МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

БОДНАР АНДРІЯНА ОЛЕГІВНА

Допускається до захисту:
завідувач кафедри
конституційного, міжнародного і
кримінального права,
к.ю.н., доцент
_____ О.Г. Турченко
«___» _____ 2020 р.

МІЖНАРОДНА ІНФОРМАЦІЙНА БЕЗПЕКА

Спеціальність 081 Право

Магістерська робота

Науковий керівник:
Щебетун І.С., доцент кафедри
конституційного, міжнародного і
кримінального права,
к.ю.н., доцент

Оцінка: _____ / ___ / _____
(бали/за шкалою ЄКТS/за національною шкалою)
Голова ЕК: _____
(підпис)

Вінниця 2020

ЗАТВЕРДЖЕНО:
Науковий керівник: Щебетун І.С.,
кандидат юридичних наук, доцент,
доцент кафедри конституційного,
міжнародного і кримінального
права
_____
«09» січня 2020 р.

МАГІСТЕРСЬКЕ ЗАВДАННЯ
студентки 1 курсу СО «Магістр» групи «Г»,
заочного відділення спеціальності 081 Право
Боднар Андріяни Олегівни

1. **Тема роботи:** Міжнародна інформаційна безпека.

2. **Строк надання студентом роботи керівнику:** «30» жовтня 2020 р.

3. **Вихідні дані до роботи:** наукова література, міжнародні акти, акти міжнародних організацій, законодавство України та зарубіжних країн щодо забезпечення міжнародної інформаційної безпеки.

4. **Робота виконується на базі:** кафедри конституційного, міжнародного і кримінального права Донецького національного університету імені Василя Стуса.

5. **Результати дослідження:** уточнення поняття «міжнародної інформаційної безпеки», виявлення особливостей системи забезпечення міжнародної інформаційної безпеки.

6. **Область застосування результатів роботи:** наукова діяльність.

Тема магістерської роботи зареєстрована № 04/08 «09» січня 2020 року.
Лаборант кафедри_____ (підпис)

УЗГОДЖЕНО:
«09» січня 2020 р.
Зав. кафедри
конституційного, міжнародного і
кримінального права,
доцент, к.ю.н. О.Г. Турченко

АНОТАЦІЯ

Боднар А.О. Міжнародна інформаційна безпека. Магістерська робота. Кафедра конституційного, міжнародного і кримінального права юридичного факультету Донецького національного університету імені Василя Стуса Міністерства освіти і науки України, Вінниця, 2020 – 92 с.

В роботі проаналізовано складові елементи інституту міжнародної інформаційної безпеки, ключові аспекти, принципи і підходи до розуміння інформаційної безпеки з позицій міжнародного права, уточнено поняття міжнародної інформаційної безпеки, охарактеризовані моделі міжнародної інформаційної безпеки, організаційна структура забезпечення міжнародної інформаційної безпеки, виявлені особливості забезпечення кібербезпеки

Ключові слова: міжнародне правове регулювання, безпека, міжнародна інформаційна безпека, кібербезпека, інформаційні загрози.

Бібліограф.: 115 найм.

SUMMARY

A. Bodnar. International information security. The Master's Thesis. Constitutional, International and Criminal Law department of Law Faculty, Vasyl' Stus Donetsk National University Ministry of Education and Science of Ukraine, Vinnitsa, 2020 - 92 p.

The work analyzes the components of the international institute of information security, of the key issues, principles, elements of the information security from the standpoint of international law, specifies the concept of international information security, characterizes the models of international information security, the organizational structure of ensuring international information security, reveales the peculiarities of cybersecurity.

Keywords: international legal regulation, security, international information security, cybersecurity, information threats.

Bibliography: 115 items.

ЗМІСТ

ВСТУП

Об’єктивно розглядаючи категорію «інформаційна безпека» можна дійти висновку, що вона виникла у той же саме час, що і засоби інформаційних комунікацій між людьми, а також з усвідомленням наявності у людей інтересів, через які з’являється можливість завдати збитків шляхом інформаційних комунікацій, які забезпечують зв'язок між усіма людьми.

В умовах глобалізаційних процесів, зміни міжнародної системи, зміни характеру загроз трансформується і сучасна система загальної безпеки. Простір безпеки трансформується з переважно військового в «комплексне», що включає в себе елементи з суміжних предметних областей світової взаємодії. Як зазначає О.Л. Хилько, на сьогоднішній день зростає розуміння усіма елементами міжнародної системи взаємозалежності світу і, зокрема, необхідності взаємодії безпеки, подолання розділових ліній і «вакууму безпеки» на світовому, європейському, євразійському просторах.

У зв'язку з цим відбувається розширення простору безпеки і вирівнювання пріоритетності різних сфер т.зв. «широкої безпеки».

Необхідно відзначити, що проблема розширення простору безпеки достатньо давно привертає увагу представників різних напрямків - економістів, юристів, міжнародників, істориків і т.д. Так, Кулагін В. зазначає, що в сучасних умовах слід говорити «... не тільки про «міжнародну безпеку» в її міждержавній іпостасі, а про явище з більш широким набором дійових осіб, яке з цієї причини більш коректно було б називати «світовою безпекою»» [1].

У свою чергу, прихильник «широкого» тлумачення предметного поля безпеки, відомий економіст, професор Емма Ротшильд визначає розширення простору світової безпеки в чотирьох вимірах. Перше стосується розширення безпеки «вниз від держав до індивідуумів». Друге - втілює бачення «вгору від держав до біосфери». Третє стосується горизонтального аспекту безпеки - «від військової до політичної, економічної, соціальної, екологічної безпеки,

або безпеки людини». Четвертий вимір передбачає політичну відповідальність за забезпечення безпеки, яка «розпорошується» у всіх напрямках - від держав «вгору до міжнародних інститутів, вниз до регіональних і місцевих властей, а також до неурядових організацій, громадської думки і преси, абстрактних сил природи або ринку» [2, с.15].

Як представляється, горизонтальний аспект безпеки необхідно розширити і включити в нього інформаційну безпеку, увага до забезпечення якої значно зросла останнім часом.

Водночас, сучасний світ надто неоднорідний у можливостях забезпечення національних систем сучасними інформаційно-комунікаційними технологіями (далі – ІКТ) обробки, передачі, накопичення та збереження інформації і їх захисту від зовнішніх загроз. Використання високих технологій як інструментів політичного тиску для забезпечення національних інтересів у міжнародній взаємодії, розробка й упровадження інноваційних стратегій національної безпеки, якісні зміни принципів міждержавних відносин і практичних механізмів та технологій реалізації національних стратегій інформаційної безпеки призвели до кардинальних змін в підходах до формування концепцій міжнародної інформаційної безпеки [3, с.69]. Інформаційна безпека в умовах зростаючих взаємозв’язків та взаємозалежності держав при збереженні та появі нових глобальних небезпек і загроз стає складовою загальної світової безпеки [4, с.46].

Забезпечення національної інформаційної безпеки усередині держави перебуває на стадії розвитку. Це можна пояснити невідповідностями між зміцненням інформаційного суспільства і усвідомленням та потребами у забезпеченні інформаційної безпеки, перед державою постає завдання визначити положення і пріоритет інформаційної безпеки та її захисту в системі ієрархії державних завдань [5, с.342].

В свою чергу, формування єдиної міжнародної системи інформаційної безпеки дозволить в однаковій мірі гарантувати захист національного інформаційного простору кожній державі.

Нагадаємо, що ще в 1998 році Резолюція Генеральної Асамблеї Організації Об'єднаних Націй (далі – ГА ООН) 53/70 «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки» пропонувала державам - членам ООН продовжити обговорення питань інформаційної безпеки, дати конкретні визначення загроз, запропонувати свої оцінки проблеми, включаючи розробку міжнародних принципів забезпечення безпеки глобальних інформаційних систем. А аналогічна Резолюція ГА ООН 54/49 від 1 грудня 1999 року вперше вказала на загрози міжнародній інформаційній безпеці стосовно не тільки до цивільної, але й до військової сфери.

Зростаючий інтерес до інформаційної безпеки на сьогоднішній день підтверджується, наприклад, і прийнятим на вищому рівні керівництва НАТО рішенням про посилення уваги до проблеми забезпечення інформаційної безпеки і здатності вести інформаційні війни, обумовленим збільшенням активності потенційних супротивників блоку і прагненням організації відповідати рівню возростаючих загроз кібербезпеки; акцентуванням НАТО на транскордонній природі загроз інформаційній безпеці і проблемах координації дій на наднаціональному рівні; наявністю служб інформації в практично у всіх міжнародних організаціях, в тому числі і військових [6, с.213].

Наявність активного концептуально-теоретичного дискурсу щодо проблематики інформаційної безпеки (національної, регіональної, міжнародної) зумовлює необхідність аналізу визначень, які існують сьогодні щодо цієї комплексної й складної категорії, визначення засад забезпечення міжнародної інформаційної безпеки.

Дослідженнями інформаційної безпеки займалися В. Беляков, М. Демкова, Л. Задорожня, В. Кирик, А. Крутських, Н. Кушакова-Костицька, А. Леваков, К. Макаренко, В. Роговець та інші, але ряд питань, залишилися не висвітленими у науковій літературі. Що стосується дослідження інформаційної безпеки в міжнародному контексті, то можна назвати таких

вчених, як О. Білорус, Н. Винер, А. Гуз, Д. Лук'яненко, Є. Макаренко, С. Расторгуєв, Н. Рашевський, О. Турченко, Р. Хартлі, К. Шеннон та інші.

У сучасній науці визначення актуальних проблем інформаційної безпеки стало предметом також комплексних досліджень, проведених І.А. Лазарєвим, В.Н. Лопатіним, Ю.С. Уфімцевим, Є.А. Єрофєєвим. У подальшому проблеми забезпечення інформаційної безпеки знайшли відображення у працях Є.М. Брандмана, Б.В. Вербенко, А.А. Ніколаєва, Т.А. Полякової.

Поява і наукове закріплення дефініції «інформаційна безпека» безпосередньо пов'язане і з осмисленням феномена інформатизації та вивченням змісту процесу формування інформаційного суспільства. Даній проблемі присвячені роботи зарубіжних теоретиків Д. Белла, Е. Тоффлера, Т. Стоуньер, А. Турена, У. Дайзард, М. Кастельса, К. Кояма, Є. Масуда.

Отже, метою цього дослідження є уточнення поняття «міжнародної інформаційної безпеки», виявлення особливостей системи забезпечення міжнародної інформаційної безпеки.

Мета дослідження досягається через виконання таких завдань:

- дослідити загальнотеоритичні засади, підходи до розуміння інформаційної безпеки та міжнародної інформаційної безпеки;

- уточнити поняття «міжнародної інформаційної безпеки», виділити її ключові аспекти;

- розкрити сутність системи міжнародної інформаційної безпеки, а саме: організаційну структуру забезпечення міжнародної інформаційної безпеки;

- виявити особливості забезпечення кібербезпеки.

При вирішенні поставлених задач були використані наступні методи дослідження: емпірико-теоретичний при виченні питань, пов'язаних з забезпеченням міжнародної інформаційної безпеки; порівняльно-правовий метод при порівнянні підходів держав до забезпечення інформаційної безпеки, функцій різних держав у системі забезпечення міжнародної

інформаційної безпеки; метод узагальнення при формуванні визначень, формулювання та обгрунтуванні висновків; метод аналізу – при вивченні організаційної структури забезпечення інформаційної безпеки (суб'єктів забезпечення); дедукції – при формуванні висновків до окремих частин роботи. Системно-структурний метод дозволив визначити особливості забезпечення міжнародної інформаційної безпеки. Формально-логічний метод дозволив розробити пропозиції щодо вдосконалення системи забезпечення міжнародної інформаційної безпеки.

Об'єктом дослідження є суспільні відносини, що виникають при забезпеченні міжнародної безпеки.

Предметом дослідження є суспільні відносини, що виникають при забезпеченні міжнародної інформаційної безпеки.

Окремі результати магістерської роботи викладені в науковій статті «Загрози і моделі системи глобальної інформаційної безпеки» (*Вісник студентського наукового товариства Донецького національного університету імені Василя Стуса.* 2020. Том 1. №12. С.22-27.).

Магістерська робота складається з вступу, двох розділів, чотирьох підпунктів, висновків, списку використаних посилань, додатків. Обсяг роботи - 91 стор., використано джерел - 115.

РОЗДІЛ 1
ЗАГАЛЬНОТЕОРЕТИЧНІ ЗАСАДИ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Поняття міжнародної інформаційної безпеки

Поняття інформаційної безпеки сьогодні - одне з базових в інформаційному праві. Інформаційне суспільство, а саме суспільство, в якому інформаційні процеси здійснюються головним чином на основі використання інформаційно-комунікаційних технологій, а інформаційні ресурси доступні всім верствам населення, переживає один з найактивніших етапів свого розвитку. Це говорить про актуальність всього, що пов'язано з поняттям безпеки в інформаційному суспільстві і в умовах формування електронного уряду [7, с.34].

В наш час, у зарубіжних країнах, поняттю «інформаційна політика» та «інформаційна безпека» приділяють значну увагу. З 1994 року пріоритетним напрямком державної інформаційної політики в багатьох країнах світу є побудова інформаційного суспільства, підвищення інформаційної свідомості, у тому числі розвиток національних і глобальних інформаційних систем [8, с.23].

Серед юристів також поки не вироблено єдиного підходу до визначення поняття інформаційної безпеки.

«Інформаційна безпека є найважливішою складовою національної безпеки в цілому. Суть цього інституту інформаційного права полягає у здійсненні правових, організаційних, технічних заходів, що забезпечують безпечний стан всіх складових інформаційно-комунікаційного комплексу держави, окремих організацій та кожної людини» [9, с. 398].

На думку В.Н. Лопатіна, об'єктивно категорія «інформаційна безпека» виникла з появою засобів інформаційних комунікацій між людьми, а також з

усвідомленням людиною наявності у людей і їх спільнот інтересів, яким може бути завдано шкоди шляхом впливу на засоби інформаційних комунікацій, наявність і розвиток яких забезпечує інформаційний обмін між усіма елементами соціуму. Виділяючи окремо інформаційно-психологічну безпеку [10, с.45], В.Н. Лопатін трактує її як «стан захищеності життєво важливих інтересів особи, суспільства і держави від впливу шкідливої інформації» [11, с.134].

Інформаційна безпека розглядається також як стан інформаційної захищеності (безпека об'єкта від інформаційних загроз), за якої «унеможливлюється негативний інформаційний вплив та негативні наслідки функціонування інформаційних технологій або спеціальні інформаційні операції, акти зовнішньої інформаційної агресії та негласного зняття інформації (за допомогою спеціальних технічних засобів), інформаційний тероризм і комп'ютернізлочини не завдають суттєвої шкоди національним інтересам держави та не заважають стабільному розвитку інформаційної інфраструктури, належному функціонуванню національного інформаційного простору» [12, с.8].

Такі визначення, як відмічає К. Захаренко [13, с.108], концентруються на проблематиці запобігання тим шкідливим наслідкам, що можуть становити різноманітні інформаційні загрози, а також усунення й подолання цих наслідків із якомога меншою шкодою для суспільства та людини.

Аналіз різних підходів до визначення змісту поняття «інформаційна безпека» уможливлює зауважити про недоцільність суворого обрання тієї чи іншої позиції. Сьогодні існує необхідність розглядати дану проблему більш комплексно і системно, при цьому найбільш прийнятним є інтегральний підхід, за якого інформаційна безпека визначатиметься за допомогою «окреслення найбільш важливих її сутнісних ознак з урахуванням постійної динаміки інформаційних систем і становлення не лише інформаційного суспільства а й інформаційної цивілізації» [14, с.35].

Відповідно кожна теоретична праця з проблематики інформаційної безпеки, навіть якщо вона стосується конкретної держави, спільноти чи технологічної характеристики, обов’язково має враховувати принцип глобальності інформаційного середовища, його системності й усеохопності.

Стан досягнення інформаційної безпеки може розглядатися як потреба не тільки держави, але й інших суб'єктів інформаційних відносин: громадян, юридичних осіб, а також технологічних механізмів, систем, інформаційно-комунікаційних технологій - об'єктів інформаційної безпеки [15, с.123].

Суб’єкт перебуває в стані інформаційної безпеки тоді, коли ефективність його діяльності забезпечена повною, достовірною та достатньою для прийняття рішень інформацією. Такий стан досягається соціальною активністю в трьох взаємопов’язаних групах суспільних відносин, що представляють собою структурні елементи інформаційної безпеки: суспільні відносини у сфері використання інформаційних технологій, у сфері забезпечення доступу до інформаційного ресурсу й у сфері формування інформаційного ресурсу. В межах першої групи забезпечується функціонування ефективних засобів інформаційної діяльності, у межах другої – забезпечується можливість суб’єктів отримувати доступ до необхідних інформаційних ресурсів, у межах третьої – формується інформаційний ресурс, що відповідає потребам суб’єктів [16, с. 271].

В словосполученні «інформаційна безпека» два терміни є ключовими. Загального визначення інформації досі не вироблено. Найпоширеніші з них є:

- «фундаментальна першооснова і загальна властивість Всесвіту, яка існує незалежно від нас, виявляється в тривимірному процесі взаємодії мікро- і макропроцесів енергії, руху і маси у просторі та часі»;
- «результат відображення руху об'єктів матеріального світу в системах живої природи»;
- «властивість матерії змінюватися і відображати ці зміни»;
- «повідомлення, опис фактів» [17, с.89];
- «новини, нові відомості»;

- «знята невизначеність, пов'язана з випадковими процесами, а також з перетворенням можливості на дійсність»;
- «властивість об'єкта зменшувати невизначеність процесу зміни його стану в часі» [18, с.33];
- «зняття (усунення) невизначеності, де невизначеність - недостатнє знання про об'єкти і явища (ототожнюється з непоінформованістю суб'єкта)»;
- «зменшення невизначеності в результаті поєднання»;
- «ступінь модифікації структури вхідними даними»;
- «передача, основа зв'язку і управління в живій природі і машинах»;
- «відомості про осіб, предмети, події, явища і процеси незалежно від форми їх подання, що використовуються в цілях отримання знань, прийняття рішень»;
- «інформація - відображення в психіці закону існування світу (психічне відображення світу)»:
- «як інваріант оборотних трансформацій надходить до суб'єкта повідомлення»;
- «інваріант: величина, що залишається незмінною при тих чи інших перетвореннях»;
- «одиниця, що містить у собі всі основні ознаки своїх конкретних реалізацій»;
- «відомості про навколишній світ і процеси, що протікають у ньому, які сприймаються біологічним об'єктом або спеціальним пристроєм»;
- «інформація про об'єкт є зміна параметру спостерігача, що викликана взаємодією спостерігача з об'єктом» [19, с.123].

Що ж до «безпеки», то, на думку В.М. Заплатинського, «безпека - це такі умови, в яких перебуває складна система, коли дія зовнішніх і внутрішніх чинників не призводить до процесів, що вважаються негативними по відношенню до даної складної системи у відповідності до наявних, на

даному етапі, потреб, знань та уявлень» [20, с.92] або «безпека - це такий стан складної системи, коли дія зовнішніх та внутрішніх факторів не призводить до її неможливості або погіршення функціонування та розвитку» [21, с.124].

Безпека - одна з головних цілей і невід'ємна частина діяльності людей, суспільства, держави, світового співтовариства, одна з умов самовизначення, саморозвитку особи, людей, людства. Турбота про безпеку характерна для кожної складової соціальної структури суспільства - від індивіда до всього людства в цілому.

Необхідність безпеки в силу розвитку людини поступово ставала масштабнішою і багатообразнішою. Безпеку охоплювало не лише життя людини, його майно, але і суспільство, потім держави, а також різні сфери діяльності і людини, і суспільства, і держави.

В об'єднаній доктрині США «Інформаційні операції» йде мова про те, що інформаційна середа - це сукупність індивідів, організацій або систем, які збирають, люрабативают або поширюють інформацію, сюди також включається сама інформація.Такім чином, інформаційний простір включає дві складові: саму інформацію та інформаційну інфраструктуру [22].

Переходячи безпосередньо до розгляду поняття «інформаційна безпека», необхідно відзначити складність даного явища, що обумовлює різноманіття підходів до формулювання понять «інформаційна безпека». Інформаційна безпека підкреслює важливість інформації в сучасному суспільстві - розуміння того, що інформація - цінний ресурс, більше, ніж окремі елементи данних.

Інформаційною безпекою називають заходи щодо забезпечення захисту інформації від неавторизованого доступу, руйнування, модифікації, розкриття і затримкою в доступі. Інформаційна безпека включає в себе заходи з захисту процесів створення данних, їх введення, обробки і виведення.

Метою інформаційної безпеки є убезпечення цінності системи, захист і гарантування точності і єдності інформації, мінімізація руйнувань, які можуть мати місце, якщо інформація буде модифікована або знищена. Інформаційна безпека вимагає врахування всіх подій, під час яких інформація створюється, модифікується, до неї забезпечується доступ або вона поширюється [23, с.79].

Аналіз наукової літератури, актів права ЄС, міжнародних актів, законодавства України, зарубіжних країн дозволяє виділити кілька основних підходів до змісту поняття інформаційної безпеки:

1. поняття інформаційної безпеки як стану інформаційної сфери суспільства (інформаційного середовища суспільства); стан захищеності інформації (інформаційного простору); життєво важливих інтересів особистості, суспільства, держави від різного роду загроз.

Так, російські вчені В.Д. Курушін і В.А. Мінаев розуміють інформаційну безпеку як «стан інформаційної сфери суспільства, що забезпечує її формування і розвиток в інтересах громадян, організацій, держави» [24, с.141]. Аналогічно трактує інформаційну безпеку І. Панарін, визначаючи інформаційну безпеку як «стан інформаційного середовища суспільства та політичної еліти, що забезпечує її формування та розвиток в інтересах керівництва держави, громадян і суспільства» [25, с.128].

Аналогічно розуміють інформаційну безпеку і вітчизняні правознавці (І.М. Колодій [26, с.302], В.М. Брижко, О.М. Гальченко, О.А. Орєхов, А.М. Чорнобров [27, с.79-80]): інформаційна безпека - це стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій, держави; стан захищеності національних інтересів України в інформаційному середовищі, при якому не допускається або зводиться до мінімуму заподіяння шкоди особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інформації та несанкціоноване її поширення і використання, а також через

негативний інформаційний вплив і негативні наслідки функціонування інформаційних технологій.

2. інформаційна безпека тлумачиться як складова національної безпеки. Для цього підходу характерним є поєднання у визначенні понять «стан» і «здатність».

У свою чергу, національна безпека як правове поняття має певну універсальність, що виражає ідею єдності станів безпеки. Ця єдність і служить основою для напрацювання як національних, так і міжнародних правових систем. Тобто, з одного боку, національна безпека характеризується таким важливим фактором, як єдність. При цьому вона завжди поліпредметного. Це протиріччя усувається за засобом правового забезпечення національної безпеки шляхом правового відображення загрози безпеці, її розмірів та законодавчої фіксації способів реагування на загрозу, а також визначенням компетенції органів влади в цьому процесі [28, с.12].

Аналогічно під інформаційною безпекою відповідно до Принципів, що стосуються міжнародної інформаційної безпеки, які відображені в доповіді Генерального секретаря ООН від 10 червня 2000 року «Досягнення у сфері інформатизації і телекомунікації в контексті міжнародної безпеки», розуміється стан захищеності основних інтересів особистості, суспільства і держави в інформаційному просторі, включаючи інформаційно-телекомунікаційну інфраструктуру і власне інформацію щодо таких її властивостей, як цілісність, об'єктивність, доступність і конфіденційність [29].

Відповідно до Концепції національної безпеки Республіки Білорусь, затвердженої Указом Президента Республіки Білорусь від 9 листопада 2010 р. № 575 «інформаційна безпека - стан захищеності збалансованих інтересів особистості, суспільства і держави від зовнішніх і внутрішніх загроз в інформаційній сфері» [30].

Згідно Інструкції про організацію системи внутрішнього контролю в банках, небанківських кредитно-фінансових організаціях, банківських групах

і банківських холдингах, затвердженої Постановою Правління Національного Банку Республіки Білорусь від 30 листопада 2012 р. № 625 «інформаційна безпека - багаторівневий комплекс організаційних заходів, апаратно-програмних і технічних засобів, що забезпечують захист від випадкових і навмисних загроз, в результаті реалізації яких можливе порушення властивостей доступності, цілісності, автентичності або конфіденційності оброблюваної, що зберігається або передається інформації» [31].

В Угоді про співробітництво держав - учасниць Співдружності Незалежних Держав у галузі забезпечення інформаційної безпеки від 20 листопада 2013 р. інформаційна безпека визначається як «стан захищеності особи, суспільства і держави та їх інтересів від загроз, деструктивних та інших негативних впливів в інформаційному просторі» [32].

Постанова Міжпарламентської Асамблеї Євразійського економічного співтовариства від 28 травня 2004 р. № 5-20 «Про типові проекти законодавчих актів МПА ЄврАзЕС у сфері інформаційних технологій («Про інформатизацію», «Про інформаційну безпеку», «Основні принципи електронної торгівлі»)» містить таку норму: «інформаційна безпека - стан захищеності прав, свобод, охоронюваних законом інтересів фізичних, юридичних осіб і держави в інформаційній сфері від внутрішніх і зовнішніх загроз» [33].

Постанова Міжпарламентського Комітету Республіки Білорусь, Республіки Казахстан, Киргизької Республіки, Російської Федерації та Республіки Таджикистан від 15 жовтня 1999 № 9-9 «Про модельний закон «Про безпеку»» визначає інформаційну безпеку як «стан захищеності державних інформаційних ресурсів, а також прав особистості та інтересів суспільства в інформаційній сфері» [34].

Відповідно до Концепції інформаційної безпеки держав - учасниць Співдружності Незалежних Держав у військовій сфері, затвердженої Рішенням Ради глав урядів Співдружності Незалежних Держав від 4 червня 1999 р. «інформаційна безпека – стан захищеності інформаційного

середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій, держави» [35].

Стаття 13 Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 р. № 537-V також визначає інформаційну безпеку як «стан захищеності життєво важливих інтересів людини, суспільства й держави, за якого запобігають заподіянню шкоди через неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання й порушення цілісності, конфіденційності та доступності інформації» [36].

При цьому ні у Законі України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII, ні в Законі України «Про Концепцію Національної програми інформатизації» від 04.02.1998 р. № 75/98-ВР зміст інформаційної безпеки не розкривається, вона визнається одним із напрямів державної політики у сфері національної безпеки і оборони або невід'ємною частиною політичного, економічного, оборонного та інших складників національної безпеки відповідно.

Т.А. Полякова інформаційну безпеку розглядає також як «стан захищеності національних інтересів Російської Федерації в інформаційній сфері, що складаються з сукупності збалансованих інтересів особистості, суспільства і держави від внутрішніх і зовнішніх загроз, що відповідає принципу забезпечення національної безпеки в інформаційній сфері, визначеним у Стратегії розвитку інформаційного суспільства в Російській Федерації» [37, с.21].

3. Інформаційна безпека розглядається як суспільні відносини щодо створення і підтримання на усвідомленому, належному рівні функціонування відповідної автоматизованої (комп'ютеризованої) інформаційної системи (зокрема, систем телекомунікацій); комплекс організаційних, правових та інженерно-технологічних (технічних і програмно-математичних) заходів з

підтримки (охорони, захисту, збереження), попередження та подолання природних, техногенних та соціогенних загроз, здатних порушити життєдіяльність конкретної соціотехніческой інформаційної системи (В.С. Цимбалюк [38, с.91]).

4. Інформаційна безпека визначається через комплекс прав людини: по-перше, це комплекс прав людини вільно, безперешкодно, на свій розсуд бути суб'єктом інформаційних процесів: шукати, одержувати і поширювати інформацію, причому це право не обмежується територіально державними кордонами і не пов'язане з територіальною юрисдикцією держави. І, по-друге, це комплекс прав людини на захист від неправомірного інформаційного втручання, тобто право на конфіденційність інформації про особисте життя і право на захист від поширення вигаданою і спотвореної інформації, що завдає шкоди його честі і репутації (А.І. Марущак [39, с.82]).

На думку В.Ф. Пилипенка, інформаційна безпека держави - стан збереження інформаційних ресурсів держави і захищеності законних прав особистості і суспільства в інформаційній сфері [40].

Зустрічаються і інші підходи до розуміння інформаційної безпеки, що відрізняються певною оригінальністю. Так, наприклад, О.Г. Додонов вважає, що інформаційна безпека є, насамперед, властивістю системи мінімізувати інформаційні загрози. При розгляді проблеми інформаційної безпеки слід спочатку говорити про загрози і вже потім - про захищеність від цих загроз [41, с.123].

Таким чином, інформаційна безпека є поняттям багатогранним і комплексним. Вона має два основних аспекти: змістовний (духовна сфера) і технічний (матеріальна сфера). До першого з них можна віднести зміст і спрямованість всієї циркулюючої інформації. Технічний аспект - сукупність інформаційно-телекомунікаційних засобів, технологій, систем, ресурсів, призначених для створення, зберігання, поширення, передачі та обробки інформації [42, с. 207].

Крім того, аналіз наукової літератури свідчить про те, що при визначенні змісту поняття «інформаційна безпека» одна група авторів (наприклад, В.І. Ярочкин) ототожнюють два різних поняття - «захист інформації» та «інформаційна безпека» [43, с.125]. Інші автори (наприклад, А.Н. Асаул) розуміють цей термін вузько, як набір апаратних і програмних засобів для забезпечення збереження, доступності та конфіденційності даних в комп'ютерних мережах [44, с.169]. Треті автори (наприклад, В.А. Галатенко, В.К. Левін) під безпекою в інформаційній сфері розуміють захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, можуть призвести нанесенням шкоди власникам або користувачам інформації та підтримуючої інфраструктури [45, с.590-591].

У сучасному соціумі інформаційна сфера має дві складові: інформаційно-технічну (штучно створений людиною світ техніки, технологій і т п.) і інформаційно-психологічну (природний світ живої природи, що включає і саму людину). Відповідно, в загальному випадку інформаційну безпеку суспільства (держави) можна представити двома складовими частинами: інформаційно-технічною безпекою та інформаційно-психологічною (психофізичною) безпекою [46, с.179].

Значний інтерес представляє питання аналізу, поряд з правовим аспектом, підходів філософів, політологів, соціологів, дослідників технічних наук до визначення поняття «інформаційна безпека». Зупинимося на деяких з них.

Так, Г.А. Атаманов поєднує в цій дефініції три аспекти: задоволення інформаційних потреб суб'єктів; забезпечення безпеки інформації; забезпечення захисту суб'єктів [47, с.108].

Тобто, в сутнісному плані інформаційна безпека, згідно філософському підходу, є такий стан об'єкта, при якому стан інформаційного середовища, в якому він знаходиться, дозволяє йому зберігати здатність і можливість приймати і реалізовувати рішення згідно своїм цілям, спрямованим на

прогресивний розвиток. Це означає, що інформаційна безпека може досягатися як в результаті проведення заходів, спрямованих на підтримку інформаційного середовища в безпечному для об'єкта захисту стані, захист об'єкта від деструктивного впливу, так і шляхом зміцнення імунітету і розвитку здатності об'єкта ухилятися від деструктивного інформаційного впливу (в тому числі за рахунок передбачення їх можливості).

Отже, завдання забезпечення інформаційної безпеки держави полягає в тому, щоб створити такі умови функціонування інформаційної інфраструктури (головним елементом якої є не комп'ютер, а чоловік), при яких окремі громадяни, колективи, органи влади могли б приймати управлінські рішення і домагатися їх реалізації сумісних із цілями , спрямованим на прогресивний розвиток всього суспільства [48, с.56].

Політичний аналіз проблематики інформаційної безпеки - сьогодні один з найбільш активних і вказує, насамперед, на зростаючу необхідність об'єднання зусиль приватного сектору, політичних інститутів та правоохоронних структур, експертно-аналітичних спільнот в пошуку способів протистояння різноманітним загрозам в даній області [49, с.69].

Соціологи розвивають поняття інформаційної безпеки в рамках одного з напрямків соціології - соціології інформатики, тим самим взаємоповязуючи соціологічний і інформаційний підходи [50, с.15].

Представлені погляди вчених на поняття і проблему інформаційної безпеки виявляють як наявність спільних поглядів, так і специфіку кожного їх підходів. Зрозуміло одне: рішення проблем інформаційної безпеки можливо тільки за рахунок скоординованих і об'єднаних єдиним задумом політичних, організаційних, соціально-економічних, військових, правових, інформаційних, спеціальних та інших заходів.

Вважаємо, що поняття міжнародна інформаційна безпека повинно узагальнити усі вищенаведені визначення та увібрати в себе найголовніше, для того, щоб воно могло бути застосовано усіма державами як консолідоване поняття. Тоді, зміст поняття безпеки буде базуватися на

інтересах світового співтовариства, суспільств у системі міждержавних відносин, які увібрали в себе сукупність інтересів особи, держави та суспільства, від збалансованості яких залежить рівень загроз на міжнародному рівні.

Загалом, міжнародну інформаційну безпеку необхідно визначити як складову всеосяжної безпеки, стан захищеності особи, суспільства, держави і світового співтовариства, при якому досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний) та негативний сторонній інформаційно-психологічний та інформаційно-технічний вплив через неповноту, несвоєчасність і недостовірність інформації, що використовується, несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації не завдають істотної шкоди [51, с.231].

Як представляється необхідно погодитися з позицією І.М. Забари [52, с.65], що оскільки поняття міжнародної інформаційної безпеки в міжнародно-правовій термінології не є усталеним, то за критерій віднесення до складу інституту міжнародної інформаційної безпеки необхідно взяти відносини держав в інформаційній сфері, що підлягають регулюванню.

Відповідно, ці відносини можна структурувати на підставі трьох складових.

До першої складової (в доктрині її визначають в якості кримінального аспекту міжнародної інформаційної безпеки (термінологічно – комп'ютерна злочинність, кіберзлочинність тощо)) відносять всі прояви використання інформаційно-комунікаційних технологій на шкоду основним правам і свободам людини, що реалізуються в інформаційній сфері, тобто ця складова полягає у необхідності забезпечення належного і стійкого балансу між правоохоронними інтересами і повагою до основних прав і свобод людини.

З цього приводу інтерес представляє концептуальний підхід до проведення спільних дій, запропонований проєктом універсальної Конвенції про забезпечення міжнародної інформаційної безпеки 2011 року [53], який

передбачає, що держави забезпечать встановлення, виконання та застосування процедур з метою проведення кримінального розслідування та судового розгляду за фактами скоєння в інформаційному просторі соціально небезпечних діянь у відповідності з їх національним законодавством, що забезпечуватиме належний захист прав і свобод людини.

Друга складова міждержавних відносин в інформаційній сфері (в доктрині визначається як терористичний аспект міжнародної інформаційної безпеки (термінологічно – «інформаційний тероризм», «кібертероризм» тощо)) полягає у протидії використанню інформаційного простору у терористичних цілях [54], коли мають місце прояви використання інформаційно-комунікаційних технологій державними і недержавними структурами, організаціями, групами і окремими особами в терористичних, екстремістських та інших злочинних діях. На відміну від попереднього кримінального аспекту, терористична діяльність в інформаційному просторі проводиться в політичних цілях.

Більш докладно про ці аспекти мова піде у підпункті 2.2.

Третя складова міждержавних відносин в інформаційній сфері полягає у попередженні військових конфліктів з використанням інформаційно-комунікативних технологій, а також підготовки та ведення інформаційної війни (військово-політичний аспект, термінологічно – «інформаційні війни», «інформаційні операції» тощо). Докладно про цей аспект - у підпункті 2.1.

Таким чином, міжнародна інформаційна безпека забезпечується взаємодією акторів міжнародних відносин з операцій підтримання сталого миру на основі захисту міжнародної інфосфери, глобальної інфраструктури, суспільної свідомості світового співтовариства від реальних та потенційних загроз.

1.2. Правове забезпечення міжнародної інформаційної безпеки

В умовах об'єктивно формується глобального інформаційного простору, суть проблеми міжнародної інформаційної безпеки (МІБ) корениться в лавиноподібному процесі розвитку та впровадження новітніх інформаційних, телекомунікаційних та кібернетичних технологій. Забезпечуючи безпрецедентні можливості накопичення і використання інформації, ці технології та засоби одночасно створюють фундаментальну залежність від їх нормального функціонування всіх сфер життєдіяльності суспільства і держави: економіки, політики, культури, забезпечення національної та міжнародної безпеки.

Світова інформаційно-технологічна революція поряд з очевидними благами, які вона вже дала людству, одночасно створює принципово нові потенційні загрози використання досягнень науково-технічної думки в цій галузі з метою, несумісних із завданнями підтримки міжнародної стабільності і безпеки, дотримання принципів відмови від застосування сили, невтручання у внутрішні справи держав, поваги прав і свобод людини.

Заклопотаність виникає, насамперед, у зв'язку з можливістю застосування колосального потенціалу інформаційно-кібернетичних технологій в інтересах забезпечення військово-політичної переваги, силового протиборства, шантажу [55, с.167].

Збільшення за рахунок новітніх інформаційних технологій військового потенціалу розвинених країн веде до зміни глобального і регіональних балансів сил, напруженості між традиційними і новими центрами сили, появі нових сфер конфронтації. Виникає спокуса скористатися перевагами у володінні інформаційними технологіями для інформаційної, політичної, економічної, культурної та військової експансії. З іншого боку, країни втягуються в процес створення у себе потенціалу для «міжнародного хакерства», «інформаційного піратства» та агресії. До цієї діяльності вже

підключилися певні політичні угруповання, «новий» збройовий бізнес, а поряд з ними - терористичні та кримінальні організації і групи.

А.А. Стрільців поняття «забезпечення інформаційної безпеки» розкриває як «складне явище, що включає об'єкт безпеки, утворений сукупністю інформаційних потреб держави та її діяльності щодо задоволення цих потреб, загроз об'єкту безпеки, діяльності держави з протидії загрозам, а також суб'єктів цієї протидії» [56, с.16].

Правове забезпечення інформаційної безпеки являє собою діяльність законодавчих і виконавчих органів державної влади з розробки, реалізації та контролю виконання сукупності нормативнио-правових актів, що регламентують практичну діяльність з захисту інформації особистості, суспільства і держави.

Виходячи з трьох складових міжнародної інформаційної безпеки, можна зробити висновок, що правове забезпечення інформаційної безпеки спрямовано на: забезпечення ефективної реалізації, захисту конституційних прав особистості та недоторканності приватного життя, особисту і сімейну таємницю, захист честі і гідності; створення сприятливих умов для вільного і оперативного доступу органів державної влади та органів місцевого самоврядування до інформації, що безпосередньо зачіпає права і свободи людини; захист прав учасників електронної комерції; захист інтелектуальної власності; забезпечення захисту інформації, що містить відомості, що становлять державну таємницю, та іншої інформації з обмеженим доступом; захист інтересів держави і суспільства у сфері використання державних інформаційних ресурсів і т.д.

У структурі правового забезпечення міжнародної інформаційної безпеки як виду діяльності виділяються:

- нормативне правове забезпечення інформаційної безпеки;
- правове забезпечення інформаційної безпеки як напрям юридичної науки;

- правове забезпечення інформаційної безпеки як системи навчальних курсів, що використовуються в процесі підготовки кадрів для діяльності в галузі протидії загрозам інформаційної безпеки.

В свою чергу, в залежності від об'єкта забезпечення міжнародної інформаційної безпеки у складі нормативного правового забезпечення виділяються чотири складових:

- нормативне правове забезпечення безпеки інформації в формі відомостей;

- нормативне правове забезпечення безпеки інформації у формі повідомлень;

- нормативне правове забезпечення безпеки інформаційної інфраструктури суспільства;

- нормативне правове забезпечення безпеки правового статусу суб'єктів інформаційної сфери [57, с.15].

Важливою складовою частиною структури правового забезпечення інформаційної безпеки є наукові дослідження відносин, що складають його предмет, вивчення правової характеристики об'єктів, національних інтересів в інформаційній сфері, способів прояву загроз цим об'єктам, правових засобів і механізмів, здатних забезпечити протидію загрозам, способів взаємодії різних галузей права в процесі функціонування механізмів правового регулювання відносин у даній галузі, а також проведення порівняльних досліджень методів правового регулювання аналогічних відносин у різних країнах світу, питань взаємодії національного права та міжнародного права.

Ще однією складовою частиною правового забезпечення інформаційної безпеки є результати узагальнення досліджень та аналізу законодавства з виділеним вище складовим нормативного правового забезпечення.

Дослідження правового забезпечення включають такі основні етапи:

- аналіз правових характеристик об'єкта національних інтересів в інформаційній сфері, в рамках якого з'ясовуються питання правового

закріплення об'єкта відносин, основні групи пов'язаних з ним суспільних відносин і механізми їх правового регулювання;

- аналіз змісту загрози безпеки об'єктів національних інтересів, в рамках якого з'ясовуються основні способи нанесення шкоди цим об'єктам внаслідок прояву загроз;

- аналіз правового забезпечення безпеки об'єктів, в рамках якого з'ясовується його предмет, а також цілі, принципи та методи правового регулювання суспільних відносин, що становлять даний предмет, що закріплюють їх правове норми, їх достатність для ефективної протидії загрозам безпеки об'єктів національних інтересів;

- розробка пропозицій щодо вдосконалення правового забезпечення інформаційної безпеки, в рамках якої готуються пропозиції щодо розвитку правових норм і механізмів, що регулюють відносини, що виникають внаслідок прояву загроз безпеки об'єктам національних інтересів в інформаційній сфері, з метою підвищення захищеності цих об'єктів [58, с.378].

Таким чином, правове забезпечення міжнародної інформаційної безпеки як вид діяльності направлено на протидію загрозам безпеці основних об'єктів інтересів в інформаційній сфері.

Структурно воно включає самостійний напрям правового регулювання, самостійну область юридичної науки. Кожна з виділених складових правового забезпечення інформаційної безпеки базується на певній системі принципів і використовує для вирішення поставлених перед нею завдань властиву їй систему методів.

Зважаючи на глобальність проблеми інформаційної безпеки, країни розпочали реалізацію довгострокових державних програм, спрямованих на забезпечення захисту критично важливих інформаційних структур, а з 1996 року проблему міжнародної інформаційної безпеки було винесено на політичний та міжнародно-правовий рівень: по-перше, на міжнародній конференції з проблем становлення інформаційного суспільства та

глобальної цивілізації (ПАР, 1996 р.) було обговорено концепцію міжнародної інформаційної безпеки; по-друге, у спільному комюніке зустрічі на найвищому рівні США -Російська Федерація було підкреслено загрозу створення інформаційної зброї і визнано наявність воєнної складової глобального процесу інформатизації; по-третє, прийняттям Резолюції 53/70 1998 року Генеральна Асамблея ООН поклала початок обговоренню створення нового міжнародно-правового режиму, об'єктом якого в перспективі повинні стати інформація та інформаційна технологія.

За результатами роботи 55-ій сесії Генеральної Асамблеї ООН у 2000 році схвалено нову редакціію резолюції (A/RES/55/28), в якому наголошується, що цілям обмеження погроз у сфері інформаційної безпеки відповідало би «вивчення відповідних міжнародних концепцій, направлених на зміцнення безпеки глобальних інформаційних і телекомунікаційних систем» [59].

Відповідно до рекомендацій резолюції 55/28, було підготовлено проект документу (A/56/164/Add.1) «Досягнення в сфері інформатизації і телекомунікації в контесті міжнародної безпеки. Загальна оцінка проблем інформаційної безпеки. Погрози міжнародній інформаційній безпеці», в якому виділені та описані одинадцять основних чинників, що є найбільшими загрозами міжнародній інформаційній безпеці:

- розробка і використання засобів несанкціонованого втручання в роботу ІКТ, неправомірне використання та нанесення збитку інформаційним ресурсам іншої держави;

- цілеспрямована інформаційна дія на критичні інфраструктури і населення іншої держави;

- дії, направлені на домінування в інформаційному просторі, заохочення тероризму та ведення інформаційних війн [60].

Положення вказаних резолюцій знайшли свій розвиток у прийнятій консенсусом 22.11.2002 року ГА ООН резолюції A/RES/57/53, яка наголошує на неприпустимості використання інформаційно-телекомунікаційних

технологій і засобів в цілях надання негативної дії на інфраструктуру держав [61].

Згодом положення вказаних резолюцій були розвинуті та доповненені резолюціями 58/32 від 08.12.2003 р., 59/61 від 03.12.2004 р., 60/45 від 08.12.2005 р., 61/54 від 06.12.2006 р., 62/17 від 05.12.2007 р., 63/37 від 02.12.2008 р., 64/25 від 02.12.2009 р., 65/41 від 08.12.2010 р., 66/24 від 02.12.2011 р., 67/27 від 03.12.2012 р., 68/243 від 27.12.2013 р., 69/28 від 02.12.2014 р., 70/237 від 23.12.2015 р., 71/28 від 05.12.2016 р.

Загалом, всі резолюції спрямовані на забезпечення мирного використання інформаційно-комунікаційних технологій (ІКТ) в інтересах загального блага людства і подальшого сталого розвитку всіх країн незалежно від їх наукового і технологічного розвитку.

У доповіді Групи урядових експертів з досягнень в сфері інформатизації і телекомунікацій в контексті міжнародної безпеки 2015 року особливо підкреслюється, що при розгляді питання про можливість застосування норм міжнародного права на використання ІКТ державами найважливіше значення мають зобов’язання держав відповідно до загальних принципів міжнародного права, і що міжнародне право може бути застосовано і має важливе значення для підтримки міжнародного миру і стабільності, а також створення відкритого, безпечного, стабільного, доступного і мирного інформаційного середовища, що добровільні і необов'язкового норми, правила і принципи відповідальної поведінки держав у сфері використання ІКТ можуть знизити ризик порушення міжнародного миру, безпеки і стабільності і що з урахуванням унікальних особливостей ІКТ можуть бути розроблені додаткові норми [62].

Необхідно відзначити, що проблематика міжнародної інформаційної безпеки обговорювалася на Всесвітній зустрічі на вищому рівні з питань інформаційного суспільства (ВСІС). Перший етап цієї зустрічі проходив у грудні 2003 р в Женеві, другий - у листопаді 2005 р в Тунісі. Важливу роль в її популяризації відіграла 16-я Повноважна конференція Міжнародного

союзу електрозв'язку, що пройшла в Марракеші (Марокко, вересень-жовтень 2002).

У якості одного із заходів, можливих для вивчення в ході підготовки до ВСІС, країни назвали розгляд існуючих і потенційних загроз для безпеки інформаційних і комунікаційних мереж.

Учасники ВСІС також погодилися внести вклад в реалізацію зусиль ООН, спрямованих на оцінку стану інформаційної безпеки, а також в розгляд питання про розробку (в довгостроковій перспективі) міжнародної конвенції з безпеки в середовищі інформаційних мереж і мереж зв'язку.

Формулювання міжнародної інформаційної безпеки, що знайшли відображення в документах Міжнародного союзу електрозв'язку (МСЕ), в подальшому лягли в основу положень підсумкових документів регіональних конференцій ВСІС: загальноєвропейської (Бухарест, 7-9 листопада 2002р.) і азіатської (Токіо, 13-15 січня 2003р.).

В якості заходів зміцнення довіри і безпеки при використанні ІКТ автори «Плану дій» виділяли:

- сприяння співробітництву в рамках ООН з метою аналізу реальних і потенційних загроз у сфері ІКТ;
- вирішення питань безпеки мереж;
- вивчення проблем вдосконалення законодавства;
- проведення ефективних розслідувань і припинення випадків неналежного використання ІКТ.

Проведений у Тунісі в листопаді 2005 р. другий етап Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства схвалив два підсумкових документа: політичний («Туніське зобов'язання») і юридичний («Туніська програма для інформаційного суспільства»). Перший підтвердив і конкретизував положення схваленої Женевським етапом ВСІС декларації принципів «Побудова інформаційного суспільства - глобальне завдання в новому тисячолітті». Другий документ визначив механізми реалізації рішень саміту, фінансові аспекти та питання управління Інтернетом [63].

У січні 2015 року держави-члени Шанхайської організації співпраці (ШОС) внесли на розгляд Генеральної Асамблеї ООН нову редакцію «Правил поведінки в області забезпечення міжнародної інформаційної безпеки (МІБ)» [64].

Документ спирається на підходи, закладені в проекті «Правил поведінки в області забезпечення МІБ», поширеному від імені держав-членів ШОС в ході 66-ої сесії Генеральної Асамблеї ООН в 2011 році. У новій редакції дані ідеї отримали конструктивний розвиток з врахуванням реалій, що змінилися, і пропозицій, поступили від зацікавлених держав. Ключовою особливістю документа є миротворчий характер. Він націлений на запобігання конфліктам в інформаційному просторі. У ньому закріплено зобов'язання держав не застосовувати інформаційно-комунікаційні технології, які ведуть до порушення міжнародного миру і безпеки, а також втручання у внутрішні справи інших держав і підривання їх політичної, економічної і соціальної стабільності. Крім того, документ передбачає зобов'язання держав утримуватися від погроз і застосування сили в ході вирішення міжнародних спорів, що виникають в цифровій сфері.

До нової редакції також включений розширений «праволюдський» розділ, що закріплює збалансований підхід до даної проблематики. Відмічено, що права, які людина має в оф-лайновому середовищі, повинні захищатися також і в он-лайновому. При цьому користування даними правами може бути пов'язане з деякими обмеженнями відповідно до статті 19 Міжнародного пакту про громадянські і політичні права. Особлива увага приділена проблематиці нарощування потенціалу в сферах інформаційної безпеки і надання країнам, що розвиваються, сприяння в подоланні цифрового розриву [65, с.6].

У сфері забезпечення інформаційної безпеки в межах СНД можна виділити наступні угоди - Угода про співробітництво держав – учасниць Співдружності Незалежних Держав у галузі забезпечення інформаційної безпеки від 20 листопада 2013 р., постанова Міжпарламентської Асамблеї

держав-учасниць Співдружності Незалежних Держав від 18 Листопад 2005 р. № 26-7 «Про гармонізації законодавства держав -учасниць СНД в галузі інформатизації та зв'язку», Угода між Урядом Республіки Білорусь та Урядом Республіки Казахстан про співробітництво в галузі захисту інформації, Угода між Урядом Республіки Білорусь та Урядом Російської Федерації про співробітництво в галузі захисту інформації, постанова Міжпарламентського комітету Республіки Білорусь, Республіки Казахстан, Киргизької Республіки, Російської Федерації та Республіки Таджикистан від 15 жовтня 1999 р. № 9-9 «Про модельний закон «Про безпеку»» тощо.

РОЗДІЛ 2
ЗАБЕЗПЕЧЕННЯ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Організаційна структура забезпечення міжнародної інформаційної безпеки

В сучасних умовах міжнародне співробітництво у сфері забезпечення інформаційної безпеки вимагає пошуку спільних рішень щодо протидії сучасним інформаційним та кіберзагрозам, інформаційному тероризму та кіберзлочинності.

О.Г. Додонов вважає, що інформаційна безпека є, насамперед, властивістю системи мінімізувати інформаційні загрози. При розгляді проблеми інформаційної безпеки слід спочатку говорити про загрози і вже потім - про захищеність від цих загроз.

Первинною є саме інформаційна загроза. Для окремої особистості існують одні інформаційні загрози, для суспільства - інші, для держави - ще інші. І якщо говорити про інформаційну безпеку як про властивість мінімізувати загрози для певних об'єктів і суб'єктів інформаційної діяльності, то це, на мою думку, правильно. Використовуючи такий підхід, можна розглядати не загальнометодичні питання інформаційної безпеки, а різні рівні інформаційної взаємодії, інформаційних відносин, виділити методологічні та теоретичні проблеми забезпечення інформаційної безпеки, які необхідно вирішити. А тоді вже можна шукати засоби, методи протидії інформаційним загрозам, закладати ці методи у відповідні інформаційні системи для адекватного реагування на загрози.

Таким чином, необхідно розмежовувати безпосередні загрози інформаційній безпеці і засоби забезпечення цієї безпеки, що спрацьовують лише при виникненні загроз. Аналізуючи проблему загроз інформаційної безпеки необхідно визначити, що саме може розцінюватися як загроза.

Як видається, по-перше, загрозу можуть нести лише певні дії (діяльність або бездіяльність), що мають прямий причинно-наслідковий зв'язок із зміною відповідних умов і параметрів інформаційних процесів, які визначають безпечні умови існування суспільства і держави.

По-друге, ці дії повинні бути конкретно-визначеними, а не загальними. По-третє, як зазначає Б.А.Корміч, ще одним фактором має бути рівень суспільної небезпеки цих дій. Безумовно, дії, які можуть розцінюватися як загроза інформаційній безпеці, повинні мати виключно високу суспільну небезпеку, оскільки їх об'єктом є не просто права або законні інтереси певних суб'єктів, а правові відносини щодо забезпечення умов, порушення яких ставить під сумнів саму можливість нормального існування цих суб'єктів [66, с.195].

Таким чином, замахом на інформаційну безпеку є ті дії, за які законом передбачена відповідальність.

Традиційно дії, що зачіпають інформаційну безпеку, підрозділяють на внутрішні і зовнішні. При цьому внутрішні дії пов'язані з діяльністю або з факторами, які мають своє походження всередині держави. Відповідно, зовнішні дії являють собою фактори або дії, що беруть початок за межами території держави.

Зазначені дії можна класифікувати залежно від змісту цих дій і від характеру і ступеня їх небезпеки для особистості, суспільства, держави і міжнародного співтовариства в цілому. Таким чином, можна визначити три види дій:

1. Найбільш небезпечні для держави і міжнародного співтовариства дії, що зачіпають інформаційну безпеку, що здійснюються однією державою або групою держав щодо іншої держави або групи держав. В даний час подібні дії більшістю дослідників об'єднуються в понятті «інформаційна війна».

2. Небезпечні для держави і суспільства дії, що здійснюються для досягнення політичних, релігійних та інших цілей, для створення обстановки страху в державі або державах. Такі дії здійснюються, як правило,

організованими терористичними угрупованнями і отримали назву «інформаційний тероризм».

3. Дії, що зачіпають інформаційну безпеку, які походять від осіб, які переслідують злочинні цілі, або «інформаційні злочини».

Основи державної політики Російської Федерації в галузі міжнародної інформаційної безпеки на період до 2020 року, наприклад, визначають в якості основної загрози в галузі міжнародної інформаційної безпеки використання інформаційних та комунікаційних технологій (ІКТ):

- в якості інформаційної зброї у військово-політичних цілях, що суперечать міжнародному праву, для здійснення ворожих дій та актів агресії, спрямованих на дискредитацію суверенітету, порушення територіальної цілісності держав і становлять загрозу міжнародному миру, безпеки та стратегічної стабільності;

- в терористичних цілях, у тому числі для надання деструктивного впливу на елементи критичної інформаційної інфраструктури, а також для пропаганди тероризму та залучення до терористичної діяльності нових прихильників;

- для втручання у внутрішні справи суверенних держав, порушення громадського порядку, розпалювання міжнаціональної, міжрасової та міжконфесійної ворожнечі, пропаганди расистських і ксенофобських ідей або теорій, що породжують ненависть і дискримінацію, підбурюють до насильства;

- для вчинення злочинів, у тому числі пов'язаних з неправомірним доступом до комп'ютерної інформації, із створенням, використанням та поширенням шкідливих комп'ютерних програм.

При цьому в запропонованій 25 вересня 2013 р. Радою безпеки Російської Федерації Концепції Конвенції про забезпечення міжнародної інформаційної безпеки в якості основних загроз в інформаційному просторі, що призводять до порушення міжнародного миру і безпеки, розглядаються наступні:

- використання інформаційних технологій і засобів для здійснення ворожих дій та актів агресії;

- цілеспрямований деструктивний вплив в інформаційному просторі на критично важливі структури іншої держави;

- неправомірне використання інформаційних ресурсів іншої держави без узгодження з державою, в інформаційному просторі якої розташовуються ці ресурси;

- дії в інформаційному просторі з метою підриву політичної, економічної та соціальної систем іншої держави, психологічна обробка населення, що дестабілізує суспільство;

- використання міжнародного інформаційного простору державними та недержавними структурами, організаціями, групами та окремими особами в терористичних, екстремістських та інших злочинних цілях;

- транскордонне розповсюдження інформації, що суперечить принципам і нормам міжнародного права, а також національним законодавствам держав;

- використання інформаційної інфраструктури для поширення інформації, що розпалює міжнаціональну, міжрасову і міжконфесійну ворожнечу, расистських і ксенофобських письмових матеріалів, зображень або будь-якого іншого представлення ідей або теорій, які пропагують, сприяють або підбурюють до ненависті, дискримінації чи насильства проти будь-якої особи або групи осіб;

- маніпулювання інформаційними потоками в інформаційному просторі інших держав, дезінформація і приховування інформації з метою спотворення психологічного та духовного середовища суспільства, ерозія традиційних культурних, моральних, етичних та естетичних цінностей;

- використання інформаційно-комунікаційних технологій і засобів на шкоду основним правам і свободам людини, реалізованим в інформаційному просторі;

- протидія доступу до новітніх інформаційно-комунікаційних технологій, створення умов технологічної залежності в сфері інформатизації на шкоду іншим державам;

- інформаційна експансія, придбання контролю над національними інформаційними ресурсами іншої держави.

На забезпечення безпеки держави, суспільства, людини всередині держави і на міжнародній арені активно впливають внутрішні і зовнішні фактори, види діяльності головних (генеральних) суб'єктів в особі вищих посадових осіб держав, державних органів влади та управління, транснаціональних корпорацій і підпорядкованих їм виконавчих суб'єктів в особі структур зовнішньополітичних відомств, загальнонаціональних державних спецслужб, спецслужб недержавних структур, правоохоронних органів.

Так, для проведення усестороннього дослідження проблеми міжнародної інформаційної безпеки резолюцією ГА ООН A/RES/56/19 [67] схвалена ідея створення в 2004 році спеціальної Групи урядових експертів держав-членів ООН (ГУЕ), прерогативою діяльності якої є розгляд існуючих і потенційних загроз у сфері інформаційної безпеки та сумісних заходів з їх усунення, а також вивчення міжнародних концепцій зміцнення безпеки глобальних інформаційних і телекомунікаційних систем.

Перше засідання Групи пройшло в липні 2004 року в Нью-Йорку, результатом чого стали підсумкові документи - Декларація принципів і План дій.

У Плані дій проголошувалося, що головними опорами інформаційного суспільства є довіра і безпека. В якості головних напрямів дій у цій сфері були виділені наступні:

- сприяння співробітництву між державами в рамках ООН та з усіма зацікавленими сторонами в рамках відповідних форумів з метою аналізу існуючих і потенційних загроз ІКТ, а також вирішення інших питань інформаційної безпеки та безпеки мереж;

- попередження та виявлення органами державного управління у співпраці з приватним сектором проявів кіберзлочинності та неналежного використання ІКТ і реагувати на ці прояви шляхом розробки відповідних керівних принципів;

- вивчення законодавства, що дає можливість ефективно розслідувати і піддавати переслідуванню неналежне використання ІКТ;

- сприяння ефективним заходам взаємодопомоги у цій сфері, а також профілактиці комп'ютерних інцидентів;

- обмін прикладами найкращої практики в галузі інформаційної безпеки та безпеки мереж та заохочення їх використання всіма зацікавленими сторонами;

- призначення координаторів у всіх зацікавлених країнах для реагування в режимі реального часу на події у сфері безпеки та формування відкритої спільної мережі таких координаторів для обміну інформацією і технологіями реагування на події;

- заохочення активної участі зацікавлених країн у проведенні ООН діяльності щодо зміцнення довіри і надійності при використанні ІКТ.

Резолюція ГА ООН A/RES/57/53 визначила наступні напрями діяльності ГУЕ ООН:

- узгодження понятійного апарату у сфері міжнародної інформаційної безпеки;

- розгляд чинників, що впливають на її стан з урахуванням наявності загроз терористичного, кримінального та військового характеру;

- визначення взаємоприйнятних заходів запобігання використанню інформаційних технологій та засобів в терористичних і інших злочинних цілях, а також заходів щодо обмеження застосування інформаційної зброї, перш за все відносно критично важливих структур держав;

- розгляд можливих шляхів міжнародної взаємодії правоохоронних органів по запобіганню і припиненню правопорушень в інформаційному просторі, зокрема, по виявленню джерел інформаційної агресії;

- аналіз проблеми регулювання національних законодавств окремих країн щодо питань інформаційної безпеки для забезпечення уніфікованої класифікації правопорушень у сфері інформаційної безпеки, а також визначення відповідальності, яка виникає у зв’язку зі здійсненням дій, що класифікуються як злочинні;

- оцінка можливості надання міжнародної допомоги країнам, що стали жертвами інформаційних атак, в цілях пом’якшення наслідків порушення нормальної діяльності перш за все об’єктів критичних інфраструктур держав.

Серед усіх учасників особливе місце займає так звані виконавчі суб'єкти (насамперед, спецслужби, правоохоронні органи), які забезпечують сприятливі та безпечні умови реалізації генеральними суб'єктами стратегічних і поточних завдань, захисту національних корпоративних інтересів, реалізації перспектив стратегії розвитку націй, народів, держав, міждержавних об'єднань, цивілізацій [68, с.24].

Заслуговують на увагу рекомендації науковців та експертів сектору безпеки європейських країн, зокрема Женевського центру демократичного контролю над збройними силами [69, с.25, 61-62], відповідно до яких в основу подальшого розвитку суб'єктів сектору безпеки мають бути покладені не чергові зміни їх організаційної побудови, а саме змістовні трансформації, зокрема:

- розвиток законодавчого регулювання організації та діяльності суб'єктів сектора безпеки;

- створення ефективної системи управління сектором безпеки;

- підвищення професіоналізму та ефективності діяльності спецслужб і правоохоронних органів;

- формування належного правового захисту і забезпечення державою соціальних гарантій для персоналу спецслужб і правоохоронних органів, а також для осіб, які співпрацюють з ними на конфіденційній основі;

- розвиток системи демократичного контролю.

Б. Корміч оперує декількома поняттями: «державно-правовий механізм інформаційної безпеки» й «інституційний механізм інформаційної безпеки». При цьому, якщо державно-правовий механізм інформаційної безпеки автор визначає як сукупність державних інституцій, задіяних у процесі формування та впровадження політики інформаційної безпеки, їх ролей і відносин, що підпорядковані чіткій ієрархії правових норм та, то інституційний механізм інформаційної безпеки, що є складовим елементом державно-правового механізму, має декілька визначень.

Відповідно до першого, інституційний механізм інформаційної безпеки України - це сукупність державних інституцій, задіяних у процесі формування та впровадження політики інформаційної безпеки принципів [709, с.148-149].

Згідно з другим, інституційний механізм інформаційної безпеки представляє собою сукупність інститутів публічної влади й інститутів громадянького суспільства, до компетенції яких входить вирішення питань щодо забезпечення умов функціонування та розвитку інформаційної сфери.

Таким чином, поняття «інституційний механізм інформаційної безпеки» має широке та вузьке розуміння. У вузькому значенні інституційний механізм інформаційної безпеки охоплює виключно державні інституції, задіяні в процесі формування та впровадження політики інформаційної безпеки. У широкому значенні, крім інститутів публічної влади, до його складу входять також інститути громадянського суспільства.

Перелік інституцій, які можуть брати участь у проведенні політики або виробленні конкретних політичних рішень, практично невичерпний і він не обмежується лише органами державної влади та місцевого самоврядування.

Цікавими з точки зору визначення суб'єктів забезпечення безпеки в цілому є наукові досягнення П.С. Коршикова, який впровадив нову категорію - «сили забезпечення державної безпеки». До них він запропонував віднести суспільство (як суб'єкт), державу в цілому, органи держбезпеки та інші державні органи, громадські організації [71, с.5].

Відсутня система забезпечення інформаційної безпеки на національному рівні, що унеможливлює надійне її забезпечення у середині держави та на міждержавному рівні. Головне призначення цієї системи полягає у досягненні цілей національної безпеки в інформаційній сфері та на міждержавному рівні.

Беручи до уваги масштаб проблеми інформаційної безпеки, розвинуті країни розпочали реалізацію довгострокових державних програм, які спрямовані на забезпечення захисту найважливіших інформаційних структур.

Як вже зазначалось, з 1996 року проблема міжнародної інформаційної безпеки була винесена на політичний та міжнародно-правовий рівень:

а) концепцію міжнародної інформаційної безпеки було обговорено на міжнародній конференції з проблем становлення інформаційного суспільства та глобальної цивілізації (ПАР, 1996 р.);

б) у спільному комюніке зустрічі на найвищому рівні США – Російська Федерація було підкреслено загрозу створення інформаційної зброї і визнано наявність воєнної складової глобального процесу інформатизації;

в) на 53-ій сесії ГА ООН було консенсусом прийнято Резолюцію 53/70 від 4 грудня 1998 р., де зазначалося, що міжнародна спільнота визнає проблему інформаційної безпеки як багатоаспектний стратегічний напрям взаємодії держав у світі, пропонувалося державам-членам ООН розглянути конкретну типологію інформаційних загроз, визначити критерії проблеми, включаючи розробку міжнародних принципів безпеки глобальних інформаційних систем, внести пропозиції до комплексної доповіді Генерального секретаря ООН для створення міжнародного механізму протидії використанню інформаційних озброєнь та розпалюванню інформаційних війн.

В наш час, багато країн приділяють значну увагу інформаційній безпеці. Вони займаються політикою захисту інформаційних потоків та систем, але не тільки як джерел національних таємниць, але і як джерел економічного прибутку.

Франція, наприклад, створила власний сегмент Інтернет ресурсів на французькій мові. Вона почала контролювати прибутковий ринок комп'ютерної техніки, програмного забезпечення та інформаційних потоків на всьому франкомовному просторі, як, в свою чергу, колись зробив Китай, який досяг суттєвого економічного росту за рахунок переорієнтації інформаційних потоків та акумуляції капіталів в інформаційній сфері [72].

За результатами досліджень аналітики виділяють такі моделі системи глобальної інформаційної безпеки:

Модель 1 – створення абсолютної системи захисту країни-інформаційного лідера проти будь-якого виду наступальної інформаційної зброї, що обумовлює об'єктивні переваги в потенційній інформаційній війні, змушує інші країни шукати альянсу у військово-інформаційних діях з країною-інфолідером. При цьому може бути використано систему жорсткого контролю над інформаційним озброєнням противника на підставі потенційних міжнародних документів з інформаційної безпеки.

Погляд на такий розвиток подій викладено у відомому дослідженні Дж. Ная та У. Оуенса «America's Information edge strategy and force planning», 1996 р. («Головна сила Америки – її інформаційні можливості») [73], в якому домінуюча роль в інформаційній революції належить США, а саме у використанні надважливих засобів комунікації та інформаційних технологій (супутникового спостереження, прямого мовлення, швидкісних комп'ютерів, унікальних можливостей в інтегруванні складних інформаційних систем), у політиці стримування і нейтралізації традиційних воєнних загроз та нових видів озброєнь.

Модель 2 – створення значної переваги держави-потенційного ініціатора інформаційної війни в наступальних видах озброєнь, у знешкодженні систем захисту держави-противника засобами інформаційного впливу, координація дій із союзними державами з використаннями визначених засобів інформаційної зброї для ідентифікації джерел і типів інформаційних загроз.

Практичне втілення моделі спостерігається в перебігу інформаційної операції «Союзницька сила» (1999 р.), яку США та країни-члени НАТО здійснили проти Союзної Республіки Югославії. Експерти підкреслюють формування безпрецедентної за масштабами системи управління інформаційними потоками для проведення військових операцій (спроможність надавати розвідувальну інформацію безпосередньо кожному з учасників бойових дій), масових пропагандистських кампаній з широким спектром інформаційних методик (від технологій PR для формування сприятливої світової громадської думки, вибіркового інформування із заданим ефектом сприйняття контенту до всебічної дискредитації політики противника, і навіть відвертої дезінформації світової громадськості), спрямованого інформаційно-психологічного впливу, потужного використання Internet та комп'ютерного протиборства для модифікації національного інформаційного простору і контролю за інфоінфраструктурою Югославії [74].

– Модель 3 – наявність кількох країн-інфолідерів та потенційного протиборства між ними, визначення фактору стримування експансії інформаційних загроз, забезпечення в перспективі домінування однієї з держав у сфері міжнародної інформаційної безпеки з можливостями значного впливу на глобальну інфосферу та переважного права вирішення проблем глобального світопорядку.

Дослідження ЦРУ 90-х років XX ст. та на перспективу до 2020 року визначали як основні джерела загроз в кіберпросторі для США тільки дві країни – Росію і Китай. У новій військовій доктрині збройних сил США (Концепція Force XXI, 1996 р.), де було запропоновано дві складові театру воєнних дій – традиційний простір і кіберпростір, основними об'єктами впливу стали інформаційна інфраструктура і психологічна сфера (human network) противника [75].

Модель 4 – всі конфліктуючі сторони використовують транспарентність інформації для формування ситуативних альянсів, для

досягнення переваг локальних рішень, які спроможні заблокувати технологічне лідерство, для використання можливостей інфоінфраструктури на окремих територіях з метою організації внутрішнього конфлікту між опозиційними силами (політичні, сепаратистські, міжнаціональні конфлікти) для проведення міжнародних антитерористичних інформаційних операцій.

У рамках міжнародної антитерористичної операції «Помста» (Афганістан, 2001 р.) мета спеціалізованих центрів США, відповідальних за проведення інформаційних операцій, полягала у плануванні психологічних кампаній, реагуванні на зміну ситуації, у підтримці інформаційних ресурсів та безпеки військових сил і цивільного населення. При цьому Північний Альянс вперше в історії застосував статтю 5 Статуту НАТО, яка спрямована на забезпечення загального захисту країн-членів перед викликами зовнішніх загроз; держави ЄС, країни-учасниці ГУАМ підтвердили підтримку дій США в акції «Помста» і консолідацію зусиль міжнародного співтовариства у протиборстві з міжнародним тероризмом у спільній заяві та меморандумі дій.

Модель 5 – протиборство світової спільноти та міжнародної організованої злочинності, здатної контролювати перебіг політичних, економічних, суспільних і, зрештою, цивілізаційних процесів. Можливість такої моделі передбачена в дослідженні Національної ради розвідки США «Mapping the global future» – 2020 у версії «Коло страху» («Cycle of fear»), яка є найбільш песимістичним сценарієм майбутнього світової спільноти.

Враховуючи високу здатність інформаційних озброєнь до інтеграції з іншими традиційними і технологічно новими видами військових засобів, потенційні наслідки безконтрольного застосування багатошарового страту можуть виявитися катастрофічними для існування людства. Тому тільки широке багатостороннє співробітництво може гарантувати світові вирішення нових складних проблем інформаційної доби і забезпечити реальну міжнародну інформаційну безпеку [76, с.292].

Для того щоб більш детальніше розглянути конкретні моделі міжнародної безпеки в загалі, які пропонуються фахівцями-міжнародниками

необхідно провести моделювання на основі різних підходів і критеріїв. Пропонуємо розглянути два типи моделей:

Моделі міжнародної безпеки, що відносяться до першого типу, конструюються залежно від кількості суб'єктів системи безпеки. Виділяються чотири основні моделі, що конкурують між собою:

1. Однополярна система безпеки

Після розпаду Радянського Союзу США залишилися єдиною наддержавою, яка, на думку прибічників подібної моделі, намагається нести «тягар» світового лідерства, щоб не допустити «вакууму сили» в міжнародних відносинах і забезпечити поширення демократії по всьому світу. Однополярна модель припускає посилення системи військово-політичних союзів, створених США. Так, НАТО, на думку багатьох аналітиків, повинна забезпечувати стабільність в трансатлантичній підсистемі міжнародних відносин, гармонізувати стосунки між США і європейськими державами в стратегічній області, забезпечувати американську військову присутність в Європі і гарантувати недопущення конфліктів на цьому континенті.

США ясно дали зрозуміти (і продемонстрували це на ділі в ході війни на Балканах 1999 р.), що саме НАТО повинно стати головним гарантом європейської безпеки.

Інші регіональні організації - ЄС, ОБСЄ і ін. - можуть лише грати другорядну роль в архітектурі європейської безпеки XXI ст. Відповідно до нової стратегічної концепції НАТО, прийнятої весни 1999 року, зона відповідальності цього блоку розширюється за рахунок включення в неї суміжних регіонів. Цікаво, що, з точки зору ряду експертів, НАТО не лише виконує завдання військово-політичного союзу, але і все більше придбаває ідентифікаційно-цивілізовані функції. Членство в НАТО служить свого роду індикатором приналежності до західної, «демократичної» цивілізації. Ті ж, хто не є членами НАТО і не мають шансів увійти до цієї організації, відносяться до «чужих» і навіть ворожих цивілізацій.

НАТО на сьогодні є найбільш впливовою міжнародною організацією, що модернізувала політику інформаційної безпеки, кібербезпека виступає основним пріоритетом її діяльності. Для розробки доктрини кібербезпеки, вдосконалення міждержавної взаємодії, впровадження теоретичних напрацювань у практиці протидії кіберзагрозам, обміну досвідом кіберзахисту організація заснувала передові центри НАТО у країнах-членах як багатонаціональні інститути.

Наприклад, експерти Естонського центру спільно з Комітетом Червоного Хреста та Кібернетичним командуванням США представили доповідь «Керівні принципи міжнародного права, що можуть бути застосовані під час кібернетичних війн» та «Талліннські керівні принципи 2.0», які, незважаючи на їх рекомендаційний характер, вважаються базовими засадами щодо ведення кібервійн і відповідають положенням сучасного міжнародного права про регулювання операцій у кіберпросторі, а держави несуть відповідальність за кібератаки проти інших держав, які ведуться з їх території.

Згідно доповіді кібервійни можна розглядати в якості «збройних конфліктів», що дозволяє засосовуавати контрзаходи у відповідь [77].

У положеннях 2019 року знов підтверджено, що кібербезпека вважається складовою основних завдань колективної оборони НАТО, що у кіберпросторі застосовуються принципи міжнародного права і кібербезпека спрямована на захист власних мереж організації та підвищення її обороноздатності.

Відповідно, визнаючи кіберпростір середовищем операцій, держави підтвердили оборонний мандат НАТО у кіберпросторі, в якому НАТО має ефективно захищатися, як це відбувається в інших фізичних середовищах протиборства.

У 2019 році було схвалено рекомендації НАТО, що містять низку інструментів для подальшого зміцнення здатності НАТО реагувати на агресивні кібератаки, для активізації співпраці у сфері кіберпромисловості та

надання можливостей скористатися кіберпростором союзникам на основі передбачуваних та безпечних норм» [78].

Необхідно, проте, відмітити, що однополярна модель міжнародної безпеки піддається обґрунтованій критиці як в Росії, так і в самих США. Інші центри сили - ЄС, Японія, Китай - також висловлюють своє неприйняття американської гегемонії (у відкритій або завуальованій формі).

Крім того, основний інструмент здійснення американського лідерства - військово-політичні альянси - погано пристосований для вирішення сучасних проблем. Ці союзи були створені в період «холодної війни», і їх головним призначенням було відвертання військових загроз. Багато аналітиків - російських і зарубіжних - вважають, що для адекватної відповіді на виклики з області «м'якої безпеки» (фінансово-економічні кризи, екологічні катастрофи, тероризм, наркобізнес, незаконна міграція, інформаційні війни і ін.) військова машина, успадкована з минулого, просто не годиться.

2. «Концерт держав».

Деякі фахівці пропонують в якості найкращої моделі міжнародної безпеки союз декількох великих держав (за зразком Священного союзу, що визначав облаштування Європи після завершення наполеонівських воєн), які могли б узяти на себе відповідальність як за підтримку стабільності у світі, так і за відвертання і врегулювання локальних конфліктів. Позитив "концерту держав", на думку прибічників цієї концепції, полягає в його кращій керованості і, відповідно, більшій ефективності, бо у рамках такої конструкції легше погоджувати позиції і прийняти рішення, чим в організаціях, що налічують десятки або навіть сотні (ООН) членів.

Але, існують розбіжності з приводу складу такого «концерту». Якщо одні фахівці пропонують сформувати цей союз на базі "вісімки" високорозвинених індустріальних держав" (особливо впливовою ця точка зору стала після закінчення війни в Іраку), то інші наполягають на неодмінній участі Китаю і Індії.

3. Багатополярна модель.

Деякі вчені вважають, що в період після закінчення «холодної війни» склалася не одно-, а багатополярна система міжнародних відносин. Проте критики цієї моделі вказують, що вона дискримінаційна по відношенню до малих і середніх держав. Система ж безпеки, створена на основі диктату декількох сильних держав, не буде легітимною і не користуватиметься підтримкою більшості членів світової спільноти. Крім того, ефективність цієї моделі може бути підірвана суперництвом між великими державами або виходом з союзу одного або декількох його членів.

Лідерство США багато в чому є міфічним, ілюзорним, бо такі актори, як ЄС, Японія, Китай, Індія, АСЕАН, Росія, визнаючи потужність США, все ж проводять свій курс в міжнародних справах, часто неспівпадаючий з американськими інтересами. Зростанню впливу цих центрів сили сприяє той факт, що змінюється сама природа сили в міжнародних відносинах. На передній план висуваються не військові, а економічні, науково-технічні, інформаційні і культурні складові цього феномену. А за цими показниками США не завжди є лідером. Так, по економічному і науково-технічному потенціалу ЄС, Японія і АСЕАН цілком порівнянні із США. Наприклад, за обсягом допомоги країнам Японія, що розвиваються, порівнялася із США (10 млрд. дол. щорічно). У військовій сфері ЄС також проявляє все більшу норовистість, збираючись регулярно почати формування європейської армії. Китай, що здійснює широкомасштабну програму модернізації своїх збройних сил, за оцінками фахівців, перетвориться до 2020 р. в одну з провідних військових держав не лише АТР, але і всього світу [79, с.124].

Опоненти багатополярності підкреслюють, що подібна модель не принесе стабільності в міжнародних відносинах. Адже вона виходить з бачення системи міжнародних відносин як поля вічної конкуренції між "центрами сили". А це, у свою чергу, неминуче приведе до конфліктів між останніми і постійних переділів сфер впливу.

4. Глобальна (універсальна) модель.

Прибічники цієї концепції виходять з тези про те, що міжнародна безпека може бути по-справжньому забезпечена тільки на глобальному рівні, коли усі члени світової спільноти беруть участь в її створенні. За однією версією, створення цієї моделі можливе тільки тоді, коли усі країни і народи розділятимуть деякий мінімум загальнолюдських цінностей і виникне глобальне громадянське суспільство з єдиною системою управління. Менш радикальні варіанти цієї концепції зводяться до того, що подібна модель стане результатом поступової еволюції вже існуючої системи режимів міжнародної безпеки і організацій при провідній ролі ООН [78, с.82].

Що стосується суб'єктів забезпечення міжнародної інформаційної безпеки то згідно ч.4 ст. 5 Конвенції про забезпечення міжнародної інформаційної безпеки (концепція): всі держави-учасники в інформаційному просторі користуються суверенною рівністю, мають однакові права і обов'язки і є рівноправними суб'єктами інформаційного простору незалежно від відмінностей економічного, соціального, політичного або іншого характеру.

Таким чином, організаційний (інституційний) механізм забезпечення міжнародної інформаційної безпеки охоплює держави, міжнародні організації та інституції, державні інституції, задіяні в процесі формування та впровадження політики інформаційної безпеки.

Можна виділити 4 моделі системи глобальної інформаційної безпеки: модель 1 – створення абсолютної системи захисту країни-інформаційного лідера (дана модель конструюється залежно від кількості суб'єктів системи безпеки, відповідно виділяються чотири основні моделі, що конкурують між собою: однополярна система безпеки, «концерт держав», багатополярна модель, глобальна (універсальна) модель); модель 2 – створення значної переваги держави-потенційного ініціатора інформаційної війни; модель 3 – наявність кількох країн-інфолідерів та потенційного протиборства між ними; модель 4 – всі конфліктуючі сторони використовують транспарентність інформації для формування ситуативних альянсів.

Забезпечення прав і безпеки суб'єктів інформаційної взаємодії – як національного, транскордонного, міжнародного, можливе лише на основі спільного комплексного вирішення правових, організаційних і технологічних питань, для чого необхідно прийняти міжнародні правила (кодекс) поведінки в глобальному інформаційному просторі або універсальну конвенцію під егідою ООН.

2.2. Забезпечення кібербезпеки. Технічний захист інформації

Генеральна Асамблея ООН, відзначаючи, що дієвий захист найважливіших інфраструктур включає, зокрема, виявлення загроз і зменшення їх уразливості, мінімізацію збитку і часу на відновлення в разі пошкодження або спроб порушення захисту, виявлення причин пошкодження або джерел таких спроб; визнаючи , що дієвий захист вимагає комунікації і співпраці на національному та міжнародному рівнях між усіма зацікавленими сторонами і що національні зусилля повинні підкріплюватися ефективним, реальним міжнародним співробітництвом, посилаючись на свої резолюції 57/239 від 20.12.2002 р. про створення глобальної культури кібербезпеки, 55/63 від 4.12.2000 р., 56/121 від 19.12.2001 р. про створення правової основи для боротьби зі злочинним використанням інформаційних технологій, прийняла резолюцію 23 грудня 2003 року 58/199 про створення глобальної культури кібербезпеки і захисту найважливіших інформаційних інфраструктур [81], де запропонувала необхідні елементи такого захисту.

Резолюція ГА ООН A/RES/64/211 від 21 грудня 2009 року «Створення глобальної культури кібербезпеки і оцінка національних зусиль з захисту найважливіших інформаційних інфраструктур» відносить довіру і безпеку у використанні інформаційно-комунікаційних технологій до фундаментальних основ інформаційного суспільства та наголошує на необхідності заохочення,

формування, розвитку та активного впровадження сталої глобальної культури кібербезпеки.

У резолюції ГА ООН від 22 грудня 2018 року 73/266 «Заохочення відповідальної поведінки держав в кіберпросторі в контексті міжнародної безпеки» особливо звертається увага на необхідність забезпечення відкритої, інтероперабельної, надійної і безпечної інформаційно-комунікаційного середовища, виходячи з необхідності зберегти вільний потік інформації; підвищення зусиль, що вживаються на національному рівні для зміцнення інформаційної безпеки та сприяння міжнародному співробітництву в цій галузі [82].

Положення даної Резолюції були враховані і ОБСЄ. Треба зазначити, що ще у 2013 році ОБСЄ прийняла інноваційні рекомендації про «заходи щодо зміцнення довіри» у сфері кібербезпеки, спрямовані на підвищення прозорості та забезпечення безпеки в регіоні, які передбачали взаємодію з приватним сектором і провайдерами найважливішої інфраструктури, а також спільні підходи до управління кібербезпекою [83].

На Австрійській конференції ОБСЄ «Кібербезпека критичної інфраструктури: зміцнення формування довіри в ОБСЄ» 2017 року відбувся обмін найкращими практиками для ефективного та своєчасного реагування на критичні інциденти та до спільних заходів було віднесено: подолання терористичної та злочинної діяльності у кіберпросторі відповідно до зобов'язань ОБСЄ; захист критичної інфраструктури від шкідливої діяльності у галузі ІКТ; захист прав людини в інтернеті на засадах чинного міжнародного права.

Братиславська ж конференція ОБСЄ «Кібербезпека та безпека в галузі ІКТ для безпечного майбутнього: роль ОБСЄ у сприянні регіональній кіберстабільності» (2019 р.) передбачала, аналогічно Резолюції ГА ООН, створення платформи для представників громадського, приватного та неурядового секторів з усього регіону ОБСЄ для проведення всебічного

діалогу з питань безпеки ІКТ на глобальному, регіональному та національному рівнях [84, с.105].

В українській науковій літературі досить багато уваги приділяється темі розвитку інформаційного суспільства та формування його безпеки. Але при цьому, крім певної активізації наукових розробок, ні законодавець, ні практики істотно не зрушили у формуванні концепцій інформаційної безпеки та кібербезпеки, як її складової [85, с.102].

В. Полянський [86, с.50] пропонує кібернетичну безпеку розуміти як стан захищеності прав, свобод, інтересів особи, суспільства, держави від внутрішніх, зовнішніх загроз, пов'язаних з використанням ресурсів кіберпростору, який базується на національному законодавстві та міжнародному праві.

При забезпеченні кібербезпеки можна виділити кілька суттєвих проблем.

По-перше, однією з основних проблем при забезпеченні кібербезпеки є забезпечення безпеки середовища Інтернет.

Інтернет швидко став основним інструментом для здійснення права на вираження думок, ідей, поглядів реалізації права на свободу слова. Він поєднує в собі можливості здійснення права на отримання, вільного вираження і поширення інформації, ідей і думок як у письмовій формі, так і за допомогою аудіо- та відеозасобів.

Специфіка Інтернету полягає в тому, що, по-перше: це - унікальний засіб комунікації, що дозволяє багатомільйонній аудиторії по всьому світу спілкуватися миттєво і одночасно; по-друге: це - величезна «бібліотека» інформації в різних сферах наукових досліджен ь; по-третє: це - освітній інструмент, який використовується багатьма університетами світу, які пропонують свої Інтернет-курси. По-четверте, все частіше традиційні ЗМІ (газети і радіостанції) використовують «онлайн», забезпечуючи міст між «паперовим світом» і киберпространством і гарантуючи міжнародний доступ до місцевих газет.

Однак, через різноманітність змісту та простоти використання, Інтернет-інформація стала спірною і суперечливою і може використовуватися в різних цілях. З одного боку, наприклад, це дозволяє отримати відомості про поточні події в країнах, де інші засоби масової інформації зазнають жорсткої цензурі; з іншого - Інтернет може бути використаний з метою сприяння злочину, поширенню терористичної пропаганди, пропаганди расистського змісту, відвертої порнографії, в т.ч. дитячої. Крім того, критерії допустимості та моральності інформації в різних країнах відрізняються, звідси один і той же інформаційний матеріал в одній країні може бути повністю законним, а в іншій вважатися непристойним (порнографічним) або політично неприпустимим [87, с.31-32].

Комітетом міністрів Ради Європи 29 квітня 1982 прийнята Декларація про свободу вираження поглядів та інформації, що закликає, зокрема, держави-члени «забезпечити в розумних межах доступ, передачу і поширення інформації та ідей, як усередині держави, так і за його межами» [88].

Генеральна Асамблея ООН 18 вересня 2000 року прийняла Декларацію тисячоліття, заявивши, що «досягнення нових технологій, особливо інформаційних і комунікаційних, повинні бути доступні для всіх». А 11 листопада 2004 року ОБСЄ прийняла рішення № 633, в якому держави-учасниці зобов'язалися «вжити заходів для того, щоб Інтернет залишався відкритим і загальнодоступним форумом, що забезпечує закріплені у Загальній декларації прав людини свободу думки і свободу вираження, і сприяти розширенню доступу до Інтернет як через домашні підключення, так і через навчальні заклади ... » [89].

Першими державами, що закріпили право на доступ до Інтернету як фундаментального права їхніх громадян, стали Фінляндія та Естонія. Фінляндія закріпила в Законі «Про ринок комунікацій» право громадян на доступ до широкосмугового з'єднання зі швидкістю один мегабіт на секунду [90]. В Естонії діє Закон «Про публічну інформацію», який гарантує

«кожному можливість мати вільний доступ до суспільної інформації за допомогою Інтернету в публічних бібліотеках ...».

Також право на доступ до Інтернету гарантується конкретним законодавством в таких державах, як Албанія, Франція, Німеччина, Іспанія, Туреччина, Чорногорія. У таких державах, як Україна, Російська Федерація, Грузія, Греція, Кіпр, Португалія право на доступ до Інтернету переплітається з правом на інформацію, захищене в більшості випадків Конституцією.

Але при цьому багато держав стурбовані доступністю терористичної пропаганди, расистського контенту (змісту інформації), ксенофобних матеріалів, контенту явно сексуального характеру, зокрема дитячої порнографії, закликів до державних переворотів (серія протестів і демонстрацій по всьому Близькому Сходу і Північній Африці, відома як « арабська весна », почалася і здійснювалася за допомогою соціальних Інтернет-сервісів) [91].

Вважається, що США демонструють успішну інформаційну політику, вдалу організацію забезпечення кібербезпеки, хоча, наприклад, у 2017 р.близько 143 млн. американців постраждали внаслідок кібератак, що складає більшість американського дорослого населення, яке користується Інтернетом. Близько восьми із десяти людей (77%) зазнали шкоди внаслідок кіберзлочину або ж знають тих, хто зазнав шкоди. У результаті кібератак американські споживачі, які стали жертвами кіберзлочинності, втратили близько 19,4 млрд. дол. США, що в середньому становить 96 дол. на одну жертву [92].

«Національну стратегію захисту кіберпростору» в США розроблено у лютому 2003 року, в ній визначено комплексний підхід до захисту життєво важливих комунікаційних технологій американської нації і в якості основної мети визначено виокремлення організаційних завдань й пріоритетність зусиль задля їх досягнення, визначення напрямів та кроків, які мають зробити як урядові структури, так і підприємства й приватні користувачі для досягнення безпеки кібернетичного простору США. У сфері кібернетичної

безпеки - «запобігання кібернетичним нападам на критичну інфраструктуру, зниження вразливості нації до таких нападів і мінімізаціюзбитківтачасувідновлення» [93].

У «Огляді з кібербезпеки» (Cyber Security Review), оприлюдненому 29 травня 2009 р., до ключових завдань керівництва США у сфері кібербезпеки віднесено:

- забезпечення центральної ролі Білого Дому у формуванні кібербезпекової політики, аби продемонструвати аудиторії як усередині США, так і міжнародним партнерам серйозність намірів американського керівництва у сфері кібербезпеки;

- перегляд законодавства та політики у сфері кібербезпеки;

- посилення федерального законодавства та відповідальності у сфері кібербезпеки;

- просування інформаційних проектів державного, регіонального та локального рівнів.

Серед ключових завдань, спрямованих на посилення кібербезпеки США: підвищення готовності суспільства до кіберзагроз; посилення кібербезпекової освіти, збільшення кількості федеральних працівників із підготовкою у сфері інформаційних технологій; просування кібербезпеки як важливого елементу відповідальності урядів усіх рівнів.

На початку березня 2010 року Президентом США затверджено чергову «Ініціативу зі всеосяжної національної кібербезпеки» Ради національної безпеки США, яка є складовою частиною розділу Воєнної доктрини США, що стосується кібернетичної оборони, складається з дванадцяти загальних положень, реалізація яких дасть змогу захистити країну й уряд від кібератак та хакерів. Стратегія кібербезпеки США 2011 р. ж передбачила право США вживати заходи у відповідь на ворожі дії в кіберпросторі, розглядаючи їх як будь-які інші загрози, тобто хакерські атаки прирівняні керівництвом США до оголошення війни.

У кінці квітня 2012 року Сенат США прийняв Закон CISPA («Cyber Intelliggence Sharring and Protection Act»), який дав змогу уряду США, приватним агентствам безпеки та будь-яким приватним компаніям за наявності підозр про вчинення кіберзлочину отримати доступ до конфіденційної інформації користувачів і комерційних організацій [94, с.68].

Китай же реалізовує систему жорсткого контролю за інформацією й інформаційною діяльністю китайських громадян, «функціонує складна система файрволлів, яка обмежує доступ до проблемних зовнішніх ресурсів і застосовується провайдерами не лише для захисту від вірусів і хакерів, але й для блокування доступу до певних сайтів, що містять небажану для політичного режиму інформацію». Фільтрації, піддаються ресурси західних мас-медіа, такі як сайти BBC, CNN, ABC і CBS News, журнал «Time», сайти більшості американських університетів, пошукова система Alta Vista.

Фактично йдеться про інформаційне залякування політичної опозиції, конкуренцію інформаційних потенціалів та інформаційних стратегій, використання інформаційних озброєнь, інформаційну агресію економічного і культурного змісту, інформаційні війни в контексті «гострої сили» [95, с. 23].

В рамках ЄС, як зазначають К. Ветров та Є. Вознюк, інформаційна безпека загалом розглядається, насамперед, як стан інформаційних мереж і систем, що забезпечує належний рівень захисту цілісності, доступності, достовірності та конфіденційності інформації й відповідного рівня протидії зовнішнім негативним впливам.

Серед пріоритетів політики ЄС у сфері інформаційної безпеки виділяють: створення та реалізація програм і різних технічних засобів захисту інформаційно-комунікаційних технологій; розробка правових актів, що встановлюють перелік злочинів у сфері ІТ та кримінальної відповідальності; забезпечення високого рівня обізнаності населення про ризики, загрози й способи захисту їхніх інформаційних систем / мереж від небажаних наслідків [96, с.38]

Великобританія підійшла до питання законодавчого регулювання Інтернету досить педантично, зробивши при розробці законопроекту особливий акцент на згубний вплив Інтернету для дітей. Так, на засіданні Комітету з питань культури, мас-медіа та спорту - безпосереднього розробника законопроекту - професор Лівінгстон, експерт-психолог, надав класифікацію інтернет-ризиків для дітей.

Перша група ризиків називається «анкетна»: часто для доступу на сайт потрібно пройти авторизацію, де людина повинна залишити деяку інформацію про себе. Звичайно, не обов'язково заповнювати всі поля, а тільки зазначені, як правило, це ім'я, прізвисько (нікнейм), вік і e-mail. Але діти дуже часто заповнюють всі поля, таким чином, надаючи інформацію про те, де живуть, навчаються, ким працюють батьки, скільки заробляють і т.д. Для професійних злочинців не складе великих труднощів розкрити подібні анкети (profiles), а потім використовувати отриману інформацію в злочинних цілях [97, с.132].

Інша група інтернет-ризиків носить назву «кібер-знущання»: діти в школі спеціально б'ють новачка, зафіксувавши цю сцену на мобільну відеокамеру, а потім розміщують зняте «шоу» в Інтернеті.

Третя, найнебезпечніша група ризику - інтернет-залежність: загальнодоступні жорстокі ігри в комп'ютерних клубах вже стали «чумою XXI століття» [98].

В країнах Європейського Союзу діє також Директива з питань аудіовізуальних медіа-послуг 2007/65/ЄС, в ст. 22 розділу 5 якої передбачено, що країни-учасниці повинні застосовувати заходи для забезпечення того, щоб телевізійні трансляції, що здійснюються телекомпаніями під їх юрисдикцією, не містили жодних програм, здатних шкідливо впливати на фізичний, психічний або моральний розвиток дітей, в т.ч. програм, що містять елементи порнографії та необґрунтованого насильства. Такі програми повинні бути обмежені для перегляду дітей за допомогою певних технічних

засобів, наприклад, обмеженням часу трансляції, звуковим повідомленням, позначенням відповідним графічним символом протягом всієї трансляції.

У багатьох країнах впроваджена і ефективно використовується система маркування продукції, яка поширюється друкованими та електронними ЗМІ та новими медіа. Вона розроблена, насамперед, для допомоги батькам, які піклуються про моральне і психічне здоров'я своїх дітей. Соціальні дослідження свідчать, що близько 90% батьків в країнах Європейського Союзу повністю підтримують таку політику захисту дітей та молоді від потенційно шкідливого контенту [99, с.123].

Однією і дієвих систем захисту дітей у світі вважається система «Кайквайзер», розроблена Нідерландським інститутом класифікації телепродукту. Вона містить п'ять вікових категорій: «для всіх», а також не рекомендовано до 6, 9, 12, 16-ти років. Крім того, вона складається з шести характеристик програмного наповнення: насильство, жахи, статеві стосунки, дискримінація, наркотики, лайка.

Європейський Парламент 20.11.2012 року прийняв резолюцію «Про захист дітей у цифровому світі» (Protecting children in the digital world). Вона спрямована на підвищення медіа-грамотності дітей і розробці заходів для їх захисту від шкідливого Інтернет-контенту. Відповідно до цієї резолюції, країни-учасниці повинні забезпечувати медіа-освіту в шкільній програмі, роз'яснювати дітям особливості використання мережі Інтернет, нових медіа та можливих он-лайн небезпек в цілому.

У литовському законі «Про захист неповнолітніх від негативного впливу публічної інформації» (2002 р) упор у зв'язку із захистом неповнолітніх робиться не на державний орган, а на суспільні інститути. За застосуванням закону стежить інспектор з журналістської етики (ст. 9), який приймає скарги громадян та юридичних осіб. При інспекторі діє «група експертів з бездоганною репутацією, що володіють спеціальними знаннями», яка оцінює вплив громадської інформації на неповнолітніх та представляє свої висновки інспектору. Мінімальна чисельність такої групи

конкретизується, сказано лише, що кількість експертів не повинно перевищувати 9 осіб. Група діє за принципом ротації, регламент роботи приймає самостійно зі схвалення інспектора. Її робота фінансується з державного бюджету. Експертів призначає сам інспектор. На жаль, в законі не прописана процедура, яка передбачає безпосереднє спілкування з інспектором самих журналістів, мовників, власників і розповсюджувачів громадської інформації, вона могла б підвищити ефективність цього документа, а також полегшити розуміння того, яку саме інформацію слід в тих чи інших випадках відносити до категорії надає негативний вплив на неповнолітніх. Тим не менш, наявність у Законі механізму діяльності контрольного органу - чималий крок до вирішення проблеми захисту неповнолітніх від негативного впливу інформаційного середовища. Підводячи підсумок всьому вищесказаному, слід зазначити, що підхід Литви ближче до системи саморегулювання, ніж механізми регулювання, прийняті в інших розглянутих країнах [100, с.18].

З урахуванням обмеженої ефективності національного законодавства та відсутності гармонізації на міжнародному рівні деякі країни почали блокувати доступ до сайтів та соціальних мереж, які можливо містять незаконний контент і сервери яких розташовані за межами їх територій. У деяких державах засобом правового захисту є видалення контенту; інші держави забезпечують заходи блокування доступу на додаток до заходів видалення. Частина держав почали розробляти заходи блокування та арешту доменних імен на державному рівні (Чеська Республіка, Молдова, Швейцарія та Сполучене Королівство) [101].

Другою проблемою, але не більш складною проблемою є проблема розвитку кіберзлочинності.

Одна з концепцій міжнародної інформаційної безпеки виходить з того, що в основу останньої покладений тільки один елемент - боротьба із кримінальними злочинами у сфері інформаційно-комунікаційних технологій, і саме цей елемент потребує міжнародно-правового регулювання. Другим

вірогідним складовим елементом, який має певну перспективу подальшого міжнародно-правового регулювання, є боротьба із тероризмом у сфері ІКТ.

Наступ епохи глобалізації є новим етапом і відправною точкою розвитку кримінального права та юриспруденції. Першорядне значення глобалізація теорії кримінального права набуває в умовах триваючого зростання глобалізації злочинності. В першу чергу велику загрозу безпеці людства несе собою міжнародний тероризм, організована економічна злочинність і корупція. Жодна країна не може самостійно впоратися з цими погрозами.

Глобалізація злочиності та кримінального права вимагає від фахівців і вчених різних країн посилити міжнародне співробітництво та постійний обмін думками щодо важливих теоретичних і практичних проблем [102, с.110].

У міжнародних документах, чинних нормативно-правових актах в інформаційній сфері та кримінальному законодавстві України, вітчизняної та зарубіжної наукової літератури використовуються різні терміни для найменування комп'ютерних злочинів: «злочини в сфере комп'ютерної інформації», «кіберзлочини», «злочини у сфері використання комп'ютерної техніки», «злочини, пов'язані з використанням комп'ютерів», «злочини у сфері використання комп'ютерних технологій», «злочини у сфері високих інформаційних технологій», «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», «мережеві комп'ютерні злочини», «інформаційні злочину», «злочини у сфері інформатизації» та інші. Узагальнюючим, як вважає Н. Козак [103, с.40] є термін «комп'ютерні злочини».

Дефініція «комп'ютерна злочинність» з'явилася спочатку в американських, а потім в інших іноземних друкованих виданнях на початку 60-х років XX ст., коли були виявлені перші випадки злочинів, скоєних з використанням електронно-обчислювальних машин (ЕОМ).

Вперше термін «комп'ютерний злочин» використано в доповіді Стенфордського дослідницького інституту в 1973р., а потім, в дещо зміненому вигляді, - в документах 1979р. і 1989р. У 1986 р в Парижі групою експертів Організації економічного співробітництва та розвитку вперше формулюється кримінологічне визначення комп'ютерного злочину - будь-яка незаконна, неетична або недозволена поведінка, що стосується автоматизованої обробки та передачі даних [104, с.11].

На думку Д.А. Ястребова, кіберзлочин у вузькому сенсі - це будь-яке протиправне діяння, здійснюване за допомогою електронних операцій, метою якого є подолання захисту комп'ютерних систем і оброблюваних ними даних; в широкому сенсі – будь-яке протиправне діяння, скоєне за допомогою або в зв'язку з комп'ютерною системою або мережею, включаючи такі злочини, як незаконне зберігання, пропозиція або розповсюдження інформації за допомогою комп'ютерної системи або мережі

О. Музика, Д. Азаров пропонують під «комп'ютерним» злочином в широкому значенні розуміти передбачені кримінальним законом суспільно-небезпечні дії, вчинені переважно з використанням засобів комп'ютерної техніки, в яких електронна обробка інформації є або засобом, або об'єктом злочинного посягання. У вузькому значенні - протиправні дії, передбачені кримінальним законодавством [105, с.87].

У довідковому документі для семінару - практикуму зі злочинів, пов'язаних з використанням комп'ютерної мережі Десятого Конгресу ООН з попередження злочинності та поводження з правопорушниками, вживається термін «кіберзлочинність»", який визначається як будь-який злочин, який може скоюватися за допомогою комп'ютерної системи або мережі, в межах комп'ютерної системи або мережі або проти комп'ютерної системи або мережі.

У Рекомендаціях Ради Європи з приводу комп'ютерних злочинів зазначалося, що дати визначення комп'ютерного злочину надзвичайно

складно, оскільки це не будь-яке використання комп'ютерної системи, а діяння, що містить в собі склад комп'ютерного злочину [106, с.204].

Кіберзлочини поділяють на дві категорії:

1) кіберзлочини у вузькому сенсі (комп'ютерні злочини) – «будь-які протиправні дії, що здійснюються за допомогою електронних операцій, метою яких є подолання захисту комп'ютерних систем і даних, ними оброблюваних»;

2) кіберзлочини в широкому сенсі (злочини, пов'язані з використанням комп'ютерів) - будь-які протиправні дії, що здійснюються за допомогою або в зв'язку з комп'ютерною системою або мережею, у тому числі такі злочини, як незаконне зберігання, пропозиція або розповсюдження інформації з допомогою комп'ютерної системи або мережі.

А.В. Кубишкін до числа злочинів, пов'язаних з утриманням інформації включає діяння, спрямовані на виробництво, розповсюдження, передачу або інші способи, що роблять доступною інформацію, заборонену до поширення міжнародним правом або національним законодавством, а саме такої інформації: пропаганди війни, підбурювання до війни, пропаганда насильства, расової ненависті, дискримінації, апартеїду, геноциду, дитячої порнографії.

І до числа злочинів, пов'язаних з інформаційною інфраструктурою відносить злочини, в яких комп'ютери та інформаційні системи та мережі виступають як об'єкт злочину; злочини, в яких комп'ютер та інформаційна система виступають як засіб скоєння звичайних злочинів; злочини, пов'язані з порушенням авторських та суміжних прав.

Таким чином, родовим об'єктом цих злочинів є суспільні відносини у сфері безпеки комп'ютерної інформації і нормального функціонування електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж.

Як видається, прийнята в літературі дефініція «комп'ютерні злочини» об'єднує злочини, вчинені з використанням комп'ютерних засобів і систем.

Дефініція повинна використовуватися не в кримінально-правовому аспекті, оскільки це ускладнює кваліфікацію діяння, а в криміналістичному оскільки вона пов'язана не з кваліфікацією, а зі способом здійснення та приховування злочину і, відповідно, з методикою його розслідування [107, с.128].

З юридичної точки зору проблема полягає також у відсутності в національному та міжнародному праві чітких критеріїв відділення актів звичайного комп'ютерного хуліганства від таких нападів, які через свою серйозності мають характер військового нападу на державу чи є початком військової агресії проти певної держави.

У сучасній літературі поняття «кібервійна» є багатозначним. При цьому все частіше використовують нові інформаційні технології та Інтернет зі злочинною метою терористичні організації. Такі терористичні угруповання, як Hizbollah, HAMAS, the Abu Nidal organization и Bin Laden's al Qa'ida використовують комп'ютерні файли, електронну пошту і шифрування (криптографію і комп'ютерної стеганографії) для підтримки своєї протиправної діяльності. І хоча терористи ще не використали кіберзброю за призначенням, вони використовують нові інформаційні технології та досягнення комп'ютерного прогресу, а це вже сигнал про небезпеку.

Кібертероризм можна визначити як використання сучасних інформаційних технологій, насамперед мережі Інтернет, з метою ураження важливих державних інфраструктур (таких, як енергетична, транспортна, урядова) - в недалекому майбутньому може стати реальною загрозою національній безпеці розвинених країн світу [108, с.117] .

Необхідно погодитися з О. Мережком і під кібервійною розуміти застосування комп'ютерних технологій та Інтернету однією державою або при її безпосередній підтримці проти іншої держави, спрямоване проти її безпеки і оборони, яке є настільки інтенсивним і серйозним, що становить реальну загрозу безпеці та суверенітету цієї іншої держави [109, с.94].

Необхідно зазначити, що один з перших у світі законів, що визначає поведінку в кіберпросторі та призначення покарання за електронні злочину,

був прийнятий в США - Compter Fraud and Abuse Act 1986. При цьому в США акти кіберзагроз та кібератаки розглядаються як акти проголошення війни. На рівні законодавства ці питання не врегульовані і вирішуються в рамках керівництва Агентства національної безпеки. Щодо інших держав, то в основному розглядаються питання не знаходять свого розвитку, навіть в ЄС не прийнято жодного документа, в якому були б чітко виписані процедури виявлення кібератак, здійснено їх класифікацію за певними критеріями на відповідні рівні загроз як інформаційного суспільства, так і кіберпростору , мережам, критичної інфраструктури [110, с.102].

При цьому з метою уніфікації національних законодавств ще 13 вересня 1989 на засіданні Комітету міністрів Європейського Союзу був вироблений список правопорушень, рекомендований країнам-учасницям ЄС для розробки єдиної кримінальної стратегії при розробці законодавства, пов'язаного з комп'ютерними злочинами. Він містить так звані Мінімальний і Необов'язковий списки правопорушень. Відповідно, до першого списку входить: комп'ютерне шахрайство, комп'ютерна підробка, пошкодження комп'ютерної інформації та комп'ютерних програм, комп'ютерний саботаж; несанкціонований доступ до комп'ютерних мереж, несанкціоноване перехоплення інформації, несанкціоноване копіювання захищених комп'ютерних програм, незаконне виготовлення топографічних копій; а до другого - зміна інформації або комп'ютерних програм, комп'ютерне шпигунство, протизаконне використання комп'ютера, несанкціоноване застосування захищених комп'ютерних програм.

Перші спроби напрацювання міжнародних механізмів протидії злочинності в кіберпросторі були здійснені Радою Європи у 2001 році при прийнятті Конвенції про кіберзлочинність, в якій підкреслено «необхідність швидкодіючої та ефективної системи міжнародного співробітництва, яка б належним чином врахувала специфічні вимоги боротьби з кіберзлочинністю» [111]. 28.01.2003 року до Конвенції був прийнятий Додатковий протокол,

який стосується криміналізації дій расистського та ксенофобського характеру, вчинених через комп'ютерні системи.

Щодо ефективності вказаної Конвенції, то наявність низки спірних питань, зокрема статті 32, яка передбачає право держав здійснювати транскордонний доступ до публічно відкритих комп'ютерних даних, не отримуючи згоди країни, де ці дані знаходяться, негативно впливає на бажання держав приєднуватися до Конвенції.

Достатньо подібна за змістом до Конвенції Угода про співробітництво держав-учасниць Співдружності Незалежних Держав у боротьбі із злочинами у сфері комп'ютерної інформації від 01.06.2001 р. [112].

Певним чином позитивно на реалізацію цієї Конвенції може вплинути зовнішньополітична ініціатива США «Міжнародна стратегія стосовно дій в кіберпросторі» 2011 року, про яку вже йшла мова.

Запрошуючи держави, громадянське суспільство та приватний сектор приєднатись для реалізації в рамках Стратегії до ідеї «процвітання, безпеки і відкритості», уряд США має намір спонукати відповідні урядові структури інших країн визначитись щодо їх ролі у міжнародній кіберпросторовій політиці та координації подальших дій і, відповідно, передбачає співробітництво з міжнародними партнерами та приватним сектором за певними напрямами, серед яких у галузі правозастосування -розширення співробітництва і верховенство закону. В цьому зв'язку проводиться ідея щодо підтримки і поширення Конвенції про кіберзлочинність, із внесенням до неї певних доповнень і поправок. При цьому не береться до уваги не тільки регіональний характер Конвенції, а й те, що деякі викладені в ній положення вже сьогодні не влаштовують частину країн [113, с.287].

Стаття 25 Конвенції про кіберзлочинність передбачає також, що сторони надають одна одній взаємну допомогу у найширшому обсязі з метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збору доказів у електронній формі у кримінальних правопорушень.

Необхідно відзначити також Рекомендації Комітету Міністрів Ради Європи №R (85) 10, що стосується практичного застосування Європейської Конвенції про взаємодопомогу у кримінальних справах стосовно листів, що створюють необхідність перехоплення телекомунікацій, №R (88) 2 про піратство у сфері авторських і суміжних прав, №R (87) 15, що регулює використання особистих даних у поліцейській галузі, №R (95) 4 про захист особистих даних у сфері телекомунікаційних послуг, з особливим посиланням на телефонні послуги, а також №R (89) 9 про злочини, пов'язані з комп'ютерами, що встановлює орієнтири для національного законодавства щодо визначення окремих комп'ютерних злочинів, і №R (95) 13, що стосується проблем кримінально-процесуального права, пов'язаних з інформаційними технологіями.

Крім того, Резолюція №1, прийнята європейськими міністрами юстиції на своїй 21-й Конференції (Прага, 10-11 червня 1997р.), рекомендує Комітету Міністрів підтримати роботу, що проводиться Європейським комітетом з проблем злочинності (ЄКПТ) відносно кіберзлочинності для зближення внутрішньодержавних положень кримінального права і створення можливостей для застосування ефективних засобів розслідування таких правопорушень, Резолюція №3, прийнята на 23-й Конференції європейських міністрів юстиції (Лондон, 8-9 червня 2000р.), заохочує сторони переговорів до пошуку відповідних рішень для збільшення кількості держав-учасниць Конвенції та визнає необхідність швидкодіючої і ефективної системи міжнародного співробітництва, яка б належним чином враховувала специфічні вимоги боротьби з кіберзлочинністю.

А.Д. Софаер і С.Є. Гудман вважають, що для того, щоб забезпечити розробку та імплементацію технічних і правових стандартів попередження та кримінального переслідування за скоєння кіберзлочинів і тероризму, держави повинні створити міжнародне агентство по аналогії з Організацією міжнародної цивільної авіації (ІКАО), але компетенція якого буде відображати специфічні потреби та природу кіберсвіту [114, с.3].

Вважаємо, що необхідно, поділяючи позицію Н.О. Мороз [115, с.318], не погодитися з даною думкою, оскільки, по-перше, злочини у сфері високих технологій не завжди здійснюються у віртуальному середовищі, яку А.Д. Софаер і С.Є. Гудман намагаються порівняти з повітряним простором, що використовується для польотів цивільної авіації; по-друге, практика міждержавного співробітництва показує, що боротьба зі злочинами міжнародного характеру досить ефективно здійснюється за допомогою створення спеціалізованих структур міжнародних організацій загальної компетенції, Інтерполу, а також шляхом укладення міжнародних угод.

Отже, основним призначенням політики кібербезпеки є збереження міжнародного миру і безпеки, самобутності націй, держав, забезпечення інформаційних прав і свобод людини в кіберпросторі, створення неможливості маніпулювання масовою свідомістю та введенню обмежувальних поправок, інформаційних режимів через різні бажання суб'єктів управління.

Проведений аналіз дозволяє виділити наступні основні напрями забезпечення кібернетичної безпеки:

- координація та взаємодія органів всередині держави щодо забезпечення безпеки національного кібернетичного інформаційного простору;

- організація технічної та інституційної співпраці державних органів різних держав між собою і з міжнародними організаціями;

- уніфікація основних понять у сфері забезпечення кібербезпеки - кібернетична безпека, кібернетична атака, кіберзлочинність тощо.

ВИСНОВКИ

В результаті проведеного дослідження були отримані наступні висновки та результати.

Уточнено поняття міжнародної інформаційної безпеки, під якою пропонується розуміти складову міжнародної безпеки, стан захищеності особи, суспільства, держави і світового співтовариства, за якого досягається сталий інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний), при якому унеможливлюється чи мінімізується негативний сторонній інформаційно-психологічний та інформаційно-технічний вплив через неповноту, несвоєчасність і недостовірність інформації, що використовується, несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації.

Обґрунтовано, що міжнародна інформаційна безпека забезпечується взаємодією акторів міжнародних відносин з операцій підтримання сталого миру на основі захисту міжнародної інфосфери, глобальної інфраструктури, суспільної свідомості світового співтовариства від реальних та потенційних загроз.

Набули подальшого розвитку положення щодо складу інституту міжнародної інформаційної безпеки та додатково обґрунтовано, що міжнародну інформаційну безпеку можна структурувати з трьох складових:

1. протидія порушенням основним правам і свободам людини, що реалізуються в інформаційній сфері - кримінальний аспект (кіберзлочинність);

2. протидія використанню інформаційного простору у терористичних цілях, коли мають місце прояви використання інформаційно-комунікаційних технологій державними і недержавними структурами, організаціями, групами і окремими особами в терористичних,

екстремістських та інших злочинних діях - терористичний аспект (кібертероризм);

3. попередження військових конфліктів з використанням інформаційно-комунікативних технологій, а також підготовки та ведення інформаційної війни - військово-політичний аспект (інформаційні війни).

Встановлено, що правове забезпечення міжнародної інформаційної безпеки як вид діяльності направлене на протидію загрозам безпеці основних об'єктів інтересів в інформаційній сфері.

Уточнено, що організаційний (інституційний) механізм забезпечення міжнародної інформаційної безпеки охоплює держави, міжнародні організації та інституції, державні інституції, задіяні в процесі формування та впровадження політики інформаційної безпеки.

Получили подальшого розвитку положення щодо виділення 4 моделей системи глобальної інформаційної безпеки: модель 1 – створення абсолютної системи захисту країни-інформаційного лідера (дана модель конструюється залежно від кількості суб'єктів системи безпеки, відповідно виділяються чотири основні моделі, що конкурують між собою: однополярна система безпеки, «концерт держав», багатополярна модель, глобальна (універсальна) модель); модель 2 – створення значної переваги держави-потенційного ініціатора інформаційної війни; модель 3 – наявність кількох країн-інфолідерів та потенційного протиборства між ними; модель 4 – всі конфліктуючі сторони використовують транспарентність інформації для формування ситуативних альянсів.

Додатково обгрунтовано, що забезпечення прав і безпеки суб'єктів інформаційної взаємодії – як національної, так транскордонної, міжнародної, можливе лише на основі спільного комплексного вирішення правових, організаційних і технологічних питань, для чого необхідним вважаємо прийняття міжнародних правил (кодексу) поведінки в глобальному інформаційному просторі або універсальної конвенції під егідою ООН.

Аргументовано, що основним призначенням політики кібербезпеки є збереження міжнародного миру та безпеки, самобутності націй, держав, забезпечення інформаційних прав і свобод людини в кіберпросторі, створення неможливості маніпулювання масовою свідомістю та введенню обмежувальних поправок, інформаційних режимів через різні бажання суб'єктів управління.

Проведений аналіз дозволив виділити, по-перше, два основні функціональні напрями міжнародно-правового регулювання використання ІКТ:

- інформаційний («змістовний»), що визначає засади, принципи, форми, способи протидії транскордонному поширенню за допомогою ІКТ інформації, що протирічить принципам і нормам міжнародного права, розпалює міжнаціональну, міжрасову та міжконфесійну ворожнечу, поширює расистські, ксенофобські матеріали, зображення або будь-яку демонстрацію ідей або теорій, що пропагують, підбурюють до ненависті, дискримінації або насилля проти будь-якої особи або групи осіб;

- комунікаційний («технічний»), що визначає засади, принципи, форми, способи протидії використанню комунікаційних систем, процесів и ресурсів проти комунікаційних мереж і критично важливих структур інших держав, що заподіює шкоду функціонуванню фінансовій, політичній, економічній та соціальній системам.

По-друге, основні напрями забезпечення кібербезпеки:

- координація та взаємодія органів всередині держави щодо забезпечення безпеки національного кібернетичного інформаційного простору;

- організація технічної та інституційної співпраці державних органів різних держав між собою і з міжнародними організаціями;

- уніфікація основних понять у сфері забезпечення кібернетичної безпеки - кібернетична безпека, кібернетична атака, кіберзлочинність.

СПИСОК ВИКОРИСТАНИХ ПОСИЛАНЬ

1. Державний суверенітет: теоретико-правові проблеми: монографія / за ред. Ю.П. Битяка, І.В. Яковюка; НДІ держ. будівництва та місцевого самоврядування, Нац. акад. прав. Наук України. Х.: Право, 2010. 272с.

2. Волинець В. Функція гарантування національної безпеки в контексті державно-правового розвитку сучасної України. *Юридична Україна.* 2013. №1. С.9-16.

3. Копійка М. «Гостра сила» в стратегії інформаційної безпеки Китаю. Міжнародні відносини, суспільні комунікацій та регіональні студії. 2020. №1(7). С.68-80. URL: https://relint.vnu.edu.ua/index.php/relint/article/view/129/114.

4. Макаренко Є.А. Політичні доктрини глобальної інформаційної безпеки. *Вісник інституту міжнародних відносин Київського Національного университету*. 2007. №2. С.45-51.

5. Білорус О. Г. Глобалізація і безпека розвитку / О. Г. Білорус, Д. Г. Лук'яненко, М. О. Гончаренко, В. А. Зленко, О. В. Зернецька, А. І. Кудряченко, Ю. М. Мацейко, В. Є. Новицький, Ю. М. Пахомов; ред.: О. Г. Білорус; НАН України. Ін-т світ. економіки і міжнар. відносин. К., 2011. 734с.

6. Васенко В.К., Тереніна О.В. Безпека життєдіяльності та її особливості у правоохоронних органах. *Право і безпека.* 2012. №1. С.213-217.

7. Лазарев І.А. Інформація і безпека. Композиційна технологія. М.: Изд-во Московського міського центру науково-технічної інформації, 2002. 178с.

8. Іноземцев В.Л. За межами економічного суспільства. Постіндустріальні теорії і постекономічних тенденції в сучасному світі. М.: Наука, 1998. 190с.

9. Бачило І.Л. Інформаційне право: Підручник для вузів. М.: Вища освіта; Юрайт-Издат, 2009. 560с.

10. Лопатин В.Н. Інформаційна безпека Росії: людина, суспільство, держава. Серія: Безпека людини і суспільства. СПб.: Фонд Університет, 2000. 428с.

11. Лопатин В.Н. Інформаційне право: Підручник. СПб.: Юридичний центр Пресс, 2005. 474с.

12. Абакумов В. Правове регулювання протидії інформаційним війнам в Україні: автореф. дис. ... канд. юрид. наук / спец. 12.00.07 - «Адміністративне право і процес; фінансове право; інформаційне право». Запоріжжя, 2011. 22 с.

13. Захаренко К. Теоретичні засади дослідження інформаційної безпеки. *Міжнародні відносини, суспільні комунікацій та регіональні студії.* 2018. №2(4). С.107-116. URL: https://relint.vnu.edu.ua/index.php/relint/article/view/77/71.

14. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. Київ: КНТ, 2006. 280 с.

15. Мазур Н.Н. Правове забезпечення національних інтересів Російської Федерації в інформаційній сфері. М .: Логос, 2010. 258с.

16. Карчевський М. До питання визначення інформаційної безпеки як об'єкта кримінально-правової охорони. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2012. №1(27). С.267-272.

17. Гуз А. М. Історія захисту інформації в Україні та провідних країнах світу: навчальний посібник. К.: КНТ, 2007. 260 с.

18. Роговец В. Информационные войны в современном мире: причины, механизмы, последствия. *Персонал*. 2010. № 5. С.33-38.

19. Манойло А.В. Государственная информационная политика в особых условиях: монография. М.: МИФИ, 2003. 388 с.

20. Заплатинський В.М. Логіко-детермінантні підходи до розуміння поняття «безпека». *Вісник Камянець-Подільського національного університету імені Івана Огієнка. Фізичне виховання, спорт і здоров'я людини*. 2012. Випуск 5. С. 90-98.

21. Заплатинский В.М. Терминология науки о безопасности. Zbornik prispevkov z medzinarodnej vedeckej konferencie «Bezhecnostna veda a bezpecnostne vzdelanie». Liptovsky Mikulas: AOS v Liptovskom Mikulasi, 2006. S.123-129.

22. Joint doctrine for information operations-Joint Pub 3-13, 1998. - P.GL-7. URL: http://www.c4i.org/jp3_13.pdf.

23. Емельянова Н.Н. Эволюция концепции «международная безопасность» в международном праве. *Международное право*. 2011. №1-2 (45-46). С. 74-83.

24. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность: Справочник. М., 1998. 630с.

25. Панарин И. Технология информационной войны. М., 2003. 400с.

26. Колодій І.М. Інформаційна безпека: деякі проблеми визначення понять. *Держава і право.* 2008. Випуск 40. С.300-305.

27. Брижко В.Н., Гальченко О.М., Цимбалюк В.С., Орєхов О.А., Чорнобров А.М. Інформаційне суспільство. Дефініції: людина, її права, інформація. Інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція / За ред. Р.А. Калюжного, М.Я. Швеця. К., 2002. 523с.

28. Кочетков А.П., Мехед Н.Г. Современная Россия: ключевые проблемы безопасности. *Власть.* 2008. №10. С.12-19.

29. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности: Доклад Генерального секретаря /Документы ООН A/55/140. URL: http://www.un.org/ru/documents/ods.asp?m=A/55/140.

30. Об утверждении Концепции национальной безопасности Республики Беларусь: Указ Президента Республики Беларусь от 9 ноября 2010г. № 575. *Эталон- Беларусь* [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. Минск, 2014.

31. Об утверждении Инструкции об организации системы внутреннего контроля в банках, небанковских кредитно-финансовых организациях, банковских группах и банковских холдингах: Постановление Правления Национального банка Республики Беларусь от 30 ноября 2012 г. № 625. *Эталон-Беларусь* [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. Минск, 2014.

32. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 г. *Эталон-Беларусь* [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. Минск, 2006.

33. О типовых проектах законодательных актов МПА ЕвраАзЭС в сфере информационных технологий («Об информатизации», «Об информационной безопасности», «Основные принципы электронной торговли»): Постановление Межпарламентской Ассамблеи Евразийского Экономического Сообщества от 28 мая 2004 г. № 5-20. *Эталон-Беларусь* [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. Минск, 2014.

34. О модельном законе «О безопасности»: Постановление Межпарламентского Комитета Республики Беларусь, Республики Казахстан, Кыргызской Республики, Российской Федерации и Республики Таджикистан от 15 октября 1999 г. № 9-9. *Эталон-Беларусь* [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. Минск, 2014.

35. Об утверждении Концепции информационной безопасности государств- участников Содружества Независимых Государств в военной сфере: Решение Совета глав правительств Содружества Независимых Государств от 4 июня 1999 г. *Эталон-Беларусь* [Электронный ресурс] / Нац. цент правовой информ. Респ. Беларусь. Минск, 2014.

36. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007р. № 537-V. URL: http://zakon4.rada.gov.ua/l.

37. Полякова Т.А. Правовое обеспечение информационной безопасности при формировании информационного общества в России: автореф. дис. ... докт. юрид. наук. М., 2008. 35с.

38. Цимбалюк В.С. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації). *Підприємництво, господарство і право.* 2004. №3. С.90-94.

39. Марущак А.І. Інформаційне право: доступ до інформації: навч. посіб. К., 2007. 280с.

40. Безопасность: теория, парадигма, концепция, культура. Словарь-справочник / Автор-сост. профессор В. Ф. Пилипенко. 2-е изд., доп. и перераб. М.: ПЕР СЭ-Пресс, 2005. 320с.

41. Турченко О.Г. Правовое регулирование информационной безопасности в Украине: монография. Донецк, 2010. 228с.

42. Национальная безопасность Республики Беларусь / С.В. Зась [и др.]; под ред. М.В. Мясниковича и Л.С. Мальцева. Минск: Беларус. навука, 2011. 557 с.

43. Антонов В.О. Проблема формування та релізації стратегії національної безпеки України на тлі посилення загроз на регіональному рівні. *Держава і право.* 2014. Випуск 64. С.122-127.

44. Наливайко О.Ю. Методологічні аспекти класифікації персональних даних. *Держава і право.* 2014. Випуск 64. С.167-172.

45. Бачило, И.Л., Лопатин В.Н., Федотов М.А. Информационное право: учебник / под ред. акад. РАНБ.Н. Топорнина. 2-е изд., с изм. и доп. СПб.: Издательство Р. Асланова «Юридический центр Пресс», 2005. 725 с.

46. Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009. 340с.

47. Атаманов Г.А. Інформаційна безпека: сутність і зміст. *Бізнес і безпека в Росії.* 2007. №47. С.106-109.

48. Уэбстер Ф. Теории информационного общества / Фрэнк Уэбстер; Пер. с англ. М. В. Арапова, Н. В. Малыхиной; Под. ред. Е. Л. Вартановой. М.: Аспект Пресс, 2004. 400 с.

49. Кастельс М. Информационная эпоха: э, общество и культура. М.: ГУ ВШЭ, 2000. 340с.

50. Шемякін В.П. Информационная безопасность в современных российских условиях: социолого-управленческие аспекты: автореф. дис. ... канд. соціол. наук. М., 2004. 19с.

51. Турченко О.Г., Бешуля П.В. Поливариантность определения понятия «информационная безопасность государства» в контексте международной информационной безопасности. *Науковий Вісник Ужгородського національного університету. Серія Право.* 2013. Випуск 23. Ч.1. Т.3. С.228-231.

52. Забара І.М. Інститут міжнародної інформаційної безпеки: правові аспекти. *Правова інформатика.* 2014. №1(41). С.64-74.

53. Проект Конвенции об обеспечении международной информационной безопасности. URL: //www.mid.ru/bdomp/ns-osndoc.nsf/e2f289bea62097f9c325787a0034c255/42df9e13d28e06ec3257925003542c4!Open Document.

54. Касьяненко М.А. Правовые проблемы при использовании Интернет в транснациональном терроризме. *Информационное право.* 2012. №1(28). С. 21-25.

55. Каримов И.А. Узбекистан на пороге XXI века: угрозы безопасности, условия и гарантии прогресса. Ташкент: Узбекистан, 2007. 315с.

56. Стрільців А. А. Зміст поняття «забезпечення інформаційної безпеки». *Інформаційне суспільство.* 2001. Вип.4. С.14-19.

57. Міжнародна інформаційна безпека: сучасні виклики та загрози. К.: Центр вільної преси, 2006. 257с.

58. Давидюк О.О. Оцінка стану соціальної безпеки в умовах поглиблення соціального розшарування. *Держава і право.* 2014. Випуск 65. С.376-385.

59. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция ГА ООН A/RES/55/28 от 20.12.2000 г. URL: https://undocs.org/ru/A/RES/55/28.

60. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности. Общая оценка проблем информационной безопасности Угрозы международной информационной безопасности: Резолюция ГА ООН A/56/164/Add.1 от 03.10.2001 г. URL: https://undocs.org/ru/A/56/164/Add.1.

61. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция ГА ООН A/RES/57/53 от 22.11.2002 г. URL: https://undocs.org/ru/A/RES/57/53.

62. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2015 (A/70/174) URL: https://undocs.org/ru/A/70/174.

63. Крутских А. К политико-правовым основаниям глобальной информационной безопасности. *Международные процессы.* 2011. №2. URL: http://www.intertrends.ru/thirteen/003.htm.

64. Правила поведения в области обеспечения международной информационной безопасности. URL: http://rus. rusemb. org. uk/data/doc/internationalcoderus. pdf.

65. Оніщенко Н.М., Сунєгін С.О. Відповідальність держави перед особою в контексті розвитку громадянського суспільства. *Держава і право*. 2014. Випуск 64. С.3-11.

66. Кормич Б.А. Правова регламентація інформаційної безпеки України. *Держава і право.* 2003. Випуск 17. С.193-198.

67. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция ГА ООН A/RES/56/19 от 07.01.2002г. URL: https://undocs.org/ru/A/RES/56/19.

68. Кузьменко А. Інформаційно-психологічна війни епохи глобалізації (Частина 10. Доктринальний підхід Російської Федерації). *Юридичний журнал.* 2008. №9(75). С.23-50.

69. Деятельность спецслужб и демократический контроль - профессиональный взгляд. Бюллетень № 3. - Женева/Киев; Geneva centre the democratic control of armed forces (DCAF), 2005. 180с.

70. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України. О., 2003. 472 с.

71. Коршиков П.С. Обеспечение государственной безопасности СССР как объект чекистской науки. *Труды ВШ КГБ.* 1984. №32. С.3-18.

72. Пухова К. Совбез занялся СМИ: Доктрина информационной безопасности может сработать против российских масс-медиа. URL: http://www.ng.ru/printed/8786.

73. Nye J.S. America's Informational edgel Strategy and force planning. URL: http://ics.leeds.ac.uk/papers/vp01.cfm?outfit=pmt&requesttimeout=500&folder=49&paper=155.

74. Гриняев С. Особенности информационной войны во время агрессии НАТО против Югославии (по материалам открытой печати). URL: http://www.narod.ru/warfare/grinyaev/page008.htm.

75. Гриняев С.Н. Информационная война: история, день сегодняшний и перспектива. URL: http://www.narod.ru/warfare/grinyaev/page009.htm.

76. Соснін О.В., Грушова Г.В. Міжнародна інформаційна безпека як актуальна проблема сучасності. *Держава і право.* 2014. Випуск 66. С.290-297.

77. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations to Be Launched // NATOCCDCOE. – 2017. URL: https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operationsbe-launched.html.

78. A cyber-security framework fordevelopment, defense and innovation at NATO. URL: https://innovation-entrepreneurship.springeropen.com/track/pdf/10.1186/s13731-019-0105-z.

79. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. М., 2006. 456с.

80. Ліпкан В.А. Теоретичні основи та елементи національної безпеки України. К., 2013. 600с.

81. О создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур: Резолюция ГА ООН 58/199 от 23.12.2003г. URL: https://undocs.org/ru/A/RES/58/199.

82. Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности: Резолюция ГА ООН A/RES/73/266 от 22.12.2018 г. URL: https://undocs.org/ru/A/RES/73/266.

83. Organization for Security and Co-operation in Europe – OSCE. URL: https://www.osce.org/whatistheosce.

84. Копійка М.В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки. *Політичне життя.* 2020. №1. С.102-109.

85. Кір'ян В. Парадигмальна трансформація концепцій інформаційного суспільства. *Підприємництво, господарство і право.* 2013. №5. С.102-104.

86. Полянська В. Кібернетична безпека України в умовах розвитку глобальної інформаційної системи. *Підприємництво, господарство і право.* 2013. №7. С.48-50.

87. Турута Е.В. Интернет и право на свободу слова (сравнительно-правовой аспект). *Публічне право.* 2012. №4(8). С31-37.

88. Declaration on the freedom of expression and information (Adopted by the Committee of Ministers on 29 April 1982 at its 70th Session). URL: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=601273&SecMode=1&DocId=675536&Usage=2.

89. OSCE PC.DEC/633 on Promoting Tolerance and Media Freedom on the Internet, endorsed by MC.DEC/12/04 at the OSCE Ministerial Council in Sofia, 7 December 2004. URL: http://www.osce.org/mc/23133.

90. Finnish Ministry of Transport and Communications Press Release, 1 Mbit Internet access a universal service in Finland from the beginning of July, 29.06.2010. URL: http://www.lvm.fi/web/en/ pressreleases/view/ 1169259.

91. Khalidi R. The Arab Spring. The Nation. March 21. URL: http://www.thenation.com/article/158991/arabspring.

92. Norton Cyber Security Insights Report 2017 United States Result. URL: http: //now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/NCSIR-global-results-US.pdf.

93. Andress J. The Basics of Information Securit. URL: http://www.sciencedirect.com/science/article/pii/B9781597496537 000013.

94. Ничипорчук Н., Вознюк Є. Секрет успіху США у сфері інформаційної безпеки. Міжнародні відносини, суспільні комунікацій та регіональні студії. 2018. №1(3). С.66-71. URL: https://relint.vnu.edu.ua/index.php/relint/article/view/28/15.

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

96. Vetrov K., Voznyuk Ye. Information Terrorism as a modern Threat for information Security of European States. Міжнародні відносини, суспільні комунікацій та регіональні студії. 2019. №1(5). С.34-41. URL: https://relint.vnu.edu.ua/index.php/relint/issue/view/8/5.

97. Карчевський М. Спам може бути корисним: досвід правового регулювання розсилки множинних електронних повідомлень у США. *Підприємництво, господарство і право.* 2011. №6. С.131-135.

98. Палийчук Г. Трансграничное Интернет-регулирование. *Юридическая практика.* 2008. №35(557). 26.08.

99. Marsoof A. Onlain social networking and the right to privawacy: The conflicting rights of privacy and expression. *International j. of law and information technology.* Oxford, 2011. Vol.19, №2. P.110-132.

100. Белицкая А. Защита несовершеннолетних от вредного воздействия информационной среды в законодательстве постсоветских стран. *Законодательство и практика масс-медиа.* 2006. Выпуск 7-8 (июль-август). С.16-23.

101. Freedom of Expression on the Internet Organization for Security and Co-operation in Europe The Office of the Representative on Freedom of the Media Dunja Mijatovi? Report 2010. URL: www.osce.org/fom/80723.

102. Хавронюк Н. Декларация Международного форума по проблемам преступности у уголовного права в эпоху глобализации (МФППУПЭГ). *Предпринимательство, хозяйство и право.* 2013. №1. С.109-110.

103. Козак Н. Криміналістичні аспекти поняття «комп'ютерні злочини». *Підприємництво, господарство і право.* 2013. №2. С.40-43.

104. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., 2002. 496с.

105. Музика А., Азаров Д. Про поняття злочинів у сфері комп'ютерної інформації. *Право України.* 2003. №4. С.86-89.

106. Паклин Н.Б., Орешков В.И. Бизнес-аналитика: от данных к знаниям. Спб., 2010. 704с.

107. Карчевський М.В. Злочини у сфері використання комп'ютерної техніки. К., 2010. 168с.

108. Гуцалюк М. Протидія комп'ютерній злочинності. *Право України.* 2003. №6. С.114-119.

109. Мережко О. Проблеми кібервійни та кібербезпеки в міжнародному праві. *Юридичний журнал.* 2009. №6(84). С.94-95.

110. Сопілко І. Концептуальні засади формування кіберпезпекової політики України. *Підприємництво, господарство і право.* 2013. №1. С.101-103.

111. Конвенція про кіберзлочинність від 23 листопада 2001 року. URL: http://zakon2.rada.gov.ua/laws/show/994_575.

112. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г. *Московский журнал международного права.* 2008. № 4(72). С. 244-250.

113. Гіда О.Ф. Міжнародні ініціативи у сфері інформаційної безпеки (порівняльний аналіз). *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. №2(8). С.283-291.

114. Sofaer Abraham D. Cyber Crime and Security. The Transnational Dimension / Abraham D. Sofaer. Seymour E. Goodman // Transnational Dimension of Cybercrime and Terrorism, Hoover Inst Pr., 2001. Hoover Inst Pr. P.1-34.

115. Мороз Н.О. Формы и направления международного сотрудничества в борьбе с преступностью в сфере высоких технологий. *Ученые записки Таврического национального университета им. В.И. Вернадского. Серия «Юридические науки».* 2011. Том 24 (63). №1. С.315-325.