і К, 2011. – 334 с.

60. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України [Текст] : монографія / Б. А. Кормич. – Одеса : Юридична література, 2007.– 471 с.

61. Костецький Р. Інформаційна безпека особистості: Інформаційна безпека Електронний ресурс. URL: https://sites.google.com/site/infobezpekaosobu/informacijnabezpeka

62. Крысько В.Г. Секреты психологической войны (цели, задачи, методы, формы, опыт). Минск, –1999. –С. 86

63. Кубявка М.Б. Моделі та методи управління інформаційним супроводженням в умовах гібридної війни/ Кубявка М.Б.// : дис… канд. техн. наук. Спец. 05.13.06 «Інформаційні технології». Київ, – 2017. – С.199

64. Левченко О.В. Класифікація інформаційної зброї за засобами ведення інформаційної боротьби./ Левченко О.В.// Сучасні інформаційні технології у сфері безпеки та оборони. – 2014. – № 2(20). – С. 142–146.

65. Левченко, О.В. Проблеми і шляхи формування системи інформаційної безпеки держави / Левченко, О.В. // Збірник наукових праць Харківського університету Повітряних Сил. – 2014. – №2. – С. 166–168.

66. Липкан В.А. Основы права национальной безопасности./ Липкан В.А. // Публичное и частное право. –2009. –№ 2. –С. 34–46.

67. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції [Текст] : навч. посіб. / В. А. Ліпкан, Ю. Є. Макименко, В. М. Желіховський. – К. : КНТ, 2006.

68. Ліпкан В. Зміст пропаганди на сучасному етапі. [Електронний ресурс] GOAL. –2016. – Режим доступу: http://goal-int.org/zmist-propagandi-na-suchasnomu-etapi/.

69. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах євроінтеграції : навчальний посібник./ Ліпкан В.А., Максименко Ю.Є., Желіховський В.М.// Київ : КНТ. – 2006. – 280 с.

70. Малик Я.Й. Інформаційна війна і Україна./Малик Я.Й.// Демократичне врядування.–2015. – №15.

71. Маркова М.В. Інформаційно-психологічна війна: медико-психологічні наслідки та стратегії протидії./ Маркова М.В.// Проблеми безперервної медичної освіти та науки. –2016. –№ 4. – С. 6–10.

72. Марута Н.О., Маркова М.В. Інформаційно-психологічна війна як новий виклик сучасності: стан проблеми та напрямки її подолання./ Марута Н.О., Маркова М.В.// Український вісник психоневрології. – 2015. – Т. 23. – № 3(84). – С. 21–28.

73. Марутян Р. Р. Рекомендації щодо вдосконалення політики забезпечення інформаційної безпеки України [Електронний ресурс] / Р. Р. Марутян. – Режим доступу: http://www.dsaua.org/index. php?option=com_content&view=article&id=198%3A2014-08- 13-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid= 90&lang=uk;

74. Марущак А.І. Петров С.Г. Зміст поняття «державні електронні інформаційні ресурси». /Марущак А.І. Петров С.Г.// Інформація і право. –2018. –№ 4(27). – С. 15–21.

75. Марущак А.І., Панченко В.М. До визначення поняття «інформаційна безпека»./ Марущак А.І., Панченко В.М.// Правничий вісник Університету «КРОК». –2010. –№5(1). –С. 125–130.

76. Медвідь Ф. Інформаційна безпека України: виклики та загрози [Електронний ресурс] / Ф. Медвідь. – Режим доступу: http://www.nato.ru. if.ua/journal/2009-2-28.pdf.

77. Методи інформаційного захисту простору. Інформаційна безпека України [Електронний ресурс]. – Режим доступу: http://www.ua. textreferat.com/referat-7471.html

78. Остроухой, Б.В., Петрик, Б.М., Присяжнюк, М.М. та ін. ред. Інформаціна безпека (соціально-правові аспекти): підручник / Остроухой, Б.В., Петрик, Б.М., Присяжнюк, М.М. та ін. ред.. – Київ, 2010. – 776 с.

79. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / В. Петрик. – Режим доступу: http://www.justinian.com.ua/article.php?id=3222

80. Почепцов Г. Пропаганда vs. информационные операции: сходства и различия [Електронний ресурс] / Почепцов Г. // MediaSapiens. – 2016. – Режим доступу до ресурсу: https://ms.detector. media/mediaanalitika/post/16443/2016-04-17-propaganda-vs-informatsionnye-operatsii-skhodstva-i-razlichiya/

81. Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. – К. : Вид.дім "Києво-Могилянська академія", 2015. – 497 с.

82. Почепцов Г.Г. Информационные войны./ Почепцов Г.Г.// М., Рефл-бук; К., Ваклер, –2000. –С. 576

83. Почепцов Г.Г. Смисли і війни: Україна і Росія в інформаційній і смисловій війнах./ Почепцов Г.Г.//Київ : Вид. дім «Києво-Могилянська академія», – 2016. –С.316

84. Почепцов Г.Г., Чукут С.А. Інформаційна політика : навч. посіб./ Почепцов Г.Г., Чукут С.А.// 2-ге вид. Київ : Знання, – 2008. –С. 559

85. Почепцов Г.Г., Чукут С.А. Інформаційна політика: навч. посіб. — Київ: Знання, 2006. – 665 с.

86. Про основи національної безпеки України : Закон України // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351. Із змінами, внесеними згідно із Законом № 3200-IV (3200-15) від 15.12.2005. ВВР. – 2006. – № 14. – С. 116.

87. Роль і значення інформаційних технологій в оперативно-розшуковій діяльності [Електронний ресурс] – Режим доступу до ресурсу: http://vjhr.sk/archive/2016_4/part_1/37.pdf.

88. Сєдая Ю.С. Кібервійна: основні теоретичні положення./ Сєдая Ю.С.// У зб.: Українське суспільство в умовах війни: виклики сьогодення та перспективи миротворення: матеріали Всеукраїнської науково-практичної конференції, м. Маріуполь, 9 червня 2017 р. Маріуполь. ДонДУУ, – 2017. – С. 249–252.

89. Сопілко І.М. Інформаційні загрози та безпека сучасного українського суспільства./ Сопілко І.М. // Юридичний вісник. Повітряне і космічне право. – 2015. –№ 1. – С. 75–80.

90. Сопілко І.М. Роль доктрини інформаційної безпеки України в реалізації державної інформаційної політики України./ Сопілко І.М.// Журнал східноєвропейського права. –2014. – № 2. – С. 36–41.

91. Сопілко І.М. Роль Закону України «Про основи національної безпеки України» в реалізації державної інформаційної політики України./ Сопілко І.М.// Юридичний науковий електронний журнал. Електронне наукове фахове видання. – 2014. –№ 2. –С. 75–78.

92. Сопілко І.М. Становлення мережевого суспільства та питання кібербезпеки./ Сопілко І.М. // Юридичний вісник. Повітряне і космічне право. – 2016. – № 1. – С. 79–86.

93. Сулейманова Ш.С., Назарова Е.А. Информационные войны: история и современность: Учебное пособие./ Сулейманова Ш.С., Назарова Е.А.//М. Международный издательский центр «Этносоциум». – 2017. – С. 90

94. Турченко Ю.В. Засоби масової комунікації як суб'єкт реалізації державної інформаційної політики України в сфері оборони: політико-правове регулювання./ Турченко Ю.В.//Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – 2013. – № 43. – С. 113–119.

95. Шестаков В.І., Міхєєв Ю.І. Методичний підхід до виявлення ознак інформаційно-психологічного впливу в системі попередження та захисту від зовнішніх інформаційних загроз./ Шестаков В.І., Міхєєв Ю.І.// Українське суспільство в умовах війни: виклики сьогодення та перспективи миротворення: матеріали Всеукраїнської науково-практичної конференції, м. Маріуполь, 9 червня 2017 р. Маріуполь. ДонДУУ, – 2017. – С. 277–281