«ЗАКЛАД ВИЩОЇ ОСВІТИ
«УНІВЕРСИТЕТ КОРОЛЯ ДАНИЛА»

Факультет суспільних та прикладних наук
Кафедра права та публічного управління

на правах рукопису

ПАСТЕРНАК АНДРІЙ ВАЛЕРІЙОВИЧ

УДК 358.486

ТЕМА РОБОТИ:
«ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Спеціальність 281 «Публічне управління та адміністрування»

Наукова робота на здобуття кваліфікації магістра

Науковий керівник:
Мельничук В. І.

Івано-Франківськ - 2024

«ЗАКЛАД ВИЩОЇ ОСВІТИ
«УНІВЕРСИТЕТ КОРОЛЯ ДАНИЛА»
Факультет суспільних та прикладних наук
Кафедра права та публічного управління

Освітній рівень*: «магістр»*
Спеціальність: *«281 Публічне управління та адміністрування»*

ЗАТВЕРДЖУЮ
в. о. завідувач кафедри права та публічного управління
к.ю.н., Ходак С. М.
_____
«29» серпня 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Пастернаку Андрію Валерійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи *« Державна політика у сфері інформаційної безпеки»*
2. Керівник роботи Мельничук В. І.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом ректора університету від *«30» серпня 2023 року №59/1 с*

3. Строк подання студентом роботи *31 грудня 2023р.*
4. Зміст кваліфікаційної роботи (перелік питань, які потрібно розробити)

1. Теоретичні засади інформаційної безпеки

2. Особливості державної політики у сфері інформаційної безпеки

3. Проблеми та перспективи формування державної політики у сфері інформаційної безпеки

5. Дата видачі завдання*: 30 серпня 2023 року*
7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір та вивчення джерел інформації для написання кваліфікаційної роботи	до 22 вересня 2023 року	*виконано*
2	Складання плану кваліфікаційної роботи та затвердження керівником	до 29 вересня 2023 року	*виконано*
3	Написання розділу 1 *Теоретичні засади інформаційної безпеки*	до 27 жовтня 2023 року	*виконано*
4	Написання розділу 2 *2. Особливості державної політики у сфері інформаційної безпеки*	до 24 листопада 2023 року	*виконано*
5	Написання розділу 3 *3. Проблеми та перспективи формування державної політики у сфері інформаційної безпеки*	до 25 грудня 2023 року	*виконано*
6	Написання вступу, висновків та формування списку використаних джерел	до 31 грудня 2023 року	*виконано*

Студент _____ Пастернак А. В.

(підпис) (прізвище та ініціали)

Керівник роботи _____ Мельничук В. І.

(підпис) (прізвище та ініціал)

АНОТАЦІЯ

У кваліфікаційній роботі обґрунтовано та узагальнено теоретико-методологічні засади необхідності реалізації державної політики у сфері інформаційної політики, визначено роль міжнародної співпраці у формуванні стратегії інформаційної безпеки, охарактеризовано особливості забезпечення інформаційної безпеки держави в умовах війни. В першому розділі роботи розкрито теоретичні засади інформаційної безпеки, зокрема розглянуто інформаційну безпеку як соціальне явище, виокремлено її структурні елементи. У другому розділі проаналізовано особливості державної політики у сфері інформаційної безпеки. За результатами проведеного аналізу в третьому розділі роботи висвітлено проблеми та перспективи формування державної політики у сфері інформаційної безпеки.

Ключові слова: інформаційна безпека, державна політика, інформаційна політика, інформаційний простір, євроатлантичне співробітництво.

ANNOTATION

The qualification work justified and summarized the theoretical and methodological principles of the need to implement state policy in the field of information policy, determined the role of international cooperation in the formation of information security strategy, characterized the features of ensuring the state's information security in conditions of war. In the first chapter of the work, the theoretical foundations of information security are disclosed, in particular, information security is considered as a social phenomenon, its structural elements are singled out. The second chapter analyzes the peculiarities of state policy in the field of information security. Based on the results of the analysis, the third section of the work highlights the problems and prospects of the formation of state policy in the field of information security.

Key words: information security, state policy, information policy, information space, Euro-Atlantic cooperation.

ЗМІСТ

ВСТУП

Актуальність теми. У непростий для нашої країни час важливість інформації як інструменту у протидії агресору важко переоцінити. Фактично вона стає потужною зброєю. Це й не дивно, бо інформація може забезпечити перемогу у війнах, конфліктах, або стати засобом для подолання суспільно-політичної кризи. Особливої важливості набуває використання інформації набуває останнім часом, зокрема, у гібридних війнах, де безпосередній військовий аспект – лише частина загального плану.

Необхідно зважати, що в умовах, коли інформаційний контент спрямований на маніпулювання громадською думкою через фізіологічні та психологічні методи сприйняття, питання низького рівня інформаційної грамотності набуває виняткового значення, оскільки призводить до неможливості належним чином аналізувати інформацію та приймати необхідні рішення.

У такому випадку індивідуальна спроможність критично мислити фактично відсутня. Тому варто зазначити, що формування продумної державної політики щодо інформаційної безпеки має безумовно містити такі елементи як:

–високий та професійний рівень інформаційної освіти, який передбачає усі складові інформаційного захисту і забезпечує збалансований розвиток в інформаційному суспільстві, незважаючи на потенційні виклики;

– спроможність країни забезпечити умови для задоволення інформаційних потреб громадян незалежно від можливих ризиків;

– забезпечення, розвиток та використання інформаційного середовища з метою задоволення потребі усіх членів суспільства;

– протидія потенційним та реальним інформаційним загрозам.

Таким чином, питання формування продуманої державної політики у

сфері інформаційної безпеки є настільки важливим, особливо зараз, коли Україна бореться із російським агресором на всіх фронтах, а інформаційний фронт є одним із пріоритетних напрямів боротьби.

Метою магістерської роботи є теоретичне, методичне та практичне обґрунтування необхідності реалізації державної політики у сфері інформаційної безпеки.

Досягнення даної мети обумовило необхідність вирішення наступних **завдань:**

– дати характеристику поняття «інформаційна безпека» визначити її правову основу ;

– проаналізувати інформаційну безпеку як соціальне явище;

– вказати структуру інформаційної безпеки та її елементи;

–дати характеристику державної політики у сфері інформаційної безпеки;

– проаналізувати правові та політичні засади державної політики у сфері інформаційної безпеки;

– визначити роль міжнародної співпраці у формуванні стратегії інформаційної безпеки;

– охарактеризувати особливості забезпечення інформаційної безпеки держави в умовах війни;

– проаналізувати стан євроатлантичного співробітництва України в контексті формування державної політики у сфері інформаційної безпеки.

Об’єктом дослідження є процес формування державної політики у сфері інформаційної безпеки.

Предметом дослідження є механізми та способи реалізації державної політики України у сфері інформаційної безпеки.

Методи дослідження Для досягнення поставленої мети дослідження застосовувалася система загальних та спеціальних методів наукового пізнання.

Зокрема, *діалектичний метод* дав можливість забезпечити повноту, об'єктивність, всебічність та конкретність результатів дослідження; *системно-структурний метод* застосовано при узагальненні нормативної бази та наукової літератури; *логіко-догматичний метод* – став у нагоді при тлумаченні окремих наукових та законодавчих термінів, формулюванні визначень юридичних понять; *метод аналізу і синтезу*, а також *порівняльний* метод були використані для дослідження процесу формування державної політики України у сфері інформаційної безпеки.

Новизна отриманих результатів полягає в обґрунтуванні важливості формування державної політики у сфері інформаційної безпеки. У результаті проведеного дослідження сформульовано низку концептуальних положень, що вирізняються науковою новизною та мають важливе теоретичне та практичне значення, зокрема, формування державної політики у сфері інформаційної безпеки в умовах війни та значення євроатлантичного співробітництва для підвищення її ефективності.

Практичне значення одержаних результатів полягає в тому, що сформульовані в роботі положення, висновки, пропозиції та рекомендації можуть бути використані у:

– науково-дослідній діяльності – як основа для подальшого дослідження проблем формування державної політики у сфері інформаційної безпеки в умовах війни;

–правозастосовчій діяльності – для формування критеріїв ефективності процесу формування державної політики у сфері інформаційної безпеки та її вдосконалення;

– навчальному процесі – при розробленні нових та оновленні існуючих навчальних курсів за спеціальністю «Публічне управління та адміністрування».

Опис структури роботи. Магістерська робота складається із вступу, трьох розділів, що включають вісім підрозділів, висновків та списку використаних джерел. Загальний обсяг роботи – 90 сторінок. Список джерел містить 72 найменування.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Характеристика змісту поняття «інформаційна безпека» та її правова основа

У сучасному інформаційному суспільстві питання, пов'язані з безпекою інформації, привертають значну увагу як в наукових та професійних колах, так і серед загальної громадськості. Терміни, такі як «інформаційна безпека», «кібербезпека», «захист інформації» і т.д., вже давно використовуються повсюдно, але їхнє визначення не завжди є однозначним у міжнародних та національних правових актах. Отже, існує потреба у встановленні чіткого визначення "інформаційної безпеки", оскільки відсутність загальноприйнятого розуміння цього терміну створює методологічну неоднозначність щодо інших понять та термінів у цій галузі.

Під час розгляду терміна «інформаційна безпека» важливо з'ясувати значення поняття «безпека». Безпека може розглядатися як стан складної системи, в якому дія зовнішніх та внутрішніх факторів не призводить до погіршення функціонування системи або до її неможливості працювати та розвиватися. Безпеку можна розглядати з різних точок зору: як потребу і інтерес, як цінність для особи чи суспільства, як соціальні відносини, соціальну функцію, яку виконує держава, систему заходів.

Інформаційна безпека визначається як стан захищеності інтересів будь-якого суб'єкта в інформаційній сфері. Це охоплює різні рівні суспільства, починаючи від людства і держави, і закінчуючи організаціями, групами та окремими особами, а також технічні аспекти, такі як інформаційно-телекомунікаційні системи, засоби зв'язку, автоматизовані системи управління, окремі комп'ютери та інші засоби обробки та передачі інформації.

Як зазначає Т. Мужанова: «Існує досить багато варіантів визначення

поняття інформаційної безпеки. Основну групу становлять бачення, у рамках яких інформаційну безпеку держави розглядають як стан, тенденції розвитку, умови життєдіяльності соціуму, його структур, інститутів і установ, за яких забезпечується збереження їх якісного, вільного, відповідного власній природі та інноваційного функціонування» [33].

Далі авторка наводить декілька визначень досліджуваного нами поняття:

«Інформаційна безпека – стан захищеності інтересів особи, суспільства та держави в інформаційній сфері, який виключає можливість заподіяння їм шкоди через неповноту, несвоєчасність і недостовірність інформації, а також негативні наслідки використання інформаційних технологій або законодавчо забороненої чи обмеженої для поширення інформації.

Інформаційна безпека - це стан захищеності об'єкта (людини, суспільства, держави) від інформаційних загроз, який визначається рівнем шкоди, яку може бути заподіяно існуванню, функціонуванню чи діяльності об'єкта в разі реалізації цих загроз через використання неповної, несвоєчасної та недостовірної інформації; здійснення негативного інформаційного впливу; протиправного застосування інформаційних технологій; несанкціонованого розповсюдження і використання інформації, порушення її цілісності, конфіденційності та доступності.

Інформаційна безпека – це стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Стан інформованості визначає ступінь адекватності сприйняття суб’єктами навколишньої дійсності і як наслідок – обґрунтованість прийнятих рішень і дій. Інформаційна безпека - це стан захищеності свідомості і буття соціальних суб'єктів від інформаційних загроз, який визначається рівнем реальної або потенційної шкоди, заподіяної внаслідок деструктивного

інформаційного впливу або порушення безпеки інформації. Інші науковці розглядають інформаційну безпеку через призму розвитку інформаційного простору держави, суспільства і розуміють під нею стан захищеності інформаційного середовища, за якого забезпечується його формування, використання й розвиток в інтересах особистості, суспільства, держави незалежно від впливу внутрішніх та зовнішніх інформаційних загроз. Під інформаційним середовищем мають на увазі сферу діяльності суб'єктів, пов'язану із створенням, обробленням та обміном інформації» [33].

При розгляді сутності поняття "інформаційна безпека" важливо відзначити, що в англійській мові існують два терміни, які перекладаються на українську мову однаково, але мають відмінний зміст: "safery" і "security". Перший з них вказує на стан захищеності об'єкта, тоді як другий акцентує увагу на діяльності, спрямованій на забезпечення цього стану. Отже, інформаційну безпеку визначають як стан, що відображає відсутність небезпеки від чинників і умов, що загрожують безпосередньо об'єкту (індивіду, спільноті, державі) у сфері інформаційно-комунікаційного середовища, а також як можливість, здатність об'єкта ефективно захистити себе, протистояти та нейтралізувати різноманітні інформаційні загрози.

На думку Т. Мужанової: «У цьому контексті можна розглянути такі визначення інформаційної безпеки.

Інформаційна безпека – це стан захищеності життєво важливих інтересів особистості, суспільства й держави від негативних інформаційних впливів в економіці, внутрішній і зовнішній політиці, в науково-технологічній, соціокультурній і оборонній сферах, системі державного управління, забезпечення самостійного й незалежного розвитку всіх елементів національного інформаційного простору та забезпечення інформаційного суверенітету країни, захищеності від маніпулювання інформацією і

дезінформування та впливів на свідомість, підсвідомість і психіку як індивіда, так і суспільства в цілому, спроможність держави нейтралізувати чи послабити дію внутрішніх і зовнішніх інформаційних загроз.

Інформаційна безпека – це стан захищеності особи, суспільства і держави від зовнішніх та внутрішніх небезпек і загроз, який базується на діяльності людей, суспільства, держави, світового співтовариства з виявлення (вивчення), попередження, послаблення, ліквідації і відбиття небезпек і загроз, здатних знищити їх, позбавити фундаментальних матеріальних і духовних цінностей, завдати неприйнятної шкоди, закрити шлях для прогресивного розвитку».

На думку авторки: «…в українській мові доцільно використовувати два терміни, які відображають зазначену різницю. Під інформаційною безпекою розуміти стан захищеності і, отже, стійкості основних сфер людської діяльності (політичної, економічної, наукової, технічної, культурної, військової сфер, сфери державного управління та суспільної свідомості тощо), по відношенню до можливих небезпечних інформаційних впливів. Аналізуючи сутність поняття «інформаційна безпека», нагадаємо, що інформаційна сфера сучасного суспільства має дві складові: інформаційнотехнічну (штучна сфера техніки, технологій, ресурсів тощо) та інформаційнопсихологічну (психіка людини, пізнання, безпосереднє спілкування). Відповідно, в загальному випадку інформаційну безпеку представляють двома складовими: інформаційно-технічною безпекою та інформаційнопсихологічною безпекою» [33].

Таким чином, інформаційна безпека означає стан захищеності особистості, суспільства та держави від інформації негативного або незаконного характеру, яка може впливати на свідомість людей та заважати сталому розвитку особистості, суспільства та держави. Крім того, інформаційна безпека також означає захищеність інформації та інформаційної інфраструктури, включаючи комп'ютери та мережі зв'язку, які забезпечують

зберігання, обробку та передавання інформації. Давайте детальніше розглянемо взаємозв'язок між поняттями "інформаційна безпека" та "безпека інформації".

Зрозуміло, що перше поняття має ширший обсяг і включає друге. Так, безпека інформації (даних) - це стан захищеності інформації (даних), що забезпечує конфіденційність, доступність і цілісність даних. Крім самої інформації, до об'єктів безпеки інформації часто включається інфраструктура, яка забезпечує її обробку та передавання. Важливо розуміти, що інформаційна безпека є однією з ключових складових національної безпеки держави, поряд з економічною, енергетичною, військовою, соціальною та іншими. В той же час стає очевидним, що роль інформаційної безпеки та її місце в системі національної безпеки держави набувають все більшого значення.

На думку Т. Мужаннової: «Це відбувається внаслідок таких чинників:

–національні інтереси, загрози їм і забезпечення захисту від цих загроз у всіх галузях національної безпеки виражаються, реалізуються і здійснюються через інформацію та інформаційну сферу;

– особа та її права, інформація та інформаційні системи і права на них це – основні об'єкти не тільки інформаційної безпеки, а й основні елементи всіх об'єктів безпеки в усіх її галузях;

– вирішення завдань національної безпеки пов'язане з використанням інформаційно-комунікаційних засобів та технологій як основних на сучасному етапі;

– проблема національної безпеки має яскраво виражений інформаційний– характер» [33].

В уявленні вітчизняних науковців, інформаційна безпека України вважається складовою національної безпеки, яка охоплює кілька напрямів: забезпечення інформаційного суверенітету, розвиток державного регулювання інформаційної сфери, впровадження новітніх технологій, наповнення

інформаційного простору достовірною інформацією, залучення засобів масової інформації до боротьби з корупцією, захист конституційних прав громадян і запобігання дискримінації в інформаційній сфері.

Зокрема, це означає протистояння інформаційним загрозам, негативному впливу на свідомість та інфраструктурі інформаційного простору. Зарубіжні фахівці підкреслюють важливість активної позиції держави, суспільства та особистості в умовах швидкого розвитку та впровадження інформаційно-телекомунікаційних технологій, а також необхідність розвитку інноваційних форм поведінки для забезпечення інформаційної безпеки.

Це означає здатність до забезпечення захищеності соціального інтелекту та інформаційних ресурсів, протидії інформаційним загрозам, розвитку навичок безпечної поведінки, готовності до інформаційного протиборства та впровадження штучного інтелекту в соціальне середовище. В інформаційному суспільстві інформаційна безпека стає ключовою цінністю, яка забезпечує стабільність та прогресивний розвиток держави.

На думку П. Яковлєва: «доцільно виокремити кілька чинників, які зумовлюють складнощі розуміння вказаного поняття. Зокрема, це різноманітність контексту, у якому тлумачиться категорія «інформаційна безпека», неоднозначність кількості складових частин структури інформаційної безпеки як явища, недостатнє врахування того, що забезпечення інформаційної безпеки є самостійним напрямом державного управління, а також особливості міжнародно-правового визначення відповідної категорії. Очевидно, що наведений перелік чинників не є вичерпним і може бути продовжений».

Яковлєв зазначає: «Першим, найбільш важливим чинником, який зумовлює проблематику визначення категорії «інформаційна безпека», є різноманітність контексту, у якому вказане явище аналізується вченими-юристами. Так, ураховуючи положення чинного законодавства, інформаційна

безпека як поняття вживається в контексті визначення функцій держави та громадянських обов'язків громадян України (ст. 17 Конституції України), в контексті визначення складових частин державної політики у сфері національної безпеки і оборони України (ст. 3 Закону України «Про національну безпеку»), в контексті розвитку інформаційного суспільства (п. 13 Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»), в контексті регламентації прав і обов'язків суб'єктів сектору безпеки і оборони держави (нормативні акти, які регламентують статус суб'єктів забезпечення національної безпеки і оборони), в контексті встановлення юридичної відповідальності за правопорушення, об'єктом яких є інформація, інформаційні інтереси держави та особи (Кодекс України про адміністративні правопорушення містить, за нашими підрахунками, 41 склад адміністративних правопорушень об'єктом посягання, у яких визначено інформацію або елементи інформаційної інфраструктури України» [65].

Також автор наголошує: «Крім цього, тлумачення категорії інформаційної безпеки відбувається в контексті регламентації розвитку та захисту технічного забезпечення національного інформаційного простору, в контексті аналізу правових аспектів планування та реалізації державної політики у сфері захисту кіберпростору України і використання ресурсів Інтернет та ін. Через те, що сучасна юридична доктрина розглядає інформаційну безпеку в контексті прив'язки до певного родового об'єкта, зміст категорії «інформаційна безпека» визначається в логічній «прив'язці» до такого об'єкта» [65].

Так, О.М. Кісілевич-Чорнойван, досліджуючи спів відношення понять «інформаційна безпека» та «міжнародна інформаційна безпека» у працях значної кількості науковців, зазначає: «Більшість сучасних правознавців

сходяться на думці, що інформаційна безпека розглядається або як стан захищеності важливих інтересів особи, суспільства і держави, за якого зводиться до мінімуму нанесення шкоди через негативний інформаційний вплив, або як стан захищеності інформаційного середовища як складової частини національної безпеки, який забезпечує його формування, використання і розвиток в інтересах громадян та організацій держави» [19].

В.І. Шульга зазначає: «Інформаційна безпеки держави є процесом, діяльністю та результатом діяльності людини, яка спрямована на забезпечення безпеки в інформаційній сфері у майбутньому з урахуванням змістовних показників. Це дає підстави вважати, що юридична доктрина впритул наблизилася до активізації дослідження інформаційної безпеки держави з урахуванням поєднання двох зазначених підходів. Другий чинник, який тривалий час зумовлював проблемність уніфікованого визначення категорії «інформаційна безпека держави», полягає в невизначеній кількості складових частин інформаційної безпеки. Ситуація дещо змінилася з набранням чинності вже згадуваної Доктрини інформаційної безпеки України. Документ визначає, що складовими частинами інформаційної безпеки держави України є національні інтереси в інформаційній сфері, які включають у себе приватний і публічний компонент. Приватний компонент вбирає в себе життєво важливі інтереси особи (забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації, на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів), а публічний – життєво важливі інтереси суспільства і держави (захист українського суспільства від агресивного впливу деструктивної пропаганди інших держав, розвиток медіа-культури суспільства та соціально відповідального медіа-середовища, формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських

впливів, розвиток технічної інфраструктури захисту національного інформаційного середовища та ін.)» [64].

На думку П. Яковлєва: «Сьогодні повноцінним елементом структури інформаційної безпеки держави слід вважати ринок інформаційних послуг та інформаційних продуктів. У сучасній державі вказаний сегмент дедалі більше розширюється і відграє з кожним днем все більшу роль у формуванні економічного потенціалу держави. Оскільки інформація охоплює всі сфери людської діяльності, забезпечуючи зростання матеріальних і духовних сил суспільства, її вплив на механізм адміністративно-правового забезпечення інформаційної безпеки видається доволі значним. Відповідно, формування інформаційних ресурсів є запорукою вирішення проблем соціально-економічного розвитку країни. Слід також наголосити, що більшість науковців під час наведення авторських варіацій тлумачення категорії «інформаційна безпека» не враховують можливостей потенційної участі громадянського суспільства у відповідних процесах. Імперативом сьогодення стало те, що інститути громадянського суспільства мають колосальні можливості для формування інформаційного простору держави. Більше того, в епоху постінформаційного суспільства генеруючий інформаційний ресурс інститутів громадянського суспільства в окремих напрямах перевищує можливості держави [65].

У подальших наукових дослідженнях щодо концепції "інформаційна безпека держави" важливо враховувати роль та можливості громадянського суспільства. Ця позиція повністю відповідає конституційному принципу про те, що забезпечення інформаційної безпеки є обов'язком всього українського народу. Сучасним науковим працям, які розглядають зміст інформаційної безпеки, не вистачає врахування національного досвіду інститутів громадянського суспільства, що активно сприяють державі у питаннях

забезпечення інформаційної безпеки. Більше того, діяльність окремих таких організацій, що протидіють інформаційним загрозам в Україні, широко висвітлена в загальнодоступному інформаційному просторі.

Як зазначає О. Степко: «Якщо вдатися до деталізованого аналізу сутності державного управління у сфері забезпечення інформаційної безпеки, то слід мати на увазі складну систему управлінських заходів. Зокрема, це розроблення нормативно-правових і організаційно-методичних документів; розроблення концепції інформаційної безпеки, спеціальних правових і організаційних заходів, що забезпечують збереження і розвиток інформаційних ресурсів; формування правового статусу суб'єктів системи інформаційної безпеки; розроблення законодавчих і нормативних актів, що регулюють порядок ліквідації наслідків загроз інформаційній безпеці; відновлення порушеного права і ресурсів, розроблення компенсаційних заходів; вдосконалення організації форм і методів запобігання і нейтралізації загроз інформаційній безпеці; розвиток сучасних методів забезпечення інформаційної безпеки, розвиток науково-практичних основ інформаційної безпеки; розвиток законодавчої і нормативно-правової бази забезпечення інформаційної безпеки» [53].

П Яковлєв вважає доцільним: «…доповнити чинну Доктрину інформаційної безпеки визначенням інформаційної безпеки саме як самостійного напряму державної управлінської політики з урахуванням конкретизації форми участі інститутів громадянського суспільства України в залученні до розробки і практичної реалізації управлінських заходів, спрямованих на забезпечення інформаційної безпеки. Сучасні джерела міжнародного права, особливо на рівні ООН, містять значну кількість правових конструкцій, які тим чи іншим чином регламентують аспекти реалізації державної політики з питань забезпечення інформаційної безпеки. Здебільшого

це положення загальних відомих документів ООН у галузі прав людини. Разом із тим найбільше інформаційна безпека згадується в резолюціях Генеральної асамблеї ООН (далі – ГА ООН), які присвячені питанню розвитку інформаційно-комунікаційного, інформаційно-технічного простору і питанням загальної безпеки на інформаційному рівні.

Висловлене вище свідчить про те, що категорія "інформаційна безпека держави" є однією з найбільш вживаних у сучасній юридичній доктрині та національному законодавстві України.

Однак, наразі в юридичній науці ще не вироблено уніфікованого визначення цього поняття. Це може мати негативні наслідки для правозастосовної практики, оскільки процес забезпечення інформаційної безпеки системою уповноважених державних органів потребує широкого спектру адміністративних дій, що можуть обмежити права та свободи громадян.

Основні складнощі в розумінні цього поняття пов'язані з різноманітністю контекстів, в яких воно тлумачиться, неоднозначністю складових частин структури інформаційної безпеки, а також недостатнім урахуванням його самостійного характеру управління та міжнародно-правового визначення.

У зв'язку з цим, перспективним напрямком наукових досліджень є формування узагальненого поняття "інформаційна безпека держави", що враховує постійний процес функціонування уповноважених державних органів у співпраці з інститутами громадянського суспільства.

Це спрямовано на запобігання загроз, уникнення ризиків та припинення дій, що впливають на національний інформаційний простір, порушують державний порядок та створюють передумови для порушення прав громадян.

1.2 Інформаційна безпека як соціальне явище

Формування інформаційного середовища є закономірним етапом еволюції сучасного суспільства, що характеризується насамперед масштабним впровадженням інформаційних технологій і розвитком глобального інформаційного простору. Процес становлення нового суспільства, зумовлений впровадженням інформаційних технологій, потребує правильного усвідомлення його інформаційної специфіки і конструктивного розвитку закладеного в ньому потенціалу.

На перехресті XX і XXI століть людство зазнало значних технологічних змін, які призвели до появи нових серйозних загроз і ризиків. Сучасні інформаційні технології розглядаються як сила, що має величезний вплив на глобальний розвиток суспільства та формування інформаційної реальності. Вони вплинули на свідомість і можливості людини, змінили життя суспільства та переосмислили його цінності.

Як ці технології, що є необхідним засобом життєдіяльності, будуть використовуватися у майбутньому, залежить від суспільства і його вибору. В контексті деформації системи цінностей інформаційна сфера стала осередком економічних, соціальних, політичних і інших конфліктів у суспільстві.

Серед численних інформаційних загроз і ризиків можна виокремити реальну загрозу "інформаційного розшарування", збільшення комп'ютерної злочинності, потенційну дегуманізацію праці, технострес, виробництво нових видів інформаційної зброї, загрозу інформаційного колоніалізму, розвиток різних захворювань та загрозу маніпулювання людською свідомістю, що може вести до психічної та соціальної дезадаптації людини.

Як зазначає О. Панченко: «перед людиною розгорнулися всі масштаби проблем інформаційної безпеки – суперечності між наданими можливостями інформаційних технологій, з одного боку, і негативними ефектами,

небезпеками, ризиками їх застосування в деструктивних цілях щодо особистості, суспільства, держави – з іншого. Внаслідок цього забезпечення безпеки результатів використання інформаційних технологій, усунення інформаційних небезпек і ризиків в рамках стратегії інформаційної безпеки стають стратегічною проблемою світового суспільства. Інформаційна безпека представлена як стійкий стан інформаційної сфери, що забезпечує свою цілісність і захист об'єктів за наявності несприятливих внутрішніх і зовнішніх впливів на основі усвідомлення соціальними суб'єктами своїх цінностей, потреб (життєво важливих інтересів) і цілей розвитку. Основний зміст поняття «інформаційна безпека» полягає в забезпеченні безпеки інформації; забезпеченні безпеки суб'єктів інформаційної взаємодії від негативного інформаційного впливу; задоволенні інформаційної потреби суб'єктів інформаційної взаємодії за допомогою забезпечення безпечного стану інформаційного середовища. Отже, основний системоутворюючий зміст інформаційної безпеки визначає її як цілісний соціальний феномен об'єктивного розвитку сучасного соціуму, спрямованого на сприяння гармонійного розвитку інформаційного суспільства. Інформаційна безпека охоплює такі напрями:

– забезпечення захисту інформаційного простору, що підтримує справедливий розподіл своїх благ і ресурсів;

– сприяння процесу переходу до сталого розвитку загальносвітового інформаційного середовища;

– забезпечення стану захищеності культурального генофонду людства в умовах глобалізації» [38].

Науковець додає: «На сучасному етапі розвитку суспільства ефективне забезпечення інформаційної безпеки дозволяє вирішувати ключові питання практично всіх видів національної безпеки. Інформаційна безпека є важливим

складником системи національної безпеки, і від успішного вирішення питань цієї сфери залежить забезпечення глобальної загальносвітової безпеки. Своєю чергою процес забезпечення інформаційної безпеки перманентний, комплексний, соціально-культурні аспекти є важливими його компонентами поряд з правовими та організаційно-технічними засобами і методами. Вивчення особливостей функціонування основних заходів інформаційної безпеки призвело до висновку, що систему захисту безпеки неможливо побудувати, ґрунтуючись винятково на технічних засобах. Насамперед міцність системи безпеки визначається професіоналізмом і особистісними якостями кожного з членів колективу, а підвищення її рівня відбувається шляхом впровадження законодавчих і морально-етичних заходів. Упроцесі забезпечення інформаційної безпеки морально-етичні принципи і відповідальність кожного, засновані на прийнятих правилах поведінки в суспільстві і підкріплені заходами законодавчого характеру, на державному рівні виступають головним чинником побудови системи захисту. На цей час є гостра потреба в цілеспрямованому формуванні інформаційної культури суспільства, від якої багато в чому залежить успішне рішення проблем і викликів, що виникають в процесі становлення глобального інформаційного простору і, відповідно, проблем інформаційної безпеки загалом». [38].

Отже, базу інформаційної безпеки складає поведінка особи в соціумі, яка розуміє свої права та обов'язки. Система морально-етичних норм виступає як керівництво для безпечного використання інформаційних технологій та формування відносин у суспільстві в інформаційній сфері.

Забезпечення безпеки інформаційних технологій передбачає акцент на інформаційній етиці, яка спрямована на освіту кожного учасника суспільства щодо його прав і обов'язків у сфері інформації, включаючи відповідальність за створення та використання інформаційно-комп'ютерних технологій та інших

форм інформації.

Українська держава включена в процес загальної інформатизації суспільства і формування єдиного світового інформаційного ринку. Такі перетворення призвели до того, що на цей час все більш актуальний характер набуває забезпечення інформаційної безпеки як невіддільного елементу її національної безпеки, а захист інформації перетворюється на одне з пріоритетних державних завдань.

Проблема створення і підтримки захищеного середовища інформаційного обміну, яке зумовлює певні правила і політику безпеки сучасної держави, є досить актуальною, оскільки сьогодні головним стратегічним національним ресурсом, основою економічної та оборонної могутності держави стає інформація та інформаційні технології.

Інформація в сучасному світі є таким атрибутом, від якого у визначальному плані залежить ефективність життєдіяльності сучасного суспільства. Інформаційні технології принципово змінили обсяг і важливість інформації, її потік в технічних засобах зберігання, обробки і передачі.

О. Панченко слушно зауважує: «Загальна комп'ютеризація основних сфер діяльності привела до появи широкого спектра внутрішніх і зовнішніх загроз, нетрадиційних каналів втрати інформації і несанкціонованого доступу до неї. Інформаційна сфера держави – це єдиний інформаційний простір, який формується державними органами, громадськими, політичними і соціальними організаціями, а також громадянами, і функціонує на основі правових, організаційних, науково-технічних, економічних, фінансових, методичних, гуманітарних і моральних принципів з урахуванням вимог і задач національної інформаційної безпеки. Політику національної інформаційної безпеки потрібно проводити тільки в тих формах і тими методами і засобами, які притаманні і прийнятні демократичною правовою державою, тобто ґрунтуються на

принципах демократії і верховенства права. Інформаційне законодавство повинно бути спрямовано на закріплення державної інформаційної політики, яка передбачає забезпечення гарантованого рівня національної безпеки в інформаційній сфері, нормального розвитку інформаційних технологій і засобів захисту інформації, виключення монополізму в цій галузі, запобігання розробці інформаційно-деструктивних технологій впливу на суспільство, захист авторських і суміжних прав тощо» [38].

О. Панченко долає: «Система забезпечення інформаційної безпеки України створюється і розвивається відповідно до Конституції України та інших нормативно-правових актів, що регулюють суспільні відносини в інформаційній сфері. Так, Закон України «Про основи національної безпеки України» розрізняє дві ключові категорії, які зумовлюють зміст і спрямованість державної політики в сфері інформаційної безпеки:

1) загрози національним інтересам і національній безпеці України в інформаційній сфері (ст. 7), до яких належать:

– прояви обмеження свободи слова та доступу громадян до інформації;

– поширення засобами масової інформації культу насильства, жорстокості, порнографії;

– комп'ютерна злочинність та комп'ютерний тероризм

– розголошення інформації, яка є державною і іншою, передбаченою законом, таємницею, а також конфіденційної інформації, яка є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– спроби маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації;

2) основні напрями державної політики з питань національної безпеки в інформаційній сфері (ст. 8):

– 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, зловживання службовим становищем, іншим явищам, які загрожують національній безпеці України;

– забезпечення неухильного дотримання конституційних прав на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації та журналістів, заборони цензури, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції, за виконання професійних обов'язків, за критику;

– прийняття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України» [38].

На думку науковця: «Пріоритетами державної політики забезпечення інформаційної безпеки України є:

– забезпечення послідовності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії;

– створення інтегрованої системи оцінки інформаційних загроз і оперативного реагування на них;

– протидія інформаційним операціям проти України, маніпуляцій суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей і зміцнення єдності українського суспільства;

– розробка і реалізація скоординованої інформаційної політики органів державної влади;

– виявлення суб'єктів українського інформаційного простору, створених для ведення інформаційної війни проти України, і неможливість їх підривної діяльності;

– створення і розвиток інститутів, що відповідають за інформаційно-психологічну безпеку;

– вдосконалення професійної підготовки в сфері інформаційної безпеки, впровадження загальнонаціональних освітніх програм з медіакультури із залученням громадянського суспільства та бізнесу.

Загалом можна зробити такі висновки:

1. Умови інформатизації суспільства призводять до швидких та постійних змін у суспільних відносинах. Суспільство має вміти ефективно реагувати на ці зміни, пристосовуючи відносини до нових реалій і запобігаючи появі небажаних процесів.

Для держави ключовою є наявність сучасної концепції переходу до інформаційного суспільства, яка відрізняється від попередніх концепцій, орієнтованих головним чином на технічне забезпечення суспільних процесів.

2. Головна мета для держави на рівні законодавства полягає в створенні механізму, який би забезпечував відповідність процесу розробки законів прогресу інформаційних технологій.

Зрозуміло, що законодавство не може оперативно реагувати на всі аспекти життя, але важливо, щоб відставання не було надто значним, оскільки це може призвести до погіршення інформаційної безпеки, серед інших негативних наслідків.

3. Інформація стає одним з ключових національних ресурсів, що визначають економічний, науково-технічний та оборонний потенціал держави.

Під впливом процесів інформатизації всі сфери суспільного життя отримують нові якості, такі як оперативність, гнучкість та динамічність.

У сучасних умовах проблеми інформаційного забезпечення у всіх сферах діяльності стають більш важливими та актуальними, ніж проблеми подальшого зростання виробництва, які раніше вважалися пріоритетними.

4. На індивідуальному рівні, інформаційна безпека повинна гарантувати захист психіки та свідомості людей від потенційно небезпечних інформаційних впливів, таких як маніпуляція, дезінформація та пропаганда самогубства.

На рівні суспільства та держави, інформаційна безпека має забезпечувати стійкість основних сфер життєдіяльності (включаючи економіку, науку, державне та військове керівництво, а також громадську свідомість) від небезпечних, дестабілізуючих та деструктивних інформаційних впливів.

1.3 Структура інформаційної безпеки та її елементи

Безпечність інформації на рівні особистості має гарантувати захист психіки та свідомості від потенційно шкідливих впливів, таких як маніпуляція, дезінформація та інші негативні впливи. На рівні суспільства та держави, інформаційна безпека спрямована на забезпечення стійкості та безпеки ключових сфер життєдіяльності від небезпечних, дестабілізуючих та руйнівних інформаційних впливів.

Як зазначає Т. Мужанова: «Суб'єктами забезпечення інформаційної безпеки є:

– держава, яка здійснює функції у цій галузі через органи законодавчої,– виконавчої та судової влади;

– комерційні, громадські, інші організації та об'єднання;

– громадяни, які відповідно до законодавства мають права й обов'язки щодо участі у забезпеченні безпеки держави» [33].

Науковець додає: «Головну роль при цьому відіграє держава, яка відповідно до чинного законодавства повинна забезпечувати інформаційну безпеку на рівні особи (дотримання прав і свобод особи в інформаційній сфері, сприяння формуванню раціонального, критичного мислення на основі принципів свободи вибору, забезпечення захисту конфіденційної інформації особи), суспільства (формування якісного інформаційно-аналітичного простору, забезпечення плюралізму, багатоканальності отримання інформації, незалежної діяльності ЗМІ) і держави (інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення внутрішньої і зовнішньої політики держави, функціонування системи захисту інформації з обмеженим доступом, протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам тощо). У залежності від об’єктного складу (особи, суспільства або держави, що є об’єктом) визначають такі види інформаційної безпеки:

–особисту (безпеку конкретної особи);

– суспільну (безпека суспільства);

– державну (безпеку окремої держави);

– міжнародну (безпеку багатьох держав, світового співтовариства загалом). [38].

А. Тручак заначає: «Держави, котрі не здатні до забезпечення власної інформаційної безпеки, перетворюються на неконкурентоспроможні і, як підсумок, втрачають змогу боротися за ринки та ресурси. Великі держави зникли частково через нездатність ефективноуправлятинавласнихтериторіях та інформаційну структуру, що не могла дієво функціонувати в нових умовах існування. Тому не можна заперечувати те, що будь-яка розвинена країна повиннамати систему, що забезпечувала б інформаційну безпеку, а перелік

закріплених за відповідними державними органами функцій та повноважень повинен бути закріплений в законодавстві. Явище «інформаційна безпека» передбачає якісне інформування людей та вільний доступ до різноманітних інформаційних баз, однак повинні бути ще й контролюючі діїщодо нерозповсюдження секретної інформації, підтримання соціуму у цілісному стані, захист від будьякого негативного інформаційного впливу таке ін. Вирішення такого комплексного проблемного питання дасть можливість як захисту суспільних і державних інтересів, так і сприяння утвердженню прав громадянина на всебічну та якісну інформацію» [33].

Науковець додає: «Щоб ефективно забезпечувати інформаційну безпеку в країні, необхідно вирішити такі масштабні завдання:

– розробити теоретичні основи по забезпеченню захисту інформації;

– створити систему структур, які б відповідали за збереження інформаційної безпеки;

– вирішити питання щодо захисту інформації і налагодити її автоматизацію;

– створити нормативно-правову базу, що регламентувала б вирішення всіх завдань, пов’язаних із забезпеченням інформаційного захисту; почати виробляти засоби інформаційної безпеки;

– організувати підготовку спеціалістів відповідного фаху тощо.

Концепція національної безпеки розглядає два аспекти терміну "інформаційна безпека". Згідно з першим підхідом, інформаційна безпека розглядається як окремий компонент національної безпеки в будь-якій країні, а згідно з другим - як важлива складова будь-якого іншого виду безпеки, такого як військова, економічна, політична» [58].

Одне з найбільш повних визначень "інформаційної безпеки" розглядає її як стан, коли особисті, суспільні та державні інтереси захищені від негативних

впливів, таких як маніпуляція, дезінформація та інші негативні наслідки. Це включає мінімізацію шкоди, спричиненої неповною, несвоєчасною та недостовірною інформацією, негативними впливами інформації та проблемами, пов'язаними з функціонуванням інформаційних технологій. Ця концепція об'єднує майже всі аспекти інформаційної взаємодії, в якій залучені державні суб'єкти.

Інформаційна безпека, як невід'ємна складова національної безпеки, вперше була визначена в Законі "Про основи національної безпеки України". Інформаційний суверенітет країни і його захист дуже пов'язані з інформаційною безпекою, яку можна розглядати як захищеність внутрішніх інформаційних ресурсів, таких як якість інформації, рівень її надійності, захищеність різних сфер інформації від розголосу та захищеність інформаційно-ресурсної бази.

З іншого боку, інформаційна безпека може розглядатися як контроль інформаційних потоків, обмеження використання провокативної, агресивної інформації для суспільства, регулювання рекламної інформації; механізм, за допомогою якого захищають національний інформаційний простір від зовнішнього інформаційного вторгнення.

Серед основних складових інформаційної безпеки держави виокремлюють: обсяг інформаційного продукту, який виробляється в державі; здатність мереж витримувати зростаюче інформаційне навантаження; можливість держави керувати розвитком вироблення та розповсюдження інформації; доступ населення до усіх можливих інформаційних джерел та відкритість більшості з них.

Потребу забезпечити інформаційну безпеку зумовлюють багато факторів: необхідність підтримати національну безпеку Української держави загалом; наявність небезпек, що загрожують інформаційному середовищу держави і

можуть нести шкоду для загальних національних інтересів; можливість шляхом інформаційного впливу частково керуватисвідомістюіповедінкоюгромадян. Інформаційна безпека України має перед собою головне стратегічне завдання: створити потужний національний інформаційний простір як головний аспект, що засвідчує присутність країни на світовій інформаційній арені.

Також така ціль передбачає потребу створити систему протистояння будь-якій інформаційній загрозі та оборону власних інформаційних ресурсів, середовища та інфраструктурної складової країни. Враховуючи те, що національному інформаційному ресурсу нині відводиться роль одного з основних чинників, на якому базується економічна потужність країни та її суб'єктів, необхідно формулювати державні інтереси, фактори і загрози для інформаційної сфери, аналізувати ефективність наявної системи захисту та можливості її покращення.

Державна інформаційна політика створює контекст для того, щоб обговорення стосувалося не лише прав людей, юридичних осіб і країни в інформаційній галузі, але і потреби захистити інтелектуальну власність, державні інформаційні ресурси та конфіденційну інформацію.

Як зазнчає А. Турчак: «Окрім того, можна виділити ряд основних положень держполітики забезпечення інформаційної безпеки:

– скорочення доступності інформації є винятком із загальних засад про відкритість інформаційних джерел і реалізується лише на законодавчій підставі;

– необхідність персоніфікації відповідальності за те, що інформацію зберігали, засекретили чи розсекретили;

– надання та вилучення доступу до інформаційних ресурсів реалізується на підставі законодавчо затвердженого права власності на цю інформацію;

– державою формується нормативно-правова база, що здійснюватиме

регулювання прав, обов'язків і відповідальності всіх суб'єктів в інформаційному просторі;

– наявність правової відповідальності юридичних і фізичних осіб, що займаються збором, нагромадженням і обробкою персональних даних і конфіденційної інформації, за її збереження і використання; країна законним чином захищає суспільство від помилкових, перекручених і недостовірних відомостей, що надходять через ЗМІ;

– влада контролює створення і використання будьякого засобу інформаційного захисту, в обов’язковому порядку сертифікуючи такий і ліцензуючи діяльність у галузі інформаційної безпеки; протекціоністська політика з боку держави, що означає підтримку вітчизняного виробника, що виготовляє засоби інформатизації і захисту інформації, і здійснення заходів для того, щоб захистити внутрішній ринок від появи на ньому неякісного інформаційного продукту;

– держава робить світові інформаційні ресурси, глобальні інформаційні мережі доступнішими для громадян;

– країна намагається відмовитися використовувати закордонні інформаційні технології для інформатизації державних владних і управлінських структур і віддати перевагу конкурентоздатним вітчизняним аналогам;

– в державі формується програма інформаційної безпеки, в якій консолідують свої сили державні організації і комерційні структури задля того, щоб створити єдину систему інформаційної безпеки;

– країна активно протидіє інформаційному вторгненню з боку решти держав, сприяє тому, щоб глобальні інформаційні мережі й системи інтернаціоналізувалися» [58].

Науковець додає: «Згідно з вищеназваними принципами і положеннями забезпечити інформаційну безпеку країни можна, зробивши ряд важливих

кроків:

– розвинути науковопрактичні основи інформаційної безпеки у відповідності до сучасної геополітичної ситуації та умов, продиктованих політичним і соціально-економічним розвитком;

– формувати законодавчу і нормативно-правову бази,щоб забезпечити інформаційну безпеку, зокрема розробити реєстр інформаційних ресурсів, регламентувати інформаційний обмін між органами держвлади, підприємствами, нормативно закріпити відповідальність посадовців і пересічних українців за відповідність критеріям інформаційної безпеки;

– розробити механізми втілення права громадянина на інформацію; формувати систему інформаційного захисту, що є складником загального механізму нацбезпеки України;

– розробити сучасні методи і технічні засоби, що забезпечували б комплексний підхід до вирішення завдань інформаційного захисту;

– розробити критерії і методи, за якими оцінюватимуться системи і засоби інформаційної безпеки з точки зору ефективності і їх сертифікації;

– дослідити форми і можливості державі цивілізовано впливати на суспільну свідомість;

–комплексно дослідити діяльність кадрів в інформаційних системах, зокрема методи мотивування, посилити моральнопсихологічну стійкість і соціальну захищеність фахівців, що мають справу із секретними і конфіденційними даними» [58].

Національну інформаційну безпеку визначають як систему заходів на загальнонаціональному рівні, спрямованих на запобігання несанкціонованому доступу, модифікації та руйнації інформаційних ресурсів. Основні цілі включають захист політичних, державних і суспільних інтересів, збереження моральних цінностей і запобігання поширенню інформації, що пропагує

агресію, насилля, дискримінацію та порушення прав людини. Українська держава має певні пріоритети, встановлені законодавством, що стосуються інформаційної сфери, такі як гарантування конституційних прав і свобод, зміцнення науково-технологічного потенціалу, захист української мови як державної, розвиток духовності, моральних цінностей і інтелектуального потенціалу українського народу.

Однією з ключових проблем безпеки в інформаційній сфері є забезпечення захисту та контролю за національною інформаційною базою та розповсюдженням інформації про державу у світовому інформаційному просторі. Під інформаційним простором мається на увазі середовище, де відбувається створення, збір, зберігання, обробка і поширення інформаційних даних, підпорядковане державній юрисдикції. Важливо забезпечити надійну роботу всіх компонентів цієї системи для забезпечення безпеки. Однією з основних мет у цій сфері є створення повноцінної відкритої інформаційної бази. Відсутність або негативний характер інформації про сучасний світ може впливати на рівень зовнішньополітичної і економічної діяльності як на державному, так і на індивідуальному рівні. Ця проблема має загальнодержавне значення, і її ігнорування може стати загрозою для національної безпеки

Як зазначає М. Гаврильців: «Інформаційна сфера стала системоутворюючим фактором життя суспільства й активно впливає на стан політичної, економічної, оборонної та інших складових частин безпеки України. Проте, оперуючи інформацією, потрібно бути переконаним у тому, що використовувана інформація якісний у процесі передачі, поширення не була спотворена. Тому питання інформаційної безпеки є важливим компонентом усієї системи національної безпеки країни.

Зрозуміло, що сьогодні українське суспільство перебуває під постійною загрозою отримання недостовірної, а подеколи – шкідливої інформації, її

несвоєчасного надходження, шпигунства, комп'ютерної злочинності тощо. Ці фактори є елементами гібридної війни, які сприяють вторгненню агресора в національну свідомість громадян, підриву національної та інформаційної безпеки» [7].

Основними складовими елементами інформаційної безпеки є як забезпечення якісного інформування громадян і вільного доступу до різних джерел інформації, так і захист від негативних інформаційних впливів, що у сукупності мають сприяти цілісності суспільства. Першочерговим завданням соціальних і державних інститутів має бути розробка термінових ефективних заходів щодо нейтралізації інформаційно-диверсійної діяльності РФ проти України та запобігання її подальшому розгортанню. Вирішення цієї комплексної проблеми дозволить захистити інтереси суспільства і держави, сприяти реалізації права громадян на отримання всебічної та якісної інформації [26].

Як зазначає М. Гаврильців: «В умовах гібридної війни держава, що стала об'єктом агресії, неминуче наражається на широкий спектр інформаційних загроз, нейтралізація яких, з одного боку, вимагає вжиття надзвичайних правових і адміністративних заходів, а з іншого – може супроводжуватися істотним згортанням демократичних прав і свобод. Пошук балансу між інтересами національної безпеки й ідеями верховенства права – це стратегічно важливе завдання держави. Нормативно-правова регламентація формування єдиного інформаційного простору України повинна сприяти гармонійному розвитку інформаційних ресурсів, інформаційних послуг та інформаційного продукту в країні. Важливість проблеми розвитку законодавства у сфері інформації та інформаційної безпеки, становлення інформаційного суспільства визначається тією обставиною, що норми законів цієї сфери суттєво впливають на законодавче регулювання відносин суб'єктів у всіх сферах життя держави. В

умовах проведення країною-агресором РФ деструктивного інформаційного впливу на цільову аудиторію України та інших держав світу можна визначити такі основні напрями вжиття заходів щодо захисту національного інформаційного простору і забезпечення національної системи інформаційної безпеки України: по-перше, удосконалити нормативно-правову базу у сфері інформаційної політики держави, яка б визначала взаємодію силових структур України з органами місцевого самоврядування, державними органами та громадськими інституціями; по-друге, створити єдиний міжвідомчий координаційний орган, який би здійснював керівництво, координацію та контроль заходів інформаційної безпеки, (його, наприклад, можна створити у вигляді міжвідомчої комісії при РНБО); по-третє, створити систему комплексного моніторингу популярних аудіовізуальних і друкованих ЗМІ, а також популярних Інтернетресурсів; по-четверте, заохочувати подальші комплексні наукові дослідження у сфері інформаційної безпеки. На основі Стратегії національної безпеки України Указом Президента України була затверджена Доктрина інформаційної безпеки України, що лягла в основу національної політики інформаційної безпеки. Метою доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу РФ в умовах розв’язаної нею гібридної війни. Доктрина визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями, пріоритети державної політики в цій сфері. Державна інформаційна політика в умовах глобалізації буде ефективною лише у тому разі, якщо вона матиме комплексний, системний характер і, безперечно, буде відкритою, направленою на удосконалення інтересів громадян, суспільства і держави».

Узагальнюючи, політика інформаційної безпеки є складним явищем, що включає в себе різноманітні аспекти, такі як внутрішньополітичні,

зовнішньополітичні, економічні, технологічні, військові та інші, тому потребує комплексного підходу. Органи державної влади повинні спрямовувати свою діяльність на досягнення конкретних цілей у цій сфері та об’єднувати свої зусилля з метою забезпечення інформаційної безпеки України. Система інформаційної безпеки країни є складовою загальної системи національної безпеки та включає в себе органи державної влади, недержавні структури та громадян, які повинні спільно діяти для забезпечення інформаційної безпеки на основі єдиної правової бази.

РОЗДІЛ 2
ОСОБЛИВОСТІ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Характеристика державної політки України у сфері інформаційної безпеки

Зростання залежності сучасного суспільства від стійкого функціонування інформаційної інфраструктури робить реалізацію національних інтересів України в інформаційній сфері важливим фактором національної безпеки. Тож для України нині необхідним кроком на шляху до інформаційного майбутнього є розроблення цілісної гнучкої динамічної державної політики у сфері забезпечення інформаційної безпеки, яка враховуватиме багатоаспектність явища інформаційної безпеки, перспективні тенденції змін інформаційного простору, особливості геополітичного становища, економічного стану країни і знайде своє відображення у суспільній свідомості. Інформаційна політика держави в сучасному політичному процесі розглядається як окремий вид політичної діяльності. Основні підходи до проблеми становлення державної інформаційної політики сформувалися ще в XIX ст. й отримали новий поштовх до розвитку в 60-х рр. XX в. у зв'язку зі вступом розвинених країн у стадію інформаційного розвитку

С. Бондаренко зазначає: «Під державною інформаційною політикою розуміє цілеспрямовану діяльність центральних органів влади з формування політико-релевантного знання про державу, його поширення та управління в інформаційному просторі з метою досягнення політичних цілей і захисту національних інтересів» [57].

Як зазначає Т. Ткачук: «Інформаційну політику держави також розглядають як діяльність держави в інформаційній сфері, спрямовану на

задоволення інформаційних потреб людини і громадянина через формування відкритого інформаційного суспільства на основі розвитку єдиного інформаційного простору цілісної держави та його інтеграції у світовий інформаційний простір з урахуванням національних особливостей і інтересів під час забезпечення інформаційної безпеки на внутрішньодержавному та міжнародному рівні. Основною метою державної політики у сфері забезпечення інформаційної безпеки при цьому є управління реальними та потенційними загрозами з метою створення необхідних умов для задоволення інформаційних потреб людини та громадянина, а також реалізації національних інтересів» [57].

Б. Кормич додає: «Інформаційна безпека забезпечується проведенням єдиної державної політики в інформаційній сфері, системою заходів економічного, політичного й організаційного характеру, які є адекватними загрозам національній безпеці, а також можливостям держави щодо здійснення управління відповідними ризиками. Система забезпечення інформаційної безпеки є інструментом реалізації державної політики у сфері забезпечення інформаційної безпеки. Головне призначення цієї системи полягає у досягненні цілей національної безпеки в інформаційній сфері, а отже, її основною функцією є забезпечення збалансованого існування інтересів особи, суспільства і держави в інформаційній сфері. Державна політика у сфері забезпечення інформаційної безпеки має три основних вектори: захист інформаційних прав і свобод людини, захист державної безпеки в інформаційній сфері та захист національного інформаційного ринку, економічних інтересів держави в інформаційній сфері, національних виробників інформаційної продукції» [57].

Враховуючи національні інтереси та загрози в інформаційній сфері, Закон України «Про основи національної безпеки України» визначає основні напрями державної політики у сфері забезпечення інформаційної безпеки» [45].

Єдність і взаємозв'язок напрямів державної політики у сфері забезпечення інформаційної безпеки має забезпечуватися визначеними на законодавчому рівні правовими механізмами, серед яких: чіткі цілі і завдання державної політики; взаємодія державних і громадських інститутів із реалізації міжвідомчих напрямів державної політики; організація системи інформування суб'єктів, що діють у сфері забезпечення інформаційної безпеки, про актуальні проблеми, виявлення потенційних і реальних загроз та їх джерела, а також доцільні заходи і засоби щодо їх попередження, нейтралізації та ліквідації можливих наслідків; узгоджені і цілеспрямовані дії суб'єктів, що діють у різних сферах життєдіяльності суспільства і держави з питань адекватного реагування на виявлені потенційні і реальні загрози; загальнодержавне керівництво, координація та контроль у сфері забезпечення інформаційної безпеки [45].

Т. Ткачук зазначає: «З огляду на необхідність вдосконалення нормативно-правового забезпечення та попередження й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері, з початком гібридної війни проти України виникла необхідність кардинальних змін у системі забезпечення інформаційної безпеки України. Основний план заходів запроваджено у рішенні РНБО від 28 квітня 2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України», затвердженого Указом Президента України № 449/2014 від 1 травня 2014 р. Згідно з рішенням РНБО, Кабінету Міністрів України було доручено розробити і внести на розгляд парламенту законопроекти про внесення змін у закони України щодо протидії інформаційній агресії іноземних держав, передбачивши, зокрема, визначення механізму протидії негативному інформаційно-психологічному впливу, зокрема шляхом заборони ретрансляції телевізійних каналів, а також щодо запровадження для іноземних ЗМІ системи інформування та захисту

журналістів, які працюють у місцях збройних конфліктів, вчинення терористичних актів, ліквідації небезпечних злочинних груп. Крім того, необхідно було розробити проект стратегії розвитку інформаційного простору України, розробити і впровадити комплексні заходи організаційного, інформаційного і роз'яснювального характеру щодо всебічного висвітлення заходів із реалізації державної політики у сфері забезпечення інформаційної безпеки, а також посилити контроль за дотриманням законодавства з питань інформаційно-психологічної та кібернетичної безпеки. Відповідно до вказаного плану заходів було розроблено, зокрема, Стратегію кібербезпеки України, за якою розвиток та безпека кіберпростору, запровадження електронного урядування, гарантування безпеки й сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів мають бути складниками державної політики у сфері розвитку інформацій- ного простору та становлення інформаційного суспільства в Україні [10], та Доктрину інформаційної безпеки України [57].

Необхідність прийняття Доктрини інформаційної безпеки України обумовлена виникненням актуальних загроз національній безпеці в сфері інформації та потребою у визначенні інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації. Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, особливо щодо протидії руйнівному інформаційному впливу РФ у зв'язку з її гібридною війною. Цей документ визначає національні інтереси України в інформаційній сфері, ідентифікує загрози їх реалізації, визначає напрями та пріоритети державної політики в інформаційній сфері. Його правовою основою є Конституція України, закони країни, Стратегія національної безпеки України, затверджена Указом Президента від 26 травня 2015 року № 287, а також міжнародні

договори, згода на обов'язковість яких надана Верховною Радою України.

Т.Ткачук слушно зауважує: «З метою реалізації Доктрини РНБО має здійснювати координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері. Зважаючи на особливі умови і ведення проти нашої держави агресивної інформаційної війни не лише на її території, але й у світі, забезпечення реалізації Доктрини можливе лише за умови належної координації заходів, здійснюваних усіма державними органами. Кабінет Міністрів України забезпечуватиме здійснення інформаційної політики держави, фінансування програм, пов'язаних з інформаційною безпекою, спрямовуватиме і координуватиме роботу міністерств, інших органів виконавчої влади у цій сфері. Доктриною також покладається низка завдань на Міністерство інформаційної політики України, Міністерство закордонних справ, Міністерство оборони, Службу безпеки України, Державну службу спеціального зв'язку та захисту інформації, розвідувальні органи, Національний інститут стратегічних досліджень. Участь у забезпеченні захисту українського інформаційного простору від пропагандистської аудіовізуальної та друкованої продукції держави-агресора, розробленні пріоритетів і стимулів розвитку українського кіно, телевізійного контенту, книгодрукування, зокрема, щодо висвітлення героїчного спротиву українського народу російській агресії також беруть Міністерство культури України, Державне агентство України з питань кіно, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України відповідно до їх компетенції» [57].

Наводячи наочні позитивні зміни у сфері формування та реалізації державної політики забезпечення інформаційної безпеки, важливо врахувати ряд проблем у цьому напрямі. Зокрема, сучасна інформаційна інфраструктура в Україні все ще у процесі формування. Нормативно-правова база у сфері масової

інформації ще не є повністю розвиненою. Відсутність конкретної державної політики у сфері національного інформаційного простору, розвитку масових медіа та організації міжнародного інформаційного обміну також видається проблемою. Також варто відзначити погіршення ситуації зі збереженням державної таємниці. Органи державної влади та місцевого самоврядування змушені користуватися імпортною технікою, оскільки вітчизняна індустрія інформаційних технологій не має достатньої підтримки від держави, що збільшує ризик несанкціонованого доступу до інформації. Особливо небезпечною є ситуація з придбанням програмного й апаратного забезпечення виробництва країни-агресора. На додаток, безпека в інформаційно-психологічній сфері в основному розглядається з технічної точки зору, і це призводить до зростання інформаційної агресії з боку Росії, яка використовує соціально-політичну ситуацію в Україні для просування своїх інтересів, включаючи участь українців.

О. Руденко зазначає: «Події, що відбуваються в Україні, свідчать про використання іноземними суб'єктами зарубіжних і вітчизняних ЗМІ, соціальних мереж для зміни стану інформаційного простору з метою справляння впливу на хід подій, що завдає нашій країні відчутних політичних і економічних збитків. Відкритість національного інформаційного простору породжує реальну загрозу негативного інформаційно-психологічного впливу на суспільну свідомість населення, що становить особливу соціальну небезпеку. Безконтрольність електронних мас-медіа та соціальних мереж, які використовуються як майданчик для вербування в екстремістські організації, злочинні угруповання, незаконні збройні формування тощо, негативно впливає на користувачів мережі Інтернет, якими переважно є молодь й освічені люди з активною життєвою позицією. Варто також враховувати, що українське суспільство нині розколоте за ставленням до таких фундаментальних

цінностей, як демократія, незалежність, приватна власність, ринок тощо. Є розбіжності щодо уявлень про форму державного устрою та правління, кількість мов офіційного спілкування та навчання, напрямки децентралізації, функції і завдання місцевого самоврядування тощо. Існує ціла низка міжрегіональних, міжетнічних, міжконфесійних розбіжностей, різна шкала цінностей та пріоритетів, а тому важко говорити про єдність інформаційного простору та спільні ціннісні орієнтації» [46].

У сучасний час в Україні відсутні належні законодавчі гарантії захисту населення від негативних інформаційно-психологічних впливів, які можуть спричинити руйнування єдиного інформаційного та духовного простору. Тому необхідно створити державну систему, яка б забезпечувала інформаційно-психологічну безпеку з належним нормативно-правовим базисом у сфері масової інформації.

Також відсутня чітка державна політика стосовно формування національного інформаційного простору, розвитку масових медіа та організації міжнародного обміну інформацією.

Це призводить до погіршення ситуації зі збереженням державної таємниці, оскільки органи державного управління змушені придбавати імпортну техніку, через недостатню підтримку вітчизняної індустрії інформаційних технологій.

Необхідно також звернути увагу на психологічний аспект забезпечення інформаційної безпеки, оскільки це може призвести до посилення інформаційної агресії з боку Росії, яка використовує соціально-політичну ситуацію в Україні для досягнення своїх цілей, включаючи маніпуляції з участю українських громадян.

Як зазначає Т.Ткачук: «Нині в Україні на законодавчому рівні відсутні достатні гарантії захисту населення від негативних інформаційно-

психологічних впливів, результатом яких може стати руйнування єдиного інформаційного й духовного простору. Тому виникає необхідність формування державної системи забезпечення інформаційно-психологічної безпеки, яка має буду а також громадських організацій. У процесі реалізації державної політики в області безпеки необхідно звернути увагу на: розроблення й реалізацію комплексних заходів щодо запобігання, нейтралізації й випередження негативних інформаційно-психологічних впливів на суспільство і державу; підготовку суспільства до активної інформаційної протидії; входження національного інформаційного поля у світовий інформаційний простір; удосконалення системи масової інформації й комунікації; формування системи підготовки кадрів для інформаційно-психологічної протидії; духовну консолідацію суспільства і віднайдення всіма верствами населення нової соціальної ідентичності. За сучасних умов інформаційна безпека має визнаватися основою інформаційної складової частини усіх сфер забезпечення національної безпеки. До головних завдань системи забезпечення інформаційної безпеки належать: прогнозування ризиків реалізації державної внутрішньої і зовнішньої політики, міждержавних та державних програм і проектів; виявлення внутрішніх і зовнішніх потенційних і реальних загроз; розроблення і впровадження адекватних заходів і засобів реагування на виклики а також громадських організацій. У процесі реалізації державної політики в області безпеки необхідно звернути увагу на: розроблення й реалізацію компексних заходів щодо запобігання, нейтралізації й випередження негативних інформаційно-психологічних впливів на суспільство і державу; підготовку суспільства до активної інформаційної протидії; входження національного інформаційного поля у світовий інформаційний простір; удосконалення системи масової інформації й комунікації; формування системи підготовки кадрів для інформаційно-психологічної протидії; духовну

консолідацію суспільства і віднайдення всіма верствами населення нової соціальної ідентичності» [57].

Р. Шаповал та В. Клочко: «За сучасних умов інформаційна безпека має визнаватися основою інформаційної складової частини усіх сфер забезпечення національної безпеки. До головних завдань системи забезпечення інформаційної безпеки належать: прогнозування ризиків реалізації державної внутрішньої і зовнішньої політики, міждержавних та державних програм і проектів; виявлення внутрішніх і зовнішніх потенційних і реальних загроз; розроблення і впровадження адекватних заходів і засобів реагування на виклики як історичного походження, так і сучасного цивілізаційного розвитку; нейтралізація або послаблення дії проявів гібридної війни та інших загроз національній безпеці України. Системний і комплексний підхід до вирішення цих завдань має відповідним чином визначати спрямування державної політики у сфері забезпечення інформаційної безпеки нашої держави» [62].

Забезпечення безпеки інформації стоїть перед владою як ключовий пріоритет, який безпосередньо впливає на життєздатність держави, її незалежність, національну безпеку, а також соціально-економічний розвиток та позицію в світовому співтоваристві. Сучасна державна інформаційна політика повинна вирішувати комплекс завдань, спрямованих на гармонійне забезпечення безпеки інформації для держави, громадян та суспільства, при цьому визначаючи найважливіші пріоритети. Це включає створення або відновлення основних пунктів захисту національної безпеки в інформаційній сфері, ефективну систему інформаційної безпеки держави, перегляд та виявлення нових загроз інформаційної безпеки, а також ліквідацію наявних, оцінку можливих наслідків і ступеня їхньої загрозливості.

2.2 Правові та політичні засади державної політики у сфері

інформаційної безпеки

Забезпечення безпеки інформації в Україні та захист її національних інтересів у цій сфері передбачає пріоритетний розвиток системи нормативно-правового регулювання відносин у цьому контексті, спрямований на протидію загрозам цих інтересів та організацію відповідного правотворчого процесу. У останній час державні установи все більше уваги приділяють обговоренню питань щодо вдосконалення правового забезпечення інформаційної безпеки України. Система правового регулювання інформаційної безпеки, в свою чергу, включає широкий спектр правових норм, які регламентують відносини в даній сфері. Ці норми складають основу забезпечення інформаційної безпеки та визначають ефективність діяльності держави, суспільства та окремих громадян у захисті національних інтересів України у сфері інформації. Склад цієї бази включає норми міжнародних договорів України, акти Президента України, розпорядження уряду та нормативні документи органів державної влади, які регулюють відносини у цьому напрямк

А.Козачинська зазначає: «Наразі перед державою постала необхідність прийняти велику кількість нормативно-правових актів, які відповідають європейським стандартам. Аналіз стану нормативно-правового регулювання інформаційної безпеки реалізується за трьома чинниками. Інформаційну безпеку України становлять три структурні елементи:

1. Інформаційна безпека у сфері прав і свобод людини та громадянина.

2. Інформаційно-психологічна безпека.

3. Інформаційно-технічна безпека» [21].

Дослідниця додає: «Нормативно-правове регулювання інформаційної безпеки у сфері прав та свобод реалізується Конституцією України та опорними законами України, такими як: «Про Концепцію Національної програми інформатизації», «Про інформацію», «Про Національну програму

інформатизації», «Про поштовий зв'язок», «Про науково-технічну інформацію» та ін. Вказані вище нормативно-правові акти регулюють питання забезпечення інформаційної безпеки, питання захисту інформації, охорони державної таємниці, забезпечення захисту конфіденційної інформації та інформаційних ресурсів. Загрози інформаційної безпеки – це існуючі або можливі явища та фактори, що утворюють загрозу буденним інтересам людини та громадянина, суспільства та держави в інформаційній сфері. Інформаційна безпека України забезпечується шляхом захисту державного інформаційного простору від інформаційних загроз та через підтримання його стійкому розвитку з метою втілення життєво важливих інтересів та потреб громадянина, суспільства та держави в інформаційній сфері. Основними положеннями забезпечення інформаційної безпеки України є:

–верховенство права;

– перевага захисту прав і свобод людини та громадянина в інформаційній сфері;

– своєчасні та адекватні заходи захисту життєво важливих державних інтересів України від дійсних та можливих загроз інформаційній безпеці; захист інформаційного суверенітету України;

– незалежність думки та слова, а також вільне виявлення своїх поглядів та принципів;

свобода збирати, зберігати, використовувати та поширювати інформацію;

– захист інформаційного суверенітету, національного суверенітету, конституційного ладу та територіальної цілісності України; утворення в інформаційному просторі української ідентичності як невід'ємного компоненту постійного суспільно-політичного дискурсу;

– сприяння розвитку в національному інформаційному просторі контенту, який підтримує збереження та захист загальнолюдських цінностей,

інтелектуальний, духовний та культурний розвиток Українського народу Козачинська.

Як зазначено в законі: «Державна політика у сфері інформаційної безпеки реалізується з метою недопущення перешкоджання виконання важливих інтересів та потреб громадянина, суспільства та держави зовнішніми та внутрішніми загрозами державній безпеці в інформаційній сфері, що є гарантією стійкого розвитку державного інформаційного простору. Загрозами національній безпеці України в інформаційній сфері є: загрози комунікативного характеру, що проявляються в сфері виконання потреб людини та громадянина, суспільства та держави щодо формування, використання, розповсюдження та розвитку державного ресурсу інформації; загрози технологічного характеру в сфері функціонування і захищеності телекомунікаційних, кібернетичних та інших систем, що утворюють матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору» [40].

У законі також зазначено: «Загрози комунікативного характеру в сфері реалізування потреб людини та громадянина, суспільства та держави щодо утворення, використання, поширення та розвитку державного контенту та інформації включають:

а) навколишні негативні інформаційні впливи на свідомість людини та товариства через інформаційні ресурси, а саме: засоби масової інформації, мережу Інтернет, які завдають шкоду державі та основною ціллю яких є спроби змінити психічні та емоційні стани людини, її фізіологічні та психологічні характеристики; керування свободою вибору, шляхом поширення у національному інформаційному просторі культу насильства та жорстокості, зверхнього ставлення до людської та національної гідності, розпалювання міжетнічної та міжнаціональної, міжрелігійної ворожнечі, ненависті за етнічною, мовною, релігійною та іншими ознаками; розповсюдження закликів

до сепаратизму, повалення конституційного ладу чи порушення територіальної єдності країни;

б) поширення суб'єктами інформаційної діяльності недостовірної та упередженої інформації для приниження органів державної влади, підриву суспільно-політичної ситуації, що перешкоджає правильному прийняттю політичних рішень, а також завдає шкоди державним інтересам країни та створює негативний імідж України.

Загрози технологічного характеру у сфері діяльності та захищеності телекомунікаційних, кібернетичних та інших автоматизованих систем, які утворюють матеріальну (технічну, інструментальну) основу внутрішньодержавного інформаційного простору включають:«

а) застосування іноземними країнами кібервійськ, кіберпідрозділів, нових видів інформаційної зброї та зброї кібернетичного характеру на шкоду нашій державі;

б) вияви кіберзлочинності, кібертероризму чи кібернетичної військової агресії, що загрожують стійкому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем, методом вторгнення, несанкціонованого доступу або недотримання діяльності телекомунікаційних, кібернетичних, автоматизованих комп’ютерних систем, які незалежать від форми власності, з метою: вчинення терористичних актів; перехоплення формації в телекомунікаційних мережах; створення радіоелектронних бар’єрів, засобів зв'язку та управління;

в) використання неліцензійного та несертифікованного програмного забезпечення, засобів та комплексів обробки інформації» [40].

А. Козачинська зазначає: «На сьогодні інформація є визначальним ресурсом розвитку сучасного суспільства. Вона активно впливає на всі сфери життєдіяльності як окремих країн, так і всього світового співтовариства завдяки

бурхливому розвитку інформаційно-комунікаційним технологіям. Зазвичай вчені виділяють такі основні зовнішні джерела інформаційної безпеки:

– негативні наслідки діяльності іноземних політико-економічних, військових, розвідувальних, інформаційних та ін. структур, які спрямовані проти національних інтересів України, а також вірогідного послаблення можливостей їх реалізації;

– діяльність або прагнення державних та приватних структур іноземних держав до ущемлення національних інтересів на міжнародній арені, нанесення потенційної та реальної шкоди такими діями; –

підсилення конкурентної боротьби на міждержавному та транснаціональному рівні за володіння та користування теперішніми технологіями, засобами, системами;

– терористична, екстремістська та інша протиправна діяльність світових злочинних об’єднань;

– робота наземних, , космічних, морських та повітряних технічних засобів та приладів (супутників, радіоелектронного обладнання, інтернетресурсів та ін.) іноземних розвідувальних служб, яка псує інтереси держави; –

– загострення енергетичних проблем;

– підготовка іншими країнами стратегій війн малої інтенсивності у інформаційній, технологічній, економічній та ін. сферах життєдіяльності, які передбачають суттєву дестабілізацію державної і недержавної складових у загальній системі забезпечення національної безпеки України» [21].

Розглядаючи найбільш назрілі та значимі для сьогодення інформаційні загрози життєдіяльності держави та суспільства, зазначимо, що внутрішні та зовнішні загрози пов'язані між собою. На сьогоднішній день в державі розроблена та затверджена Стратегія національної безпеки України (прийнята

та затверджена Указом Президента України від 26 травня 2015 року № 287 "Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України"), яка основним видом інформаційних загроз національній безпеці нашої держави визначає агресивні дії Російської Федерації в інформаційному просторі: «Безпосередньо для нормативно-правового регулювання інформаційної безпеки держави було прийнято Указ Президента України №47/2017 Про рішення Ради національної безпеки та оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України", який затвердив основні положення забезпечення інформаційної безпеки держави в умовах ведення гібридної війни з Росією. Ця Доктрина визначила основні інтереси та прагнення України в інформаційному середовищі, основні загрози їх практичній реалізації пріоритетів та векторів державної політики в інформаційній галузі. Вона також розмежувала основні види зовнішніх інформаційних загроз, передусім з боку Росії, а саме:

– проведення інформаційної експансії державою агресором та структурами, які їй підконтрольні;

– проведення інформаційних операцій, які спрямовані на зменшення обороноздатності держави, Збройних Сил України та інших військових утворень, посилення панічних, екстремістських настроїв серед населення, часткову чи повну дестабілізацію політичного чи соціально-економічного життя, провокування та розгортання міжетнічних, міжконфесійних і соціальних конфліктів;

– домінування держав-агресора в інформаційному середовищі на тимчасово окупованих територіях;

– створення засобами інформаційного впливу негативного іміджу України на міжнародній арені;

– інформаційним загрозам;

– пропаганда в світі та Україні автономістських, федералістських та ізоляціоністських настроїв і концепцій існування;

– обмеження можливостей України, окремих структур та органів ефективно протидіяти зовнішнім. Для результативної боротьби зовнішнім інформаційним загрозам розроблено комплексна система механізм протидії»

А. Козачинська зазначає: «Для того щоб ефективно протистояти інформаційним впливам, попереджувати негативні наслідки від впливу пропаганди, необхідним є боротьба із інформаційними загрозами на стратегічному і тактичному рівнях, що може включати наступні напрями:

1. Зміцнення співпраці щодо протидії пропагандистським впливам з іноземними державами.

2. Активізація виробництва власного інформаційного продукту та його поширення у Європі і світі.

3. Поліпшення нормативно-правового регулювання інформаційної безпеки, зокрема прийняття стратегії інформаційної безпеки на основі діючої доктрини. 4. Ефективна реалізація положень інформаційної доктрини в Україні.

5. Формування та зміцнення інформаційного простору держави, в якому циркулюватиме достовірна, неупереджена інформація.

6. Активізація громадських об'єднань та інших зацікавлених сторін до виявлення неправдивої інформації, що пришвидшить її нейтралізацію» [21].

Отже, під методами реалізації державної політики щодо протидії зовнішнім інформаційним загрозам слід розуміти комплексні види та способи діяльності державних структур і інституцій, а також засоби їх взаємодії, які дозволяють ефективно реагувати на зовнішні інформаційні загрози або керувати ризиками, що виникають для їх нейтралізації.

У порівнянні з традиційними методами нейтралізації інформаційних

загроз, інноваційні методи ґрунтуються на принципах управління ризиками та можуть ефективно блокувати деструктивні чинники і властивості загроз, а також сприяти розгортанню та реалізації конструктивних елементів, властивостей та процесів в інформаційному просторі України.

Для подолання інформаційних загроз надзвичайно важливо ефективно втілювати державну доктрину інформаційної безпеки, посилювати координацію та співпрацю з іншими країнами та громадянським суспільством для виявлення інформаційних загроз, а також створювати власний інформаційний простір з розповсюдженням достовірної інформації.

З точки зору нових досліджень перспективним може стати науковий пошук найбільш результативних інструментів для протидії інформаційним загрозам

2.3 Роль міжнародної співпраці у формуванні стратегії інформаційної безпеки

З впровадженням інформаційних та телекомунікаційних технологій використання інформації значно поширилося. Попри позитивні аспекти, існує кілька негативних чинників, серед яких загроза цифрового розвитку або інформаційної залежності.

Ще в 90-х роках XX століття американські експерти прийшли до висновку, що країни, що першими освоюють інформаційний простір, матимуть значну перевагу над іншими.

Наприклад, згідно з даними Світового банку, країни, такі як США, скандинавські країни, Японія, Південна Корея та Сінгапур, демонструють високий рівень знань та засобів комунікації, що переважають капіталовкладення у фізичні активи.

У США компанії щорічно витрачають все більше коштів на придбання

патентів, ліцензій та інформаційних систем на суму 32 мільярди доларів, а міжнародні витрати на нематеріальні виробничі ресурси перевищують 100 мільярдів доларів на рік.

Світові інвестиції в науку (85%) здійснюються країнами-членами Організації Економічного Співробітництва та Розвитку, 11% - Індія, Китай, Бразилія та країни Східної Азії, а 4% - інші країни світу, включаючи Україну.

Як зазначає А. Козачинська: «Важливим досягненням нашої держави став вступ до Європейського Союзу, адже ЄС є сформованим інформаційним суспільством з високим рівнем згуртованості у світі та європейським інформаційним простіром. Наразі на ринку існує потужна конкуренція інформаційних послуг та технологій у якій Україна має низький рівень. За соціологічним дослідженням 40% громадян України оцінюють рівень об'єднаності України у світовому інформаційному просторі низьким, лише 8,5% людей вважають високим. Віддаючи перевагу інформаційній сфері економіки, стратегія Європейського Союзу відрізняється своїм відкритим соціальним спрямуванням. А ось у США перевага надається технологічним аспектам інформаційної супер мережі, Європа ж свій акцент робить на соціальний вимір. Таким чином Європейська комісія розробила дослідження яке називається «Робота, та життя в інформаційному суспільстві». Національна система зберігання інформації перебуває у застарілому стані. Бібліотеки та архіви іноді перебувають у непридатних для них приміщеннях, що призводить до втрати маси інформації та обмежує громадян у вільному доступі до інформації. Україна стоїть перед завданням розробки інноваційної політики та стратегії, що має багатий людський потенціал та слугує дієвому зростанню власного історичного потенціалу. Держава узгоджує всі процеси, які трансформують основи суспільства. Здебільшого, це стосується зовнішнього напряму її діяльності. Тут український уряд працює вкрай завзято. Сьогодні

Україна представлена в одних із потужніших міжнародних організаціях, як Європейська конференція Адміністрацій зв'язку, Міжнародний Союз електрозв'язку, Регіональне співтовариство в галузі зв'язку Європейський інститут телекомунікаційних стандартів. Також успіхом є підписання Паризького меморандуму згоди щодо розвитку Інформаційного суспільства, за яким високий пріоритет у взаємовідносинах між Європейською Комісією та Україною належить побудові в Україні інформаційного суспільства. У висновку хотілося б сказати, що розвиток інформаційних технологій призвів до вільного потоку інформації» [21].

Дослідниця додає: «Розподіл інформаційних ресурсів між державами є також міжнародною проблемою, як і світовий розподіл енергетичних чи продовольчих ресурсів. Наявність багатьох загроз інформації визначають актуальність проблеми інформаційної безпеки як компонент загальної проблеми інформаційного забезпечення розвитку людини, суспільства та держави загалом. На інтернаціональному рівні інформація вважається важливим ресурсом життєзабезпеченням суспільства та має широке соціальне значення. Головними напрямками захисту інформації є: захист прав особистої інформації, захист державних інтересів, захист підприємницької та фінансової діяльності, захист інформації від комп’ютерних злочинів. Важливим кроком у регулювання питання захисту інформації стало прийняття резолюції Генеральної Асамблеї ООН 54/90 «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» у 1999 році. У цьому документі постало питання захисту глобальних та телекомунікаційних систем та питання боротьби з тероризмом та криміналом. Світове співтовариство признало міжнародну безпеку як глобальну проблему, яка вимагає негайного вирішення» [21].

Н. Логінова та Р. Дробожур зазначають: «Головним документом

правового значення в США який безпосередньо стосується інформаційної безпеки є «Закон про інформаційну безпеку» виданий у 1906 році. В ньому окреслено можливі шляхи забезпечення безпеки в комп'ютерних системах. В європейських країнах у сфері системи інформаційної безпеки в 2006 році була прийнята «Стратегія безпеки інформаційного суспільства: діалог, партнерство та розширення можливостей». У цій стратегії розглянуто сучасний стан загроз безпеці інформаційного суспільства та встановлено можливі заходи щодо забезпечення системи інформації безпеки. За останні роки в ЄС діють декілька інноваційних проектів у сфері протидії кіберзлочинності. У червні 2010 р. було прийнято рішення про заснування Спеціальної групи з кіберзлочинності в ЄС (European Union Cybercrime Task Force), покликаної сприяти транскордонній боротьбі з кіберзлочинністю» [29].

Україна визначає свій інформаційний простір через основні нормативно-правові акти, серед яких переважають Конституція України, закони про інформаційну безпеку та інші відповідні документи.

Однак, є необхідність у впровадженні європейського досвіду у цій сфері, зокрема, системи попередження та реагування на загрози. Для досягнення цієї мети потрібно адаптувати найкращі практики з різних країн та враховувати внутрішні особливості.

Поняття "інформаційне забезпечення" активно використовується у різних сферах діяльності держави, однак, наразі в Україні не існує єдиної теоретичної бази щодо цього поняття, особливо у контексті державного управління.

Неоднозначне розуміння цієї концепції ускладнює розробку методології та практичне втілення інформаційного забезпечення системи державного управління. Інформаційне забезпечення є ключовим аспектом для України в контексті розвитку сучасного інформаційного суспільства.

На думку А. Козачинської: «Роль інформаційного забезпечення полягає в

утворенні належних умов для здійснення персоналізованих функцій управління на підставі належної інформації. Із усього вище сказаного випливає потреба у класифікації видів інформаційного забезпечення. Слід зазначити, що систематизації видів інформаційного забезпечення системи державного управління серед науковців та практиків на сьогодні відсутня. Головною причиною цього є те, що традиційно інформаційне забезпечення порівнюють із інформаційноаналітичним в інтересах діяльності органів державного управління, під яким розуміють «сукупність технологій, методів збирання та обробки інформації, що характеризує об'єкт управлінського впливу (соціальні, політичні, економічні та інші процеси), специфічних прийомів їх діагностики, аналізу та синтезу, а також оцінки наслідків прийняття різних варіантів політичних рішень». При чому у кінцевому результаті продуктом інформаційно-аналітичної роботи в державному управлінні є аналітичний документ. Розглядаючи інформаційне забезпечення в системі державного управління Варто звернути свою увагу на її класифікацію. В основу класифікації входить функції, які здійснюють реалізацію компонентів інформаційного забезпечення системи державного управління. До видів інформаційного забезпечення державного управління входять:

– моніторинг стану – комплекс заходів, що спрямовані на отримання інформації на базі всіх доступних даних, з метою оцінки та передбачення розвитку процесів управління;

– інформаційно-аналітичне забезпечення – комплекс заходів, що формують процеси утворення інформаційних продуктів на основі використання статистичних інформаційних ресурсів, проведення розрахунків, моделювання ситуацій, аналізу та синтезу документованих даних та інформації з метою підтримки прийняття рішень органами державного управління всіх рівнів;

– організаційно-управлінське забезпечення – сукупність заходів, що

використовують органи державного управління, аби правильно зробити рішення та донести його до своїх підлеглих;

– іміджеве забезпечення – застосування засобів масової інформації задля висвітлення діяльності системи державного управління та підняття позитивного рейтингу серед громадськості;

– морально-психологічне забезпечення – заходи, що використовуються з метою підтримання та відновлення у персонала системи державного управління моральних та психологічних якостей, його морально-психологічного стану на рівні, необхідному для успішного виконання завдань за призначенням;

– захист інформаційних ресурсів - правові, адміністративні, організаційні, технічні та інші заходи, що забезпечують збереження, цілісність інформації (інформаційних ресурсів) та належний порядок доступу до неї (них). [21].

Усі ці аспекти представляють основний перечень інформаційного забезпечення в системі державного управління.

Таким чином, можна визначити, що роль інформаційного забезпечення полягає в створенні сприятливих умов для виконання персоналізованих управлінських функцій на основі необхідної інформації.

Деякі нові дослідження повинні бути спрямовані на обґрунтування та розкриття особливостей основних типів інформаційного забезпечення в системі державного управління та механізмів їх впровадження

РОЗДІЛ 3
ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ФОРМУВАННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Особливості забезпечення інформаційної безпеки держави в умовах війни

Під поняттям військової безпеки держави розуміється реалізація життєво важливих національних інтересів країни у воєнній сфері з метою захисту її від воєнної загрози, збройної агресії та інших дій, що використовують військову силу.

Отже, основною метою забезпечення воєнної безпеки в Україні є уникнення воєнних конфліктів, а рівень воєнної безпеки служить показником ефективності виконання військової політики країни. Таким чином, можна стверджувати, що забезпечення обороноздатності та безпеки неможливе без підтримки такого рівня обороноздатності, який гарантує запобігання військовим конфліктам і відвернення можливої збройної агресії, а також зміцнення обороноздатності країни, що сприяє глобальній та регіональній стабільності. У зв'язку з гібридними методами проведення сучасних воєн надзвичайно важливим стає забезпечення інформаційної безпеки Збройних сил України.

Замість війни гарячого типу, яка включає прямі військові конфлікти, на сцену виходить війна гібридного характеру, спрямована на спровокування громадянських конфліктів та створення контрольованого інформаційного хаосу на території противника. Для досягнення цієї мети використовуються всі доступні можливості, від хакерських атак на критичні інфраструктурні системи країни до систематичної маніпуляції засобами масової інформації. Зміна умов нашого життя вимагає перегляду підходу до питань національної безпеки.

Якщо ще рік тому світ навколо нас здавався безпечним, то сьогодні виклики, які ми стикаємося, несуть значно більше загроз, ніж у період миру. Ми спостерігаємо, як проводиться інформаційний вплив, спрямований на свідомість суспільства, як на окремих осіб, так і на цілі держави.

На думку В. Лизанчук: «Психологічний вплив здійснюється за допомогою засобів масової інформації, а основою використання такого впливу є легкість сприйняття і поверховість. Створення масових інформаційних атак, ботів, фейків, як свідчать сучасні реалії, є ефективними інструментами дезорієнтації суспільства, залякування, маніпулювання та паніки. Спеціально створені інформаційні ресурси привчають людину бездумно сприймати інформацію і вірити в неї. Питання інформаційної безпеки та культури в умовах війни є питанням виживання людини, суспільства та держави. Адже забезпечення інформаційної безпеки визначається не тільки інтересами держави, а й інтересами особи в контексті забезпечення її прав і свобод» [27].

Н. Смотрич та Д. Браілко «Основою сучасної інформаційної безпеки є цілісність даних, доступність інформації, конфіденційність і надійність її збереження Інформаційна безпека включає не лише нормативно-політичну складову, а й інституційну сферу, яка передбачає діяльність органів, що її забезпечують, а також використання програмно-технічних засобів. З метою забезпечення інформаційної безпеки в Україні Указом Президента України від 25.02.2017 р. була затверджена «Доктрина інформаційної безпеки України». В сучасних умовах війни 18 березня 2022 року прийнято рішення РНБО «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану», в якому визначено, що в умовах воєнного стану реалізація єдиної інформаційної політика є пріоритетним питанням національної безпеки». Наразі в Україні також діє Центр протидії дезінформації при РНБО України, на сайті якого можна ознайомитися з актуальною інформацією та подіями у цій сфері.

Створення глобального простору суттєво посилило загрози застосування інформаційних заходів стратегічним противником або глобальним тероризмом, як з боку розгортання окремих військово-політичних операцій, так і з боку розвитку його стратегічного потенціалу в цілому. Захист від загроз подібного характеру необхідний самим Збройним Силам та їх особовому складу, з якими в першу чергу застосовуються засоби гібридної війни. Зростає цінність інформації. Ступінь її захищеності від злочинних посягань стає все вищим, а можливості для її отримання - збільшуються. Уміння правильно управляти інформаційними масивами та їх використання стає найважливішим завданням, яке стоїть перед військовослужбовцями» [52].

Забезпечення інформаційної безпеки в Збройних Силах, як одного з ключових державних органів, є гарантією безпеки всієї держави. Охорона військових інформаційних ресурсів стає пріоритетним завданням експертів з безпеки. Для ефективного протистояння загрозам необхідно спочатку ідентифікувати та класифікувати їх за походженням, характером впливу та ступенем небезпеки.

Фахівці розрізняють дві групи джерел загроз: внутрішні та зовнішні. Іноді одне явище може мати як зовнішні, так і внутрішні джерела загроз. Це можливо, коли зовнішня дія, що походить ззовні, передається через операторів, що працюють усередині країни. Сьогодні такі підрозділи мають доступ до сучасних електронних засобів поширення інформації.

Одним з основних джерел інформаційних загроз є напруженість або дестабілізація суспільно-політичної обстановки в місцях розташування Збройних Сил. Створення штучно напруженої атмосфери, провокація конфліктів з місцевим населенням, навіть масові заворушення, спричинені цілеспрямованим інформаційним впливом, становлять серйозну загрозу стабільності у військових частинах та в армії загалом.

Протистояти цим загрозам можна лише за допомогою систематичної психолого-просвітницької роботи з особовим складом, одночасно взаємодіючи з місцевими владними структурами для запобігання провокаційної діяльності засобів масової інформації та інших джерел поширення інформаційних атак.

Важливою загрозою є спрямований вплив на моральний стан військ шляхом фальсифікації фактів військової історії, збільшення соціальної напруги та спроб втягнути особовий склад у політичні конфлікти. Виконавцями таких загроз інформаційного характеру найчастіше виступають засоби масової інформації, спрямовані на створення напруженої ситуації.

Як зазначає І Боднар: «У ряді випадків навіть контакт особового складу з представниками преси може стати способом спеціальної обробки поданої ними інформації, що призведе до можливої втрати бойового духу особового складу. Іноді заходами такого впливу досягаються не тільки психологічні зриви, що призводять до військових злочинів чи дезертирства, а й створення у військах угруповань, спрямованих на свідомий підрив обороноздатності країни. Поширення радикального ісламізму може стати серйозною загрозою інформаційній безпеці армії. Військовослужбовець, який пройшов спеціальну психологічну терапію, вважає себе вже не військовослужбовцем, а релігійною громадою, виконує радше вказівки наставників, ніж накази командування. Такий боєць стає серйозною загрозою для інформаційної безпеки військових частин, особливо розташованих у регіонах з переважно мусульманським населенням» [4].

Як зазначають Н. Смотрич та Д. Браілко: «Технічні загрози інформаційного характеру стосуються як функціонування інформаційних систем, що використовуються у військах, у тому числі систем управління, так і збереження конфіденційної інформації, що передається військовими каналами зв’язку. Види технічних загроз діяльності Збройних Сил можуть бути різного

характеру: від умисного пошкодження систем і крадіжки інформації до недбалості окремих співробітників. Заходи захисту в цьому випадку передбачатимуть підвищення рівня безпеки автоматизованих систем управління та навчання персоналу необхідним вимогам захисту інформації. Стандарти безпеки визначаються ГОСТами та іншими методиками, розробленими та затвердженими на державному рівні, але часто на практиці відбувається зволікання з впровадженням нових програмно-технічних засобів, здатних протистояти загрозам з боку противника. Така затримка зумовлена особливостями функціонування системи державних закупівель і як така стає загрозою безпеці. У рамках цього виду атаки можна розглядати навмисне пошкодження техніки і ліній зв'язку, що іноді відбувається з вини особового складу, місцевого населення, а також в результаті цілеспрямованої діяльності противника. Порушення систем життєзабезпечення військового корабля, викликане недбалістю або спланованими атаками, може призвести до загибелі екіпажу. Контроль за збереженням військової техніки – одне з найважливіших завдань, яке стоїть перед відповідальними військовослужбовцями. Особливо серйозними можуть бути проблеми з інформаційними системами космічних сил або ядерних установок» [4].

Науковці додають: «Порушення систем управління космічними кораблями через неефективний код, вбудований в програмний продукт, часто призводить не тільки до фінансових втрат, а й до порушення цілісності системи безпеки країни. Надзвичайно важливою стає загроза внесення неправдивої інформації в систему відстеження можливої атаки. Зберігається ризик спрацьовування систем ППО через неправдиву інформацію, надіслану противником навмисно. Уявні загрози в минулому мало не призводили до початку ядерної війни, зараз цей ризик зменшився, але він залишився. Серйозною проблемою сьогодні є недостатня розвиненість законодавчої бази

щодо захисту інформації та протидії новим загрозам. Значна кількість явищ інформаційного простору досі не класифікована та не відображена в нормативних актах, що ускладнює застосування заходів відповідальності за вчинення будь-яких дій чи організацію діяльності, яка може завдати шкоди інформаційній безпеці Збройних Сил та безпосередньо військовослужбовцям. Але ці напрямки розвиваються, приймаються нормативно-правові акти, які законодавчо регулюють допустимість використання в техніці, що постачається у війська, тих чи інших технологій іноземного виробництва. З моменту оголошення воєнного стану в Україні прийнято зміни до нормативно-правових актів з урахуванням реалій війни. Вони стосуються регулювання окремих аспектів інформації, правовідносин щодо заборони розповсюдження певної інформації з урахуванням її суспільно небезпечного характеру; врегулювання важливих моментів щодо технічного запису інформації в умовах воєнного стану; встановлення або посилення відповідальності за поширення певної інформації; регламентація процесуальних дій щодо отримання інформації» [52].

Так, Верховна Рада затвердила законопроект щодо кримінальної відповідальності за незаконне фото- та відеозафіксування руху Збройних Сил та міжнародної військової допомоги під час воєнного стану. Закон України, який спрощує проведення слідчих дій та надає тимчасовий доступ до речей і документів, вступив у дію 22 березня 2022 року.

Зміни до Кримінально-процесуального кодексу дозволяють слідчим фіксувати комп'ютерні дані на місці обшуку, навіть якщо про це не було зазначено у дозволі.

Посилено кримінальну відповідальність за створення та поширення забороненої інформаційної продукції згідно зі Зміною № 2110-IX від 3 березня 2022 року до деяких законодавчих актів України.

До зовнішніх джерел загроз слід віднести ті, які знаходяться за межами

території України чи її союзників. Противники постійно розробляють та використовують нові інформаційно-психологічні методи для впливу на особовий склад.

Застосування нових видів інформаційної зброї, спрямованих на виведення з ладу інформаційних систем або психологічний вплив на особовий склад, стає серйозною загрозою.

Напрям дії такої зброї, за словами аналітиків, базується на використанні ультразвуку, електромагнітних полів та інших технологій. Не виключено застосування медичних або хімічних засобів, що впливають на поведінку військовослужбовців.

Такі засоби психологічних операцій можуть використовуватися у районах, де Збройні Сили України беруть участь у поточних конфліктах. Хоча у пресі згадується велика кількість видів психологічної зброї, офіційного підтвердження її використання поки що не надходило

В. Остроухова зазначає: Ні для кого не секрет, що у збройних силах стратегічного супротивника чи організацій глобального тероризму є спеціальні підрозділи інформаційно-психологічного впливу. Їх діяльність вивчається лише на рівні профільних науково-дослідних інститутів, а заходи боротьби з новими загрозами розробляються та активно впроваджуються в практику. Часто застосування цілеспрямованого інформаційного впливу заздалегідь ретельно готується роботою засобів. Військовослужбовці зобов'язані вміти класифікувати та ідентифікувати такі загрози, для чого необхідно провести відповідну підготовку. Найбільш серйозною проблемою безпеки є соціальні мережі, за допомогою яких військовослужбовці можуть випадково оприлюднити важливу інформацію. Одним із основних завдань захисту безпеки держави має стати виявлення таких загроз та їх своєчасне усунення. Заходи, які можуть бути застосовані для захисту інформації та забезпечення безпеки, також

поділяються на дві групи:

– захист інформаційних систем від пошкодження та інформації від витоку та перехоплення;

– захист психіки особового складу від цілеспрямованого інформаційно-психологічного впливу.

Ці заходи мають здійснюватися комплексно, на основі нових наукових розробок і програмних продуктів. Перша група заходів:

– захист об’єктів військової дислокації та розташованої в них комп’ютерної техніки від пошкодження вогнем або іншого навмисного виведення з ладу;

– захист систем від віддаленого вторгнення зловмисника, зокрема з установкою програмних продуктів, що забезпечують повний захист периметра від вторгнень, наприклад, системи DLP та системи SIEM;

– захист інформації, яка становить державну або військову таємницю, від витоку чи умисного розкрадання;

– радіоелектронний захист;

– використання захищених моделей комп’ютерів і програмного забезпечення, які не можуть бути пошкоджені заздалегідь створеними проблемами в їх кодах;

– розробка засобів електронної розвідки;

– використання соціальних мереж для свідомої дезінформації противника;

– захист систем зв’язку.

Друга група заходів включає:

– запобігання навмисного психологічного впливу на психіку військовослужбовців;

– корекція інформації, що транслюється потенційним

супротивником» [37].

Як зазначають Н. Смотрич та Д. Браілко зазначають: «Розробка та впровадження комплексу цих заходів потребує створення окремих підрозділів, що працюють у сфері інформаційної безпеки. Морально-психологічне забезпечення військ передбачає застосування комплексу заходів блокування, які застосовуються під час гібридної війни. Сьогодні існують інститути і аналітичні центри, які спрямували всі свої зусилля на розробку різноманітних методик морально-психологічного стану військ. У рамках цих досліджень вивчаються психологія, безпека психоенергетичної діяльності. Для протидії спрямованому інформаційно-психологічному впливу командування Збройних Сил передбачає такі методи:

– проведення досліджень методів, спрямованих на психіку;

– використання всіх доступних видів психологічної роботи з військовослужбовцями, здійснення цілеспрямованих захисних заходів.

Усі ці заходи необхідні для створення стійкого захисту від інформаційного впливу та готовності військовослужбовця до відсікання інформації, яка має ознаки спрямованого впливу з метою дестабілізації його морально-психологічного стану. Напад противника не повинен бути причиною зниження боєздатності військ, їх мотивації, пригнічення волі. Важливим буде проведення виховної роботи та організація дозвілля військовослужбовців. Особливо важливо контролювати тих військовослужбовців, до сфери відповідальності яких входить робота із засобами зв’язку, автоматизованими системами управління та передачі інформації. Вони, швидше за все, стануть об’єктами розробки ворогом».

Науковці додають: «Передбачаючи, який саме комплекс заходів застосує потенційний супротивник, необхідно за допомогою засобів атаки перекрити його можливості.

Такі дії, як:

– навмисне введення супротивника в оману щодо намічених заходів і способів протидії загрозам інформаційній безпеці;

– руйнування засобів зв’язку та інформаційних систем;

– внесення свідомих спотворень у роботу інформаційних систем противника;

– виявлення опорних пунктів противника, що діють на території України, та їх знищення;

– отримання конфіденційної інформації про наміри противника знизити рівень безпеки військ і використання цієї інформації для формування стратегії оборони;

– застосування засобів морально-психологічного придушення інформаційних сил противника» [52].

Розробка інформаційної зброї вважається окремим аспектом оборонної стратегії, який має не лише відображати, а й передбачати потенційні загрози.

Противники ефективно використовують інформаційну зброю, навіть у країнах, які не перебувають у прямих воєнних конфліктах, але мають ризики дестабілізації. Важливо, щоб вітчизняна інформаційна зброя була такою ж ефективною, або ще ефективнішою.

Практично кожен військовий об'єкт тепер потенційно піддається ураженню, тому безпеку їх слід розглядати комплексно.

Держава активно займається цими питаннями, збільшуючи свій оборонний потенціал.

Розробка власного програмного забезпечення допомагає уникнути системних ризиків, а власні канали передачі даних в Інтернеті мають забезпечувати безпечну комунікацію.

Недостатній нагляд за постачальниками та підрядниками може призвести

до отримання військ обладнання, яке може використовуватися потенційним супротивником.

Існує серйозна загроза, що автоматизовані системи управління армії можуть стати вразливими через передачу конфіденційної інформації через недостатньо захищені зв'язки, навіть через цивільних фахівців.

Цю проблему необхідно негайно вирішувати. Згідно з Законом України "Про національну безпеку України", загрози національній безпеці - це явища, тенденції та фактори, які унеможливлюють, утруднюють або можуть унеможливити чи утруднити реалізацію національних інтересів та збереження національної цінності.

Неоспоримо, що сучасні загрози інформаційній безпеці становлять виклик, що виходить далеко за межі нашої держави і мають глобальні наслідки, що посягають не лише на національний простір.

З цього приводу, для запобігання та протидії сучасним інформаційним загрозам необхідно не лише прийняти нормативно-правову базу, але й забезпечити функціонування інституційного механізму забезпечення інформаційної безпеки, включаючи освітню складову.

Це означає послідовну системну діяльність державно-правових інституцій, які ефективно реалізовували б національні інтереси в інформаційній сфері, були б здатні не лише вчасно реагувати на поширення інформаційних фейків та неправдивої інформації, але й здатні загалом попереджати інформаційні конфлікти та формувати інформаційну культуру суспільства в цілому.

Крім того, ураховуючи існуючі глобальні загрози та виклики, здається можливим ефективно протистояти інформаційній агресії шляхом залучення до цього процесу міжнародних організацій, інституцій та міжнародної спільноти. Адже, як показує сучасність, у веденні війни в інформаційному полі немає

кордонів.

3.2 Євроатлантичне співробітництво України в контексті формування державної політики у сфері інформаційної безпеки

На сучасному етапі безпека інформаційного простору є ключовим завданням, оскільки вона стосується як пересічного громадянина, так і конкретної держави, або групи держав. Все частіше питання інформаційних загроз піднімають на міжнародних конференціях, самітах та на рівні міжнародних організацій. Тому що, шкідлива кіберактивність поширюється досить швидко, починаючи від програм, які допомагають злодіям здобути приватну інформацію, до шпигунства та кібератак, які мають політичну мету.

НАТО – військово-політична організація, яка створена підтримувати міжнародний мир та безпеку. Саме тому Альянс працює в одну ногу з сучасними загрозами безпеці, а успішна діяльність НАТО неможлива без правдивої інформація. Навіть миротворчі операції НАТО є більш успішними через обізнаність громадян у цьому питанні і в результаті це сприяє більшій ефективності. Існує безліч загроз, які спонукають Альянс вживати нових заходів у боротьбі з кіберзагрозами.

Як зазначають В. Максимець та В. Вівсяна: «Однією з таких загроз в інформаційній безпеці демократичним державам можна згадати росію. Наприклад, якщо брати до уваги політично мотивовані кібератаки, то одним з прикладів є зламана електронна пошта норвезького парламенту у 2020 році. Цей інцидент був названий як такий, що вплинув на найважливіший демократичний інститут країни. Пізніше норвезька влада визначила росію як державу, яка винна за напад [30].

Науковці додають: «З початку 2022 року український уряд зазнав серії

кібератак, які призвели до зіпсування урядових веб-сайтів та знищення даних на деяких державних комп'ютерах. У середині січня хакери зламали близько 70 українських веб-сайтів, у тому числі міністерств закордонних справ, оборони, енергетики, освіти та науки, а також ДСНС та Міністерства цифрової трансформації, портал електронного урядування якого надає український публічний цифровий доступ до десятків державних послуг. Міжнародний колектив хактивістів Anonymous оголосив «кібервійну» проти російського уряду, визнаючи заслугу за кілька кіберінцидентів, включаючи поширені атаки відмови в обслуговуванні, які знищили російські урядові веб-сайти та державну службу новин Russia Today» [30].

Кібератаки на Естонію в 2007 році вивели з ладу її урядові, медіа та фінансові веб-сайти, далі росія анексувала чистину території Грузії у 2008 році і був проведений ряд кібератак на грузинські веб-сторінки. Саме тоді члени Альянсу почали розуміти, що вони не готові до такого роду викликів. Тому починаючи з 2007 року НАТО вирішило стати більш активним користувачем соціальних мереж таких як Facebook, YouTube та Twitter. До того ж було вирішено створити телеканал та сайт куди завантажували розсекречені відеозаписи операцій. Така діяльність давала змогу протидіяти дезінформації, яку поширювали країни-противники Альянсу.

У січні 2008 року НАТО затвердила свою першу політику щодо кіберзахисту. Члени НАТО підкреслили, що настав етап, коли надзвичайно важливо аби інформаційні системи були в безпеці Тому необхідно ділитися передовим досвідом, і допомагати державам-союзникам у боротьбі з кібератакам. Російська агресія проти України починаючи з окупації Криму, а зараз вже і повномасштабна війна ввесь час супроводжується інформаційними операціями на всіх етапах. Саме тому ще у 2014 НАТО почало свою діяльність зі створення Центру передового досвіду в галузі стратегічних комунікацій

НАТО у Ризі (StratCom Centre of Excellence). Діяльність даної структури спрямована на пошук шляхів розв'язання проблем, важливо, що вони приділяють увагу російській агресії проти України (About NATO StratCom COE, 2022).

А. Жадан зазначає: «StratCom сприяє покращенню можливостей стратегічного зв'язку в Альянсі та країнах-членах. Стратегічне спілкування є невід'ємною частиною зусиль, спрямованих на досягнення політичних і військових цілей Альянсу, тому стає все більш важливим, щоб Альянс належним, своєчасним, точним і відповідальним чином повідомляв про свої цілі та місії.

Основними напрямками діяльності за 2021 рік є:

1) експеримент багатонаціональних інформаційних операцій;

2) розробка концепції моделювання інформаційного середовища;

3) розробка концепції навчального модуля моделювання дезінформаційної атаки;

4) курс та конференція в соціальних мережах (About NATO StratCom COE, 2022). Також діяльність НАТО StratCom Centre of Excellence спрямована не лише на захист держав-членів, але й на партнерів, оскільки цей орган можна вважати таким, що надає підтримку державам-членам, кожна з яких має можливість розбудовувати власну систему інформаційного захисту. У 2015 році було ухвалено стратегію щодо протидії гібридній війні і після цього країни-члени розпочали розширювати набір інструментів НАТО для реагування на ці загрози, які включають в себе дезінформацію та кібератаки. Пізніше у 2016 році на саміті НАТО члени підтвердили оборонний мандат НАТО і визнали кіберпростір як область операцій, у якій НАТО має захищати себе так само ефективно, як в повітрі, на землі або воді. Оскільки більшість криз і конфліктів сьогодні мають кібервимір» [72].

Науковець додає: «На саміті НАТО 2021 року було схвалено нову Всеосяжну політику кіберзахисту, яка підтримує три основні завдання НАТО: колективну оборону, врегулювання криз і спільну безпеку, а також її загальну позицію стримування та оборони. Оборонний мандат НАТО було підтверджено, і члени Альянсу взяли на себе зобов'язання використовувати весь спектр можливостей для активного стримування, захисту та протидії всьому спектру кіберзагроз у будь-який час. Цікавим є те, що члени НАТО розглядають злочинний вплив кіберактивності, як збройний напад Важливо зазначити, що і НАТО і Україна досить часто підпадають під Кремлівську пропаганду з метою дезінформації суспільства, і вкорінення в суспільство думок, що Альянс є ворожою небезпечною організацією, а Україна це тимчасова зброя НАТО за допомогою якої Альянс веде боротьбу проти рф. Наприклад, росія стверджувала, що розпочала СВО, щоб запобігти розміщенню військових баз НАТО в Україні. Але зараз російські медіа та експерти намагаються переконати своїх громадян, що головна мета війни - запобігти знищенню Росії НАТО. У такий спосіб, Україна стає суб'єктом пропаганди росії. Ця дезінформація поширюється, щоб утворити враження, що СВО є «священною народною війною» і спонукати росіян до військових дій, а НАТО – загроза для всієї росії» [72].

Ще одна тенденція російської дезінформації – це ствердження, що Збройні сили України ведуть боротьбу виключно в інтересах НАТО. Раніше російські ЗМІ твердили, що росія воює проти НАТО, що Альянс керує Збройними силами України, а в їх складі беруть участь найманці з інших країн. Нова теза полягає в тому, що росія воює саме проти України, але українці захищають не свої інтереси, а інтереси США та інших країн НАТО. Пропагандисти намагаються наголосити на визначальній ролі НАТО в цьому конфлікті, хоча вони визнають суб'єктність України та Збройних сил. До того

ж, російської дезінформації має на меті змінити сприйняття українцями причин війни на Донбасі та анексії Криму.

Російські пропагандисти намагаються перекласти відповідальність за конфлікт на НАТО та викликати недовіру до західних держав. Це може спричинити подальше роз'єднання між Україною та західним світом, що сприятиме інтересам росії. Важливо розуміти, що ці тези є неправдивими та є частиною гібридної війни, яку росія веде проти України та Альянсу. Ці зусилля з метою дезінформації та впливу на суспільні думки мають негативний вплив на ситуацію в регіоні та загострюють конфлікт. Саму тому надзвичайно важливо розуміти правдиву природу війни та її причин, щоб знайти шляхи до миру та стабільності.

Як зазначають автори публікації: «Загалом співпраця між Україною та НАТО стикається зі значними викликами та загрозами, але обидві сторони залишаються відданими працювати разом, щоб подолати ці виклики та посилити безпеку в регіоні. Варто згадати, ще один приклад, як фахівці НАТО реагують на інформаційні операції ворога, та спростовують фейкову інформацію шляхом поширення правдивих повідомлень різними каналами, аби досягнути різних цільових аудиторій. Важливим також є те, що Альянс намагається створити «інформаційнй імунітету», який зробить населення більш стійким до ворожих повідомлень, за допомогою яких ворог намагається переконати суспільство у негативному ставленні до НАТО. Одним з прикладів слід згадати дезінформацію з приводу COVID-19, яку поширювали Росія та Китай. Про те, що вірус виник або в Європі, або в США. Цікавим прикладом є те, що у період COVID-19 НАТО було скоординовано кілька інформаційних атак. По-перше, атака була проти присутності військ НАТО в Польщі Латвії та Литві. Саме тоді до міністра оборони Литви було направлено листа нібито від генерального секретаря НАТО в якому зазначалося про плани НАТО вивести

війська з країни. По-друге, було створене неправдиве інтерв’ю, що нібито канадські війська занесли вірус до в Латвії. І по-третє, був відправлений лист де нібито польський військовий критикує американські війська» [67].

У боротьбі проти цих форм дезінформації, НАТО утримує веб-сайт під назвою "Встановлення правдивої картини". На цьому онлайн-ресурсі доступні всі виступи, інтерв'ю, відео та зображення, що спростовують розповсюджену дезінформацію. Надзвичайно важливо, що інформація на цьому сайті доступна у кількох мовах, щоб кожен зміг знайти правдиву інформацію. Крім того, НАТО завжди закликає ЗМІ виправляти неточні історії.

Необхідно приділити увагу наступним заходам НАТО у протистоянні інформаційним загрозам. По-перше, у НАТО діє служба реагування на кіберінциденти, розташована у Бельгії. Ця служба забезпечує захист внутрішніх мереж НАТО та забезпечує централізовану та цілодобову підтримку. По-друге, НАТО створило Центр операцій у кіберпросторі, який підтримує зв'язок з військовими командирами, що мають інформацію про операції та місії, та забезпечує свободу дій у кіберпросторі. Це робить операції НАТО більш стійкими до кіберзагроз. Додатково, НАТО співпрацює з різними міжнародними акторами, включаючи Європейський Союз та країни-партнери, такі як Україна, Фінляндія та Швеція, для боротьби з кіберзагрозами. НАТО також співпрацює з партнерами у регіоні Азіатсько-Тихоокеанського регіону для обміну досвідом у протидії гібридним загрозам, зокрема збільшенню дезінформації та кібератак, що набуло особливого значення в контексті пандемії COVID-19.

Важливо відзначити, що у Фінляндії розташований Європейський центр протидії гібридним загрозам, який був створений у 2017 році представниками країн НАТО та ЄС. Цей центр займається проведенням досліджень, аналізом

гібридних загроз та визначенням методів їх подолання. Його наступною функцією є проведення консультацій на стратегічному рівні між учасниками ЄС та НАТО. Загалом, НАТО та ЄС мають сприяти побудові ефективного діалогу для взаємного обміну інформацією, звітування про різні інциденти, керування надзвичайними та кризовими ситуаціями, а також для проведення спільних тренінгів та навчань.

Як зазначає у своїй праці М. Кудіна: «У 2022 року Агентство зв'язку та інформації НАТО та Україна підписали Меморандум про угоду, який зосереджується на співпраці в проектах, пов'язаних з технологіями. Ця угода спрямована на зміцнення партнерства між НАТО та Україною шляхом надання допомоги в модернізації її інформаційних технологій та послуг зв'язку. Крім того, меморандум містить положення щодо визначення областей, де може знадобитися навчання особового складу, а також навчання, семінари та тематична експертиза для підтримки зусиль України щодо модернізації її обороноздатності» Кудіна» [67].

Також у 2022 році НАТО оголосила про впровадження нової програми швидкого реагування на кібератаки. В рамках цієї програми обіцяно посилити кіберзахист України перед загрозами з боку російських кібератак. Ключовим елементом оновленого Комплексного пакету допомоги НАТО для України є Трастовий фонд кібербезпеки, який спрямований на розвиток кіберзахисту в Україні шляхом забезпечення необхідного обладнання та навчання персоналу. Ця підтримка має на меті допомогти Україні захистити свою інфраструктуру від сучасних кіберзагроз.

Зростаюча активність російських військ проти України, а також продовження санкцій Заходу проти російської економіки може призвести до посилення кібератак з боку Росії як проти НАТО, так і проти Заходу. Такі атаки

на критичну інфраструктуру та промислові системи контролю можуть мати серйозні наслідки для НАТО і України.

Важливо враховувати, що серія кібератак між Росією та НАТО може призвести до ескалації конфлікту, в результаті якої Росія може вжити хімічну або навіть тактичну чи ядерну зброю. Росія попередила адміністрацію США про припинення надання українським військам сучасної зброї та загрожувала "непередбачуваними наслідками". Це може вказувати на те, що Росія може спробувати перешкодити поставці зброї або навіть атакувати НАТО за допомогою кіберзасобів.

Враховуючи вище зазначене, важливо відзначити, що зацікавленим сторонам слід приділити увагу наступним рекомендаціям щодо боротьби з дезінформацією:

1. Державам слід працювати над створенням нової установи, яка була б автономною та здатною проводити аналіз даних, необхідний для забезпечення незалежного контролю, відповідно до нових політичних рамок.

2. Необхідно розвивати медіаграмотність серед населення, щоб громадяни мали здатність орієнтуватися в інформаційному середовищі та отримувати доступ до достовірної та перевіреної інформації.

3. Всажливо створити сильні системи моніторингу, які могли б виявляти потоки дезінформації в усьому інформаційному середовищі кількома мовами.

4. Технологічним компаніям, таким як Meta, YouTube та Twitter, необхідно дотримуватися своєї політики заборони дезінформації, фінансованої рекламою.

5. Фінансування незалежної журналістики та перевірки фактів - ще один важливий крок у боротьбі з дезінформацією.

Загалом, досвід НАТО у протидії деструктивним інформаційним загрозам підкреслює важливість раннього виявлення та швидких та рішучих дій. Альянс визнає, що кампанії з дезінформації та інші інформаційні загрози можуть мати значний вплив на країни-члени та їх населення, і вживає заходів для посилення своєї стійкості та готовності до протидії таким загрозам.

Зусилля НАТО свідчать про організації відданість боротьбі з інформаційними загрозами та захисту безпеки своїх членів. Взаємини між Україною та НАТО мають довгу історію, яка відображає сучасні виклики та потреби міжнародної системи безпеки і розвитку. Ці відносини почалися з програми "Партнерство заради миру" і досягли важливого пункту з підписанням Хартії про особливе партнерство між Україною та НАТО. Сьогодні ця взаємодія стала більш широкою, охоплюючи співпрацю у різних сферах, включаючи політичну, військову, військово-технічну та інші. Зокрема, у контексті збройної агресії Росії проти України, співпраця з НАТО має велике значення для підтримки безпекових можливостей України.

ВИСНОВКИ

У магістерській роботі досліджено проблему розробки теоретичних, методологічних і практичних рекомендацій для реалізації державної політики у сфері інформаційної безпеки. Зокрема ґрунтовно досліджено рівень євроатлантичного співробітництва України в контексті тих викликів, які сьогодні постали перед нашою державою.

За результатами проведеного дослідження, нами зроблено наступні висновки:

1. Інформаційна безпека – це захист інформації від неправомірного доступу, втрати, пошкодження або знищення з метою забезпечення конфіденційності, цілісності та доступності цієї інформації. Це охоплює широкий спектр заходів, які спрямовані на захист інформаційних ресурсів, систем і комунікаційних засобів від зловживань та загроз.

Інформаційна безпека включає в себе технологічні, організаційні та правові аспекти, а також вимагає відповідної культури безпеки серед користувачів і фахівців з інформаційної технології. Вона є важливим аспектом для захисту конфіденційної інформації, такої як особисті дані, комерційна інформація, важливі дані компаній та державних установ.

2. Інформаційна безпека може розглядатися як соціальне явище, оскільки вона впливає на суспільство в цілому та на його окремі складові частини. Ось деякі аспекти, які підтверджують це:

Вплива на суспільну структурі: захист інформації від неправомірного доступу та зловживань може мати значення для різних соціальних груп. Наприклад, для бізнесу, державних установ, а також для приватних осіб.

Економічний вимір: недостатність або порушення інформаційної безпеки може призвести до економічних збитків для компаній, держави та індивідуальних громадян. Наприклад, втрати даних або крадіжка

ідентифікаційної інформації можуть призвести до фінансових втрат та порушення довіри.

Політична значущість: забезпечення інформаційної безпеки також є важливим аспектом для збереження стабільності та функціонування державних інститутів. Зловживання або порушення інформаційної безпеки може мати серйозні політичні наслідки.

Спільна відповідальність: захист інформації часто вимагає спільних зусиль суспільства, уряду та приватного сектору. Це включає в себе освіту громадян щодо кібербезпеки, розробку відповідних законів та належних рекомендацій.

3. Структура інформаційної безпеки може бути організована на кількох рівнях для ефективного захисту інформаційних ресурсів, систем та комунікаційних засобів. Основні компоненти структури інформаційної безпеки включають стратегічний, тактичний, технічний і правовий рівні. Ці рівні взаємодіють між собою для забезпечення повноцінного захисту інформації від різних загроз та загроз. Організації можуть адаптувати цю структуру відповідно до їхніх конкретних потреб та обставин.

4. Державна політика у сфері інформаційної безпеки визначається комплексом стратегій, законодавчих актів, програм, заходів та регулятивних механізмів, які спрямовані на захист інформації, що має стратегічне значення для держави, суспільства та громадян. Державна політика у сфері інформаційної безпеки спрямована на забезпечення стабільності, захисту прав і свобод громадян, конфіденційності та цілісності інформації, а також підтримку економічного розвитку та інноваційного потенціалу країни.

5. Засади державної політики у сфері інформаційної безпеки можуть бути сформульовані наступним чином:

Конфіденційність: забезпечення конфіденційності інформації, що має

стратегічне значення для держави, громадян та підприємств, шляхом використання захисних технологій та прийняття відповідних правових норм і стандартів.

Цілісність: гарантування цілісності інформації шляхом запобігання несанкціонованим змінам, втратам або пошкодженням даних.

Реагування на загрози: розробка та впровадження механізмів реагування на загрози інформаційній безпеці, включаючи попередження, виявлення, відновлення та реагування на інциденти.

Міжнародне співробітництво: розвиток та підтримка міжнародного співробітництва у сфері кібербезпеки для обміну інформацією, координації заходів та спільного вирішення проблем.

Освіта і свідомість: розробка та впровадження програм освіти та підвищення свідомості про інформаційні загрози та методи захисту інформації серед громадян, бізнесу та державних службовців

6. Міжнародна співпраця України у сфері інформаційної безпеки є важливим аспектом захисту національних інтересів та забезпечення кібербезпеки в умовах глобалізації та цифрової трансформації.

Держава активно співпрацює з іншими країнами, міжнародними організаціями та структурами з метою обміну досвідом, розробки спільних стратегій та стандартів, а також спільного вирішення проблем кібербезпеки. Основні напрямки міжнародної співпраці України у цій сфері включають: обмін інформацією, спільні заходи, зокрема конференції, присвячені інформаційній безпеці, спільні програми та стажування.

7. Євроатлантичне співробітництво України - це набір взаємовигідних відносин України з країнами та організаціями, в тому числі і в контексті інформаційної безпеки, які входять до європейського та атлантичного простору. Основними складовими євроатлантичного співробітництва для України є

партнерство з Європейським Союзом та НАТО.

Євроатлантичне співробітництво є важливим напрямком зовнішньої політики України, сприяючи зміцненню її позицій на міжнародній арені та підтримці реформ для досягнення стандартів та цілей європейського та атлантичного співтовариства.

8. Євроатлантичне співробітництво України в умовах війни зазнає певних змін та викликів, але залишається важливим елементом національної стратегії безпеки та зовнішньої політики.

Війна на сході країни, конфлікт з російською федерацією та окупація частини території України Криму породжують нові виклики та обмеження, але не змінюють загальної спрямованості на інтеграцію до європейського та атлантичного простору.

Співробітництво здійснюється у сфері безпеки, тому числі інформаційної, економічного та політичного партнерства та реформах, в тому числі і в інформаційній сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антонюк В. В. Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці / В. В. Антонюк. Державне управління: удосконалення та розвиток. Випуск 8(10). 2014. с. 1-5.

2. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти / За загальною редакцією д-ра юрид. наук, проф. Бандурки О.М..: Монографія. Харків: Вид-во Ун-ту внутр. Справ, 2000. 368 с.

3. Бєлай С.В., Корнієнко Д. М. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки. Актуальні проблеми управління інформаційною безпекою держави. Київ: Національна академія Служби безпеки України, 2018. 408 с.

4. Боднар І. Інформаційна безпека як основа національної безпеки. Механізм регулювання економіки. 2014. № 1. С. 68-75

5. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. 449 с.

6. Варналій З. С. Економічна та фінансова безпека України в умовах глобалізації : монографія. Київ : Знання України, 2020. 423 с.

7. Гаврильців М. Т. Інфрмаційна безпека держави в системі національної системи. URL : http://lsej.org.ua/2_2020/54.pdf.

8. Дереко В. Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки / Інформаційна безпека людини, суспільства, держави. 2015. № 2. С. 16-22.

9. Дмитренко М. А. Проблемні питання інформаційної безпеки України. Міжнародні відносини. Серія Політичні науки. 2017. № 17. С. 236–243.

10. Довгань О. Д. Правові засади формування і розвитку системи

забезпечення інформаційної безпеки / О. Д. Довгань Інформаційна безпека людини, суспільства, держави. 2015. Випуск 3 (19) с. 6-17.

12. Доктрина інформаційної безпеки України : затверджено Указом Президента України від 25 лютого 2017 р. № 47/2017. URL: http://zakon.rada.gov.ua/laws/show/47/2017.

13. Забезпечення інформаційної безпеки держави: навчальний посібник / В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. Львів : Видавництво Львівської політехніки, 2017. 204 с.

14. Закон України «Про захист інформації в інформаційно-комунікаційних системах». Редакція від 01.01.2022. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

15. Закон України «Про Інформацію» від 2 жовтня 1992 року № 2657- XII 39.

16. Закон України «Про Національну програму інформатизації» від 04.02.1998 № 74/98-ВР.

17. Захаренко К.Основні суб'єкти та інститути інформаційної безпеки. Науковий вісник. Серія «Філософія». Харків : ХНПУ. 2017. Вип. 48 (частина І). С. 212–219

18. Іванченко Є. В., Іванченко І. С., Хорошко В. О., Хохлачова Ю. Є. Забезпечення інформаційної безпеки держави Є.В. Іванченко; за ред. проф. В.О. Хорошка ; Вид-во Нац. авіац. ун-ту, 2016. 254 с.

19. Кісілевич-Чорнойван О. М. Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять. Інтернет-сайт «Правник. Бібліотека наукової юридичної літератури». URL : http://www.pravnuk.info/2013-12-27-15-12-23/120-informacijna-bezpeka-ta-mizhnarodnainformacijna-bezpeka-problema-viznachennya-1ponyat.html

20. Климчук О. О. Забезпечення інформаційної безпеки держави :

підручник / О. О. Климчук, В. М. Петрик, М. М. Присяжнюк та ін.. ; за заг. ред. О. А. Семченка та В. М. Петрика. – К. : ДНУ «Книжкова палата України», 2015. – 672 с.

21. Козачинська А. С. Державна політика у сфері інформаційної безпеки України: кв. робота на здоб ступ «магістр», спеціальність 281 «Публічне управління та адміністрування. URL : http://ir.polissiauniver.edu.ua/bitstream/123456789/12144/1/Kozachynska_AS_KR_281_2021.pdf.

24. Конституція України: Основний Закон України від 28.06.1996 № 254к/96-ВР. URL: http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

25. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: монографія / Б. А. Кормич. Одеса: Юридична література, 2003. 472 с.

26. Левченко Ю. О. Проблеми протидії інформаційній окупації в умовах гібридної війни. Інформаційна безпека в умовах гібридної війни: Міжнародна науково-практична конференція (м. Хмельницький, 16–17 листопада 2017 р.). Хмельницький : МВС УКРАЇНИ, 2017. 50 с.

27. Лизанчук В. В. Інформаційна безпека України: теорія і практика: підручник. Львів: ЛНУ ім. Івана Франка, 2017. 725 с.

28. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. Київ : КНТ, 2006. 280 с.

29. Логінова Н. І., Дробожур Р. Р. Правовий захист інформації: навчальний посібник / Логінова Н. І., Дробожур Р. Р. Одеса: Фенікс, 2015. 264 с.

30. Максимець В. Є., Вівсяна В. І. Співробітництво України та НАТО у протидії деструктивним інформаційним впливам російської федерації Вісник

НТУУ «КПІ». Політологія. Соціологія. Право. Випуск 2(58). 2023.

31. Мануйлов Є. М., Калиновський Ю.Ю. Аксіологічний вимір інформаційної безпеки української держави / Вісник Національного університету “Юридична академія України імені Ярослава Мудрого”. № 3 (34) 2017. С. 13-30.

32. Мохова Ю. Л., Луцька А. І. Сутність та головні напрямки державної інформаційної політики України. URL: http://www.dy.nayka.com.ua/pdf/12_2018/27.pdf

33. Мужанова Т. М. Інформаційна безпека держави: навчальний посібник. URL: https://nubip.edu.ua/sites/default/files/u34/posibnik_ibd_muzhanova_2019.pdf.

34. Ларін С. В. Сутність та зміст поняття “національні цінності” в контексті сучасних дослідницьких підходів / Вісник НАДУ при Президентові України. 2016. № 2. С. 44-49.

35. Олійник О. В. Структура суб’єктів забезпечення інформаційної безпеки в Україні / Актуальні проблеми держави і права. Випуск 68. 2016. с. 485-491.

36. Онищенко С. В., Глушко А. Д. Концептуальні засади інформаційної безпеки національної економіки в умовах діджиталізації. Соціальна економіка. ХНУ, 2020. Вип. 59. с. 14–24. URL: https://periodicals.karazin.ua/soceconom/article/view/16114

37. Остроухов В. В., Присяжнюк М. М., Петрик В. М. та ін. Інформаційна безпека (соціально-правові аспекти): підручник / За ред. Є.Д.Скулиша. К., 2010. – 776 с.

38. Панченко О. А. Іфнормаційна безпека держави як складних розвитку суспільних відносин. URL: https://www.rdc.org.ua/download/stati/inf-security2.pdf

39. Петрик В. М., Присяжнюк М. М., Мельник Д. С. та ін. Забезпечення інформаційної безпеки держави: підручник ; за заг. ред. О. А. Семченка та

В. М. Петрика. - К.: ДНУ «Книжкова палата України», 2015. - 672 с.

40. Печенюк А. В. Інформаційна безпека України як складова національної безпеки. URL: https://www.ndifp.com/1561/.

41. Почепцов Г. Г. Інформаційна політика: навчальний посібник. Київ : Вид-во УАДУ, 2002. 88 с.

42. Руденко Ю. Ю. Плюралізм в Україні як складова інформаційної політики у контексті забезпечення національної безпеки / Ю. Ю. Руденко. Актуальні проблеми управління інформаційною безпекою держави: зб. матер. наук.-практ. конф. – К. : Наук-вид. відділ НА СБ України, 2012. С. 96–97.

43. Про основи національної безпеки України : Закон України від 19.06.2003 р. № 96. URL: http://zakon2.rada.gov.ua/laws/show/964-15.

45. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про національну безпеку України": Указ Президента України від 26.05.2015 № 287/2015. URL: www.president.gov.ua/ documents/ 2872015190.

46. Руденко Ю. Ю. Плюралізм в Україні як складова інформаційної політики у контексті забезпечення національної безпеки / Актуальні проблеми управління інформаційною безпекою держави: зб. матер. наук.-практ. конф. К. : Наук-вид. відділ НА СБ України, 2012. Є Ж С. 96–97

47. Ситник Г. П. Інституційно-цивілізаційна парадигма дослідження проблем та державно-управлінських аспектів забезпечення національної безпеки. Вісник НАДУ. 2011. вип. 2. С.25-34 .

48. Ситник Г. П. Національна безпека України: теорія і практика : монографія. К. : Вид-во "Кондор", 2007. - 616 с.

49. Ситник Г. П. Сутність кризових ситуацій соціального характеру у контексті національної безпеки: філософсько-управлінський аспект Державне

управління: удосконалення та розвиток. 2019. № 8. URL: http://www.dy.nayka.com.ua/?op=1&z=1479.

50. Ситник Г.П., Орел М.Г. Публічне управління у сфері національної безпеки: підручник. 2020. 360 с.

51. Смолянюк В. Ф. Системні засади національної безпеки // Вісник Національного університету "Юридична академія України імені Ярослава Мудрого" № 2 (37) 2018. С. 107-126

52. Смотрич Д. В., Браілко Л. Інформаційна безпека в умовах воєнного стану. URL : http://visnyk-pravo.uzhnu.edu.ua/article/view/284104

53. Степко О.М. Аналіз головних складових інформаційної безпеки держави. Науковий вісник Інституту міжнародних відносин НАУ. Серія: Економіка, право, політологія, туризм. Київ : Видавництво Національного авіаційного університету. 2011. Вип. 1(3). С. 90–99.

54. Стратегія інформаційної безпеки (затверджена Указом Президента України від 28 грудня 2021 року). URL: https://www.president.gov.ua/documents/6852021-41069.

55. Стратегія кібербезпеки України, Указ Президента України від 15 березня 2016 року № 96/2016. URL : https://zakon.rada.gov.ua/laws/show/96/2016#n11

56. Стратегія кібербезпеки України, Указ Президента України від 15 березня 2016 року № 96/2016. URL : https://zakon.rada.gov.ua/laws/show/96/2016#n11

57. Ткачук Т. Ю. Державна політика у сфері забезпечення інформаційної безпеки на сучасному етапі. URL : https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/34230/1/%D0%94%D0%95%D0%A0%D0%96%D0%90%D0%92%D0%9D%D0%90%20%D0%9F%D0%9E%D0%9B%D0%86%D0%A2%D0%98%D0%9A%D0%90%20%D0%A3%20%D0%A1%D0%

A4%D0%95%D0%A0%D0%86%20%D0%97%D0%90%D0%91%D0%95%D0%97%D0%9F%D0%95%D0%A7%D0%95%D0%9D%D0%9D%D0%AF.pdf

58. Турчак А. Основні складові інформаційної безпеки держави. URL : https://aspects.org.ua/index.php/journal/article/view/600.

59. Федченко Д. І. Система забезпечення кібербезпеки: проблеми формування та ефективної діяльності / Д. І. Федченко // Молодий вчений. Випуск 5 (57). 2017. – с. 653-658

60. Філософія і методологічні проблеми воєнної теорії та практики / Л.М. Будагьянц, І.С. Печенюк, М.М. Шевченко та ін., під заг. ред. В. Ф. Баранівського. К. НАОУ, 2012. 524 с.

61. Храбан І. А. Система європейської безпеки і напрями воєннополітичної інтеграції України до її структур: монографія. К.: Варта, 2005. 544 с.

62. Шаповал Р. В., Клочко В. О. Вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України / Р. В. Шаповал, В.О. Клочко. Наше право. 2014. № 6. С. 5–9.

64. Шульга В. І. сучасні підходи до трактування поняття інформаційна безпека. Електронний журнал «Ефективна економіка». 2015. № 4. URL : http://www.economy.nayka.com. ua/?op=1&z=5514

65. Яковлєв П. О. Проблематика тлумачення категорії «Інформаційна безпека держави» в сучасній юридичні доктрині Україні. URL: http://nvppp.in.ua/vip/2020/1/7.pdf.

66. Ярема О.Г., Єсімов С.С. Предмет правового забезпечення інформаційної безпеки в інформаційному праві // Науковий вісник Львівського державного університету внутрішніх справ. – (Серія Право). – 2016. – № 2. – С. 244-252

67 . Cyber defence. (2022, March 23). Official site of North Atlantic Treaty Organization. URL: https://www. nato.int/cps/en/natohq/177273.htm

68. Brown H. Thinking About National Security. Defense and Foreign Policy in a Dangerous World. Colorado, 1983. p. 4.

69. U.S. National Security: A Framework for Analysis / Ed. By Kauffman, J.McKittrick, T.Leney. Lexington (Mass), 1985. pp. 12, 14.

70. Types of EUlaw. An official website of European Union. Види законодавства ЄС. Офіційнийвеб-сайт Європейського Союзу. URL:https://ec.europa.eu/info/law/law-making-process/types-eu-law_en.

71. What the European Commission does in strategy and policy. An official website of EuropeanUnion. URL: https://ec.europa.eu/info/about-european-commission/what-european-commission-does/strategy-and-policy_en..

72. Zhadan A. (2022, May 17). Countries brace for cyberattacks as Sweden and Finland move to join NATO. Latest Cybersecurity and Tech News, Research & Analysis. URL: https://cybernews.com/cyber- war/countries-brace-for-cyberattacks-as-sweden-and-finland-move-to-join-nato .

ВІДГУК
на кваліфікаційну роботу
на здобуття освітнього ступеня магістр
студента факультету суспільних та прикладних наук
спеціальність 281 «Публічне управління та адміністрування»
Пастернака Андрія Валерійовича

на тему: **«Державна політика у сфері інформаційної безпеки»**

Актуальність теми: У непростий для нашої країни час важливість інформації як інструменту у протидії агресору важко переоцінити. Фактично вона стає потужною зброєю. Це й не дивно, бо інформація може забезпечити перемогу у війнах, конфліктах, або стати засобом для подолання суспільно-політичної кризи. Особливої важливості набуває використання інформації набуває останнім часом, зокрема, у гібридних війнах, де безпосередній військовий аспект – лише частина загального плану.

Необхідно зважати, що в умовах, коли інформаційний контент спрямований на маніпулювання громадською думкою через фізіологічні та психологічні методи сприйняття, питання низького рівня інформаційної грамотності набуває виняткового значення, оскільки призводить до неможливості належним чином аналізувати інформацію та приймати необхідні рішення.

Самостійні розробки і пропозиції автора: розглянуто інформаційну безпеку як соціальне явище; досліджено структуру інформаційної безпеки та її елементів; охарактеризовано державну політику України у сфері інформаційної безпеки; окреслено особливості забезпечення інформаційної безпеки держави в умовах війни.

Практичне значення роботи: полягає в тому, що сформульовані в роботі положення, висновки, пропозиції та рекомендації можуть бути використані у: науково-дослідній діяльності – як основа для подальшого дослідження проблем формування державної політики у сфері інформаційної безпеки в умовах війни; правозастосовчій діяльності – для формування критеріїв ефективності процесу

формування державної політики у сфері інформаційної безпеки та її вдосконалення; навчальному процесі – при розробленні нових та оновленні існуючих навчальних курсів за спеціальністю «Публічне управління та адміністрування».

Зауваження: до роботи суттєвих зауважень немає.

Загальний висновок: Кваліфікаційна робота є завершеною самостійною працею та містить окремі ґрунтовні теоретичні та практичні рекомендації щодо реалізації державної політики у сфері інформаційної безпеки. Дослідження виконано та оформлено відповідно до встановлених вимог, відповідає вимогам Вищої школи, заслуговує високої оцінки, а її автор – Пастернак Андрій Валерійович – на присвоєння освітнього ступеня «магістр» за спеціальністю 281 «Публічне управління та адміністрування».

Науковий керівник:
доктор філософії,
доцент кафедри права
та публічного управління
ЗВО «Університет Короля Данила» Василь МЕЛЬНИЧУК

«23» 02. **2024 р.**

РЕЦЕНЗІЯ
на кваліфікаційну роботу
на здобуття освітнього ступеня магістр
студента факультету суспільних та прикладних наук
спеціальність 281 «Публічне управління та адміністрування»
Пастернака Андрія Валерійовича

на тему: **«Державна політика у сфері інформаційної безпеки»**

Актуальність теми: Перехід будь-якої країни до інформаційного суспільства вимагає переосмислення, а у окремих випадках і розробки нових механізмів регулювання відносин, що виникають між громадянами, їх об'єднаннями та державою. Всі суб'єкти інформаційних відносин повинні усвідомлювати і виконувати свою роль у цьому процесі, але саме держава призначена активно впливати на якісну сторону трансформаційних процесів, залучати до співпраці політиків, науковців, практиків, громадськість.

Найбільш суттєві висновки і рекомендації: інформаційна безпека включає в себе технологічні, організаційні та правові аспекти, а також вимагає відповідної культури безпеки серед користувачів і фахівців з інформаційної технології. Вона є важливим аспектом для захисту конфіденційної інформації, такої як особисті дані, комерційна інформація, важливі дані компаній та державних установ. Структура інформаційної безпеки може бути організована на кількох рівнях для ефективного захисту інформаційних ресурсів, систем та комунікаційних засобів.

Наявність самостійних розробок автора: державна політика у сфері інформаційної безпеки визначається комплексом стратегій, законодавчих актів, програм, заходів та регулятивних механізмів, які спрямовані на захист інформації, що має стратегічне значення для держави, суспільства та громадян. Державна політика у сфері інформаційної безпеки спрямована на забезпечення стабільності, захисту прав і свобод громадян, конфіденційності та цілісності інформації, а також підтримку економічного розвитку та інноваційного потенціалу країни.

Практична цінність розроблених питань: полягає в розробці положень, полягає в розробці положень, висновків та рекомендацій щодо ефективної реалізації державної політики у сфері інформаційної безпеки , які можуть бути використані для підвищення рівня розробки державної політики в сфері забезпечення національної безпеки Україні.

Наявність недоліків: разом з тим, окремі положення кваліфікаційної роботи потребують конкретизації під час захисту. На думку автора інформаційна безпека – це захист інформації від неправомірного доступу, втрати, пошкодження або знищення з метою забезпечення конфіденційності, цілісності та доступності цієї інформації. Тому при захисті кваліфікаційної роботи варто було б звернути увагу проблеми забезпечення інформаційної безпеки в умовах війни.

Загальний висновок про відповідність якості роботи рівню вищої освіти і оцінка, що пропонується: На основі проведеного аналізу кваліфікаційної роботи Пастернака А.В. можна зробити висновок про її відповідність вимогам вищої освіти. Робота виявляє глибоке розуміння обраної теми, систематизований підхід до її вивчення та аргументованість висновків. Дослідження відображає широкий огляд наукових джерел і літератури, а також використання різноманітних методів аналізу, що свідчить про професійну компетентність автора. З огляду на вищезазначене, кваліфікаційна робота Пастернака А.В. заслуговує на високу оцінку та рекомендується до захисту.

Рецензент:
кандидат юридичних наук,
професор, професор кафедри
цивільного і господарського
права та процесу,
декан факультету права
Львівського торговельно-
економічного факультету Олександр КОТУХА

ЛЬВІВСЬКИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ПРАВА
№ 01597980
УКРАЇНА

«23» 02 2024 р.

метадані

Заголовок

Державна політика у сфері інформаційної безпеки

Автор

Пастернак А.В. Науковий керівник / Експерт **Мельничук В.І.**

підрозділ

King Danylo University

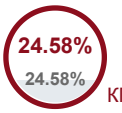
Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

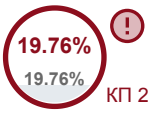
Заміна букв		23
Інтервали	A→	0
Мікропробіли		120
Білі знаки		0
Парафрази (SmartMarks)	a	77

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.



КП 1



КП 2

25
Довжина фрази для коефіцієнта подібності 2

17754
Кількість слів

155157
Кількість символів