**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**КИЇВСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА**

**ФАКУЛЬТЕТ ПРАВА ТА МІЖНАРОДНИХ ВІДНОСИН**

Кафедра міжнародних відносин та міжнародного права

**Спеціальність 291 “Міжнародні відносини, суспільні комунікації та регіональні студії ”**

**БАКАЛАВРСЬКА РОБОТА**

**на тему:**

**ПОЛІТИЧНІ ТА ПРАВОВІ ПРОБЛЕМИ МІЖНАРОДНЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

**Студентки 4 курсу**

**Денної форми навчання**

**Жмурко Таїсії Романівни**

**Науковий керівник:**

**Кандидат юридичних наук, доцент**

**Мельник Ганна Мирославівна**

**Київ – 2021**

ЗМІСТ

[**ВСТУП** 2](#_Toc70415543)

[**РОЗДІЛ 1 .**](#_Toc70415544)[**ТЕОРЕТИКО-МЕТОДИЧНІ АСПЕКТИ ТЕМИ ДОСЛІДЖЕННЯ 6**](#_Toc70415545)

[1.1. Стан наукової розробки та джерельна база теми дослідження 6](#_Toc70415546)

[1.2. Понятійно-категоріальний апарат та методи дослідження 16](#_Toc70415547)

[**РОЗДІЛ 2 .**](#_Toc70415548)[**ПОЛІТИКО-ПРАВОВІ ПРОБЛЕМИ РОЗБУДОВИ СИСТЕМИ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ГЛОБАЛІЗАЦІЇ** 24](#_Toc70415549)

[2.1. Проблема військового застосування інформаційно-комунікаційних технологій 24](#_Toc70415550)

[2.2. Інформаційно-комунікаційні технології (ІКТ) як інструмент терористичної і антигромадської діяльності 34](#_Toc70415551)

[**РОЗДІЛ 3 .**](#_Toc70415552)[**МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ** 44](#_Toc70415553)

[3.1. Формування міжнародних режимів інформаційної безпеки на різних рівнях світової політики 44](#_Toc70415554)

[3.2. Перспективні тенденції забезпечення інформаційної безпеки 50](#_Toc70415555)

[3.3 Пріоритети удосконалення інформаційної безпеки України 54](#_Toc70415556)

[**ВИСНОВКИ** 61](#_Toc70415557)

[**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ** 65](#_Toc70415558)

## ВСТУП

**Актуальність дослідження**. Роль інформації в забезпеченні всіх сторін життєдіяльності суспільства важко переоцінити. Починаючи з 1950 року її кількість в світі подвоювалося кожні десять років, з 1970 – кожні 5 років, а з 1990 року – щорічно [20, 14]. Розвиток інтернету прискорив цей процес. Якщо в 2016 р. обсяг даних оцінювався в 16 зетабайт, то до 2025 року цей показник виросте до 163 зетабайт. До 2025 року близько 20% всієї інформації в глобальній інфосфері буде відігравати критично важливу роль в повсякденному житті, а 20% генерованих даних будуть передаватися в режимі реального часу [5].

Розвиток інформаційно-комунікаційних технологій (ІКТ) відкривнебувалі можливості для досягнення прогресу у всіх областях діяльності. Будучи як ніколи раніше могутньою в оперуванні інформацією, людство стає все більш залежним від ІКТ, оскільки без них сьогодні неможливі ні забезпечення безпеки, ні соціально-економічний розвиток. В епоху, коли дані про індивідів і організаціях зберігаються в різноманітних комп'ютерних системах, які часто не знаходяться під прямим контролем їх користувачів, забезпечення інформаційної безпеки стає пріоритетним завданням практично в будь-якій сфері діяльності.

Типовою проблемою в таких умовах стає пошук балансу між продуктивністю і безпекою. Загрози інформаційної безпеки, породжені розвитком ІКТ, є сьогодні вкрай актуальною науковою і практичною проблемою, складність якої посилюється тим, що пошуки механізмів узгодження інтересів учасників розвитку глобального інформаційного простору також є її складовими.

Прогрес в інформаційно-технологічній сфері поряд з об’єктивними благами, створив принципово нові потенційні загрози використання досягнень з цілями несумісними із завданнями підтримки миру та безпеки. Усвідомлення необхідності дотримання принципів міжнародного права, забезпечення прав і свобод, невикористання інформаціно-комунікаційних технологій з протиправною метою, – все це привернуло увагу до розгляду проблем міжнародно-правового регулювання інформаційної безпеки, у тому числі і як підстави для обмеження інформаційних прав людини. Обмеження інформаційних прав людини повинні застосовуватися лише «в особливих випадках»… в разі «неминучої потреби»…і державні органи мають застосовувати подібні заходи лише у разі, якщо вони дійсно необхідні в даній ситуації і ніякими іншими засобами поставлені завдання рішити неможливо [3].

Інформаційна безпека – це стан захищеності встановлених законодавством норм та параметрів інформаційних процесів та відносин [4]. Причини виникнення інформаційної небезпеки можуть бути різними, але у всіх випадках вони зв’язані з природою інформації, її сутністю і роллю в життєзабезпеченні соціальних систем [1].

Стрімкий розвиток і широке використання ІКТ привів до формування фундаментальної залежності критичних національних інфраструктур від цих технологій і зумовив виникнення принципово нових загроз. Ці загрози пов’язані, насамперед, з можливістю використання ІКТ в цілях, несумісних із завданнями підтримки міжнародної стабільності та безпеки, дотримання принципів відмови від застосування сили, невтручання у внутрішні справи держав, забезпечення прав і свобод людини. Загострення потенційної небезпеки обґрунтована можливістю розробки, застосування та розповсюдження інформаційної зброї, загрозою інформаційних війн і інформаційного тероризму, здатних викликати інформаційні конфлікти зі значними руйнівними наслідками.

**Мета дослідження** – проаналізувати політичні та правові проблеми міжнародної інформаційної безпеки

**Об'єктом дослідження** є поняття міжнародної правової безпеки.

**Предмет дослідження** – політико-інституціональна компонента різних рівнів взаємодії міжнародних акторів з вирішення політичних та правових проблем міжнародної інформаційної безпеки.

 Для досягнення визначеної мети поставлені **наступні завдання**:

1. Описати стан наукової розробки та джерельна база теми дослідження.

2. Охарактеризувати сонятійно-категоріальний апарат та методи дослідження.

3. Проаналізувати проблему військового застосування інформаційно-комунікаційних технологій.

4. Охарактеризувати інформаційно-комунікаційні технології (ІКТ) як інструмент терористичної і антигромадської діяльності.

5. Дослідити особливості формування міжнародних режимів інформаційної безпеки на різних рівнях світової політики .

6. Визначити перспективні тенденції забезпечення інформаційної безпеки

7. Проаналізувати пріоритети удосконалення інформаційної безпеки України.

**Теоретична і методологічна база дослідження**. Методологічною основою дослідження стали сучасні положення теорії наукового пізнання політико-правових і соціальних явищ. У дослідженні застосовувалися історичний та системний підхід, що дозволяє досліджувати інформаційну безпеку як цілісну систему, що трансформується в умовах сучасних глобальних процесів. Міждисциплінарний підхід дозволив виявити комплексність і багатосторонність взаємодії державних міжнародних акторів щодо питання інформаційної безпеки; структурно-функціональний підхід, що дозволив дослідити елементи міжнародної безпеки.

Основні наукові результати та їх **наукова новизна** визначаються тим, що це дослідження є комплексним аналізом політичних та правових проблем міжнародної інформаційної безпеки.

**Теоретичне і практичне значення** отриманих результатів дослідження полягає в тому, що вони можуть бути використані науково-дослідній сфері – основні положення та висновки дослідження складають базу для подальшої розробки методології політичного співробітництва щодо проблем міжнародної інформаційної безпеки.

**Структура дослідження**. Дослідження складається зі вступ, трьох розділів, висновків та списку використаної літератури

## РОЗДІЛ 1

## ТЕОРЕТИКО-МЕТОДИЧНІ АСПЕКТИ ТЕМИ ДОСЛІДЖЕННЯ

## 1.1 Стан наукової розробки та джерельна база теми дослідження

Сучасний етап розвитку соціуму характеризується домінуванням інформаційної сфери діяльності людини. Ця сфера має визначальне значення з точки зору подальшого розвитку цивілізації. Питання існування людини в інформатизованому світі хвилювали дослідників вже в середині минулого століття, а для сучасних дослідників проблема інформаційного суспільства є однією з найважливіших.

Сучасна концепція інформаційного суспільства, на наш погляд, грунтується на теорії постіндустріального суспільства. Індустріальне суспільство базується на машинній технології, тоді як постіндустріальне суспільство в першу чергу застосовує технології інформаційно-інтелектуальні. Специфічна риса постіндустріального суспільства полягає в здійсненні процесів, змістом яких є обмін інформацією, із застосуванням технологій інформаційного і телекомунікаційного характеру.

Базисні постулати теорії постіндустріального суспільства були закладені Д. Беллом, представником соціологічної науки США. Згодом значний внесок в розвиток зазначеної теорії вніс Е. Тоффлер. Поряд із зазначеними авторами, в число теоретиків постіндустріалізму входять Г. Кан, У. Дайзард, А. Турен, Т. Стоуньер і ряд інших. М. Кастельс називає нову епоху «інформаціональною», а також світову культуру, ситуацію в соціальній та економічній сфері. Спільність поглядів дослідників спостерігається з питання про характеристику сучасного етапу розвитку цивілізації як періоду, початку відчутних змін у суспільному житті, у сфері технології та культури. При цьому оцінка майбутніх перспектив розвитку також в значній мірі ідентична.

Людство постійно нарощує технічний потенціал, що має визначальний вплив на все життя суспільства в цілому. Перші згадки про інформаційне суспільство можна зустріти в середині XX століття в звітах, підготовлених Агентством економічного планування для Уряду Японіі, потім положення, які були описані в вищевказаних звітах про винекнення інформаційного суспільства, були конкретизовані американським соціологом Д. Беллом. В рамках роботи «Соціальні рамки інформаційного суспільства» він виявив сутність нового суспільства, а також зазначив, що вирішальну роль у розвитку економічного і соціального, повсякденного життя людини буде грати принципово новий соціальний уклад, заснований на телекомунікаційному розвитку.

Інформація та знання характеризуються теоретиками постіндустріалізму як стратегічний ресурс, як фактор ключових процесів трансформації в постіндустріальному суспільстві. Канадський дослідник М. Маклюен в 1960-х роках писав про нове суспільство як про «глобальне село», в якому інформаційні технології будуть виступати фундаментальною базою для створення соціальної та економічної основи суспільства.

Англійський вчений Т. Стоуньер в роботі «Інформаційне багатство: профіль постіндустріальної економіки» вперше зазначив, що інформація є стратегічним ресурсом, який можна ототожнити з корисними копалинами, тим самим інформаційні ресурси суверенних держав стануть бажаним предметом для отримання їх іншими державами. Про новий етап розвитку суспільства – «інформаційне суспільство», а також про провідну роль нових інформаційних технологій писав у своїй праці Е. Тоффлер «Третя хвиля». У своїй роботі він зазначив, що розвиток інформаційного суспільства дасть світу необмежені можливості, а також буде стимулом для зростання інформаційного обміну та деконцентрації виробництва.

У числі дослідників, предметом наукового інтересу яких є питання постіндустріалізму, необхідно виділити У. Дайзарда. У його роботі представлений сценарний аналіз шляхів переходу суспільства в стадію інформаційного суспільства, а також проблемних питан щодо забезпечення інформаційної безпеки. У. Дайзард розділяє погляди, сформульовані Д. Беллом і Е. Тоффлером щодо проблем розвитку суспільства. У той же час він вказує, що в соціально-економічній сфері інформаційного суспільства необхідно буде докласти зусиль для вирішення ряду проблемних питань в галузі забезпечення безпеки. Автор зазначає, що можливості, що надаються новими технологіями, несуть потенційні ризики, які людство змушене буде постійно враховувати і боротися з ними. Підхід, який демонструє У. Дайзард, здається цілком обгрунтованим.

В наш час набуває особливої ​​актуальності проблема проведення ефективної політики і реалізації заходів, які необхідно вживати в перехідний період. Стратегія розвитку в цьому питанні повинна визначатися в деякій мірі прийняттям технічних і економічних рішень. При цьому ключову увагу повинно бути приділено рішенням політичного характеру. Політичні рішення будуть вираженням ступеня готовності до трансформації ключових інститутів суспільства відповідно до розвитку інформаційної сфери.

Аналізуючи соціально-філософські погляди, викладені У. Дайзардом, можна зробити висновок, що проблемні питання в сфері інформаційної безпеки не є нездоланним бар'єром на шляху розвитку суспільства нового типу. Дані проблеми обумовлені, в першу чергу, недостатньо продуманими рішеннями, такими, що порушують рівновагу в економіці і суспільстві в цілому. У зв'язку з цим потрібні узгоджені підходи і методи, що дозволяють здійснювати контроль і здатні мінімізувати негативний вплив, який потенційно можливий при використанні інформаційних технологій.

Дані підходи, методи і контрольні процедури повинні реалізовуватися системою інформаційної безпеки на рівні держави. Теоретичний образ інформаційного суспільства розглянуто японським дослідником Й. Масуда в роботі «Інформаційне суспільство як постіндустріальне суспільство», основною ідеєю якої є процес комп'ютеризації нового суспільства, перетворення інформаціонно-технологічної революції в головну виробничу силу, а також переважання в економічній сфері «інтелектуального виробництва».

Досить повна характеристика проблем, що виникають при забезпеченні інформаційної безпеки суспільства інформаційного типу представлена в роботах Й. Масуди. До числа фундаментальних небезпек він відносить можливість використання інформаційних технологій для невиправданого вторгнення в духовно-моральну сферу індивідів і соціальних організацій. Банки даних, що акумулюють відомості про стан здоров'я, роботу, підприємницьку активність, рахунки в фінансово-кредитних організаціях, несуть потенційну загрозу вторгнення в особисте і суспільне життя громадян. Й. Масуда демонструє переконаність в можливості усунення подібних загроз, вказуючи, що вірить в можливість уникнути «цього катастрофічного автоматизованого курсу ... Ми не маємо права застосовувати комп'ютер і науку для знищення духовного життя людини і людства». Як засоби, які сприяють вирішенню даних питань, автор вказує на укорінення демократичних цінностей, захист громадян з боку держави, планомірну діяльність щодо запобігання злочинних посягань в інформаційній сфері з використанням комп'ютерної техніки. Напрямки, на які вказує автор у вирішенні проблем в області інформаційної безпеки, бачаться цілком вірними. При цьому механізм, за допомогою якого подібні проблеми можуть бути вирішені, не може вважатися ефективним ні в одній з сучасних держав. Тому, щоб більш активно підвищувати ефективність подібного механізму, потрібно усвідомити всю значимість інформаційної трансформації суспільства.

Модель мережевого суспільства, як особливої ​​соціальної структури запропонував М. Кастельс, яка стала результатом інформаційно-технологічної революції. На його думку, основною рисою мережевого суспільства є не домінування самої інформації, а напрямки її використання, на підставі чого в життєдіяльності людей починають переважати глобальні і мережеві структури. Таким чином формуються мережі, такі як, інформаційна мережа «Інтернет», які пов'язують населення, громадянські інститути, органи державної влади та організації. За допомогою мережі існує можливість розділити виробничий процес в різні місця, а здійснювати і забезпечувати єдність виробничого процесу за рахунок нових ІКТ.

На думку М. Кастельса, комп'ютерні технології визначальним чином впливають на владні відносини в суспільстві і багато процесів, що відбуваються в області культури. Звертаючись до забезпечення інформаційної безпеки, можна відзначити висновок, який в 1976 році сформулював американський вчений Т. Рон в своєму звіті для корпорації «Боїнг» про те, що «інформаційна інфраструктура стає ключовим компонентом економіки, і є вразливою метою, як у воєнний, так і в мирний час».

При хронологічному аналізі розвитку підходів зарубіжних дослідників до процесів становлення інформаційного суспільства та питань забезпечення безпеки в зв'язку з активним застосуванням інформаційних технологій, необхідно відзначити наступне. Для початкових концепцій, які дають наукове осмислення формування інформаційного суспільства (таких авторів, як Д. Белл, Т. Стоуньер та інших), характерна впевненість в тому, що наука, техніка, і супутня їм раціональність охоплять всі сфери людського, суспільного існування, і сприятимуть їх гармонізації. Отже, відмінною рисою цих концепцій є оптимізм щодо встановлення технократичної влади і успішності прогресу в сфері науки і техніки.

У наступних теоріях (М. Кастельс, Т. Росзак та. ін) описується домінування питань, що безпосередньо стосуються науки і техніки, постає вже не таким всеосяжним, і більш широко зачіпаються психологічні, гуманітарні, моральні аспекти розвитку інформаційного суспільства.

Як зазначає І. Ю. Алексєєва, феномен інформаційного суспільства, як і проблеми конвергенції інформаційних технологій з нанотехнологіями, біотехнологіями, когнітивними і соціогуманітарними технологіями не можуть бути належним чином вивчені з використанням тільки лише класичних уявлень про наукові поняття і предмети дослідження. Наприклад, в книзі Ф. Вебстера «Теорії інформаційного суспільства», можна знайти багато в чому переконливий опис недоліків, якими страждають основні визначення «інформаційного суспільства». У числі таких недоліків – неточність формулювань, сумнівність тих чи інших фрагментів змісту.

Варто відзначити особливу роль, яка відводилася політичним чинником в інформаційному суспільстві, а саме забезпечення вільного доступу до інформації, що призведе до відкритого і демократичного політичного процесу зі зростаючою роллю участі в ньому різних соціальних верств населення.

 Підводячи підсумок огляду робіт авторів, які теоретично осмислюють становлення нового суспільства, слід вказати на обгрунтованість виділення ключових характеристик, притаманних сучасному етапу інформаційного розвитку. Роль інформації та знань як визначального фактора розвитку суспільства, домінуючого в порівнянні з матеріальним виробництвом, виробництвом енергії, наданням послуг, істотно зростає. Інформацію, знання, технологічні досягнення в інформаційній сфері, телекомунікації слід розглядати в якості основних факторів перетворень в соціально-економічній і політичній сфері. При цьому щодо еволюції теоретичних поглядів на інформатизацію та пов'язані з нею питання інформаційної безпеки, зумовлені активним розвитком технологічної сфери, необхідно відзначити наступне: якщо в ранніх концепціях визначальне значення приділяється аналізу науково-технічних аспектів, в наступних роботах зачіпаються психологічні, гуманітарні, моральні аспекти розвитку інформаційного суспільства, і закладаються методологічні основи для вирішення питань, пов'язаних з інформаційною безпекою.

В основних теоріях інформаційного суспільства приділяється увага і ряду значущих питань, що відносяться до забезпечення інформаційної безпеки. Так, зачіпаються такі проблеми, як процес інформаційного розшарування суспільства, вторгнення в індивідуальну і суспільну свідомість, в особисте життя громадян та ін. Відповідно, дослідження процесу і шляхів розвитку інформаційного суспільства, аналіз даного розвитку з урахуванням потенціалу, яким володіють інформаційні технології, викликає потребу у виявленні можливостей забезпечення безпеки, мінімізації негативних наслідків, які можуть виникнути при застосуванні інформаційних технології.

Для того, щоб процес подальшого розвитку інформаційного суспільства протікав з належним рівнем безпеки, еволюція суспільства протікала в динамічній рівновазі і необхідно докладати зусилля в напрямі забезпечення інформаційної безпеки. При цьому виявлення сутності поняття «інформаційна безпека» має дозволити глибше осмислити зміст цього поняття. Захист від загроз, що виникли на сучасному етапі внаслідок інформатизації, представляє актуальну науково-практичну проблему.

Слід зазначити постійне збільшення числа досліджень з питань інформаційної безпеки. При цьому аналіз наукових робіт дозволяє наголосити на необхідності подальшого дослідження методологічних аспектів цієї дефініції. На нашу думку, необхідно в першу чергу приділити увагу аналізу термінології. Значне число фахівців у сфері інформаційної безпеки відзначає складність подання повного визначення змісту інформаційної безпеки.

В силу того, що загальноприйняті поняття та категорії не вироблені, в наявності полісемія, а часто і омонімія. Наслідком цього є зниження ефективності наукових робіт, присвячених питанням безпеки, як теоретичної, так і практичної області. Слід зазначити безперервні спроби формування ясного і точного визначення, яке в повній мірі виражає сутність інформаційної безпеки. Вироблення подібного визначення має важливе значення в теоретичному і прикладному відношенні.

На нашу думку, інформаційну безпеку слід розглядати в якості унікального явища сучасного суспільства. Питання формування інформаційної безпеки характеризується глобальним значенням для людської цивілізації на сучасному етапі. Відповідно, значення формування об'єктивного і практичного визначення даного феномена важко переоцінити. Процес аналізу проблем в сфері інформаційної безпеки обумовлений тим, що загальноприйнятий підхід до розуміння термінів, що застосовуються для характеристики відповідної предметної області, на сьогодні відсутній. Крім поняття «інформаційна безпека» досить широко застосовується поняття «безпека інформації». Дані поняття є взаємопов'язаними. Уточнимо, що «безпека» не існує відокремлено, вона пов'язана з певним об'єктом. Змістовна сторона зазначеного поняття має визначальний вплив на вибір об'єкта. Якщо в якості об'єкта, що захищається розглядати інформацію, вищевказані терміни «інформаційна безпека» та «безпека інформації» набувають значення синонімів. Інформаційну безпеку слід розглядати в якості комплексного явища.

Також необхідно вказати на ряд специфічних факторів, що ускладнюють формування дефініції інформаційної безпеки:

– досліджуване явище існує об'єктивно, в силу реальної дійсності умов суспільного розвитку. Відчутний вплив на його становлення надає такий процес, як інформатизація. При цьому інформатизація характеризується динамічним розвитком, і в зв'язку з цим повинна також виступати в якості об'єкта більш детального наукового аналізу.

Слід звернути увагу, що особливості інформаційної безпеки в Україні в значній мірі обумовлені трансформацією механізму забезпечення національної безпеки на рівні держави. Складність формулювання повного визначення цієї дефініції обумовлена ​​дією вищевказаних чинників.

– формулювання поняття досліджуваного явища утруднено також необхідністю врахування своєрідного прояву інформаційної безпеки з точки зору права, психології, суспільного розвитку, її технічного забезпечення, і ін. Дослідники, що займаються в різних сферах знань, аналізують інформаційну безпеку під різними кутами зору, виходячи з особливостей наукової спеціалізації. У зв'язку з цим досліджуване явище наділяється різноманітним вмістом. Подібна широта діапазону підходів дозволяє повніше охопити сутність феномену інформаційної безпеки, однак з очевидністю ускладнює формування єдиної дефініції.

Охарактеризувавши ключові фактори, що ускладнюють виявлення сутнісних характеристик аналізованого феномена, вважаємо необхідним розглянути в змістовному аспекті існуючі базові підходи до формулювання визначення інформаційної безпеки.

Соціологічний підхід до дослідження інформаційної безпеки передбачає вивчення інформаційної безпеки в рамках інформаційного протиборства, яке є ціннісним і ідеологічним, що виявляється в мас-медіа, електронних ЗМІ. Оцінка результатів подібного протиборства проводиться за допомогою виявлення громадської думки, фіксується соціологічними методами. Поряд з соціологічними, до числа методологічних підходів в аналізі питань, пов'язаних з інформаційною безпекою, відноситься соціально-психологічної. Як вважають прихильники зазначеного підходу, необхідно оцінювати, наскільки ефективним є інформаційний вплив на людину. На ефективність зазначеного впливу впливають установки, які сформувалися у індивіда. Ефективність впливу залежить і від ступеня довіри в суспільстві до інформації, яку поширюють засоби масової інформації.

До числа методологічних підходів в аналізі даного явища входить також соціокультурний підхід, в якому інформаційна культура трактується у вигляді інформаційної складової загальнолюдської культури. Вона відображає рівень, на якому реалізуються всі інформаційні процеси в суспільстві і інформаційні відносини. Відповідно, соціокультурний підхід інформаційної безпеки передбачає необхідність виявлення можливостей протистояння руйнуванню соціальних цінностей і їх підміні цінностей на уявні. Основним принципом в соціокультурному підході до інформаційної безпеки є виявлення і забезпечення можливостей щодо безпечного розвитку особистості в інформаційному суспільстві, утвердження цінностей, які виступають як змістовно-орієнтуючі координати при інформаційних взаємодіях.

Вищевказані підходи дозволяють збагачувати наукове знання. Однак, з урахуванням того, що глобальний процес інформатизації відбувається одночасно з формуванням інформаційного суспільства, зазначені підходи не дають можливості досягти необхідного рівня узагальнення, що дозволяє охарактеризувати системний характер даного суспільства. У зв'язку з цим їх не слід розглядати в якості надійної методологічної основи дослідження питань, пов'язаних з інформаційною безпекою.

Поняття інформаційної безпеки представляється як комплексне явище, розглянуті підходи не суперечать один одному, що доводять багатогранну природу цього поняття.

## 1.2 Понятійно-категоріальний апарат та методи дослідження

Проблеми сутності, природи і закономірностей розвитку інформації привертали увагу мислителів з давніх часів. У ХХ ст. вивчення інформації почало здійснюватися в рамках кібернетики та інформатики. Найважливішим кроком у становленні сучасних уявлень про інформацію стали роботи М. Вінера і У. Ешбі, які пов'язували інформацію з теорією управління, а також роботи К. Шеннона, який запропонував математичну теорію інформації. Інформація (від лат. Informatio ознайомлення, уявлення, роз'яснення, виклад) може бути визначена як відомості (повідомлення, дані) незалежно від форми їх подання; сукупність даних, зафіксованих на матеріальному носії, збережених і поширених в часі і просторі [10].

Інформація може розумітися як абстрактна фікція, фізичний феномен, функції самоврядних систем і ін. [38]. Філософський енциклопедичний словник містить чотири визначення інформації:

- повідомлення, інформування про стан справ, відомості, що передаються людьми;

- зменшення невизначеності, що досягається завдяки передачі повідомлень;

- повідомлення, пов'язане з управлінням, сигнали з урахуванням їх прагматичних характеристик;

- відображення різноманітності в будь-яких об'єктах і процесах неживої і живої природи [40].

Однією з перших спроб створення масштабної теорії інформації стало вчення В. І. Вернадського про ноосферу як про новий стан біосфери, в якій думка може змінювати матеріальні процеси [9]. Творець кібернетики Н. Вінер розумів інформацію як позначення змісту, одержуваного людиною із зовнішнього світу завдяки пристосуванню до нього. Його колега К. Шеннон трактував інформацію як комунікацію і зв'язок, в процесі якої усувається невизначеність. Ф.Махлуп запропонував кілька точок зору, згідно з якими інформація це:

1) процес передачі знань, сигналів, повідомлень;

2) поточні дані про змінні величини, систематизовані відомості щодо основних причинних зв'язків, що містяться в знанні;

3) передані або отримані знання;

4) знання про якусь особливу подію або випадок [26, 36-37].

Залежно від того, як розуміється інформація, вирішується питання, чи є інформація властивістю тільки розумних істот або має місце в усіх організованих об'єктах. Відповідь на це питання дозволяє зробити парадигмальний вибір між технічним і гуманітарним аспектами цього явища. Вивчення гуманітарного (людського) аспекту інформації дозволяє розглядати її як зміст повідомлень, призначених для передачі від одних людей до інших в певних знаково-смислових системах, тобто в культурних контекстах. На думку французького дослідника А. Моля, інформативність повідомлень пропорційна їй відносній оригінальності, тобто непередбачуваності, яка зменшується зі збільшенням надмірності [27, 203- 204].

Інакше кажучи, інформація – це не сенс, значення або значимість, а міра складності, яку одержувач здатний сприйняти і використовувати, наприклад, перетворивши її в знання. Проблема визначення поняття «знання» також не має однозначного вирішення. А. В. Соколов пропонує наступну класифікацію підходів до розуміння зв'язку між знанням та інформацією:

- інформація – об'єктивний енергетичний процес, а знання – ідеальне явище, результат функціонування усвідомлення;

- інформація – знання, яке передається в процесі комунікації;

- інформація – основа для отримання знання;

- інформація – це знання, втілене в знаковій формі [38].

Інформація, знання і розуміння допомагають людям бути продуктивними, тобто досягати своїх цілей при оптимальному співвідношенні ймовірності успіху і витрачених ресурсів [41]. Отже, хоча поняття інформації є загальнонауковою, в його інтерпретаціях існують різні трактування. В інформації можна виявити технічне і людське, тобто гуманітарне вимірювання, які пов'язані між собою.

Юридичними особливостями і властивостями інформації можна назвати:

1) матеріальність – наявність сприйманого людиною носія у вигляді об'єкта фізичного світу;

2) сприйняття – схильність до обробки, яка зберігає або створює можливість людині її розпізнавати, розуміти, осмислювати;

3) перетворювальність – можливість бути переробленою;

4) відособленість – можливість існувати порційно, подільність на частини, які можуть існувати окремо;

5) оборотоздатність – властивість, що дозволяє інформації брати участь в цивільному обороті в якості продукту;

6) системність – наявність зв'язків між елементами інформації, зв'язків між ними і властивостей, що дозволяє інформації зберігатися при зверненні в просторі і часі;

7) невичерпність – здатність до необмеженого обігу в просторі, часі та за колом осіб;

8) руйнація – властивість інформації піддаватися зміні і знищенню;

9) невідчужуваність – ознака інформації, що дозволяє лише таке правомірне фізичне переміщення інформації, яке супроводжується оформленням відповідних прав на її відчуження і передається разом з цими правами, однак, по суті, інформація продовжує залишатися у першоджерела;

10) розповсюджуваність – тиражування необмежену кількість разів;

11) сформованість – наявність структури, можливість бути представленою в певній формі (бази даних, документа, графічного об'єкта та ін.) [16, 22-24].

Дослідники виділяють п'ять груп відносин, що підлягають правовому регулюванню, які становлять предмет інформаційного права:

1) реалізація основних інформаційних прав і свобод людини і громадянина, законних інтересів суспільства і держави в інформаційній сфері;

2) розвиток і модернізація інформаційно-телекомунікаційної інфраструктури в тісному зв'язку з глобальними інформаційними мережами;

3) створення та використання інформаційних ресурсів, розвиток ринку інформаційних засобів, продуктів і послуг;

4) державна політика в сфері інформаційної безпеки;

5) міжнародне співробітництво в сфері інформатизації [17].

Оскільки інформаційні відносини в своєму географічному вимірі є транскордонними, значною мірою глобальними, то всі ці області формують нове середовище суспільних відносин, що іменується інформаційним простором. Традиційно простір тісно пов'язувався з територією, але сьогодні цей зв'язок руйнується. З точки зору політики простір можна розуміти як такі галузі суспільних відносин, які:

1) створюють потенційні джерела влади;

2) забезпечують поширення впливу і засоби досягнення цілей;

3) активізують нові сервіси, ресурси, знання або ринки;

4) реалізують нові можливості, що укріплюються і підтримувані технологічними досягненнями [43, 5].

Інформаційний простір в цілому і кіберпростір зокрема усіма цими властивостями володіють. Інформаційний простір як особлива реальність усвідомлюється політичними акторами, що знаходить відображення в різного роду документах.

Частиною інформаційного простору є кіберпростір – онлайн-світ комп'ютерних мереж, який виступає в ролі смислового середовища електронної комунікації. Кіберпростір можна трактувати як вид концептуального простору або порядок співіснування предметів в сприйнятті людей, що відображає фізичний простір і залежить від соціально обумовлених моделей сприйняття світу.

До характеристик кіберпростору можна віднести:

- особливі фізичні властивості: кіберпростір без проблем долає фізичні перепони і географічну віддаленість;

- особливі тимчасові характеристики, пов'язані з тим, що комунікація в них є практично миттєвою;

- мінливість, обумовлена ​​безперервними змінами його конфігурацій під впливом змін в потоках інформації;

- проникність щодо правових обмежень і юрисдикції.

Слід зазначити, що кіберпростір не є нейтральним по відношенню до людини, яка в ньому знаходиться. Знижуючи бар'єри для самовираження і символічної взаємодії з іншими, кіберпростір виявляється сприятливим середовищем для модифікації ідентичності особистості і прояву різних форм соціальної активності. Будучи створеним за допомогою технологічних інновацій, кіберпростір дозволяє користувачам залучатися до активності, не зустрічаючи при цьому територіальних, юридичних або економічних перешкод.

Маючи своїм матеріальним втіленням лише інфраструктуру мереж комп'ютерно-опосередкованої комунікації, кіберпростір створює проблеми, пов'язані з встановленням державних кордонів і визначенням юрисдикції. Реалізація принципу суверенітету держав в кіберпросторі сьогодні є проблематичною. Щодо порядку визначення віртуальних меж в експертному співтоваристві сьогодні сформувалися три підходи:

- за приладами, що використовуються для доступу в інтернет ( «межа реальності»);

- фізичним кордоном, де лінії зв'язку переходять з території однієї держави на іншу;

- «віртуальним кордоном», якщо інтернет-адрес буде поділений між різними країнами [1].

Правові інструменти регулювання розвитку інформаційної сфери не завжди виявляються ефективними в силу технічної легкості їх нейтралізації, що веде до збільшення таких проблем сучасного суспільства, як тероризм, релігійний екстремізм, торгівля людьми, нелегальна міграція, наркоторгівля і ін. Більш того, розвиток інформаційних технологій провокує виклики державам з боку тих політичних сил, які випереджають їх в освоєнні ІКТ.

На сьогоднішній день в сучасних умовах державно-правового розвитку та переходу на цифрові технології, актуальним є питання про забезпечення інформаційної безпеки на міжнародному рівні. Ця актуальність обумовлена ​​однією з головних рис сучасного етапу науково-технічного прогресу: глобальною інформаційною революцією і зростаючою роллю інформаційно-комунікаційних технологій (ІКТ) в сучасному світі.

У науковій літературі відсутнє визначення поняття «міжнародна інформаційна безпека». Зінов'єва Е.С. вважає, що, виходячи з термінології ООН, міжнародна інформаційна безпека – це захищеність глобальної інформаційної системи від так званої «тріади загроз» злочинних, терористичних та військово-політичних (інформаційні війни та інформаційне протиборство) [4, с. 14]. В інших джерелах міжнародну інформаційну безпеку визначають як «стан міжнародних відносин, який виключає порушення світової стабільності і створення загрози безпеці держав і світової спільноти в інформаційному просторі» [1].

Отже, поняття «міжнародна інформаційна безпека» є комплексним, тому що включає в себе стан захищеності основних інтересів особистості, суспільства, держави в інформаційному просторі, а також безпеку інформаційних систем, мереж, інформаційний вплив та ін. В результаті розвитку ІКТ, досить швидке і практично повсюдне поширення масових засобів комунікації сформувало глобальний інформаційний простір для міжнародної спільноти, однак з ризиками для міжнародної та національної безпеки [5, 6]. Інформаційні системи та інтернет-ресурси схильні до зростаючої кількості і більш широкої різноманітності загроз і вразливості, що також викликає нові проблеми для безпеки [11].

Сьогодні найбільш небезпечними загрозами міжнародній інформаційній безпеці вважаються постійне зростання масштабів комп'ютерної злочинності, використання ІКТ для «силового» вирішення міждержавних протиріч, а також підготовка та реалізація актів комп'ютерного тероризму. Цифрова безпека і захист конфіденційності стали пріоритетами державної політики. Так, на думку Організації економічного співробітництва та розвитку (далі OECD), ключовим завданням для урядів, підприємств і приватних осіб, повинні стати захист таких сфер інтернет-простору, як «Персональні дані і конфіденційність», «Цифрова безпека», «Захист дітей онлайн», «Страхування компаній від кібер-ризиків», «Вимірювання практики управління ризиками цифрової безпеки на підприємствах» та ін., для того, щоб знизити можливі ризики інтернет-злочинності та підвищити рівень довіри без обмеження можливостей, які пропонуються цифровою економікою [10 ].

Розвиток Інтернету як однієї з найбільш динамічних галузей інформаційних технологій також загострив питання правового регулювання та мережевого регулювання суспільних відносин в мережі Інтернет. Отже, Інтернет-сфера потребує правового регулювання питань, які пов'язані з таким швидким поширенням інформації [2, с. 217] і які відносяться до нормативно-правової бази як функціонування самої мережі Інтернет, так і здійснення різних операцій в ній [8, с. 3-4]. На підставі того, що забезпечення інформаційної безпеки будь-якої держави на національному рівні невіддільне від забезпечення її на міжнародному рівні, то всі питання в рамках регулювання міжнародної інформаційної безпеки повинні розглядатися і розвиватися в рамках міжнародного права [4, с. 10].

Міжнародна інформаційна безпека спрямована на формування міжнародно-правового режиму і забезпечення інформаційної безпеки на основі загальновизнаних принципів і норм міжнародних договорів і міжнародного права, що регулюють, в першу чергу, правове становище інформаційного простору і порядок його використання публічними особами. Це все відноситься до нової галузі міжнародного права міжнародної інформаційної безпеки [4, с. 14].

Отже, можна зробити висновок, що проблема міжнародної інформаційної безпеки розуміється як забезпечення міжнародної безпеки в цілому. А сучасне середовище ІКТ є не тільки новим фактором сталого розвитку суспільства, а й фактором посилення соціальної небезпеки в результаті вчинення дій, які пов'язані із здійсненням злочинних намірів, терористичної діяльності, новим простором міжнародних суперечок і конфліктів. У зв'язку з цим представляється перспективним регламентувати основні проблеми забезпечення інформаційної безпеки саме на рівні міждержавних угод, в тому числі, спираючись на стандарти, пропоновані OECD, а також акумулювати питання регулювання міжнародної інформаційної безпеки в рамках нової галузі міжнародного права міжнародної інформаційної безпеки.

Очевидно, що в умовах глобалізації та динамічного розвитку ІКТ жодна держава не може самотужки забезпечити безпеку національного інформаційного простору, однак механізми запобігання подібних загроз поки знаходяться на початковій стадії формування. Держави Азії активно включаються в процес будівництва будівлі міжнародного режиму інформаційної безпеки. Їх розбіжності з Заходом в цій сфері обумовлені різними доктринальними і правовими підходами, а також логікою розвитку сучасного світового політичного процесу, характерною рисою якого є суперництво за глобальне і регіональне лідерство, неминуче в умовах незавершеності трансформації системи міжнародних відносин.

Сьогодні опоненти вже готові співпрацювати в таких сферах, як протидія тероризму та злочинній діяльності в Інтернеті, а також у вирішенні проблем, пов'язаних з шахрайством з кредитними картами, дитячою порнографією, пропагандою насильства та нездоровим способу життя і т. ін.

## РОЗДІЛ 2

## ПОЛІТИКО-ПРАВОВІ ПРОБЛЕМИ РОЗБУДОВИ СИСТЕМИ МІЖНАРОДНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ГЛОБАЛІЗАЦІЇ

## 2.1 Проблема військового застосування інформаційно-комунікаційних технологій

Під інформацією розуміються відомості про об'єктивно існуючі об'єкти і процеси, про їхні зв'язки і взаємодії, доступні для практичного використання в діяльності людей [4]. Завдання інформатизації складаються в скороченні різних видів матеріальних, енергетичних, фінансових та інших потоків даних за рахунок їх часткової заміни і компенсації.

Інформаційними ресурсами є формалізовані ідеї і значення, дані, методи і засоби їх накопичення, зберігання та обмін між джерелами і споживачами інформації. Для вирішення завдань інформатизації застосовуються інформаційні системи, що реалізують відповідні інформаційні технології. Інформаційні технології (ІТ) – це нова галузь сучасної науки і техніки. Незважаючи на все більш широке їх поширення, в світі до сих пір немає чіткого визначення поняття «інформаційні технології», складно чітко виділити власне предмет вивчення даної області. Іноді невиправдано звужують цю область до комунікативних технологій: мережі, інтернет, зв'язку і т. ін.

В інших випадках використовують широке розуміння інформаційних технологій, включаючи в них виробництво комп'ютерної техніки, і навіть побутові електронні прилади. У поняття інформаційно-комунікативні технології об'єднуються методи, засоби і системи, пов'язані зі збором, виробництвом, обробкою, передачею, розповсюдженням, зберіганням, експлуатацією, поданням, використанням, захистом різних видів інформації [5, с. 12]. Сьогодні область ІТ розвинулася у велику наукову галузь знань, що має фундаментальний характер, яка об'єднує десятки наукових напрямів, таких, як, наприклад: штучний інтелект, обчислювальна математика, комп'ютерні науки, інженерія програмного забезпечення, архітектура комп'ютерних систем, автоматизація наукових досліджень, WEB-технології та т.д.

В інформаційній індустрії виділяється чотири основних напрямки [5, с. 14]: 1) Computer Sciences – комп'ютерні науки, завдання яких зручніше і ефективніше вводити, обробляти, перетворювати, передавати інформацію на основі розвитку математичних основ інформатики.

2) Бази даних – зберігання величезних обсягів інформації, оперативний доступ до неї, наочна видача інформації і т.п.

3) ІКТ – інформаційно-комунікаційні технології, способи передачі інформації (електронна пошта, глобальні та локальні мережі і т.д.).

4) Розробка програмного забезпечення: операційні системи, прикладні програми тощо.

Отже, інформаційні технології – це особлива сфера діяльності. За цією сферою майбутнє, вона покликана змінити цивілізацію, починаючи з елементарного виробництва до культурних і міжособистісних взаємин (не кажучи вже про високі космічні технології, медицину та ін.). Сьогодні інформаційні ресурси, стають головним надбанням і найважливішим фактором економічного розвитку, а інформаційна індустрія – однієї з основних галузей економіки, рівень суспільного прогресу в значній мірі визначається рівнем розвитку в області ІТ. Організація роботи органів державної влади на основі інформаційно-комунікаційних технологій надає нові можливості для підвищення ефективності управління і виведення його на принципово новий рівень. Ефективність інформаційної технології визначається, в кінцевому рахунку, кваліфікацією суб'єктів процесів інформатизації. При цьому технології повинні бути максимально доступні споживачам.

Інформаційні технології можна розрізняти по типу оброблюваної інформації. Поділ досить умовний, тому що більшість інформаційних технологій дозволяє підтримувати і інші види інформації. Наприклад, в текстових процесорах можлива і нескладна розрахункова діяльність, а табличні процесори обробляють не тільки цифрову інформацію, а й можуть генерувати графіки. Однак кожна з видів технології в основному орієнтована на роботу з інформацією певного виду. Модифікація елементів, що становлять інформаційні технології, дає можливість утворення нових технологій в різних комп'ютерних середовищах. В даний час проблема розробки і застосування інформаційно-комунікаційних технологій (ІКТ) в деструктивних військово-політичних цілях вивчається не тільки на внутрішньодержавному рівні і позначена в документах багатьох країн, але і на міжнародному рівні, в порядку денному ООН.

Все більшого занепокоєння викликають фізичні особи, групи або організації, включаючи злочинні організації, які виконують посередницькі функції в здійсненні підривної мережевий діяльності від імені інших. ІКТ поширені повсюдно і широко доступні. За своєю суттю вони не є чисто цивільними або чисто військовими технологіями, і мета їх використання диктується, головним чином, мотивами, якими керуються користувачі.

В рамках дослідження проблеми застосування ІКТ у військово-політичних цілях під інформаційно-комунікаційними технологіями (ІКТ) (інформаційні технології (ІТ)) будемо розуміти сукупність методів, виробничих процесів, програмно-технічних та лінгвістичних засобів, інтегрованих з метою формування, перетворення, передачі, відображення використання і зберігання інформації в інтересах її користувачів.

В залежності від характеру мети прийнято розглядати кримінальний, терористичний і військово-політичний аспекти інформаційних загроз. Використання ІКТ у військово-політичних цілях для здійснення ворожих дій і актів агресії є найбільш проблемним в контексті забезпечення національної та міжнародної безпеки, стаючи причиною міждержавних протиріч.

Це пов'язано, зокрема, з тим, що ІКТ є надзвичайно «зручним» інструментом впливу, дає практично безмежні можливості для впливу з того чи іншого питання в сфері міжнародних відносин, світової політики і економіки. Причому, дії можуть бути замасковані під кримінальні або терористичні таким чином, що виявлення справжнього джерела, цілі і навіть остаточного об'єкта впливу стає дуже складним завданням.

Ртже, актуальність проблеми військово-політичного застосування інформаційних технологій в деструктивних цілях підтверджує всеосяжний характер ІКТ, що породжують новий виток розвитку і розробки нового класу озброєнь і, як наслідок, появи нового класу загроз в військово політичній сфері.

Традиційно нові технології і в мирний, і у воєнний час розробляються для оптимізації розподілу ресурсів, які необхідно затратити для досягнення військової мети: тимчасові, фінансові та людські. У мирний час застосування ІКТ дає додаткову можливість досягти військово-політичної мети, не розв'язуючи збройні дії, при цьому маскуючи військову операцію під кримінальні або шахрайські дії недержавних акторів.

За даними Корпорації RAND, ще в 70-ті роки минулого століття США, як глобальний лідер у розвитку та використанні інформаційних систем, що володіє найпотужнішим потенціалом, що дозволяє стати супердержавою в наступальному стратегічному інформаційному протиборстві, усвідомили необхідність розробки відповідної державної стратегії по використанню всього цього потенціалу для забезпечення безпеки країни. При цьому зазначалося, що такими інформаційними можливостями можуть опанувати як союзники, так і противники, а можливість розробки новітніх засобів інформаційного протиборства потенційними противниками США послаблює лідерські позиції Сполучених Штатів і становить потенційну загрозу національній безпеці.

У 1976 році Томас Рон в своїй роботі «Системи озброєнь і інформаційна війна» для корпорації «Боїнг» зазначив, що не існує реальної концептуальної відмінності між оборонними і наступальними інформаційними операціями. Тобто технології, використовувані для руйнування інформаційних систем противника, можуть застосовуватися для захисту своїх власних. Автор зазначив, що в міру збільшення летальності зброї зміщується фокус дій по захисту від ворожої атаки: замість посилення фізичного захисту необхідно докласти всіх зусиль, щоб запобігти нападу на неї. Іншими словами, мова йде про необхідність нанесення попереджувального інформаційного удару. А ідея «попереджувального удару» як ефективного методу захисту національної безпеки безпосередньо пов'язана з ідеєю «технічної переваги» і «панування» у військовій сфері.

При цьому інформаційні операції надають не тільки унікальні можливості, а й методи їх використання для створення деструктивного бажаного ефекту. Військові засоби, що сприяють проведенню інформаційних операцій, включають стратегічні комунікації, міжвідомчі координаційні групи, операції в кіберпросторі, операції в космосі, військові операції по підтримці інформації, розвідку, спеціальні технічні процедури, спільні операції електромагнітного спектра і участь ключових лідерів.

В наш час під наступальними інформаційними операціями розуміють інтегроване використання певних можливостей і дій, підтримуваних розвідкою для впливу на осіб, що приймають рішення з боку противника, для досягнення або просування особливих цілей. Вони включають військовий обман, психологічні операції, електронне протиборство, фізичні атаки і / або руйнування, спеціальні інформаційні операції, в тому числі комп'ютерні мережеві операції.

І наступальні, і оборонні інформаційні операції проводяться в інформаційному середовищі, яке являє собою сукупність фізичних осіб, організацій та систем, задіяних в зборі, обробці, розповсюдженні та інших діях з інформацією.

Середовище складається з трьох взаємопов'язаних компонентів – фізичного, інформаційного і когнітивного. Фізичний компонент складається з систем контролю і управління, задіяних в процесі прийняття ключових рішень і підтримці інфраструктури, що дає можливість впливати фізичним особам і організаціям. Інформаційний компонент забезпечує збір, обробку, зберігання, поширення і захист інформації. Когнітивний компонент діє на свідомість тих, хто оперує з інформацією.

Нагадаємо, що через 20 років після роботи Т. Рона фахівець Корпорації RAND Мартін Лібікі, один з творців теорії інформаційного протиборства представив своє бачення класифікації інформаційних методів, кожен з яких включає захист, маніпуляцію, спотворення і заперечення інформації, в роботі «Що таке інформаційне протиборство?»:

1) боротьба з системами управління (завдає удар у голову і шию ворога);

2) інформаційно-розвідувальні операції (включає створення, захист і руйнування систем, що містять необхідні відомості для домінування на полі бою);

3) електронне протиборство (радіоелектронні операції або криптографічний метод);

4) психологічне протиборство (використання інформації для зміни думки людей);

5) «хакерське» і кібернетичне протиборство (атака на комп'ютерні системи);

6) економічне інформаційне протиборство (блокування інформації та / або маніпулювання для досягнення економічної переваги).

На сьогоднішній день створено широкий спектр інформаційно-технічних та інформаційно-психологічних засобів для застосування у військово-політичній сфері.

Розглянемо методи інформаційного протиборства в рамках зазначеної класифікації М. Лібікі.

1. Боротьба з системами управління (Command and Control Warfare (C2W)) – військова стратегія з застосуванням інформаційного середовища на поле бою, спрямована на фізичне руйнування командної структури противника. Удар може бути завдано як в центр системи командування, так і по лініях комунікацій – «удушення», через які вказівки командування передаються виконавцям, минаючи обробку в командному управлінні (як це робилося раніше).

2. Інформаційно-розвідувальні операції (Intelligence-Based Warfare (IBW)) – операції, в результаті яких отримані відомості про вказівки або завдані збитки надходять безпосередньо учасникам операції. Проводяться за допомогою автоматизованих систем, які, в свою чергу, є потенційними об'єктами атак методів боротьби з системами управління. У зв'язку з цим виділяються «наступальні» і «оборонні» інформаційно-розвідувальні операції.

3. Електронне протиборство (Electronic Warfare) – військові дії, що включають використання електромагнітної і спрямованої енергії для контролю електромагнітного спектра і / або атаки противника. Складається з трьох підрозділів: електронна атака, захист і підтримка електронного протиборства.

4. Психологічне протиборство (Information warfare) – способи ведення військових операцій, що впливають на психічний стан людини. Нові покоління озброєнь, які надають психологічну дію можуть істотно підсилити ефект вже існуючих методів ведення війни.

М. Лібікі виділяв чотири категорії впливу психологічних атак: атаки, спрямовані проти структур державного управління; атаки, спрямовані проти структур військового командування; атаки по деморалізації особового складу збройних сил; культурний конфлікт.

Методи інформаційно-психологічного впливу розвивалися, зокрема, на базі розробленої Джозефом Найемом концепції «м'якої сили», яка будується на принципі: держава може досягти результатів (військово-політичних цілей) шляхом переконання інших країн робити те, що вигідно їй. Така здатність і називається «м'якою силою» на противагу «жорсткій силі» військового примусу. У своїй роботі автор описує цей принцип на прикладі взаємин батьків і підлітка: якщо батьки протягом життя дитини формують її переконання і переваги, то їх вплив буде більш значним і довгостроковим, ніж спроби встановлювати контроль над її життям. За такою логікою політичні лідери забезпечують свій вплив в довгостроковій перспективі за рахунок привабливих ідей, здатності встановлювати вигідний для себе порядок і визначати потрібні рамки переговорів таким чином, щоб формувати переконання і переваги інших у вигідній для себе формі. Можливість формування переконань і уподобань інших людей в масштабах країни забезпечують нематеріальні ресурси влади: культура, ідеологія і міжнародні інститути.

В рамках цієї концепції логічно обґрунтовується наступна ситуація: якщо держава може легітимізувати свою владу в очах інших держав, то вона буде стикатися з меншим протистоянням своїх дій на міжнародній арені. Якщо національна культура і ідеологія привабливі, інші будуть більш охоче їм слідувати. Якщо вона може підтримувати інститути, які змушують інші країни направляти або обмежити свою діяльність таким чином, як вважає за краще домінуюче держава, вона може заощадити на вартості застосування примусової або жорсткої сили.

Інструментами «м'якої сили» для впливу на свідомість людей і зміни їх сприйняття можуть служити публічна дипломатія, пропаганда ідей через ЗМІ та інші. У США з кінця ХХ століття розробляються концепції і стратегії ведення інформаційних операцій, що включають комплексні заходи щодо впливу на цільову аудиторію як всередині Сполучених Штатів, так і за їх межами. Так, Уряд США, визнаючи важливість використання методів психологічного впливу у військових цілях, ще в 2003 році розробили концепцію інформаційних операцій, яка відображена в Доктрині Спільних психологічних операцій Комітету начальників штабів ВС США, згідно з якою, мета психологічних операцій – викликати або посилити думку і поведінку іноземних громадян, яка буде вигідною для цілей ініціатора операцій.

Під психологічними операціями в цьому документі розуміються сплановані операції по розкриттю обраної інформації та показників іноземної аудиторії, з метою вплинути на емоції, мотиви, цілепокладання і поведінку іноземних урядів, організацій, груп та осіб. Психологічні операції є невід'ємною частиною широкого спектра американської дипломатичної, інформаційної, військової та економічної діяльності США.

Виділяють три категорії інформаційних операцій:

- стратегічні (міжнародна інформаційна діяльність, що проводиться урядом для впливу на ставлення, сприйняття і поведінку інших держав в інтересах певної країни);

- операційні (проводяться поряд з військовими операціями, включаючи мирний час в певній зоні для підтримки ефективності кампаній і стратегій Об'єднаних командних сил);

- тактичні (проводяться в зоні тактичного командування поряд з військовими операціями для підтримки тактичної місії проти сил противника).

Всі ці операції в мирний час проводяться без застосування сили або загрози силою, можуть підтримуватися спільними операціями, включаючи державну і недержавну гуманітарну допомогу, іноземну внутрішню оборону, управління наслідками.

5. Хакерське і кібернетичне протиборство – різновид збройної боротьби, в ході якого здійснюється цілеспрямований і організований вплив апаратно-програмними засобами на апаратно-програмні комплекси автоматизованих систем управління військового і цивільного призначення противника, спрямоване на порушення їх нормального функціонування.

В наш час існує безліч видів і інструментів впливу на комп'ютерні мережі і автоматизовані системи управління в мирний час. При цьому інформаційні атаки цивільного характеру загрожують національній і міжнародній безпеці, коли вони проводяться в військово-політичних цілях. Отже, інформаційно-технічні атаки в мирний час можуть привести до втрат, які можна порівняти з втратами під час бойових дій. За допомогою подібних методів державний і недержавний актор може переслідувати і досягати своїх цілей військово політичного характеру.

6. Економічне інформаційне протиборство – застосування інформаційно-технічних засобів і методів боротьби для встановлення контролю, впливу і дестабілізації економічно-фінансової системи держави або її окремих елементів. Виділяють дві основні форми економічного інформаційного протиборства: інформаційна блокада і інформаційний імперіалізм.

Отже, методи інформаційного протиборства є потужною зброєю в руках держав, що розробляють і застосовують ІКТ для досягнення своїх політичних і військових цілей. Різноманіття таких методів і недостатній рівень існуючих міжнародно-правових норм в області регулювання деструктивного використання ІКТ дає можливість державам «приховувати своє обличчя» під різними масками, в тому числі, під маскою тероризму, приховуючи справжні цілі атак.

Використовуючи класифікацію М. Лібікі, наведемо приклади застосування ІКТ у військово-політичних цілях в операціях, що проводяться в Іраку і Афганістані в кінці XXпочатку XXI століть.

Прикладом боротьби з системами управління може служити виведення з ладу командного центру збройних сил і комунікаційних ліній супутникового зв'язку, розрив кабельних ліній зв'язку іракської армії і руйнування фізичних об'єктів командно-управлінських структур Іраку. Засоби космічної розвідки при цьому дозволили визначати ключові елементи інфраструктури супротивника для подальшого наведення на них балістичних і крилатих ракет.

Під час операції «Буря в пустелі» 1991 року спецслужбами США застосовувався широкий спектр інформаційно-розвідувальних операцій, зокрема, так звані «жучки» і «лінки» (links) – спеціальні ідентифікатори, що підключаються до оптико волоконного зв'язку і дозволяють перехоплювати переговори по мобільних станціях частин іракської армії. Інший технологією є підключення до комутаційного центру, який обслуговує декілька оптоволоконних магістральних ліній, що дозволяє перехоплювати переговори терористичного (або військового) керівництва, відстежувати місце розташування, а також забезпечити плацдарм для проведення кібератак на програмне забезпечення комп'ютерів.

Прикладом психологічних операцій служать дії, які велися в період підготовки і здійснення бойових операцій в зоні Перської затоки (1991-1992 роки) за двома напрямками: зовнішньополітична область і безпосереднє інформаційно пропагандистське забезпечення бойових дій. Перший напрямок забезпечував підтримку контрзаходів багатонаціональних сил щодо Іраку, зміцнення позицій антиіракської коаліції і ослаблення супротивника. Другий напрямок був направлений на посилення психологічного тиску, породжуваного військовою обстановкою, що сприяло погіршенню морально-психологічного стану населення і особового складу збройних сил Іраку, зниження їх боєздатності. Психологічний вплив здійснювався із застосуванням цілого спектра засобів, що дозволило мобілізувати світову громадську думку проти Іраку і поглибити розкол в арабському світі.

США є безумовним лідером за обсягом інвестицій в інформаційно-комунікаційні технології, з виробництва та торгівлі інформаційними технологіями і послугами. І в зв'язку з цим є найбільш уразливими в цій сфері. Тому самі Сполучені Штати також протягом багатьох років є жертвою атак. У доповіді Комісії США з кібербезпеки в 2008 році підкреслювалося, що

Важливим прикладом є великі аварії в енергосистемі США в 2003 і 2008 роках, коли територія штатів Мічиган, Огайо, Нью-Йорк виявилися знеструмленими. Від аварій постраждало близько 50 млн. осіб. Експерти вважають, що причиною аварії стали навмисні дії китайського хакера, який працює на Народно-визвольній армії Китаю. З тих пір рівень подібних загроз тільки підвищується. Але якщо раніше Сполучені Штати, спираючись на свою технологічну перевагу, вважали себе здатними самостійно забезпечити свою безпеку від кібератак, то тепер і США розглядають норми поведінки держав в кіберпросторі як додатковий інструмент стримування інших держав і посилення контролю за міжнародною обстановкою в області інформаційної безпеки, що робить досягнення міжнародних домовленостей зі Сполученими Штатами більш перспективними.

## 2.2 Інформаційно-комунікаційні технології (ІКТ) як інструмент терористичної і антигромадської діяльності

З 60-х років XX століття в вживання міцно увійшов термін «інформаційне суспільство». З'явившись приблизно одночасно в роботах японського антрополога Тадао Умесао і австро-американського економіста Фріца Махлупа, це поняття зайняло своє місце в сучасних суспільних науках. Теорія інформаційного суспільства отримала свій розвиток в роботах Д. Белла2 і Е. Тоффлера, які сформулювали основні принципи побудови постіндустріального суспільства, передбачивши глобальну інформатизацію та розвиток інформаційно-телекомунікаційних технологій (ІКТ) як основного локомотива світової економіки в XXI столітті.

Сьогодні людство здійснило небувалий технологічний прорив в області обміну інформацією та створенні глобального і загальнодоступного інформаційного простору. Однак разом з безсумнівним підвищенням продуктивності інтелектуальної праці, повсюдного поширення ІКТ супроводжують загрози, які знаходяться як в сфері несанкціонованого доступу до конфіденційної інформації, так і в області впливу на поведінку конкретних людей-користувачів інформаційно-телекомунікаційних систем.

Найбільш яскравим прикладом використання інтернет-маркетингу сьогодні є пропагандистська робота так званого «Ісламської держави» забороненої в Росії терористичної організації. Сьогодні вона широко представлена в глобальному інформаційному просторі, а її рекламна кампанія визнається досить небезпечною керівниками спецслужб провідних країн світу. Мережева пропаганда ненависті і насильства виявляється ефективним механізмом тиску на органи влади і управління розвинених держав, включених в глобальну інформаційну мережу. На думку багатьох політиків, сьогодні саме терористична, а не військова загроза є провідним фактором міжнародних відносин. Питання ж протидії поширенню ідеології тероризму лежать не тільки у військовій сфері та питаннях правового регулювання в інформаційно-телекомунікаційній мережі Інтернет, а й, можливо і в більшій мірі, в області соціальних наук і психології.

Революція зростаючих очікувань – термін, що вперше з'явився ще в роботі А. Токвілля «Революція і старий порядок», де автор звернув увагу на істотне підвищення рівня життя французів в період, що передує Великій Французькій революціі. Подальший розвиток теорія «революції зростаючих очікувань» отримала в роботах Дж. Девіса. В сучасній політології ця теорія іноді називається «психологічною». Суть її полягає в тому, що революційні настрої з'являються у населення в ситуації стабільного зростання рівня життя, який супроводжує і зростання потреб. Так як задовольнити постійно зростаючі запити громадян неможливо, вони відчувають стан незадоволеності (фрустрації). Залежно від інтенсивності фрустрації змінюється ймовірність революційного сценарію.

Разом з тим дослідження, проведені американським соціальним психологом Ф. Мохаддамом, наочно демонструють, що ті ж самі психологічні механізми покладені в основу пропаганди ідеології так званого «Ісламського тероризму». Саме на осіб, які найбільш гостро переживають стан відносної депривації, ідеологічна обробка має найбільш сильний вплив.

У сучасному світі створення протестного настрою в суспільстві або вербування бойовиків терористичних організацій цілком може бути здійснене і без участі великих державних або фінансових структур. Більш того, розвиток соціальних мереж і маркетингових технологій в інформаційному просторі породило новий вид товару: мережеві спільноти. Часто їх адмініструванням займаються люди, далекі від ідеології, метою яких є задоволення запиту користувачів на протест і опозиційність. Такі мережеві структури, які є безпосередньо пов'язаними з екстремістськими або терористичними організаціями, небезпечні тим, що працюють на естетизацію деструктивної ідеології, втілюючи їх у привабливу для споживача оболонку. Створення в мережі різного роду «демотиваторів», «фотожаб» та інших продуктів з явним деструктивним підтекстом може мати на окремих членів товариства не менший негативний вплив, ніж провокаційні карикатури скандального французького видання «Charlie Hebdo».

Небезпека поширення деструктивної ідеології полягає не тільки в спонуканні окремих осіб до вчинення злочинних актів, а й у формуванні у широких народних мас хибних моральних орієнтирів, що цілком здатні привести суспільство і державу до чергових політичних і економічних потрясінь. Експлуатуючи образ безкорисливих борців за суспільне благо, лідери терористичних організацій отримують необхідний елемент здійснення політичного впливу.

Широкі суспільні верстви схильні довіряти безкорисливим акторам, нехай і з екстремістськими гаслами, протиставляючи їх корумпованим представникам владних еліт. Відповідно до теорії Нобелівського лауреата 2001 р. Ендрю М. Спенс, витратні сигнали набувають особливої ​​достовірності для реципієнта, якщо йому відомо, що вони дорого обійшлися тому, хто їх посилає. Таким чином, навіть які скоїли тяжкі та безглузді на перший погляд злочини з ідеологічних мотивів особи, які заплатили за свої переконання «високу ціну», охоче сприймаються аморфним і неструктурованим протестним електоратом як «моральні орієнтири» і зразки для наслідування, що є одним з основних засобів управління масами.

Останнім часом значне поширення отримують саме технології інтерактивного впливу, які є більш привабливими для користувачів. У об'єкта впливу створюється ілюзія власної участі в тих чи інших віртуальних процесах, ілюзія власної значущості. Разом з тим, власники відповідних ресурсів за допомогою інтерактивних технологій здійснюють додаткове вивчення цільової аудиторії, аналізуючи реакції користувачів на поданий для них матеріал. З розвитком технологій аналіз великих обсягів інформації, частка інтерактивних сервісів неухильно зростає.

Для поширення деструктивної інформації використовуються методи мовного маніпулятивного впливу. Звернення до авторитету, тобто апеляція до різного роду офіційної або експертної інформації, що підвищують довіру аудиторії до поданого матеріалу, як до позитивного, так і до негативного, дозволяє вводити тезу або аргумент в процесі аргументування, не наводячи обгрунтувань їх істинності, грунтуючись на довірі адресата до авторитету як майже ідеального наприклад хорошого або поганого.

Нав'язування пресупозиції полягає у введенні в свідомість людини, в її уявлення про дійсність деяку інформацію, що не піддається критичному аналізу, не усвідомлюється ним як щось, що вимагає обговорення.

Метафора полягає в образному порівнянні об'єкта з метою позначити твку властивість, правомочність якої не обговорюється. Натяк використовується в імпліцитно мовному психологічному впливі на реципієнта, направленому на вироблення у нього певного і бажаного розуміння тез, заснованих на здогадці. Натяк передає в непрямій формі деякий зміст, використовуючи модель світу реципієнта, його знання про ситуацію і інструменти дійсності, зрозумілі йому терміни.

Формування негативних установок по відношенню до різних соціальних груп, закріплення за ними різко негативних характеристик полягає в усвідомленому неодноразовому і нічим не підкріпленому використанні різко негативних визначень по відношенню до національної групи.

Соціальні мережі як один з результатів розвитку комунікаційних технологій є унікальним і значущим інструментом спілкування, яке отримало людство в XXI столітті. В епоху Web 2.0 соціальні мережі і блоги є одним з найважливіших джерел інформації. Прискорений розвиток інформаційно-комунікаційних технологій (ІКТ) призвів до того, що доступ до соцмереж перестав обмежуватися певним колом осіб. Статистика показує, що не тільки соцмережі, але і блоги почали активно витісняти новинні агентства і тематичні сайти. Переважна більшість людей використовують їх в мирних цілях: інформування населення, реклама, маркетинг, поширення ідей, пропаганда загальноприйнятих цінностей і ін. Але цілком закономірно, що, як і будь-яке нове досягнення людства, соцмережі використовуються і у шкідливих цілях. Таким чином, зловмисники, злочинці і терористи здобули новий інструмент для здійснення своїх задумів.

Одна з найважливіших загроз пов'язана з тим, що соцмережі можуть використовуватися як інструмент інформаційно-психологічного впливу, тому що надають дуже багато інформації про особу користувача. Крім того, існують широкі можливості по розповсюдженню візуальних і аудіматеріалов, а також пошуку користувачів в соцмережі за певним параметром: вік, стать, місце проживання, освітній заклад, політичні погляди, віросповідання та ін. Інформація в соціальних мережах часто розміщується без посилання на джерело, відповідно, інформація може бути не достовірною, неактуальною або неповною. Таким чином, виникає загроза дезінформації населення через соціальні мережі в Інтернеті.

Соцмережі стають майданчиком для здійснення шкідливого впливу, тому що мають ряд властивостей, які роблять їх уразливими. Це можливість створення облікових записів вигаданих персонажів, що ускладнює ідентифікацію. Це недосконалість системи контролю над інформацією в соцмережах: часто користувачі не дотримуються правил використання соцмереж, незважаючи на те, що дають такі зобов'язання при реєстрації. Це прихованість особистого листування користувачів. Крім того, інформація в соцмережах часто розміщується без посилання на джерело, відповідно, виникає загроза навмисної дезінформації населення. При цьому Інтернет дає унікальні небувалі можливості для здійснення дистанційного впливу як цілеспрямованого перенесення інформації від одного учасника взаємодії до іншого. Причому дистанція практично не обмежена. Крім того, мова йде про одночасний вплив на багатотисячну, а то і мільйонну аудиторію, яку практично неможливо зібрати в одному місці фізично.

І таким чином комп'ютерні мережі використовуються для здійснення інформаційно-психологічного впливу як комплексу психологічних операцій за допомогою спеціально підготовленої інформації, пропаганди та агітації. Аналіз застосування широкого спектра подібних методів в Грузії в 2003 і 2008 роках, а також на Україні в 2004 і 2013 році, доводить, що підготовка ключових подій цих процесів були відзначені зростанням ролі соціальних мереж з боку громадян РФ.

Дослідження з виявлення й аналізу механізмів використання методів інформаційно-психологічного впливу в соцмережах, алгоритмів їх використання, моніторингу таких загроз інформаційній безпеці від використання соцмереж як рекрутинг (вербування) нових прихильників в терористичні організації; дезінформація населення; розміщення у відкритому доступі екстремістської та іншої інформації, що завдає шкоди психічному здоров'ю і розвитку дітей та молоді, є в даний час дуже актуально.

Крім того, необхідно розробляти методики виявлення випадків розміщення інформації, що не носить протиправний характер, але при цьому відповідає ознаками методів здійснення інформаційно-психологічного впливу.

Соціальні мережі можуть використовуватися як інструмент інформаційно-психологічного впливу (ІПВ), адже мають ряд ознак, які роблять їх оптимальним майданчиком для його здійснення:

- користувачі публікують в мережі інформацію про себе, про коло свого спілкування, про свої інтереси;

- користувачі об'єднуються в спільноти за інтересами;

- є можливість поширення візуальних та аудіовізуальних матеріалів;

- є можливість ведення публічного спілкування на певну тему;

- є можливість пошуку користувачів у соціальній мережі за певним параметром: вік, стать, місце проживання, освітній заклад, політичні погляди, віросповідання та ін.

Соціальні мережі мають ряд властивостей, які роблять їх уразливими до дій злочинців:

- можливість створення облікових записів вигаданих персонажів, що ускладнює ідентифікацію того, хто розміщує контент або розсилає повідомлення;

- недосконалість системи контролю за інформацією, що розміщується в соціальних мережах, фактично користувачі користуються повною свободою слова, не дивлячись на те, що зобов'язуються дотримуватися правил використання соціальної мережі;

- особисте листування користувачів не контролюється.

В даний час існують різні програмні засоби для моніторингу соціальних мереж і блогів в мережі Інтернет. Пошукові системи не мають функцію пошуку по соціальним мережам, блогам і мікроблогам, тому виникає необхідність у таких програмних засобах. Для проведення даного контент-аналізу використовувався сервіс моніторингу соціальних мереж IQBuzz, який представляє собою інтернет-сайт, доступ до якого можливий за наявністю облікового запису користувача. При вході на сайт створюється рубрика, задаються параметри пошуку. У рубриці задаються пошукові критерії: ключові слова, дата створення документів (під документами в даному сервісі розуміються будь-які текстові повідомлення, розміщені в соціальних медіа), тип документів.

Перелічимо основні вимоги, що визначають образ сучасної системи контролю оперативної обстановки в Інтернеті.

I. Контроль оперативної обстановки в Інтернеті і соціальних мережах.

Система повинна автоматично збирати найбільш важливі новини за тематикою, визначеною керівником, в тому числі факти підготовки та проведення кібератак, рівень захищеності власних інформаційних ресурсів, загрози бізнесу, репутації і сталого розвитку компанії. Список тематик і об'єктів інтересу визначає сам керівник.

II. Зручний інтерфейс керівника для презентаційних екранів, а також планшетів і смартфонів.

Керівник повинен мати доступ до екрану системи по захищеному каналу з будь-якого місця офісу, автомобіля, у відрядженні і т.д. Повинен бути реалізований зручний графічний інтерфейс для оперативного контролю обстановки. Кожна новина представлена ​​з фотографією, заголовком, коротким змістом, датою і часом появи, посиланням на першоджерело та поточною кількістю дублів в ЗМІ. Зручний графічний інтерфейс дозволяє вибирати стрічки новин і тематичні блоки рухом пальця.

III. Автоматичне визначення рівня загроз.

Кожен тематичний блок повинен бути забезпечений індикаторами рівня загроз.

IV. Автоматичне ведення досьє на об'єкти інтересу.

Система повинна автоматично накопичувати досьє на різноманітні питання, що цікавлять спостерігача, а також дозволяє окремо відстежувати дані про номери телефонів, акаунти в соціальних мережах, адреси електронної пошти, банківські рахунки і т. ін.

V. Виявлення зв'язків об'єктів і першоджерел новинних вкидань.

Система повинна дозволяти виявляти і накопичувати інформацію про різноманітні зв'язки об'єктів інтересу.

Необхідна можливість побудови ланцюжків зв'язків між об'єктами, навіть якщо їх взаємозв'язок на перший погляд неочевидний.

VI. «Теплова карта» ворожої активності в соціальних мережах.

Система дозволяє контролювати хід поширення інформації і будувати так звану «Теплову карту» активності обговорення ключових новин з урахуванням позитивної та негативної тональності обговорення.

VII. Виявлення резонансних тем в соціальних мережах та ЗМІ.

Система повинна давати можливість проводити порівняльний аналіз згадок різних персон і компаній, активності обговорення цільових новин в ЗМІ та соціальних групах.

VIII. Управління роботою мобільних штабів.

Система повинна забезпечувати організацію роботи мобільних оперативних штабів в найстисліші терміни (в тому числі нарад територіально розподілених підрозділів, міжвідомчих груп і т.д.).

IX. Робота з великими даними (BigData).

Система повинна дозволяти проводити складну аналітичну обробку великих обсягів даних і відображати підсумкові результати в графічному вигляді, зручному для сприйняття керівником.

X. Автоматична генерація дайджестів і звітів.

Система повинна дозволяти автоматично формувати довідки, дайджести та звіти по заданих темах і активності об'єктів інтересу.

## РОЗДІЛ 3

## МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 3.1 Формування міжнародних режимів інформаційної безпеки на різних рівнях світової політики

Міжнародне співробітництво щодо забезпечення інформаційної безпеки на глобальному рівні наштовхується на протиріччя в державних інтересах. Від позицій держав, як найбільш впливових акторів світової політики, залежить перспектива формування глобального режиму щодо забезпечення інформаційної безпеки. Як відзначають дослідники, найчастіше відсутність інституційно або формально закріпленого режиму відображає інтереси окремих держав, що прагнуть зберегти лідерство в якій-небудь області.

Схожою стратегією може бути підтримка формування безлічі розрізнених організацій та інститутів, що регламентують взаємодію в окремій галузі міжнародних відносин, так як це дозволяє вибирати різні норми і правила взаємодії, зафіксовані в цих угодах, в залежності від ситуативних інтересів. Схожа ситуація склалася в сфері забезпечення міжнародної інформаційної безпеки та управління Інтернетом, де сформувалося безліч функціональних і ряд регіональних режимів.

Зарубіжні експерти в якості ключових суб'єктів міжнародного співробітництва в області інформаційної безпеки називають такі країни – США, Росія, Китай, а також країни ЄС (Великобританія, Франція і Німеччина) [9], відзначаючи, що вони мають найбільший потенціал в цій галузі. Більш того, вони також виступають в якості найбільш активних учасників переговорного процесу.

Зарубіжні експерти з великою стурбованістю відзначають загострення протиріч між США і Китаєм у сфері забезпечення інформаційної безпеки [12]. Ці дві держави пропонують два різних бачення проблеми забезпечення інформаційної безпеки. Якщо Китай виступає за державне регулювання інформаційної сфери та забезпечення інформаційної безпеки на підставі міжнародних договорів, то США вважають за краще приватну модель регулювання і ухиляються від визнання військово-політичної складової інформаційної безпеки, роблячи акцент на терористичному і злочинному компонентах.

Для країн, що розвиваються в ході міжнародних переговорів, як правило, пріоритетними є питання інформаційного розвитку і скорочення «цифрового розриву», допомоги в створенні «цифрових потенціалів». На сьогоднішній день США є державою-лідером в області розвитку ІКТ і, отже, не зацікавлені в прийнятті на себе міжнародних зобов'язань у цій сфері.

В наш час склався державно-приватний режим управління інтернетом, в рамках якого функції технічної координації простору імен і адрес інтернету покладені на ICANN, некомерційну організацію, зареєстровану в США і яка формально підпорядковується законам США. Зараз все більша кількість держав оскаржують роль ICANN в управлінні Інтернетом, бачачи в ній інструмент впливу США. Відзначимо, що режим управління інтернетом історично формувався при вагомому впливі експертного співтовариства (так званої «інтернет-спільноти») дослідників і інженерів, проте зараз деожави прагнуть відігравати в управлінні Інтернетом більш істотну роль.

З позицій теорії міжнародних режимів період домінуючого впливу організацій «інтернет-спільноти» був періодом навчання, формування базових принципів регулювання, оскільки США і їх союзники не були впевнені в тому, яким чином слід здійснювати управління цією новою технологією, тому вони надали свободу дій експертам.

Зупинимося детальніше на прогнозах розвитку режиму управління інтернетом в цілому і ICANN зокрема, пропонованих різними дослідниками і аналітиками. Більшість дослідників погоджується з тим, що ВСІС і робота Форуму з питань управління Інтернетом ознаменували початок нового етапу в даному процесі, який буде характеризуватися втратою США свого впливу і посиленням позицій урядів інших держав. Можливі два варіанти: або ICANN збереже свій вплив (можливо, при цьому їй доведеться значно модифікувати свою структуру і склад), або ж функції технічної координації інфраструктури інтернету перейдуть до міжурядової організації.

Прихильники точки зору, згідно з якою ICANN в майбутньому перестане існувати, по-різному бачать майбутній розвиток режиму управління інтернетом. Зокрема, висловлюються припущення, що управління Інтернетом буде передано міжурядовій організації з глобальним охопленням дій, можливо, МСЕ. Розглядається також і такий варіант, що в результаті розвитку глобального ринку електронної комерції, проблеми економічної конкуренції вийдуть на передній план у процесах управління інтернетом і ICANN може стати набагато менш впливовою організацією в даній області в порівнянні, наприклад, з СОТ. Складаються сприятливі умови, щоб передати контроль управління інтернетом до МСЕ.

Отже, можна сказати, що інтернаціоналізація управління інтернетом в тій чи іншій формі неминуча. Однак очевидно, що США, які розглядають втрату контролю над Інтернет-простором як одну із загроз національній безпеці країни, зроблять все можливе, щоб зберегти контрактні відносини з ICANN і свій вплив в рамках режиму управління інтернетом. ICANN – приватна некомерційна організація, рішення якої мають значні економічні, політичні та суспільні наслідки і саме її статус став джерелом проблем, що перешкоджають її ефективному виконанню своїх функцій. На прикладі ICANN можна простежити, наскільки тісно переплетені між собою технічні та політичні аспекти в інтернет-просторі, часто їх неможливо розділити. Ще в 1999 р. авторитетний юрист в області інтернет-права Л. Лессіг відзначив той факт, що політичне і технічне регулювання інтернету невіддільні одна від одної. «Кіберпростір вимагає нового розуміння того, яким чином здійснюється регулювання і що регулює життя тут ... У реальному світі регулювання здійснюється за допомогою законів, а в кіберпросторіе – за допомогою програмного коду. У кіберпросторі програмне забезпечення – це закон»[11, с. 17]. Л. Лессіг також застерігав, що в міру того як сучасне суспільство дедалі більше потрапляє залежність від інтернету, зростає і небезпека того, що суспільні відносини будуть регулюватися програмним кодом, а не законодавчими нормами [10, с. 17].

Подібний підхід видається деяким перебільшенням, однак не можна не погодитися з тим фактом, що будь-яке технічний рішення завжди має політичні наслідки, так як воно сприяє просуванню певних інтересів і підсилює позицію тих чи інших груп як на міжнародній арені, так і всередині держави.

Можна виділити два підходи до того, яким чином існуючі правові норми застосовні до інформаційного простору.

1.) «Реальне» право – підхід, в рамках якого Інтернет розглядається як явище, аналогічне попереднім йому технологіям комунікації (які пройшли в своєму розвитку довгий шлях від сигнальних багать до телефону). Хоча Інтернет швидший і масштабніший, він як і раніше є способом дистанційного спілкування між окремими людьми. Отже, будь-які існуючі правові норми можуть застосовуватися і по відношенню до Інтернету.

2.) «Кіберправо» виходить з припущення, що Інтернет породив нові види соціальних взаємин, що здійснюються в кіберпросторі. Отже, для їх регулювання виникає необхідність формулювати нові «кіберзакони». Доказом на підтримку цього підходу є той факт, що неймовірна швидкість і обсяг міжнаціонального спілкування, яке ведеться за допомогою Інтернету, перешкоджає застосуванню існуючих правових норм [6, с. 85].

Згідно найбільш поширеній думці, велика частина існуючого законодавства може застосовуватися по відношенню до Інтернету. Однак в ряді випадків існуючі в реальному світі правові норми доведеться видозмінити для того, щоб мати можливість застосувати їх до кіберпростору. Для інших, вужчих проблем необхідна розробка абсолютно нових законів [6, с. 85]. Разом з тим, в сучасних умовах проблема адаптації міжнародного права до інформаційної сфери є вкрай політизованою, що пов'язано з міждержавними протиріччями.

Незважаючи на специфічні характеристики ІКТ, що випливають з Статуту ООН загальновизнані принципи міжнародного права jus cogens і відповідні норми міжнародного права, а саме невтручання у внутрішні справи держав і незастосування сили і загрози силою залишаються непорушними як в традиційному, фізичному, так і цифровому просторі.

Зупинимося детальніше на питаннях застосування існуючого корпусу міжнародного гуманітарного права до інформаційної сфери, перш за все, до застосування інформаційної зброї проти об'єктів критичної інформаційної інфраструктури. Інформаційні війни за багатьма параметрами відрізняються від протистояння держав в «реальному» світі. Проте це не відміняє необхідності нормативно-правової регламентації. Багато з положень міжнародного гуманітарного права були вироблені стосовно до звичайних умов ведення війни і в сучасних умовах вимагають удосконалення. Право збройних конфліктів, незважаючи на свою відірваність від політичної практики, визначає правила цивілізованого ведення збройних дій.

Тим часом існує нагальна потреба у виробленні правил регулювання конфліктів в інформаційній сфері. Це пов'язано з тим, що інформаційні атаки за своїми наслідками стають все більш масштабними, створюючи реальну загрозу безпеці держави. Більш того, учасниками інформаційних конфліктів можуть бути не тільки держави, а й неурядові учасники, в тому числі терористичні угруповання. На цей час існує безліч міжнародно-правових актів, що регулюють відносини держав в період збройного конфлікту. До розглянутих в роботі групи експертів джерел міжнародного гуманітарного права віднесені: Женевська конвенція 1964 року про поліпшення стану поранених на полі бою, Гаазька конвенції 1899 і 1907 рр. про закони і звичаї сухопутної війни, Женевський протокол 1928 року про заборону використання на війні задушливих газів і бактеріологічної зброї, Женевська конвенція 1949 року про поліпшення стану поранених і хворих і членів екіпажу суден на морі, Женевська конвенція 1949 року про поводження з військовополоненими, Женевська конвенція 1949 року про поліпшення становища цивільного населення під час війни, Женевська конвенція 1975 про заборону розробки створення і зберігання бактеріологічних і токсичних озброєнь і їх знищення, Додаткові протоколи до Женевських конвенцій 1977 року про захист жертв міжнародних збройних конфліктів, про захисту жертв неміжнародних збройних конфліктів, Додатковий протокол 2005 року про вживання додаткових відмітних знаків.

Отже, міжнародне гуманітарне право застосовується до захисту об'єктів критичної інформаційної інфраструктури, що використовується в цивільних цілях, як, наприклад, інформаційні ресурси і системи, що забезпечують роботу госпіталів і лікарень. Відзначимо, що серед критичних інформаційних інфраструктур можна виділити лише незначну кількість систем, що використовуються виключно в цивільних цілях, що звужує можливість застосування норм гуманітарного права. Велика частина може використовуватися як у цивільній, так і у військовій сферах, внаслідок чого норми права потребують доопрацювання.

Цивільні інформаційні ресурси і системи не володіють відмінними знаками, що потенційно підвищує їх уразливість і знижує ступінь захисту. У більшості випадків в інформаційній сфері складніше визначити цивільні об'єкти, так як в наступальних і оборонних операціях можуть бути задіяні цивільні об'єкти. Відповідно до джерел міжнародного гуманітарного права, військовим вважаються об'єкти, «які в силу свого характеру, розміщення, призначення або використання вносять ефективний внесок у військові дії і повне або часткове руйнування, захоплення чи нейтралізація яких за існуючих в даний момент обставин дає певну військову перевагу».

Майже всі держави розглядають інформаційну безпеку об'єктів критичної інфраструктури як проблему національної безпеки. Відзначимо, що, незважаючи на прогалини в міжнародному праві, інформаційна безпека в більшості країн регулюється внутрішніми законодавчими нормами. Піонерами в даному контексті є США, в яких після подій 11 вересня 2001 р. безпека критичних інформаційних інфраструктур починає розглядатися в контексті антитерористичної стратегії.

Група американських вчених виробила наступні рекомендації щодо міжнародно-правової регламентації інформаційної сфери:

1) залучення приватного сектора і неурядових організацій до впровадження заходів по розділенню захищених і незахищених інфраструктур;

2) необхідність використання відмітних знаків для захищених об'єктів в інформаційній сфері;

3) слід визнати зростання впливу недержавних акторів і користувачів Інтернету [13].

Підводячи підсумок розгляду застосовності міжнародного гуманітарного права до інформаційних війн, відзначимо, що, незважаючи на те що більша частина його положень розроблялася по відношенню до звичайних озброєнь, його положення розроблялися з метою гуманізувати війну, уникнути страждань мирного населення, тому якщо вони і застаріли, то лише формально, але не по суті.

## 3.2 Перспективні тенденції забезпечення інформаційної безпеки

За останній час з'явилася значна кількість публікацій з різних аспектів інформаційної безпеки. Дійсно, ця проблематика набуває все більшої актуальності. Пов'язано це з кількома обставинами. Стрімкий розвиток і використання інформаційно-комунікаційних технологій (ІКТ) мало вирішальне значення для переходу від індустріального до постіндустріального, інформаційного суспільства, що відкриває найширші позитивні можливості для прогресивного розвитку людини, суспільства, держави і міжнародного співтовариства в цілому, поширення процесів демократизації, досягнення стійкого економічного зростання. Динамічне розширення інформаційного сектора спричинило за собою серйозні зміни в структурі світової економіки.

Індустрія інформатизації і телекомунікацій, інформаційних послуг на сучасному етапі розвитку людства є однією з сфер світової економіки, що найбільш стрімко розвиваються. Вона зробила ринок значно масштабнішим, динамічним і конкурентним, дала стимул до зародження безлічі нових видів бізнесу. ІКТ за своєю природою є унікальним засобом обробки, зберігання та передачі інформації з виходом на практично необмежену аудиторію. Ця можливість дозволяє урядам надавати громадянам послуги в рамках програм електронного уряду (e-government); організаціям – інформувати про свою діяльність, впроваджувати в виробничі процеси і процеси виконання робіт та надання послуг безпаперові технології (так звані CALS-technologies), переходити на методи електронної комерції; банківським і фінансовим установам – надавати послуги управління банківським рахунком через Інтернет, здійснювати, задіявши інформаційні канали, платежі в режимі реального часу; громадянам – брати участь в процесах прийняття політичних рішень, ефективно шукати і отримувати інформацію, поширювати результати своєї творчої праці, вступати в віртуальні спільноти відповідно до своїх інтересів.

Сьогодні правомірно стверджувати: чим більші можливості в інформаційній сфері має держава, тим з більшою ймовірністю при інших рівних умовах вона може досягти стратегічних геополітичних переваг і економічного процвітання. Разом з тим глобальна інформатизація може в ряді випадків прямо або опосередковано призводити до негативних наслідків: посилення «цифрового розриву» – нерівності в рівнях розвитку і впровадження ІКТ, а також доступу до них як між різними державами, так і всередині окремих країн (саме такий – внутрішньодержавний – «цифровий розрив» характерний для України на сучасному етапі), що може спричинити за собою подальшу поляризацію світу; розмивання поняття суверенітету держав; ослаблення національної безпеки країн; порушення основних прав і свобод людини в інформаційній сфері.

Висока складність і одночасно уразливість всіх систем, на яких базуються національний, регіональний та світовий інформаційні простори, а також фундаментальна залежність від їх стабільного функціонування практично всіх інфраструктур держав як в цивільному, так і в оборонному секторі, в тому числі критичних, призводять до виникнення принципово нових загроз. Особливі побоювання пов'язані з можливістю використання ІКТ в злочинних, терористичних і ворожих військово-політичних цілях проти інформаційних ресурсів і інфраструктур.

Незважаючи на зусилля правоохоронних органів і спецслужб, які спрямовані на боротьбу з кіберзлочинністю і кібертероризмом, число злочинних актів з використанням ІКТ не зменшується, а, навпаки, постійно збільшується, зростає їх суспільна небезпека. В наш час в світі налічуються десятки тисяч різних вірусних програм і їх модифікацій, збільшується кількість зломів баз даних і мережевих ресурсів компаній, ростуть загрози розкрадання конфіденційної інформації.

ІКТ вже освоєні міжнародними терористичними і екстремістськими організаціями (ХАМАС, Аль-Каїда). ІКТ надають терористам можливість потай, планомірно і ефективно впливати на індивідуальну і масову свідомість, громадську думку, процеси прийняття рішень; поширювати інформацію для вербування в свої ряди нових членів, пропаганди власних ідей; здійснювати збір коштів для фінансування своєї діяльності; проводити дезінформацію; викликати паніку, а також безпосередньо здійснювати терористичні акти. ІКТ дозволяють терористичним групам, більшість з яких мають в наш час мережеву організаційну структуру, яка може ефективно і приховано здійснювати взаємодію між її розрізненими осередками та окремими членами, проводити збір інформації про майбутні цілі.

Відбувається трансформація всієї військової інформаційної архітектури: спостерігається «інформатизація» традиційних збройних сил і «інтелектуалізація» озброєнь. Активно розвивається концепція сетецентричного ведення військових дій, що передбачає досягнення переваги над ворогом шляхом ефективної організації збору, обробки та використання інформації.

Можна прогнозувати, що в майбутньому частка інформаційного протиборства при проведенні військових операцій буде зростати. Використання інформаційної зброї не вимагає великих фінансових витрат, що робить інформаційну війну небезпечним засобом збройної боротьби. Інформаційна зброя стирає відмінності між військовими цілями і цивільними об'єктами, що обумовлено значною взаємозалежністю військових і цивільних інформаційних інфраструктур. Можна припустити, що в майбутньому високотехнологічні цивільні інформаційні системи, які в тому числі підтримують роботу критичних цивільних інфраструктур, стануть все більш частими цілями нападів з боку можливих супротивників. З іншого боку, той факт, що у військовому секторі багатьох країн використовуються комерційні програмні продукти, які майже завжди мають вади в захисті, робить обороноздатність держав потенційно вразливою для комп'ютерних нападів як хакерів і терористів, так і держав

Існуючі багатосторонні механізми, спрямовані на забезпечення інформаційної безпеки, недостатні для ефективного вирішення питань міжнародної інформаційної безпеки, адекватним загрозам у цій сфері. Підхід, який передбачає багатоаспектне і всебічне забезпечення інформаційної безпеки на національному, регіональному та глобальному рівнях в прив'язці до тріади загроз військово-політичного, кримінального та терористичного характеру, полягає в ефективній протидії загрозам в інформаційній сфері за рахунок кодифікації і прогресивному розвитку відповідних норм міжнародного права для забезпечення ефективного регулювання відносин, що виникають в інформаційному просторі, на базі продовження консультативного і переговорного процесів на двосторонньому, регіональному і міжнародному рівнях, в тому числі шляхом вироблення і прийняття нового політико-правового документа, такого як принципи діяльності або кодекс поведінки держав в галузі міжнародної інформаційної безпеки, багатостороннього договору про боротьбу з інформаційним тероризмом, а в перспективі – юридично обов'язкового міжнародного договору, що регулює відносини в галузі міжнародної інформаційно й безпеки.

При цьому, роблячи необхідні зусилля на міжнародному рівні в напрямку зниження загроз інформаційній безпеці, які мають зовнішній характер і можуть виходити як від злочинців, терористів, так і від окремих держав, вкрай важливо вести роботу всередині країни щодо зміцнення інфобезпеки на національному рівні.

## 3.3 Пріоритети удосконалення інформаційної безпеки України

Фактором, що послаблює здатність держави нейтралізувати загрози, є посилення взаємозалежності країн та їх відкритість до зовнішніх впливів. Здебільшого держава перестає бути монополістом на власній території, її інформаційна політика все більш обмежується, корегується, нівелюється діями інших держав, міжнародних та недержавних організацій, неформальних об’єднань негативної спрямованості, кримінальних угруповань тощо. Слабка ідеологічно, інституційно, економічно держава не здатна скористатися технологічними, економічними, соціокультурними перевагами глобалізації, проте активно переймає її негативні риси [2].

Розвиток глобальних процесів на основі всеосяжної інформатизації створює широку різноманітність інформаційних загроз – від витіснення на внутрішньому інформаційному ринку вітчизняних продуктів більш конкурентоспроможними аж до ведення цілеспрямованих інформаційних війн. Сучасна інформаційна революція розгортається на фоні інформаційних війн, які своєю головною метою ставлять підрив національної безпеки держав. З урахуванням таких підходів безпекова інформаційна функція держави в усіх регіонах світу набуває особливої важливості [3].

Наявна ситуація в світовому інформаційному просторі обумовлена наступним: більшість країн світу зіштовхнулася з проблемами кібертероризму, кіберзлочинності та іншими проблемами інформаційної безпеки; протягом останніх десятиліть спостерігається тенденція до поширення інформаційної агресії і насилля; набувають поширення агресивна реклама, спроби маніпуляції свідомістю людини, періодично проводяться інформаційно-психологічні операції; майже у 120 країнах світу (за оцінками американських експертів) ведуться розробки інформаційної зброї або її елементів (для порівняння – розробки зброї масового знищення здійснюються у близько 20 країнах); наслідки використання сучасної інформаційної зброї (згідно з висновками вчених та експертів європейських країн, України, РФ і США) можуть бути зіставленими із застосуванням зброї масового ураження; новітні виклики і загрози в інформаційній сфері становлять реальну загрозу безпеці людства та міжнародному правопорядку [4, с. 3-7].

Аналіз аспектів розвитку інформаційного суспільства, інформаційної глобалізації та інформаційного протистояння в сучасних умовах загалом засвідчив наявність низки проблем організаційно-правового змісту у сфері інформаційної безпеки України, а саме: недосконалість державної політики з питань інформаційної безпеки: відсутність стратегічного рівня забезпечення інформаційної безпеки; неналежний рівень інформаційного супроводження зовнішньої та внутрішньої політики України; відомчу автономність державних органів та установ, на які покладено завдання забезпечення інформаційної безпеки України, дублювання їх повноважень та недостатня якість наявної координаційної складової; відсутність дієвих механізмів експертної оцінки інформаційної продукції, поширення якої створює загрозу інформаційній безпеці щодо прав людини, інтересам суспільства та держави; відсутність ефективних механізмів залучення громадськості та приватного сектору України до протидії негативним інформаційним впливам, міжнародної співпраці у цій сфері; наявність законодавчих та організаційних прогалин у сфері обігу інформації з обмеженим доступом.

При цьому сучасні виклики інформаційній безпеці України зумовлені як внутрішніми, так і зовнішніми чинниками: внутрішні – найбільшою мірою пов’язані з відсталістю інформаційних технологій в Україні від провідних країн світу, низьким рівнем інформатизації, розпорошеністю повноважень органів державної влади та законодавства в інформаційній сфері; зовнішні – загальносвітові тенденції створення та застосування інформаційних технологій та намаганнями іноземних суб’єктів впливати на світовий та вітчизняний інформаційний простір з метою забезпечення власних інтересів, залежність від іноземного програмного забезпечення.

Відтак, на сучасному етапі Україні слід зосередитись на двох основних напрямах: зробити внутрішній український простір сучасним, повноструктурним та конкурентоспроможним; забезпечити інформаційну присутність держави в світі та просувати її позитивний імідж. Забезпечення національної безпеки здійснюється за умови пріоритетності національних інтересів, необхідності своєчасного вжиття заходів, адекватних характеру і масштабам загроз цим інтересам, і ґрунтується на засадах правової демократичної держави.

А оскільки інформаційна безпека є частиною національної, то тут теж повинен бути пріоритет національних інтересів в інформаційній сфері. Незважаючи на те, що на сьогодні науковцями виділяється дві складових забезпечення інформаційної безпеки – активна і пасивна (розвиток і захист) [5], у переважній більшості, система працює на протидію загрозам, тобто на пасивну складову. Проте, аналіз практики країн ЄС свідчить про те, що інформаційна безпека повинна бути побудована на моделі стратегічного мислення: вжиття заходів для захисту цілей, їх утримання й забезпечення безпеки на основі принципів демократії, прав людини, захищеного Інтернету.

Разом з тим, інформаційна безпека є невід’ємним напрямом розбудови інформаційного суспільства, розвиток якого повинен відбуватись не тільки через нарощування технологічних можливостей інформаційного обміну, але й через її глибоке усвідомлення усіма суб’єктами інформаційних відносин. Як наслідок, до проблем інформаційної безпеки на цьому етапі починають долучатися питання інформаційної етики, забезпечення приватності в умовах інформаційного суспільства, захисту від маніпулятивних інформаційних впливів тощо.

Відтак, основними напрямами державної політики з питань національної безпеки України в інформаційній сфері є: забезпечення інформаційного суверенітету України; вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до запобігання і протидії корупції, зловживанням службовим становищем, іншим явищам, які загрожують національній безпеці України; забезпечення неухильного дотримання конституційних прав на свободу слова, доступ до інформації, захист персональних даних, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність ЗМІ та журналістів, заборони цензури, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції, за виконання професійних обов’язків, за критику; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України [6].

Захист інформаційного суверенітету України виділяється як один із пріоритетних напрямів забезпечення національної безпеки. Проте законодавство не містить адекватного тлумачення зазначеного поняття, як і конкретних механізмів його забезпечення. Так, на сьогодні взагалі відсутній механізм ефективного та швидкого блокування (обмеження доступу) ресурсів з протиправним контентом, зокрема розміщених на технічних майданчиках за кордоном, як і власне визначення шкідливого контенту. Окрім цього, відсутній механізм запобігання та протидії поширенню інформаційної продукції антиукраїнського змісту, шляхом визначення загальних критеріїв її віднесення до заборонених для розповсюдження; визначення суб’єкта, який би виконував функцію експертного оцінювання інформаційної продукції, що містить заклики до порушення конституційного ладу, територіальної цілісності, пропаганду війни, фашизму, національної та релігійної ворожнечі.

Зважаючи на низку важливих проблем, що заважають створити ефективно діючу національну систему протидії загрозам в кіберпросторі, а саме: термінологічна невизначеність, відсутність належної координації діяльності відповідних відомств, залежність України від програмних та технічних продуктів іноземного виробництва, складнощі із кадровим наповненням відповідних структурних підрозділів актуальним є питання побудови системи кібернетичної безпеки. Застарілість, складність системи охорони державної таємниці та службової інформації, створення умов для її несанкціонованого розповсюдження, переважна “паперовість” носіїв такої інформації ставить питання щодо необхідності гармонізації інформаційного законодавства з нормами міжнародного права і правовими актами ЄС, РЄ і НАТО, що перш за все ґрунтується на невід’ємному праві доступу до інформації. І в першу чергу, саме держава має забезпечувати якісний доступ всіх категорій громадян до виробленої нею інформації, як до офіційних матеріалів, так і до роз’яснення змісту своєї власної діяльності.

Пріоритетами удосконалення забезпечення інформаційної безпеки є: удосконалення правового забезпечення інформаційної безпеки шляхом розробки її концептуальних основ: визначення або уточнення завдань, функцій і повноважень суб’єктів забезпечення інформаційної безпеки України; забезпечення інформаційного суверенітету України з метою недопущення інформаційної залежності та інформаційної експансії з боку інших держав чи міжнародних структур; сприяння розвитку міжнародного співробітництва в інформаційній сфері в умовах перегляду його принципів і механізмів, посиленню міжнародно-правової відповідальності за використання в інформаційній сфері сил і засобів, які негативно впливають або створюють загрози людині, суспільству, державі; зміцнення організаційних основ забезпечення інформаційної безпеки: вирішення питання координації діяльності суб’єктів забезпечення інформаційної безпеки, зокрема у сфері протидії інформаційній агресії, забезпечення кібернетичної безпеки України; налагодження системи державно-приватного партнерства у сфері забезпечення інформаційної безпеки; запровадження системи демократичного контролю за діяльністю державних суб’єктів забезпечення інформаційної безпеки; розвиток комунікаційної політики у стосунках “держава-суспільство”.

Разом з тим, необхідною є розробка програм освітньо-виховного впливу, спрямованого на формування здатностей забезпечення власної інформаційної безпеки, зокрема підвищення рівня культури використання засобів оброблення інформації, оприлюднення власної інформації та способів її захисту, критичного ставлення до інформації.

Для успішного входження нашої держави в міжнародні інформаційні обміни вона має зосередитись насамперед на таких напрямах у сфері правової діяльності: розробляти систему правових актів, спрямованих на якісне збереження національних інформаційних ресурсів, їх розвиток і ефективне використання в національних інтересах; здійснювати необхідну адаптацію національного інформаційного законодавства до загальновизнаної міжнародної правової бази з метою активізації своєї участі у інформаційних обмінах; брати активну участь у міжнародній правотворчості, що має оперативно регламентувати нові явища в сфері інформатизації; сформувати правову базу для регламентації участі у міжнародній діяльності по забезпеченню дотримання міжнародного інформаційного законодавства, боротьби з кібертероризмом та ін. видами інформаційної злочинності [9].

В умовах зростаючої активізації глобальних процесів у сучасному світі, що поряд із позитивними аспектами своїх впливів на світову спільноту створили також небезпеки інформаційної агресії, кіберзлочинності, саме загальнонаціональна система інформаційної безпеки, скоординована в своїй діяльності державою, може стати запорукою нейтралізації інформаційних загроз і використання позитивних факторів розвитку інформатизації. Важливою складовою загальної політики забезпечення інформаційної безпеки України є підвищення участі громадськості у процесах удосконалення зв’язку “суспільство – держава”. Подальше зміцнення інформаційної безпеки країни вбачається у спільних, злагоджених діях усіх державних інституцій, громадськості, медіа-спільноти. В сучасних умовах необхідно вирішувати не лише такі важливі завдання, як формування власного інформаційного простору та його захисту від загроз, а й переходити від захисних стратегій до наступальних.

## ВИСНОВКИ

Підсумовуючи проведене дослідження можемо зробити наступні висновки:

1. В теоретичній частині роботи була ретельно досліджена джерельна база та детально описано стан наукової розробки теми дослідження. Встановлено, що поряд з величезними технічними досягненнями і радикальними геополітичними змінами нового сторіччя є зміна системних властивостей світу. Світова політична система в процесі глобалізації має тенденцію до ускладнення, стає нелінійною, багатовимірною і багатофакторною, а значить, у неї з'являються нові системні властивості, з якими пов'язані як нові ресурси глобального розвитку, так і нові загрози глобальної безпеки.

2. Важливішим кроком у становленні сучасних уявлень про інформацію стало спочатку визначення понятійно-категоріального апарату та встановлення методів дослідження даної проблематики. Встановлено, що вивчення інформації почало здійснюватися в рамках кібернетики та інформатики. Вивчення гуманітарного (людського) аспекту інформації дозволили розглядати її як зміст повідомлень, призначених для передачі від одних людей до інших в певних знаково-смислових системах, тобто культурних контекстах. В роботі було описано класифікацію підходів до розуміння зв'язку між знанням та інформацією та підкреслено, що оскільки інформаційні відносини в своєму географічному вимірі є транскордонними, значною мірою глобальними, то всі ці області формують нове середовище суспільних відносин, що іменується інформаційним простором.

На сьогоднішній день в сучасних умовах державно-правового розвитку та переходу на цифрові технології, актуальним й досі є питання про забезпечення інформаційної безпеки на міжнародному рівні. Ця актуальність обумовлена ​​однією з головних рис сучасного етапу науково-технічного прогресу: глобальною інформаційною революцією і зростаючою роллю інформаційно-комунікаційних технологій в сучасному світі.

3. Аналіз проблеми військового застосування інформаційно-комунікаційних технологій показав, що інформаційні технології створили передумови для виникнення принципово нового середовища ведення бойових дій – кіберпростору як частини загального геостратегічного ландшафту, а також появи інформаційної зброї. У зв'язку з цим збройні конфлікти все більш набувають характеру інформаційних воєн, які мають багатовимірний характер і можуть одночасно вестися на різних фронтах і рівнях.

Встановлено, що в даний час проблема розробки і застосування інформаційно-комунікаційних технологій в деструктивних військово-політичних цілях вивчається не тільки на внутрішньодержавному рівні і позначена в документах багатьох країн, але і на міжнародному рівні, в порядку денному ООН. В залежності від характеру мети були виділені кримінальний, терористичний і військово-політичний аспекти інформаційних загроз.

4. Інформаційно-комунікаційні технології використовуються як інструмент терористичної і антигромадської діяльності. Найбільш яскравим прикладом використання інтернет-маркетингу сьогодні є пропагандистська робота так званого «Ісламської держави». Мережева пропаганда ненависті і насильства виявляється ефективним механізмом тиску на органи влади і управління розвинених держав, включених в глобальну інформаційну мережу.

Відзначено, що небезпека поширення деструктивної ідеології полягає не тільки в спонуканні окремих осіб до вчинення злочинних актів, а й у формуванні у широких народних мас хибних моральних орієнтирів, що цілком здатні привести суспільство і державу до чергових політичних і економічних потрясінь. Значне поширення отримали саме технології інтерактивного впливу, які є більш привабливими для користувачів.

Встановлено, що для поширення деструктивної інформації використовуються методи мовного маніпулятивного впливу. Соцмережі стають майданчиком для здійснення шкідливого впливу, тому що мають ряд властивостей, які роблять їх уразливими. Це можливість створення облікових записів вигаданих персонажів, що ускладнює ідентифікацію.

5. В роботі було досліджено особливості формування міжнародних режимів інформаційної безпеки на різних рівнях світової політики. Відмічено, що майже всі держави розглядають інформаційну безпеку об'єктів критичної інфраструктури як проблему національної безпеки. Відзначено, що, незважаючи на прогалини в міжнародному праві, інформаційна безпека в більшості країн регулюється внутрішніми законодавчими нормами. Початківцями в даному контексті є США, в яких після подій 11 вересня 2001 р. безпека критичних інформаційних структур почала розглядатися в контексті антитерористичної стратегії. Серед критичних інформаційних структур було виділено лише незначну кількість систем, що використовуються виключно в цивільних цілях, що звужує можливість застосування норм гуманітарного права. Велика частина може використовуватися як у цивільній, так і у військовій сферах, внаслідок чого норми права потребують доопрацювання.

6. Незважаючи на зусилля правоохоронних органів і спецслужб, які спрямовані на боротьбу з кіберзлочинністю і кібертероризмом, число злочинних актів з використанням ІКТ не зменшується, а постійно збільшується, зростає їх суспільна небезпека. В наш час в світі налічуються десятки тисяч різних вірусних програм і їх модифікацій, збільшується кількість зломів баз даних і мережевих ресурсів компаній, ростуть загрози розкрадання конфіденційної інформації. Тому, можна прогнозувати, що в майбутньому частка інформаційного протиборства при проведенні військових операцій буде зростати. Використання інформаційної зброї не вимагає великих фінансових витрат, що робить інформаційну війну небезпечним засобом збройної боротьби. Інформаційна зброя стирає відмінності між військовими цілями і цивільними об'єктами, що обумовлено значною взаємозалежністю військових і цивільних інформаційних інфраструктур.

7. Аналіз пріоритетів удосконалення інформаційної безпеки України показав наявність низки проблем організаційно-правового змісту у сфері інформаційної безпеки України. При цьому сучасні виклики інформаційній безпеці України зумовлені як внутрішніми, так і зовнішніми чинниками. Визначено, що пріоритетними напрямами державної політики з питань національної безпеки України в інформаційній сфері є: забезпечення інформаційного суверенітету України; вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до запобігання і протидії корупції, зловживанням службовим становищем, іншим явищам, які загрожують національній безпеці України.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абдеев Р. Ф. Философия информационной цивилизации: Диалектика прогрессивной линии развития как гуманная общечеловеческая философия для XXI в. / Р. Ф. Абдеев. – Москва: Гуманитарный издательский центр «ВЛАДОС», 1994. – С. 198.
2. Алексеева И. Ю. Информационное общество и НБИКС-революция // Рос. акад. наук, Ин-т философии; И. Ю. Алексеева, В. И. Аршинов. – М.: ИФ РАН, 2016. – С. 9.
3. Алексис Де Токвиль. Революция и старый порядок. – М.: Алтейя, 2008.
4. Бабаева Ю. Д., Войскунский, А. Е. Психологические последствия информатизации / Ю. Д. Бабаева, А. Е. Войскунский // Психологический журнал. – Том 19. -1998. – №1. – С. 89-100
5. Баровська А. Інституційне забезпечення державної комунікативної політики : досвід країн Європи : аналітична доповідь. – Режим доступу : //www.niss.gov.ua /articles/1730
6. Бахтин С. А. Интернет-экономика – новый вызов национальной экономической безопасности: общая характеристика/ С. А. Бахтин // Национальная безопасность / Nota bene. – 2012. – № 6(23). – С. 118-122
7. Белинская Е. П. Информационная социализация в поликультурном пространстве / Е. П. Белинская // Известия Саратовского университета. Новая серия. Серия Философия. Психология. Педагогика. – 2015. – том 3. – № 30. – С. 253-259;
8. Белл Д. Грядущее постиндустриальное общество. Опыт социального прогнозирования / Д. Белл, перевод с английского. Изд. 2-ое, испр. и доп. – М.: Academia, 2004, CLXX. – 788 с.
9. Бірюков Д.С. Кондратов С.І. Зелена книга з питань захисту критичної інфраструктури в Україні: зб. матеріалів міжнар. експерт. Нарад. Київ: НІСД, 2015. 176 с: URL: http www.niss.gov.ua/public/File/2016\_book/Syxodolya\_ost.pdf
10. Богданов С. А. Эволюция форм и способов ведения вооруженной борьбы в сетецентрических условиях / С. А. Богданов // Военная мысль. – 2011. – №2. – С. 49-58;
11. Бородакий Ю. В., Добродеев, А. Ю., Бутусов, И. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века / Ю. В. Бородакий, А. Ю. Добродеев, И. В. Бутусов // Вопросы кибербезопасности. – 2013. – № 1. – С. 2- 9.
12. Бухарин С. Н. Методы и технологии информационных войн / С. Н. Бухарин, В. В. Цыганов. – М.: Акад. Проект, 2007. – 382 с.
13. Васенин В. А. Информационная безопасность и компьютерный терроризм / В. А. Васенин // Научные и методологические проблемы информационной безопасности. -Москва: МЦНМО, 2004. – С. 66
14. Вачнадзе Г. Н. Агрессия против разума: информационный империализм / Г. Н. Вачнадзе. – М.: Политиздат, 1988. – С. 69.
15. Войскунский А. Е. Информационная безопасность: психологические аспекты / А. Е. Войскунский // Национальный психологический журнал. – 2010. – №1(3). – С. 50
16. Гайкович, В. Ю., Ершов, Д. В. Основы безопасности информационных технологий [Электронный ресурс] / В. Ю. Гайкович, Д. В. Ершов. – Режим доступа: <http://www.bnti.ru/dbtexts/ipks/old/analmat/1_2002/ershov.pdf>.
17. Галатенко, В. А. Основы информационной безопасности. Курс лекций: учебное пособие / В. А. Галатенко, под редакцией академика РАН В. Б. Бетелина. – М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2006. – С. 15.
18. Гарр Т.Р. Почему люди бунтуют. – СПб: Питер, 2005.
19. Генсекретар ООН закликав до глобальної боротьби проти кібервоєн URL: https://www.radiosvoboda.org/a/news/29049044.html.
20. Геополитика. Информационно-аналитическое издание. Выпуск XXI / глав. ред: Савин Л. В, 2013. – 162 с.
21. Горбулін В.П. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. Стратегічні пріоритети. К.: НІСД, 2014. № 4. С. 5–12.
22. Горовий В.М. Правові перспективи національного розвитку. – Режим доступу : http://uaforeignaffairs.com/ua/ekspertna-dumka/view/article/nablizhajuchi-derzhavu-do-suspilstva/#st hash.AgJjKJa4.dpuf
23. Діордіца І.М. Адміністративно-правове регулювання кібербезпеки в Україні.: дис. д-ра юрид. наук : 12.00.07; Запоріжжя, 2018. 521 с.
24. Дмитренко М. А. Політична система України: розвиток в умовах глобалізації та інформаційної революції : [монографія] / М. А. Дмитренко ; Нац. пед. ун-т ім. М. П. Драгоманова, Ін-т дослідж. пробл. держ. безпеки. – 2-ге вид., допов. та переробл. – К. : Ун-т «Україна», 2011. – 820 с.
25. Дмитренко М. Причини воєнного конфлікту на Донбасі та заходи з попередження таких конфліктів у майбутньому // Освіта регіону. – 2016. – № 2. – С. 69-81
26. Дмитренко М. Спеціальні інформаційні впливи // Збірник наукових праць Інституту СЗРУ – 2014. – № 8. – С. 156-167.
27. Довгань О.Д. Організація правового гарантування безпеки інформаційних обмінів у контексті глобалізації // Правова інформатика. – 2013. – № 4(40). – С. 79-88
28. Док. Генеральной Ассамблеи ООН А/55/40. Средства и системы технического обеспечения обработки, хранения и передачи информации // https://moodle.kstu.ru/ mod/page/view.php?id=28916
29. Ефимова Н.А. Эстония: опыт трансформации государственного управления в условиях цифровой экономики / Н.А. Ефимова // Самоуправление. 2019. С. 217-218.
30. Жичкина А. Е. Социально-психологические аспекты общения в Интернете / А. Е. Жичкина, М.: Дашков и Ко, 2004 – 117 с.
31. Збитки світової економіки від хакерів досягли $ 600 млрд URL: https://ua.korrespondent.net/ world/3943548-zbytky-svitovoi-ekonomiky-vid-khakerivdosiahly-600-mlrd
32. Зуев А. Г. Онлайновые сообщества в «новой экономике» / А. Г. Зуев, Л. А. Мясникова // Мировая экономика и международные отношения. – 2002. – № 11. – С. 15-22.
33. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії та практики. Монографія/ За ред. Р.А. Калюжного та В.О. Шамрая – Київ,2002.296 с
34. Кан Г. Грядущий подъем: экономический, политический, социальный / Г. Кан // Новая технократическая волна на Западе / под ред. П.С. Гуревича. – М.: Прогресс. – 1986. – С. 169-206;
35. Кастельс М. Власть коммуникации / М. Кастельс. Пер. с англ. Н. М. Тылевич; под науч. ред. А. И. Черных. – М.: Изд. дом Высшей школы экономики, 2016. – С. 165.
36. Кастельс М. Информационная эпоха: экономика, общество и культура / М. Кастельс. – Москва: ГУ ВШЭ, 2000. – С. 39.
37. Кванталиани И. Э. Проблемы международно-правового регулирования вопросов информационной безопасности // Право и государство пресс. 2013. №11 (107). С. 143-146.
38. Костенко Н. И. Международная информационная безопасность в рамках международного права (методология, теория) // Российский журнал правовых исследований. 2018. №4. С. 9-16.
39. Крутских А.В., Стрельцов А.А. Международное право и проблема обеспечения международной информационной безопасности // Журнал «Международная жизнь». 2014. No. 11.
40. Кубышкин А. В. Международно-правовые проблемы обеспечения информационной безопасности государства: автореф. дис. канд. юр. наук. // М., 2002.
41. Кульба В. В. Информационное управление. Часть 1. Концептуальные основы/ В. В. Кульба, В. Л. Шульц, А. Б. Шелков // Национальная безопасность / Nota bene. – 2009. – № 3. – С. 4-14;
42. Левин В. К. Защита информации в информационно-вычислительных системах и сетях / В. К. Левин // Программирование. – 1994. – №5. – С. 6.
43. Маклюэн М. Понимание медиа: внешние расширения человека / М. Маклюэн. – М.: Канон-Пресс-Ц, 2003. – С. 42.
44. Малюк А. А. Защита информации в информационном обществе: Учебное пособие для вузов / А. А. Малюк. – М.: Гор. линия-Телеком, 2015. – 230 с.
45. Мамаева Л. Н., Жадан, И. Э. Информационный аспект экономической безопасности / Л. Н. Мамаева, И. Э. Жадан // Информационная безопасность регионов. – 2013. – № 2 (13). – С. 67 – 70;
46. Моисеев Н. Н. Информационное общество как этап новейшей истории [Электронный ресурс] / Н. Н. Моисеев. – Режим доступа: https://www.civisbook.ru/files/File/1993-3-2-Moiseev.pdf.
47. Наберушкина Э. К., Бердник, Е. А. Социокультурные аспекты информационной безопасности в сетевом обществе / Э. К. Наберушкина, Е. А. Бердник // Научные ведомости. Серия Философия. Социология. Право. – 2016. – № 17 (238). – Выпуск 37. – С. 90 – 98;
48. Олійник О.В. Cтан забезпечення інформаційної безпеки в Україні // Юридичний вісник. – 2014. – № 2(31). – С. 59-65.
49. Онищенко О.С. Національні інформаційні ресурси як інтегративний чинник вітчизняного соціокультурного середовища : монографія / [О.С. Онищенко, В.М. Горовий, В.І. Попик та ін.] ; НАН України, Національна бібліотекака України ім. В.І. Вернадського. – К., 2014.
50. Павлов Д. Політична пропаганда: до визначення поняття . Гілея: науковий вісник. 2013. Вип. 79. С. 328-331.
51. Панченко В.М. Співвідношення понять: інформаційна та кібернетична безпека // Інформаційна безпека людини, суспільства, держави. – 2013. – № 2 (12). – С. 20-24.
52. Пилипчук В.Г. Системні правові проблеми формування інформаційного суспільства : зб. наук. ст. та тез ; наукове повідомлення за матеріалами міжнародної науково-практичної конференції [“Інформаційне суспільство і держава : проблеми взаємодії на сучасному етапі”], (Харків, 26 жовтня 2012 р.). – Х. : НДІ державного будівництва та місцевого самоврядування, 2012. – 214 с.
53. Політологія: підруч. для студ. вищ. навч. закладів / За ред. О.В.Бабкіної, В.П.Горбатенка. – К., 2001. – 526 c.
54. Про основи національної безпеки України : Закон України від 19.06.03 р. // Відомості Верховної Ради України (ВВР). – 2003. – № 39. – Ст. 351.
55. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403. URL: http://zakon2. rada.gov.ua /laws/show/2163-19
56. Прокофьев К. В. Международно-правовые проблемы обеспечения международной информационной безопасности в сети Интернет: автореф. дис. канд. юр. наук. // М., 2009.
57. Савин, Л. В. Сетецентричная и сетевая война. Введение в концепцию / Л. В. Савин. М.: Евразийское движение, 2011. – 130 с.;
58. Скворцов Л. В. Информационная культура и цельное знание / Л. В. Скворцов. – М.: изд-во МБА, 2011. – 440 с
59. Старостина Е. В. Подход к выработке единого понятия «кибертерроризм» [Электронный ресурс] / Е. В. Старостина. – Режим доступа: http://rudocs.exdat.com/docs/index-198810.html; Войскунский, А. Е. Информационная безопасность: психологические аспекты // Национальный психологический журнал. – 2010. – № 1(3). – С. 48-53;
60. Стоуньер Т. Информационное богатство: профиль постиндустриальной экономики / Т. Стоуньер // Новая технократическая волна на Западе / под ред. П.С. Гуревича. М.: Знание, 1986. – С. 392 – 409.
61. Стратегія національної безпеки України : Указ Президента України від 26.05.15 р. № 287/2015. − Режим доступу : //www.president.gov.ua
62. Сурма И. В. Цифровая дипломатия в мировой политике / И. В. Сурма // Государственное управление. Электронный вестник. – 2015. – № 49. – С. 220 – 249;
63. Топчій В. В. Кібертероризм в Україні: поняття та запобігання кримінально-правовим та кримінологічними засобами. Наукові вісник Херсонського університету. Сер. Юридичні науки. 2015. Вип. 6.Том 3 С. 65-68.
64. Тоффлер Э. Третья волна / Э. Тофлер. – М.: ООО «Фирма «Издательство ACT», 2004. – 345 с.
65. Трансформация публично-правовых средств развития экономики и финансов: монография; под редакцией М.А. Лапиной, Г.Ф. Ручкиной. Москва: КНОРУС, 2019. С. 410.
66. Урсул А. Д., Цырдя, Т.(Ф). Н. Информационная безопасность личности как решающий фактор в стратегии выживания человечества [Электронный ресурс] / А. Д. Урсул, Т.(Ф). Н. Цырдя. – Режим доступа: <http://security.ase.md/publ/ru/pubru23.html>
67. Услинский Ф. А. Кибертерроризм: его свойства и особенности / Ф. А. Услинский // Право и кибербезопасность. – 2014. – № 1. – С. 6-11;
68. Уфимцев Ю. С., Ерофеев, Е. А. и др. Информационная безопасность России / Ю. С. Уфимцев, Е. А. Ерофеев. – М., 2003. – С. 12
69. Уэбстер Ф. Теории информационного общества / Ф. Уэбстер. – М.: Аспект Пресс, 2004. – 400 с.
70. Фатали Мохаддамам. Терроризм с точки зрения террористов: Что они переживают и думают, и почему обращаются к насилию. – М.: Форум, 2011.
71. Федоров Ф. В. Информационная безопасность в мировом политическом процессе / Ф. В. Федоров. – М.: МГИМО-Университет, 2006. – 220 с.
72. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. Вип. 1 (27). С. 312–320.
73. Шемякин В. П. Информационная безопасность в современных российских условиях (Социолого-управленческие аспекты): автореф. дис. ... канд. соц. наук: 22.00.08 / Владимир Петрович Шемякин. – М., 2004. – 131 с.
74. Шерстюк В. П. О развитии в МГУ научных исследований и учебного процесса в области информационной безопасности /В. П. Шерстюк // Научные и методологические проблемы информационной безопасности (сборник статей). Под ред. В. П. Шерстюка. – М.: МЦНМО, 2004. – С. 45.
75. Яхно О. М. Україна в сучасному геополітичному просторі (політико- медійний аспект) : автореф. дис. … канд. політ. наук : 23.00.03. Київ, 2006. 14 с.
76. Bell D. The coming of post-industrial society: A venture of social forecasting. — N.Y.: Basic Books, 1973.
77. Darczewska J. The Devil is in the Details. Information Warfare in the Light of Russia’s Military Doctrine, Point of View no. 50, Warsaw: Centre for Eastern Studies. 2015
78. Global Risks Report 2018” URL: http: www.weforum.org.
79. J. C. Davies, Toward a theory of revolution, American Sociological Review, 27 (1962).
80. Joseph S. Nye, Jr. Soft Power. Foreign Policy, No 80 (Autumn, 1990). URL: [http://faculty.maxwell.syr.edu/rdenever/PPA-730-27/Nye%201990.pdf.](http://faculty.maxwell.syr.edu/rdenever/PPA-730-27/Nye%201990.pdf)
81. Martin C. Libicki. What is Information Warfare? United States Government Printing, Washington DC, 1995. URL: [https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjsxry3oYDNAhVrSZoKHbas](https://www.google.ru/url?sa=t&rct=j&q&esrc=s&source=web&cd=1&ved=0ahUKEwjsxry3oYDNAhVrSZoKHbasCtsQFggbMAA&url=http%3A%2F%2Fhandle.dtic.mil%2F100.2%2FADA367662&usg=AFQjCNGsaFUMsGtQaS8jEzcDO1h-m2Sxuw&bvm=bv.123325700%2Cd.bGs&cad=rjt) [CtsQFggbMAA&url=http%3A%2F%2Fhandle.dtic.mil%2F100.2%2FADA367662&usg=AFQjCNGsaFUMsGtQaS8jE](https://www.google.ru/url?sa=t&rct=j&q&esrc=s&source=web&cd=1&ved=0ahUKEwjsxry3oYDNAhVrSZoKHbasCtsQFggbMAA&url=http%3A%2F%2Fhandle.dtic.mil%2F100.2%2FADA367662&usg=AFQjCNGsaFUMsGtQaS8jEzcDO1h-m2Sxuw&bvm=bv.123325700%2Cd.bGs&cad=rjt) [zcDO1h m2Sxuw&bvm=bv.123325700,d.bGs&cad=rjt.](https://www.google.ru/url?sa=t&rct=j&q&esrc=s&source=web&cd=1&ved=0ahUKEwjsxry3oYDNAhVrSZoKHbasCtsQFggbMAA&url=http%3A%2F%2Fhandle.dtic.mil%2F100.2%2FADA367662&usg=AFQjCNGsaFUMsGtQaS8jEzcDO1h-m2Sxuw&bvm=bv.123325700%2Cd.bGs&cad=rjt)
82. Masuda Y. The Information Society as Postindustrial Society. Wash.: World Future Soc., 1983. – P. 109
83. Masuda, Y. The Information Society as Postindustrial Society. Wash.: World Future Soc., 1983. – P. 153.
84. OECD Digital Security and privacy // URL: http://www.oecd.org/goingdigital/topics/digital-security-and-privacy/. 11. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. 2015. // URL: http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems andnetworkstowardsacultureofsecurity.htm.
85. Parulua A. Hybrid Warfare – Contemporary Concept in Georgia’s External Security. URL: file:///C:/Users/%D0%92%D0%B0%D0%B4%D1%96%D0%BB%D0%B5%D0%BD/Desktop/ H%C3%BCbriids%C3%B5japidamine+-+kaasaegsed+Gruusia+v%C3%A4lisjulgeoleku+kontseptsioo nid.pdf.
86. Roszak T. The Cult of Information. The Folklore of computers and the True Art of Thinking. – New York: Pantheon Books, 2000.
87. Tadao Umesao Information Industry Theory: Dawn of the Coming Era of the Ectodermal Industry.
88. Thomas P. Rona. Weapon Systems and Information War, the Official Home of the Department of Defense. URL:[http://www.dod.gov/pubs/foi/reading\_room/09-F-0070WeaponSystems\_and\_Information\_War.pdf.](file:///C%3A%5CUsers%5Cuser%5CDownloads%5C%C2%A0http%3A%5Cwww.dod.gov%5Cpubs%5Cfoi%5Creading_room%5C09-F-0070WeaponSystems_and_Information_War.pdf)