Київський національний торговельно-економічний університет
Кафедра публічного управління і адміністрування

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
на тему:
ДЕРЖАВНА ПОЛІТИКА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Студента 4 курсу, 12 групи,
спеціальності 074 «Публічне управління та адміністрування»
спеціалізації «Публічне управління та адміністрування» Шилов Максим Андрійович

_____
(підпис студента)

Науковий керівник
доктор економічних наук,
доцент Ладонько Людмила Степанівна

_____
(підпис керівника)

Гарант освітньої програми
кандидат економічних наук,
доцент Головня Юлія Ігорівна

_____
(підпис гаранта)

Київ 2020

Київський національний торговельно-економічний університет

Факультет економіки, менеджменту та психології
Кафедра публічного управління та адміністрування
Освітній ступінь: бакалавр
Спеціальність: публічне управління та адміністрування
Спеціалізація: публічне управління та адміністрування

Затверджую
Зав. кафедри
Новікова Н.Л.

« 17» червня 2020р.

Завдання
на випускну кваліфікаційну роботу (проект)
студентові
Шилову Максиму Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема випускної кваліфікаційної роботи (проекту): «**ДЕРЖАВНА ПОЛІТИКА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ»**
Затверджена наказом ректора від «27» лютого 2020 р. № 757

2. Строк здачі студентом закінченого роботи (проекту): 15.05.2020

3. Цільова установка та вихідні дані до роботи (проекту)
Мета роботи (проекту): дослідження теоретичних і практичних засад та розробка практичних рекомендацій щодо вдосконалення державної політики у сфері інформаційної безпеки в Україні.

Об'єкт дослідження: процес реалізації державного управління у сфері забезпечення інформаційної безпеки України, діяльність органів державної влади щодо забезпечення інформаційної безпеки.

Предмет дослідження: теоретико-методологічні підходи та практичний інструментарій здійснення державної політики у сфері інформаційної безпеки в Україні.

4. Зміст випускної кваліфікаційної роботи (проекту) (перелік питань за кожним розділом):

5. Календарний план виконання роботи (проекту)

№ пор.	Назва етапів випускної кваліфікаційної роботи (проекту)	Строк виконання етапів роботи	
		за планом	фактично
1	2	3	4
1	Визначення напряму дослідження та затвердження теми випускної кваліфікаційної роботи	До 27.02.2020	27.02.2020
2	Складання плану та підготовка індивідуального завдання для виконання випускної кваліфікаційної роботи	До 10.03.2020	10.03.2020
3	Представлення на рецензування науковому керівнику рукопису першого розділу випускної кваліфікаційної роботи	До 01.04.2020	01-05.04. 2020
4	Представлення на рецензування науковому керівнику рукопису другого розділу випускної кваліфікаційної роботи	До 15.04.2020	20.04.2020

5	Представлення закінченої випускної кваліфікаційної роботи на кафедру	До 15.05.2020	15-20. 05.2020
6	Підготовка письмового відгуку на випускну кваліфікаційну роботу	До 25.05.2020	25.05.2020
7	Зовнішнє рецензування ВКР	До 01.06.2020	01-05. 06.2020
8	Проведення попереднього захисту випускних кваліфікаційних робіт	05-10. 06.2020	05-10. 06.2020
10	Вирішення питання про допуск випускної кваліфікаційної роботи до захисту	До 15.06.2020	До 15.06.2020
11	Направлення випускної кваліфікаційної роботи із зовнішньою рецензією у ЕК для захисту	За графіком	За графіком

6. Дата видачі завдання « 02 » березня 2020 р.

7. Науковий керівник випускної кваліфікаційної роботи (проекту) Ладонько Л.С.

(прізвище, ініціали, підпис)

8. Керівник проектної групи (гарант освітньої програми) Головня Ю.І.

(прізвище, ініціали, підпис)

9. Завдання прийняв до виконання студент Шилов М.А.

(прізвище, ініціали, підпис)

10. Відгук наукового керівника випускної кваліфікаційної роботи (проекту):

Сучасний стан суспільного розвитку характеризується як етап формування інформаційного суспільства, а впровадження новітніх інформаційних технологій значно прискорює процес отримання, обробки та аналізу інформації. Широкий і оперативний доступ до інформації підвищує ефективність її використання, що стає невід'ємним елементом управління всіма інститутами і процесами. Сучасна Україна повною мірою включена в процеси інформатизації суспільства і формування єдиного світового інформаційного ринку, тож інформаційний фактор відіграє значну роль у державотворчому процесі, у поданні та відстоюванні інтересів держави. Особливе місце у цьому спектрі суспільних відносин займають проблеми забезпечення інформаційної безпеки. Тож запропонована тема є нагальною та важливою.

Об'єкт, предмет, мета випускної кваліфікаційної роботи логічно пов'язані та чітко окреслюють поле дослідження, завдання роботи та висновки є взаємопов'язаними. Достовірність та обґрунтованість роботи підтверджуються аналізом праць вітчизняних та закордонних учених, використанням загальнонаукових та спеціальних методів дослідження.

Однак до роботи є зауваження:

Аналізуючи стан реалізації державної політики інформаційної безпеки України, на мою думку, варто було б додати більш ґрунтовний аналіз стану складових інформаційно-телекомунікаційної інфраструктури, яка, власне забезпечує технічний рівень забезпечення безпеки інформаційних потоків.

Незважаючи на окремі недоліки в роботі та висловлені зауваження, вважаю що студент на відмінно виконав дослідження. Робота може бути рекомендована до захисту, а її автор, Шилов Максим Андрійович, на присвоєння ступеня бакалавр зі спеціальності 074 «Публічне управління та адміністрування».

Науковий керівник випускної кваліфікаційної роботи: Ладонько Людмила Степанівна

(підпис, дата)

Відмітка про попередній захист Головня Юлія Ігорівна

(ПІБ, підпис, дата)

11. Висновок про випускну кваліфікаційну роботу (проект):

Випускна кваліфікаційна робота (проект) студента

Шилова М.А

(прізвище, ініціали)

може бути допущена до захисту екзаменаційній комісії.

Керівник проектної групи (гарант освітньої програми): Головня Юлія Ігорівна

(прізвище, ініціали, підпис)

Завідувач кафедри: Новікова Наталія Леонідівна

(підпис, прізвище, ініціали)

« 17» червня 2020 р.

ЗМІСТ

ВСТУП

В сучасному світі забезпечення інформаційної безпеки є однією з ключових складових політики кожної країни двадцять першого століття. Також воно має вплив на життя кожного окремного індивіда. Інформаційна безпека має тісний зв'язок з політикою, що держава проводить в інформаційній сфері. Вплив неефективної політики забезпечення інформаційної безпеки знаходить своє відображення в житті кожної особи, суспільства загалом та країни. Саме зараз наша держава знаходиться на шляху становлення інформаційного суспільства. Інформаційна незалежність лише формується. Інформаційна галузь є однією із складових національних інтересів сучасних держав, а, отже, варто звертати на неї особливу увагу. Саму тому розробка даного проекту є актуальною. В нашому суспільстві кожен громадянин повинен мати можливість створювати та накопичувати знання та інформацію, розкрити власний потенціал, створювати позитивні тенденції покращення рівня життя як на особистому, так і колективному рівні [1]. Існують дві особливості, що формують специфіку державного забезпечення інформаційної безпеки в України на сьогодні. Першою з них є євроінтеграційний вектор розвитку нашої країни з подальшим бажанням вступити до Європейського Союзу та НАТО. В наш час існують зовнішні та внутрішні інформаційні та політичні проблеми, саме тому важливим є те, щоб інформаційна безпека нашої країни була повноцінною та була зосереджена на всіх необхідних напрямках, мала прогресивний характер, тобто відповідала проблемам сучасного світу й була далекоглядною.

Другою особливістю забезпечення інформаційної безпеки в Україні є існування антиукраїнського впливу зовнішнього та внутрішнього характеру. Він полягає в пропагуванні ворожнечі на національному рівні, ідей сепаратизму, ненависті, насильства. Він спрямований на завдання шкоди та зруйнуванні української ідентичності, конституційному устрою України, а також територіальній цілісності. Саме тому необхідне існування такої державної політики в цьому напрямку, яка б дозволила захистити наш суверенітет та незалежність.

Мета роботи полягає в дослідженні теоретичних і практичних засад та розробці практичних рекомендацій щодо вдосконалення державної політики у сфері інформаційної безпеки в Україні.

Досягнення мети роботи передбачає вирішення наступних **завдань:**

1) визначити теоретичні аспекти державної політики забезпечення інформаційної безпеки;

2) дослідити досвід іноземних держав щодо забезпечення інформаційної безпеки;

3) провести аналіз вітчизняного законодавчого забезпечення інформаційної безпеки та практичних заходів державної політики щодо її реалізації;

4) визначити існуючі загрози інформаційної безпеки України та практичні рекомендації щодо їх усунення.

Об'єктом дослідження є процес реалізації державного управління у сфері забезпечення інформаційної безпеки України, діяльність органів державної влади щодо забезпечення інформаційної безпеки.

Предметом дослідження є теоретико-методологічні підходи та практичний інструментарій здійснення державної політики у сфері інформаційної безпеки в Україні.

Методи дослідження. Для теоретичного осмислення різних аспектів проблеми застосовуються аналіз і синтез (можливості адаптації світових зразків в Україні із організації інформаційної безпеки держави та її забезпечення, дослідження стану вітчизняної теоретико-методологічної бази інформаційної безпеки), абстрагування й узагальнення (визначення шляхів удосконалення організаційно-правового забезпечення державної політики у сфері інформаційної безпеки України, порівняння й уточнення новітніх функціоналів системи державного управління нею), дедукція та індукція (розклад об'єкту дослідження на складові та оцінка його стану) та графічний метод (використання схем та таблиць).

Структура роботи. Випускна кваліфікаційна робота складається зі вступу, двох розділів, які поділені на підрозділи, висновків та списку використаних джерел (50 найменувань). Обсяг роботи складає 40 сторінок.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ТА ЗАКОНОДАВЧІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

1.1. Теоретико-методичні аспекти інформаційної безпеки держави

Розгляд питання теоретичних аспекту інформаційної безпеки України варто почати з визначення основних нормативно-правових актів, що врегульовують відносини в інформаційній сфері. Вони включають в себе наступні акти: Конституція України, Закон України «Про інформацію», Закон України «Про друковані засоби масової інформації в Україні», Закон України «Про телебачення і радіомовлення», Закон України «Про інформаційні агентства», Закон України «Про рекламу», Закон України «Про Національну раду України з питань телебачення і радіомовлення», Закон України «Про національну безпеку України», інші закони.

Так, стаття 34 Конституції України зазначає, що кожному громадянину гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Кожен громадянин має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір [2].

Законодавство України має визначення поняття «інформація». Так, Закон України «Про інформацію» визначає інформацію як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Цей нормативно-правовий акт закріплює загальні засади права особи на доступ до інформації в усіх сферах суспільного і державного життя України, забезпечує громадянам можливість для участі в управлінні державними і громадськими справами, для впливу на поліпшення роботи органів державної влади і місцевого самоврядування, підприємств, установ, організацій незалежно від форм власності. Закон закріплює види інформації, врегульовує діяльність журналістів, засобів масової інформації та їх працівників, зазначає відповідальність за порушення законодавства про інформацію [3].

Розгляд інформаційної безпеки неможливий без інформаційної політики держави. Даний закон також надає визначення державній інформаційній політиці. Державна інформаційна політика - це сукупність основних напрямів і способів діяльності держави з отримання, використання, поширення та зберігання інформації. Вчені наводять визначення, яке є аналогічним законодавству, так Ю. М. Іванченко також вказує, що під поняттям інформаційної політики слід розуміти сукупність основних напрямів і способів діяльності держави з отримання, використання, поширення та зберігання інформації [4].

Цікавою є думка вченої Березовської, яка при аналізі поняття «державна інформаційна політика», вказує, що така політика повинна закласти основи для вирішення фундаментальних завдань розвитку суспільства, головними з яких є формування єдиного інформаційного простору України та її входження у світовий інформаційний простір, гарантування інформаційної безпеки особистості, суспільства й держави [5]. Закон визначає наступні основні напрямами державної інформаційної політики:

1) забезпечення доступу кожного до інформації;

2) забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;

3) створення умов для формування в Україні інформаційного суспільства;

4) забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;

5) створення інформаційних систем і мереж інформації, розвиток електронного урядування;

6) постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;

7) забезпечення інформаційної безпеки України;

8) сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору [3].

Дослідженням теоретичних та практичних аспектів інформаційної політики в період її зародження та становлення займались такі вітчизняні вчені, як О.Токар [9],

В.Іванов [10], А.Москаленко [11], С.Чукут [12], О.Литвиненко [13], Г.Почепцов [12] та інші. Чукут та Почепцов вважають, що при визначенні основних напрямків державної інформаційної політики слід враховувати сучасні умови суспільного розвитку, а саме формування інформаційного суспільства, яке сприяє поширенню процесів глобалізації, усуненню комунікаційних бар'єрів як на міждержавному рівні, так і на рівні окремих громадян. Ці вчені також розробили власну класифікацію напрямів здійснення сучасної державної інформаційної політики:

1) забезпечення свободи слова;

2) забезпечення та сприяння вільному доступу до суспільно значимої інформації;

3) збереження суспільної моралі, захист честі і гідності особистості;

4) сприяння конкуренції у сфері засобів масової інформації та ІКТ (зокрема за допомогою регулювання концентрації засобів масової інформації; державної підтримки ЗМІ тощо);

5) залучення інвестицій у розвиток ІКТ та їх пільгове оподаткування;

6) сприяння відкритості та прозорості органів державної влади та місцевого самоврядування (зокрема, розвиток електронного уряду);

7) захист культурної і мовної самобутності; переведення культурної спадщини у цифровий формат;

8) захист інтересів найбільш вразливих громадян (неповнолітніх, непрацездатних, національних меншин) в інформаційній сфері;

9) боротьба з неналежним використанням сучасних інформаційних технологій;

10) забезпечення інформаційної безпеки;

11) захист персональних даних;

12) охорона недоторканності приватного життя;

13) формування позитивного іміджу держави та державних органів [14, с.280-281].

Державну політику в інформаційній сфері розробляють і здійснюють органи державної влади загальної компетенції, а також відповідні органи спеціальної

компетенції.

Державна інформаційна політика є важливою складовою зовнішньої і внутрішньої політики країни й охоплює всі сфери життєдіяльності суспільства. Ця галузь має стати цілісною, концептуально вивіреною та перспективною. Вона має бути незалежною від тимчасових факторів, особистих уподобань і уявлень.

Суб'єктами інформаційних відносин є: громадяни України, юридичні особи, держава та об'єднання громадян. Відповідно до Закону України "Про інформацію" суб'єктами інформаційних відносин також можуть бути інші держави, їх громадяни та юридичні особи, міжнародні організації та особи без громадянства. Від імені держави виступають: Президент України, Верховна Рада України, Кабінет Міністрів України, Державний комітет телебачення та радіомовлення України, а також Національна рада з питань телебачення та радіомовлення. Всіх суб'єктів інформаційних відносин можемо об'єднати в групи, що представлені в Додатку А.

Об'єктами інформаційних відносин є: документована або публічно оголошувана інформація про події та явища в галузі політики, економіки, культури, охорони здоров'я, а також у соціальній, екологічній, міжнародній та інших сферах [3]. В свою чергу Токар визначає об'єкт інформаційної політики як національну інформаційну сферу з усіма її компонентами [8, с. 131].

Переходячи від інформаційної політики до інформаційної безпеки варто відзначити, що у вітчизняних вчених існують різні думки щодо визначення поняття «інформаційна безпека». Прикладами можуть слугувати наступні варіанти визначення:

1) Так Нашинець-Наумова характеризує «інформаційну безпеку» як стан захищеності національних інтересів України в інформаційній сфері, що визначається сукупністю збалансованих інтересів особистості, суспільства і держави. Дослідниця також надає власне бачення розуміння забезпечення інформаційної безпеки. На її думку, це сфера державного, політичного управління, вища форма свідомого регулювання процесами функціонування самої державної системи [15];

2) Боднар описує дане поняття як сукупність засобів забезпечення

інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз [16]. Варто зазначити, що ця складова національної безпеки має включати ефективну протидію існуючим інформаційним загрозам;

3) Євдоченко визначає в своїй праці «інформаційну безпеку держави» як стан державної інформаційної озброєності, за якого зовнішні інформаційні впливи не мають вирішального значення при прийнятті рішень, спрямованих на забезпечення державних інтересів. При такому визначенні показником ефективності системи забезпечення інформаційної безпеки вважається зведення до мінімуму шкоди, нанесеної через невчасність, неповноту і недостовірність інформації, а також через отримання інформації або її несанкціоноване поширення [17].

Проаналізувавши подібний плюралізм думок, що викликаний, перш за все, неоднозначністю трактування даної категорії, можна виділити, що інформаційна безпеки нерозривно пов’язана з інформаційною політикою, а саме її захищеністю від зовнішніх та внутрішніх негативних впливів, що виражається у самостійності державної політики.

Отже, державна політика забезпечення інформаційної безпеки в Україні – це напрям діяльності органів державної влади в Україні, що спрямований на забезпечення захищеності національних інтересів в інформаційній сфері. Концепція інформаційної безпеки України була створена, щоб розробити базис державного реагування на сучасні виклики, що постають перед національною безпекою України в інформаційній сфері [18].

Всі суб’єкти забезпечення інформаційної безпеки в Україні представлені в додатку А.

Напрями державної політики у сфері інформаційної безпеки:

1) Створення балансу між дотриманням прав і свобод у інформаційній сфері і здійснення владних повноважень щодо ліквідації інформаційних загроз на всіх рівнях інформаційної безпеки;

2) Розвиток нормативно-правового забезпечення інформаційної сфери та його адаптація з законодавством та критеріями Європейського Союзу;

3) Створення умов для виробництва національних інформаційних продуктів;

Таблиця 1.1

Суб'єкти забезпечення інформаційної безпеки в Україні

Державні суб'єкти	Кабінет Міністрів України, Верховна Рада України, Президент України, інші органи загальної компетенції та органи, що відповідають за забезпечення національної безпеки в інформаційній сфері, державні засоби масової інформації, державні підприємства, що займаються телекомунікаційною діяльністю, державні навчальні заклади, дослідницькі інститути, що займаються науковою діяльністю та підготовкою фахівців у сфері інформаційної безпеки.
Недержавні суб'єкти	Громадяни України, громадські об'єднання, організації, інші суспільні інституції, недержавні засоби масової інформації, підприємства, що надають телекомунікаційні послуги, та інші установи, що займаються діяльністю в інформаційній сфері, приватні навчальні заклади, дослідницькі установи, що займаються науковою діяльністю та підготовкою персоналу в інформаційній галузі.

Джерело: Розроблено автором на основі [18]

4) Створення ефективної системи стратегічних комунікацій із застосуванням підходів прогресивних країн світу;

5) Формування та впровадження ефективної національної інформаційної політики, що повинна бути спрямована на розвиток державного інформаційного простору, налагодження взаємодії між суб'єктами, які замаються провадженням державної політики в сфері інформаційної безпеки та державної інформаційної політики;

6) Забезпечення безпеки функціонування усіх суб'єктів і об'єктів національного інформаційного простору;

7) Забезпечення інформаційної безпеки у політичній, економічній, оборонній, державної безпеки і правопорядку, соціально-гуманітарній, науково-технологічній, екологічній, власне інформаційній сферах;

8) Створення системи охорони та технічного захисту інформації, віднесеної до державної таємниці та іншої інформації обмеженого доступу;

9) Виявлення інформаційних, інформаційно-психологічних впливів на особу, громадські і державні інституції, кібератак, застосування проти України інформаційної зброї та протидії і нейтралізації джерел внутрішніх і зовнішніх загроз

[18, 22].

Пріоритетами діяльності держави щодо забезпечення інформаційної безпеки є:

1) Створення та поширення українського інформаційного продукту всередині країни, а також за її межами;

2) Захист прав та свобод громадянина і людини у сфері інформації;

3) Розвиток і розповсюдження вітчизняних інформаційних технологій, послуг і ресурсів, покращення технічного стану каналів передачі даних.

Забезпечення інформаційної безпеки держави поєднує якісне забезпечення інформування громадян та надання їм відкритого доступу до різних джерел інформації, як то друковані засоби масової інформації, телебачення, радіо, а також сучасні ресурси в мережі Інтернет та соціальні мережі, а також контроль за розповсюдженням таємної інформації, що визначається чинним законодавством [19], та захист від загроз, про які мова йтиме пізніше.

Варто розглянути рівні забезпечення інформаційної безпеки, що представлені на рисунку 1.1.

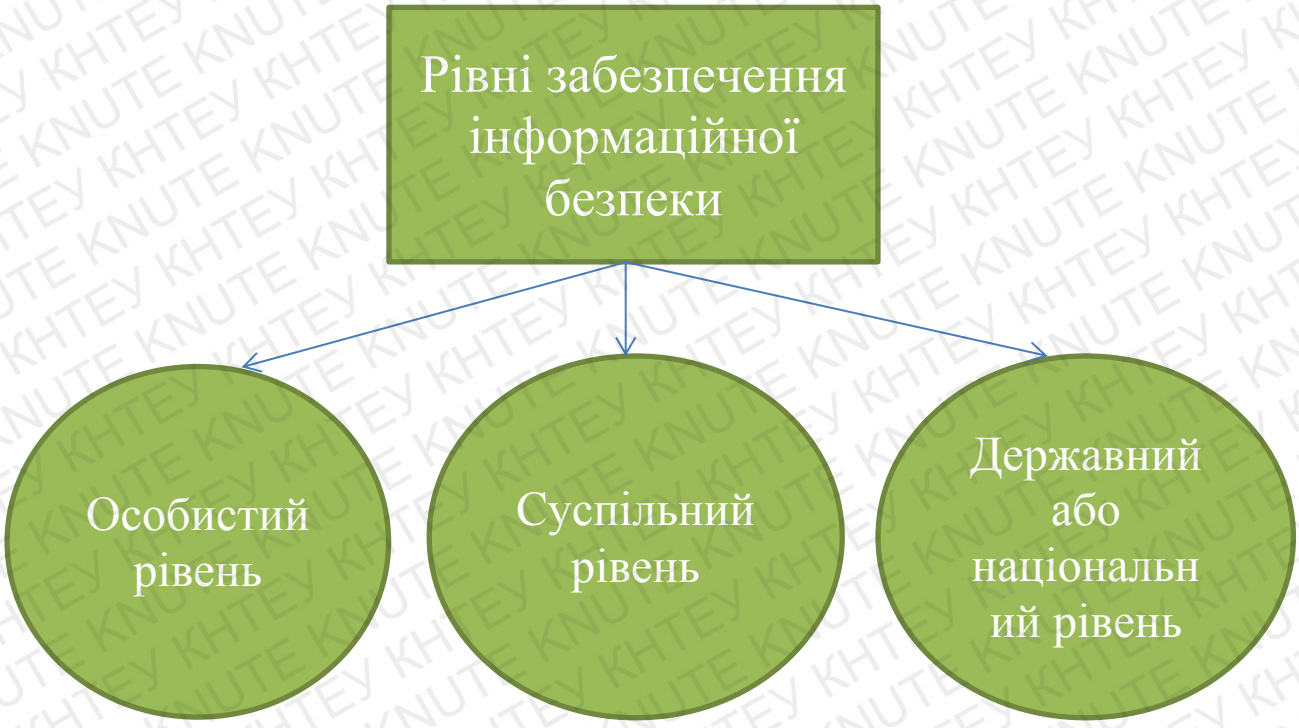


Рис. 1.1. Рівні забезпечення інформаційної безпеки

Джерело: Розроблено автором на основі [20]

Таким чином, можна виокремити три рівні забезпечення інформаційної безпеки:

1) Особистий рівень, що являє собою створення критичного, раціонального мислення на основі принципу свободи вибору;

2) Суспільний рівень, під цим рівнем варто розуміти створення якісного інформаційно-аналітичного простору, плюралізм думок, велику кількість шляхів отримання інформації, незалежність вітчизняних засобів масової інформації, що повинні належати українським власникам;

3) Державний або національний рівень. Забезпечення інформаційної безпеки на цьому рівні полягає у аналітично-інформаційному забезпеченні діяльності державних органів, достатнє забезпечення інформацією зовнішньої та внутрішньої політики на міжнародному рівні, створення системи захисту інформації з можливістю обмеженого доступу, боротьба з правопорушення в сфері інформації, а також боротьба з внутрішніми та зовнішніми інформаційними загрозами [20].

1.2. Механізми забезпечення державної політики інформаційної безпеки

Можна виділити такі механізми забезпечення інформаційної безпеки держави як законодавчі, політичні, ідеологічні, соціальні, інформаційні, технологічні, кадрового забезпечення, матеріально-технічного забезпечення та фінансового забезпечення.

Під політичними механізмами варто розуміти забезпечення реального волевиявлення українського народу, який є єдиним джерелом влади в нашій державі. Воно відбувається шляхом виборів, референдумів та інших форм демократії. Також до цих засобів відноситься створення умов для цивілізованої політичної боротьби, тобто існування різноманіття політичних партій, громадських організацій, боротьба яких відбувається під час виборчих кампаній та під час діяльності в органах законодавчої влади. При цьому під час формування зовнішньої та внутрішньої політики варто враховувати позитивні пропозиції та вимоги партій,

громадських організацій, різних масових акцій, якщо вони підтримуються переважною більшістю населення та відповідають їх інтересам.

Наступною групою механізмів є ідеологічні механізми. Загалом вони полягають у формуванні національної ідеї та об'єднанні народу навколо неї.

Соціальні механізмів являють собою сутність соціального управління. Вважається, що держава та її політика повинна застосовувати всі можливі засоби для підвищення рівня життя населення. Зростання рівня життя людини і громадянина є однією з найбільш важливих факторів, що впливають на довіру до державних інституцій, підвищення активності та відповідальності громадського суспільства щодо захисту національних інтересів. В результаті реформи децентралізації зростає роль виконавчих комітетів районних, міських, сільських та селищних рад та місцевої влади в цілому, яким делегували значні повноваження, а, отже, взаємодія центральної влади та місцевої є запорукою економічно-соціального розвитку та забезпечення інформаційної безпеки [21].

Далі варто розглянути інформаційні механізми, це механізми інформаційної політики держави, чиє спрямування пов'язане з забезпеченням державної інформаційної безпеки. Одним з засобів є формування у населення позитивного сприйняття заходів, напрямів і цілей державної політики забезпечення інформаційної безпеки. Також в сучасному реаліях важливим засобом є викриття зовнішніх і внутрішніх джерел негативних інформаційних та психологічних впливів, які застосовуються проти України, а також їх правова оцінка відносно чинного законодавства та норм міжнародного права. Ще одним засобом є координація інформаційних служб всіх гілок державної влади щодо інформування громадян нашої держави та світової спільноти щодо державної політики забезпечення інформаційної безпеки та узгодження оцінок процесів та подій, що відбуваються у даній сфері.

Технологічні механізми полягають у комплексі організаційних, організаційно-технічних, інженерно-технічних, криптографічних, спеціальних засобів, спрямованих на створення та ефективне функціонування системи забезпечення інформаційної безпеки.

Основоположним механізмом забезпечення державної політики інформаційної є чинне законодавство в цій сфері. Модель правового механізму забезпечення інформаційної безпеки в Україні представлена на рисунку 1.2.

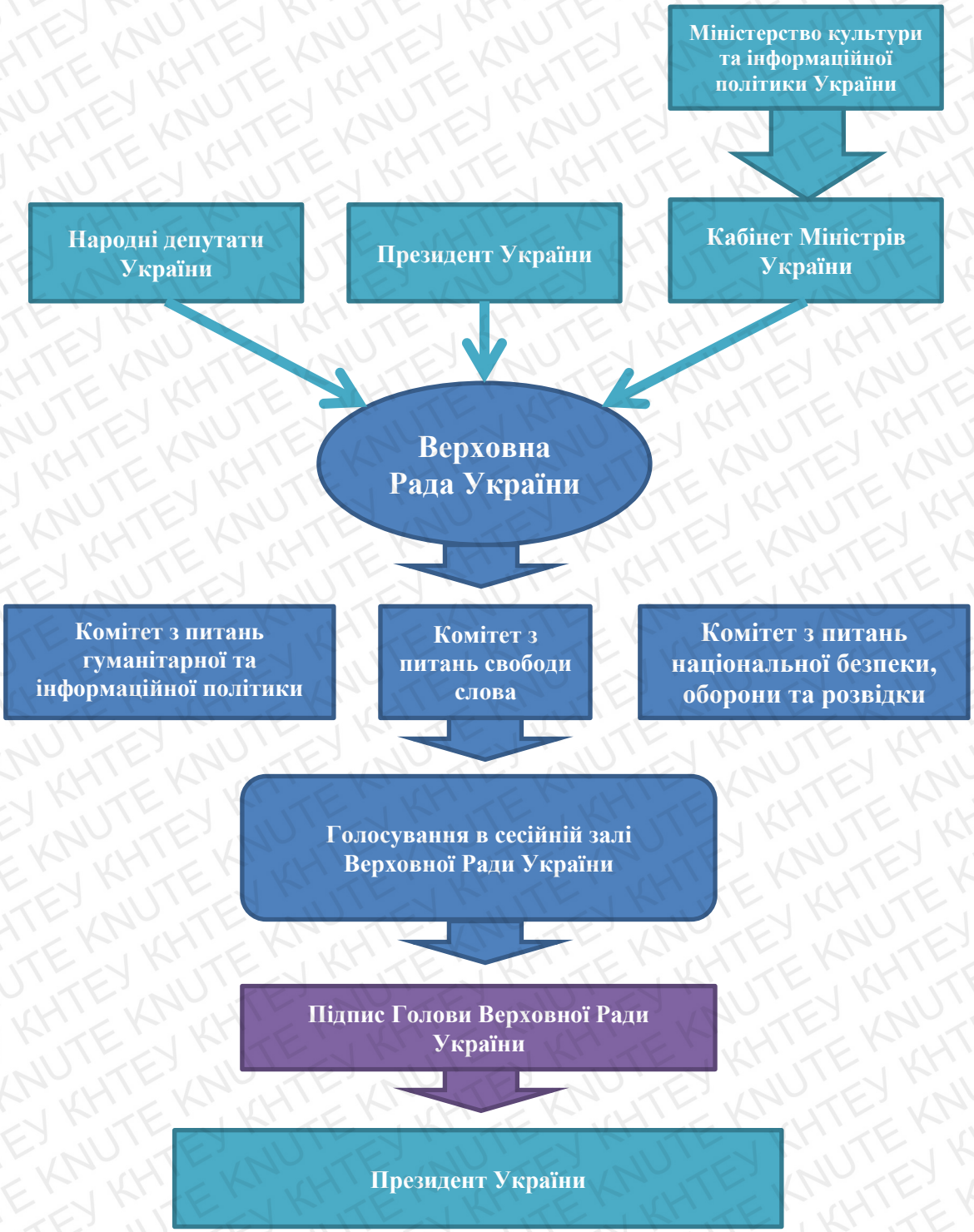


Рис. 1.2. Модель правового механізму забезпечення інформаційної безпеки

Джерело: Розроблено автором на основі даних [2; 23-25]

Сутність даної моделі полягає в тому, що Кабінет Міністрів, в якому відповідальним за інформаційну політику є Міністерство культури та інформаційної політики, Президент України та народні депутати України мають право вносити проекти законів на розгляд Верховної Ради України. Проекти законів передаються до відповідних комітетів. Після обговорення законопроекту у комітеті він виноситься на голосування в сесійній залі Верховної Ради України. У разі прийняття закону він передається на підпис до Голови Верховної Ради України. Останнім кроком у даному механізмі є підпис Президента України [2; 23-25].

Сутність механізмів кадрового забезпечення – це способи та прийоми навчання та розстановки кадрів на посадах в органах державної влади, враховуючи їх професійний рівень та морально-етичні якості. Необхідне існування спеціальних навчальних програм для підготовки персоналу для різних рівнів державного управління та забезпечення інформаційної безпеки.

Під механізмами матеріально-технічного та фінансового забезпечення варто розуміти економічний аспект створення умов для державного забезпечення інформаційної безпеки, діяльності всіх органів державної влади, їх структурних підрозділів, що здійснюють свої повноваження в цій сфері [22].

При розгляді законодавства в сфері забезпечення інформаційної безпеки варто почати з Конституції України. Стаття 17 загальних засад визначає, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, обов’язком народу України [2].

Закон України «Про інформацію» невідривно пов’язаний з інформаційною безпекою, оскільки він надає понятійну базу щодо того, що таке інформація, які бувають її види тощо. Але в нашому випадку цікавою є частина 2 статті 6 цього закону. Стаття присвячена гарантії права на інформацію, але вищезгадана частина зазначає, що право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації,

одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. Стаття 11 визначає обмеження, пов'язані з забезпеченням безпеки. Забороняється зберігання, використання та поширення конфіденційної інформації про особу, крім, визначених законом, випадків та в інтересах національної безпеки [3].

Закон України «Про друковані засоби масової інформації (пресу) в Україні» встановлює певні обмеження в діяльності друкованих засобів масової інформації в Україні. Так забороняється використання друкованих засобів масової інформації для:

1) закликів до захоплення влади, насильницької зміни конституційного ладу або територіальної цілісності України;

2) пропаганди війни, насильства та жорстокості;

3) розпалювання расової, національної, релігійної ворожнечі;

4) розповсюдження порнографії, а також з метою вчинення терористичних актів та інших кримінально караних діянь;

5) пропаганди комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів та їхньої символіки;

6) популяризації або пропаганди держави-агресора та її органів влади, представників органів влади держави-агресора та їхніх дій, що створюють позитивний образ держави-агресора, виправдовують чи визнають правомірною окупацію території України [26]**.**

Важливою складовою законодавства про інформаційну безпеку є Закон України «Про телебачення і радіомовлення». Стаття 6 регламентує неприпустимість зловживання свободою діяльності телерадіоорганізацій. Телерадіоорганізації в інформаційних блоках зобов'язані подавати інформацію про офіційно оприлюднену у будь-який спосіб позицію всіх представлених в органах влади політичних сил. Не допускається використання телерадіоорганізацій для поширення відомостей, що становлять державну таємницю, або іншої інформації, яка охороняється законом, закликів до насильницької зміни конституційного ладу України й інші обмеження. Варто зазначити, що забороняються трансляції телепередач, виготовлених після 1

серпня 1991 року, що містять популяризацію або пропаганду органів держави-агресора та їхніх окремих дій, що виправдовують чи визнають правомірною окупацію території України [27].

Під час розгляду законодавства про інформаційну безпеку необхідно розглянути такий нормативно-правовий акт як Закон України «Про національну безпеку України» [28]. Якщо розглядати інформаційний аспект, то даний закон охоплює питання кібербезпеки. Стаття 31 регламентує стратегію кібербезпеки України. Стратегія кібербезпеки України є документом довгострокового планування, в якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, підвищення ефективності основних суб'єктів забезпечення кібербезпеки, насамперед суб'єктів сектору безпеки і оборони, щодо виконання завдань у кіберпросторі, а також потреби бюджетного фінансування, достатні для досягнення визначених цілей і виконання передбачених завдань, та основні напрями використання фінансових ресурсів [28].

Стаття 10 Закону України «Про Службу безпеки України» визначає, що до складу Центрального управління Служби безпеки України входить підрозділ, що займається контррозвідувальним захистом інтересів держави у сфері інформаційної безпеки [29].

Важливою складовою забезпечення інформаційної безпеки України є Державна служба спеціального зв'язку та захисту інформації України , діяльність якої регулюється Законом України «Про Державну службу спеціального зв'язку та захисту інформації України». Він визначає, що Служба є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку. Державна служба спеціального зв'язку та захисту інформації України спрямовує свою діяльність на

забезпечення національної безпеки України від зовнішніх і внутрішніх загроз та є складовою сектору безпеки і оборони України [30].

Також варто розглянути Доктрину інформаційної безпеки України. Даний програмний документ виник через застосування Російською Федерацію технологій гібридної війни, а саме використання інформаційного та інформаційно-психологічного впливу. Доктрина була затверджена указом Президента України в 2017-му році. Доктрина інформаційної безпеки України визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері. Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни. Доктрина визначає національні інтереси України в інформаційній сфері, а саме поділяє їх на життєво важливі інтереси особи та життєво важливі інтереси суспільства і держави. Також Доктрина зазначає актуальні загрози національним інтересам та національній безпеці в інформаційній сфері. Встановлюються пріоритети державної політики в інформаційній сфері, вони поділяються на три групи пріоритетів, зокрема забезпечення інформаційної безпеки, забезпечення захисту та розвитку інформаційного простору України, конституційного права громадян на інформацію, а також відкритості та прозорості держави перед громадянами [31].

Аналіз основних законодавчих документів забезпечення інформаційної безпеки України демонструє, що елементи державної політики в цьому напрямі є складовою багатьох нормативно-правових актів нашої держави, вони часто перетинаються з інформаційною політикою та можуть знаходити відображення в одних і тих самих актах.

1.3. Інформаційна безпека зарубіжних країн

Розгляд зарубіжного досвіду варто розпочати зі Сполучених Штатів Америки. Перш за все, Законом США «Про національну безпеку», прийнятого 26-го липня

1947-го року, визначається, що відповідальність щодо забезпечення національної безпеки та інформаційної безпеки, як її складової, покладається на Президента США. Також цей Закон створив таку важливу складову забезпечення інформаційної безпеки США як Центральне Розвідувальне Управління, а також запровадив посаду директора ЦРУ, що призначається Президентом США та погоджується з Сенатом [32].

Директор ЦРУ за допомогою органу, який він очолює, займається отриманням та обробкою даних окремих людей, компаній, іноземних країн, організацій тощо. ЦРУ проводить оцінку отриманої інформації щодо пов'язаності її з національною та інформаційною безпекою, наявності потенційних загроз та повідомляє про них відповідним гілкам влади [33].

В Америці важливим документом, що регламентує державну політику інформаційної безпеки є Національна стратегія забезпечення кібербезпеки. За останні два десятиліття в США видавалися два подібні документи. Перший з них був виданий у лютому 2003-го року як реакція на серію терактів 11-го вересня 2001-го року [34]. Діюча версія національної стратегії була видана у вересні 2018-го. Національна кіберстратегія Сполучених Штатів Америки, як і попередня версія, починається зі звернення Президента Америки до народу. В своєму зверненні він пояснює причини розробки цієї стратегії. За словами Дональда Трампа, ця стратегія пояснює те, як його адміністрація буде захищати батьківщину шляхом захисту електронних мереж, систем та інформації, просувати американське благополуччя через розвиток захищеної та процвітаючої цифрової економіки та захист вітчизняних інновацій. Також аргументується забезпечення миру та безпеки шляхом посилення можливості Сполучених Штатів разом зі своїми союзниками та партнерами виявляти та, в разі необхідності, карати тих, хто використовує інформаційний інструментарій у шкідливих намірах. Виділяється важливість поширення американського впливу за кордон через поширення ключових принципів відкритої, сумісної, надійної та безпечної мережі Інтернет.

Національна стратегія складається із вступної частини та чотирьох розділів. У вступній частині прописані основні причини, чому було прийняте рішення створити

цю стратегію, а саме через те, що вплив інформаційного простору неможливо недооцінити та те, що всі більше американців велику частину свого життя проводять в Інтернеті. Виділяється те, що США розглядають всесвітню мережу як відкриту, сумісну, надійну та безпечну систему, але їх суперники мають інше бачення цієї ситуації. Згадуються численні інформаційні та хакерські атаки з боку Росії, Ірану та Північної Кореї, що мали на меті нанести шкоду американському та міжнародному бізнесу, та союзникам й партнерам Сполучених Штатів.

Перший розділ називається «Захистити американський народ, Батьківщину та американський спосіб життя». Сутність розділу в завданні захистити федеральні мережі та інформацію, централізованому менеджменті та нагляді за федеральною цивільною кібербезпекою, виділяється необхідність забезпечення безпеки критичної інфраструктури від зовнішнього та внутрішнього несанкціонованого втручання. Важливим є розуміння того, що постачальники інформаційних та телекомунікаційних технологій є частиною інформаційної безпеки. Зазначається необхідність захисту демократії шляхом забезпечення безпеки всього виборчого процесу на території США. Прогресивним є занепокоєння космічної складової інформаційної безпеки, оскільки в космос запускаються все більше різних супутників.

Другий розділ під назвою «Популяризація американського благополуччя». Даний розділ присвячений пріоритетам розвитку активної та гнучкої цифрової економіки, виділяється необхідність інновацій в цій сфері та забезпечення їх безпеки. Зазначається необхідність просувати ідеї вільного потоку даних через кордони. Важливим також є захист та розвиток винахідливості Сполучених Штатів, тобто створення сильної та збалансованої системи захисту інтелектуальної власності, наголошується пріоритетність захисту конфіденційності та недоторканності американських ідей та винаходів. Для цього необхідно розвивати кваліфіковану робочу силу, яка була б навчена працювати в інформаційному просторі.

Третій розділ має назву «Забезпечення миру шляхом власного посилення». В розділі мова йде про два напрямки. Перший з них – підвищення стабільності

інформаційного простору через норми відповідальної поведінки країн, тобто необхідне існування певних стандартів поведінки офіційних представників країн в інформаційному просторі. Другий напрямок – виявлення та недопущення неприпустимої поведінки в інформаційному просторі. Вказано, що Сполучені Штати будуть використовувати всі допустимі наявні засоби для боротьби зі шкідливим впливом в цій сфері.

Останній розділ під назвою «Просування американського» присвячений популяризації вільної та захищеної мережі Інтернет, визначається авторитетність США на цьому ринку та необхідність працювати з партнерами, що мають спільне бачення на проблему, щодо забезпечення свободи слова в мережі Інтернет. Зазначається, що створення міжнародного інформаційного потенціалу допоможе США захищати спільні інтереси зі своїми партнерами та союзниками та сприятиме досягненню дипломатичних, економічних та безпекових цілей [35].

Яскравим прикладом недемократичного забезпечення інформаційної безпеки є Китайська Народна Республіка. В інформаційній політиці Китаю домінують принципи втілення достатньо моноцентричних оборонних і наступальних доктрин. В політичному та безпековому дискурсі КНР інформація, як в її соціально-культурному, так і в технологічно-інноваційному вимірах, розглядається насамперед як збройний ресурс, як засіб впливу на власних громадян та активного захисту і протидії зовнішнім інформаційним впливам. Використання могутньої та широкої ресурсної бази дозволяє Китаю проводити достатньо ефективну інформаційну політику, навіть незважаючи на її недемократичну спрямованість [36]. Цікавим є політика Китаю щодо свободи в мережі Інтернет. В країні не функціонують більшість сайтів, якими користуються громадяни в західному світі, але існують вітчизняні аналоги. Законодавчий орган Китаю, Національний народний конгрес Китайської Народної Республіки періодично приймає закони в цій сфері, тим самим проводячи політику централізації контролю за мережею Інтернет, система контролю за мережею Інтернет має назву проект «Золотий щит» [37]. Закордонні компанії можуть працювати та отримувати доступ до інформаційного простору, отримавши відповідні дозволи в Китайському центрі огляду технологій та сертифікації в сфері

кібербезпеки, що раніше мав назву Центру сертифікації інформаційної безпеки Китаю. Китайський центр огляду технологій та сертифікації в сфері кібербезпеки є державною установою, безпосередньо під управлінням Державного управління ринкового нагляду та адміністрації, та юридичною особою. Його функціями є: проведення досліджень технологій та методів огляду мережевої безпеки; проведення досліджень щодо оцінки сертифікації мережевої безпеки та відповідних стандартів технологій та методів, проведення технічного навчання персоналу з огляду мережевої безпеки та персоналу з сертифікації мережевої безпеки; відповідно до основних стандартів сертифікації в межах затвердженої роботи. Після отримання відповідних дозволів компанії можуть функціонувати на території Китаю, дотримуючись всіх існуючих обмежень [38].

Порівняльна характеристика інформаційної безпеки Сполучених Штатів Америки та Китайської Народної Республіки наведена у таблиці 1.2.

Таблиця 1.2

Порівняльна характеристика інформаційної безпеки США та КНР

Сполучені Штати Америки	Китайська Народна Республіка
Наявність основоположного документа, що регламентує діяльність держави в напрямку забезпечення інформаційної безпеки. Ліберальний підхід, що полягає в популяризації ідеї безпечної мережі Інтернет, захисті вітчизняних технологій, інформаційних ресурсів та ідей, а також їх поширення за межами США. Інформація розглядається як інструмент захисту інтересів та досягнення дипломатичних, економічних та безпекових цілей, тобто як можливість.	Відсутність єдиного програмного документа. Консервативний підхід, що полягає в баченні інформації як зброї, засіб впливу на власних громадян, активного захисту та боротьби з зовнішніми інформаційними впливами. Характерною є цензура межені Інтернет. Для функціонування закордонним компаніям необхідно отримати дозвіл для доступу до інформаційного простору. Існування значних обмежень в сфері свободи інформації.

Джерело: Розроблено автором на основі даних [35-38]

В сучасних умовах Україна може поєднати елементи забезпечення інформаційної безпеки, що використовуються в принципово різних країнах. Наприклад, варто розробляти власні інформаційні технології, захищати інформаційні ресурси та людський потенціал в сфері інформаційної безпеки. Аналізуючи досвід Китаю, необхідним є використання інформації для захисту наших громадян від негативного інформаційного впливу зі сторони Російської Федерації.

Підсумовуючи перший розділ, можна стверджувати, що в Україні наявний плюралізм думок, щодо теоретичного осмислення інформаційної безпеки. Вітчизняне законодавство про державну політику забезпечення інформаційної безпеки є достатньо розвинутим, але сегментованим. Наявний базовий програмний документ – Доктрина інформаційної безпеки України [31]. В сучасному світі наявні різноманітні погляди щодо забезпечення інформаційної безпеки, яскравими представниками є Сполучені Штати Америки та Китайська Народна Республіка. Для подальшого розвитку вітчизняної системи забезпечення інформаційної безпеки у сучасних умовах є доцільним використання сильних сторін обох країн, оскільки, попри використання діаметрально протилежних підходів, вони є дієвими.

РОЗДІЛ 2
РЕАЛІЗАЦІЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Аналіз реалізації державної політики інформаційної безпеки України

Аналіз реалізації державної політики забезпечення інформаційної безпеки України варто проводити через призму заходів, спрямованих на захист національних інтересів України в інформаційній сфері. Відповідні інтереси зазначені в Доктрині інформаційної безпеки України.

Почнемо з інтересів на рівні особи. Аналізуючи ситуацію в країні, можна зробити висновок, що перші два інтереси, що стосуються забезпечення конституційних прав і свобод людини на інформацію та захист приватного життя, захищаються в достатньому обсязі, оскільки існує законодавча база з цього питання, зокрема розглянуті у минулому розділі нормативно-правові акти. Держава регламентує умови, за яких можуть порушуватися ці життєво важливі інтереси. Так стаття 8 Європейська конвенція з прав людини, що була ратифікована Україною 17-го липня 1997-го року, встановлює, що держава може втручатися в здійснення права людини на повагу до приватного життя у випадку, якщо втручання здійснюється згідно із законом і є необхідним в інтересах національної чи громадської безпеки [39, 40]. Законом України «Про інформацію» визначаються конкретні підстави для цього. Стаття 28 встановлює недопустимість використання інформації в цілях закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини [3]. Останнім ж життєво важливих інтересів особи в України є захищеність від руйнівних інформаційно-психологічних впливів. В контексті гібридної агресії Російської Федерації проти України забезпечення реалізації даного інтересу нерозривно пов’язане з реалізацією життєво важливих інтересів на рівні суспільства і держави [31].

На рівні суспільства і держави виділяють такі життєво важливі інтереси, що пов’язані з захистом особи від вищезгаданих впливів, а саме захист українського населення від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації, та захист населення від інформаційного впливу Російської Федерації, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України. Задля забезпечення реалізації цих інтересів в Україні приймаються відповідні рішення [31]. Заходи щодо запобігання деструктивних інформаційно-психологічних впливів з боку Російської Федерації на українське суспільство представлені у додатку Б.

Важливими складовими стали заборона на розповсюдження та показ російських серіалів та фільмів з боку Національної ради України з питань телебачення і радіомовлення. Нормативною базою став Закон України «Про внесення змін до деяких законів України щодо захисту інформаційного телерадіопростору України». Так, наприклад, заборонене розповсюдження на території України фільмів та серіалів, що популяризують органи держави-агресора, радянські органи державної безпеки, участь в яких приймають фізичні особи, що включені до Переліку осіб, які створюють загрозу національній безпеці, або в яких наявні матеріли, що створюють інформаційно-психологічний вплив, що загрожує національній безпеці України [41-43]. Наступним заходом в цьому напрямку стало блокування російських сайтів та соціальних мереж, які можуть використовуватися та використовуються в якості інформаційної зброї. Наприклад, причиною блокування російських соціальних мереж «ВКонтакті» та «Одноклассники», а також низки інших інформаційних ресурсів, включаючи сайт сервіси «Mail.ru» та «Yandex» стало розповсюдження в останніх пропагандистських матеріалів та використання їх російськими спеціальними службами. Заборона відбулась 15-го травня 2017-го року після підписання Петром Порошенко Указу Президента України №133/2017 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»». Виконання цього указу було покладене

на Секретаря Ради національної безпеки і оборони України. Донедавна існувала вірогідність, що ці заборони можуть бути скасовані, але 14-го травня 2020-го року був підписаний Володимиром Зеленським Указ Президента України №184/2020 «Про рішення Ради національної безпеки і оборони України від 14-го травня 2020-го року «Про застосування, скасування і внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»», що продовжив заборону на ці ресурси [44, 45]. Ще однією важливою групою заходів щодо захисту українського суспільства від негативних інформаційно-психологічних впливів Російської Федерації стала заборона Національною радою України з питань телебачення і радіомовлення російських телеканалів. Відбувається це шляхом вилучення іноземних програм з Переліку іноземних програм, зміст яких відповідає вимогам Європейської конвенції про транскордонне телебачення і законодавства України, відповідні програми вилучаються з даного списку за допомогою прийняття відповідного рішення Національної ради. Згідно офіційної інфографіки, представленої Національною радою, в Україні обмежене поширення 80 російських телеканалів. Причиною вилучення каналів є порушення законодавства України, про яке згадувалося раніше [46, 47]. На мою думку, реалізація таких життєво важливі інтереси як забезпечення вільного обігу інформації, де виключенням є випадки, що визначені законодавством, забезпечення розвитку інформаційних та комунікаційних технологій і інформаційних ресурсів нашої держави, а також створення позитивного іміджу країни в світі, донесення достовірної, оперативної та об’єктивної інформації про події в Україні до міжнародної спільноти знаходиться на задовільному рівні, оскільки в нашій державі існують різні джерела інформації, плюралізм думок та засоби масової інформації, що належать різним власникам, в тому числі і державі, та висвітлюють новини з різних точок зору, наша держава регулярно займається інформуванням наших закордонних партнерів щодо певних рішень та подій. Занепокоєння викликає ступінь реалізації життєво важливих інтересів в сфері розвитку та функціонування української мови в суспільному житті України, оскільки мова є важливою складовою національної ідентичності. Закон України «Про забезпечення функціонування української мови як державної», що був

прийнятий в минулому році, є прогресивним та створює умови для позитивних перетворень у суспільстві, але Державна програма сприяння опануванню державної мови не була затверджена Кабінетом Міністрів України на момент написання роботи, а Уповноважена із захисту державної мови була звільнена за власним бажанням 6-го травня 2020-го року. Тобто зараз в Україні створені законодавчі умови для розвитку цього напрямку, але не відбувається реалізація даного нормативно-правового акту з боку виконавчої гілки влади [48, 49].

Варто розглянути державні заходи щодо поширення національних інформаційних ресурсів на тимчасово окуповані території. В Україні діє План розвитку цифрового телебачення на територіях з особливим режимом мовлення 2019-2020. Він розроблений Комісією з питань забезпечення стабільного функціонування системи національного телебачення і радіомовлення. Планом передбачена розбудова національної мережі цифрового телебачення в Донецькій, Луганській та Херсонській областях. Динаміка охоплення населення сигналом вітчизняного телебачення у даних областях вказана у таблицях 2.1, 2.2, 2.3.

Таблиця 2.1

Динаміка охоплення населення українським телебаченням в Донецькій області, осіб

	2014 рік	2017 рік	2019 рік	Охоплення, осіб
Волноваха	-	140 097	219 661	+ 79 564
Гірник	-	-	411 142	+ 411 142
Краматорськ	-	551 090	897 593	+ 346 503
Маріуполь	561 591	561 591	561 591	Покращення якості сигналу, збільшення кількості програм.

Джерело: [50]

Динаміка, відображена у таблиці, свідчить про рівномірний зростання охоплення населення у вежею у Волновасі та Краматорську, проривною є створення телевежі у Гірнику, що викликало стрімке зростання даного показнику. Розвиток телемережі у Маріуполі спрямований на якісне, а не на кількісне зростання.

Таблиця 2.2

Динаміка охоплення населення українським телебаченням в Луганській області, осіб

	2014 рік	2017 рік	2019 рік	Охоплення,осіб
Бахмутівка	-	138 922	138 922	Покращення якості сигналу, збільшення території поширення
Комишуваха	76 228	-	924 696	+ 924 696
Підгорівка	137 240	137 240	137 240	Покращення якості сигналу, збільшення території поширення
Широкий	-	-	480 549	+ 480 549

Джерело: [50]

Луганська області відрізняється нерівномірним розвитком охоплення населення, відбувається якісний розвиток вежі в Бахмутівці та Підгорівці, значним проривом стало встановлення вежі в Широкому та Комишувасі.

Таблиця 2.3

Динаміка охоплення населення українським телебаченням в Херсонській області

	2014 рік	2017 рік	2019 рік	Охоплення, осіб
Скадовськ	-	-	47 061	+ 162 256
Чаплинка	34 766	34 766	116 307	
Чонгар	-	170 340	203 994	
Новотроїцьке	35 083	35 083	35 083	
Геніченськ	58 624	58 624	58 624	

Джерело: [50]

Незважаючи на помірні темпи розвитку охоплення населення в Херсонській області, ключовою є встановлення вежі в Чонгарі, оскільки вона охоплює частину території окупованої АРК, що дозволяє українським громадянам в окупованому Криму отримати доступ до українських медіа.

Якщо підсумовувати аналіз реалізації державної політики інформаційної безпеки України, то можна зробити висновок, що наразі в більшості напрямів виконується великий обсяг роботи, є позитивні тенденції та зрушення, що були зроблені вимушено під дією зовнішніх негативних чинників, але існують і проблемні питання, над якими необхідно працювати та їх вирішувати. Тому

необхідно розглянути існуючі загрози та надати практичні рекомендації щодо їх усунення та вдосконалення інформаційної безпеки в Україні.

2.2. Розробка практичних рекомендацій щодо усунення існуючих загроз та вдосконалення інформаційної безпеки в Україні

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

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

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

Існуючі загрози інформаційній безпеці України визначені Доктриною інформаційної безпеки України [31]. Всі, виявлені у ході дослідження практичні рекомендації щодо усунення існуючих загроз та вдосконалення інформаційної безпеки України, представлені у таблиці 2.4.

Таблиця 2. 4

Практичні рекомендації щодо усунення існуючих загроз та вдосконалення інформаційної безпеки України

Загроза інформаційній безпеці України	Шляхи усунення загрози
1) Здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні.	Поширення достовірної інформації через прес-служби органів державної влади, державні медіа та популяризацію офіційної позиції України в недержавних медіа. Для нейтралізації цілеспрямованих дистабілізаційних впливів через мережу Інтернет можна залучати відповідні підрозділи Служби Безпеки України та Департамент Кіберполіції Національної Поліції України. Запобігти деморалізації особового складу військових можна завдяки підвищенню військових стандартів та рівня оплати військовослужбовців.
2) Проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі.	Співпраця Президента України та Міністерства закордонних справ України з нашими міжнародними партнерами та відстоюванні наших позицій у міжнародних організаціях, наприклад, в ООН та Раді Європи. Важливим є створення іншомовних українських засобів масової інформації, які б надали змогу іноземцям дізнаватися про новини в Україні доступною їм мовою, це б дозволило боротися з агресором закордоном в інформаційному плані.

Продовження таблиці 2.4

3) Інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах.	Блокування російських телеканалів, введення санкцій щодо юридичних осіб, зокрема російських соціальних мереж, та заборони російських серіалів та фільмів. Вдосконалення механізму позбавлення ліцензії на мовлення шляхом призупинення дії ліцензії на час судової справи або надання Національній Раді України з питань телебачення і радіомовлення права позбавляти ліцензії за наявності абсолютної більшості голосів складу ради, але залишати за засобами масової інформації право на апеляцію рішення в суді. Це дозволить припинити розповсюдження інформації, що створює загрозу інформаційній безпеці, але збереже за ЗМІ право на відстоювання власних інтересів у суді. Також варто внести зміну до антимонопольного законодавства щодо концентрації засобів масової інформації в одного власника, щоб уникнути монополізації інформаційного простору одним власником або групою власників.
4) Інформаційне домінування держави-агресора на тимчасово окупованих територіях.	Створення засобів масової інформації, перш за все, телеканалів та радіостанцій, які б були спрямовані на жителів територій, які на даний момент є непідконтрольними. Державна служба спеціального зв'язку та захисту інформації повинна забезпечити технічну реалізацію цього питання.
5) Недостатня розвиненість національної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України.	Збільшення видатків державного бюджету на Національну суспільну телерадіокомпанію України з метою збільшення частки, яку займають державні засоби масової інформації в загальному інформаційному просторі. Також важливим є збільшення фінансування Державної служби спеціального зв'язку та захисту інформації, яка повинна покращити технічний стан вітчизняної інформаційної інфраструктури. Департамент кіберполіції Національної поліції повинен слідкувати за діяльністю країни-агресора в мережі Інтернет.
6) Неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства.	Уніфікація законодавства щодо забезпечення інформаційної безпеки України. Розробка Закону України «Про інформаційну безпеку». Пропонується Міністерству освіти і науки розробити курс медіа-грамотності для школярів.
7) Поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.	Вирішення даної проблеми покладається на Службу Безпеки України. Органам місцевого самоврядування та центральній владі необхідно на прикладах демонструвати переваги місцевого самоврядування як сучасної української моделі народовладдя на місцевому рівні.

Продовження таблиці 2.4

8) Відсутність комплексного інструменту ідентифікації, аналізу та нейтралізації загроз інформаційної безпеки України.	Створення координаційного органу або системи внутрішньої комунікації, яка б надала можливість швидко налагодити взаємодію всіх владних інституцій, які залучені до процесу формування та реалізації державної політики забезпечення інформаційної безпеки в Україні. Розробку подібної системи можна покласти на Міністерство цифрової трансформації та на Державну службу спеціального зв'язку, створення координаційного органу в компетенції Верховної Ради України, яка створить законодавчу основу для створення та функціонування подібного органу.

Джерело: Розроблено автором на основі даних [31]

Незважаючи на те, що на сьогодні науковцями виділяється дві складових забезпечення інформаційної безпеки – активна і пасивна (розвиток і захист), у переважній більшості, система працює на протидію загрозам, тобто на пасивну складову. Проте, аналіз практики країн ЄС свідчить про те, що інформаційна безпека повинна бути побудована на моделі стратегічного мислення: вжиття заходів для захисту цілей, їх утримання й забезпечення безпеки на основі принципів демократії, прав людини, захищеного Інтернету.

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

Державна політики забезпечення інформаційної безпеки не є ідеальною та все ще знаходиться на етапі становлення, в деяких аспектах є досить ефективною, іноді є суперечливою або неефективною, але для подолання такого важкого етапу в історії нашої держави необхідно вчитися на власних помилках та приймати рішення, які б допомогли нам впоратися з усіма загрозами, що нависають над нашої країною в інформаційній складовій національної безпеки.

ВИСНОВКИ

За результатами роботи можна зробити наступні висновки:

1) Важливість державної політики забезпечення інформаційної безпеки важко переоцінити, оскільки її вплив знаходить своє відображення як на побутовому, так і на загальнодержавному рівні. Інформаційну безпеку можна охарактеризувати як складову національної безпеки та захищеність державної інформаційної політики від зовнішніх та внутрішніх впливів. Бурхливий розвиток політики інформаційної безпеки в нашій країні пов'язаний, перш за все, з гібридною війною Російської Федерації проти нашої держави. Це спонукало визначити теоретичні аспекти державної політики забезпечення інформаційної безпеки, розглянути різні погляди вітчизняних науковців-теоретиків.

2) Був досліджений досвід зарубіжних країн, а саме Сполучених Штатів Америки та Китайської Народної Республіки. Враховуючи контекст сучасності, українську політику забезпечення інформаційної безпеки можна охарактеризувати як поєднання американського та китайського прикладів, де перетинається політика забезпечення свободи інформації, поширення мережі Інтернет, плюралізму думок та використання санаційного механізму.

3) Проведений аналіз вітчизняного законодавчого забезпечення інформаційної безпеки та практичні заходи державної політики щодо її реалізації. Українське законодавство в сфері інформаційної безпеки є сегментованим, базовим програмним документом є Доктрина забезпечення інформаційної безпеки. До джерел деструктивних впливів активно використовується санкційний механізм, насамперед заборона російського кіно та серіалів, заборона російських веб-сайтів, соціальних мереж, а також блокування каналів, що можуть транслювати матеріали, що порушують вітчизняне законодавство. Так, можливо подібні заходи в якомусь сенсі порушують свободу слова, але їй не можна зловживати, особливо коли від цього залежить суверенітет та незалежність країни. Держава застосує наявний матеріально-технічний інструментарій для надання українським громадянам, що проживають в ОРДЛО та окупованій АРК, можливості отримувати інформацію з

українських джерел. Для цього будуються вежі телезв'язку в населених пунктах поряд з лінією розмежування.

4) Були запропоновані конкретні заходи щодо нейтралізації існуючих загроз інформаційної безпеки України, а також надані практичні рекомендації по вдосконаленню нормативно-правового забезпечення та проведенню заходів щодо реалізації державної політики інформаційної безпеки.

Українська політика в досліджуваному напрямі не є ідеальною та все ще знаходиться на етапі становлення, в деяких аспектах є досить ефективною, іноді є суперечливою або неефективною, але для подолання такого важкого етапу в історії нашої держави необхідно вчитися на власних помилках та приймати рішення, які б допомогли нам впоратися з усіма загрозами, що нависають над нашої країною в інформаційній складовій національної безпеки. Врешті решт, за нами правда.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки: закон України № 537-V: за станом на 03.08.2009 р. // Відом. Верхов. Ради України, 2007, № 12 (23.03.2007), ст. 102.

2. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР//Відом. Верхов. Ради України. – 1996р. - №30

3. Про інформацію: Закон України від 02.10.1992 № 2657-XII//Відом. Верхов. Ради України. – 1992р. - №48

4. Іванченко Ю.М. Сутність, головні напрями та способи державної інформаційної політики в Україні / Ю.М. Іванченко // Державне управління: теорія та практика. – 2005. – № 2 [Електронний ресурс]. – Режим доступу : http://academy.gov.ua/ej/ej2/txts/philo/05ijmipu.pdf

5. Пожуєв В.І. Формування державної інформаційної політики в умовах глобалізації / В.І. Пожуєв // Гуманітарний вісник Запорізької державної інженерної академії. – 2010. – Вип. 43. – С. 4–12.

6. Нестеряк Ю.В. Нормативно-правові основи державної інформаційної політики України в умовах розвитку інформаційного суспільства / Ю.В. Нестеряк // Теорія та практика державного управління. – 2012. – Вип. 4(39). – С. 111–119.

7. Мельник М. Сутність поняття «державна політика розвитку інформаційного суспільства»: узагальнення європейських та вітчизняних трактувань / М. Мельник // Науковий вісник «Демократичне врядування». – 2012. – Вип. 9 [Електронний ресурс]. – Режим доступу: http://www.lvivacademy.com/vidavnitstvo_1/visnik9/fail/Melnyk.pdf

8. Березовська І.Р. Державна інформаційна політика України та основні напрями її вдосконалення / І.Р. Березовська, Д.М. Русак // Міжнародні відносини. Серія «Економічні науки». – 2014. – № 4. [Електронний ресурс]. – Режим доступу : http://journals.iir.kiev.ua/index.php/ec_n/issue/view/132

9. Токар О. Державна інформаційна політика: проблеми визначення концепту / О. Токар // Політичний менеджер. – 2009. – № 5. – С.131–141

10. Іванов В. Законодавство і журналістика. Становлення правової бази в Україні та світовий досвід. - К.: Школяр, 1998. - 80 с.

11. Москаленко А., Губерський Л., Іванов В. Основи масово-інформаційної діяльності. - К., 1999. -С. 271.

12. Почепцов Г.Г., Чукут С.А. Інформаційна політика: Навч. посіб. - К.: Вид-во УАДУ, 2002. - Ч. 1. -88 с.

13. Литвиненко О. Інформаційні технології та Україна у світовому контексті // Людина і політика. -2001. - № 1.

14. Інформаційна політика: Навч. посіб. для студентів ВНЗ, аспірантів, викладачів. — 2-ге вид., стер. / Почепцов Г.Г., Чукут С.А. — К., 2008. — 663 с.

15. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія / А.Ю. Нашинець-Наумова. – Київ: Видавничий дім «Гельветика», 2017. – 168 с.

16. Боднар І. Р. Сучасні реалії інформаційного суспільства: проблеми становлення та перспективи розвитку: монографія [Текст] / І. Р. Боднар. – Львів: Видавництво Львівської комерційної академії, 2013. – 320 с.

17. Євдоченко Л. Шляхи та методи державного забезпечення інформаційної безпеки України: теоретичний аспект / Л. Євдоченко // Науковий вісник «Демократичне врядування». – 2010. – Вип. 5 [Електронний ресурс]. – Режим доступу: http://lvivacademy.com/vidavnitstvo_1/visnik5/fail/+Jevdoch.pdf

18. Концепція інформаційної безпеки України [Електронний ресурс]. – Режим доступу: http://mip.gov.ua/files/banners/Final%20%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82%20%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D1%96%D1%97%20(%D0%A2%D0%B5%D0%BA%D1%81%D1%82)%20-%2030.09.15.pdf

19. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII//Відом. Верхов. Ради України. – 1994р. -№16

20. Особливості проблем законодавчого забезпечення інформаційної безпеки держави, суспільства і громадянина в умовах інформаційно-психологічного

протиборства / А.М. Кузьменко // Часопис Київського університету права. — 2010. — № 4. — С. 317-321. — Бібліогр.: 12 назв. — укр.

21. Про схвалення Концепції реформування місцевого самоврядування та територіальної організації влади в Україні: Розпорядження Кабінету Міністрів України; Концепція від 01.04.2014 № 333-р

22. Олійник О.В. Адміністративно-правові засоби забезпечення інформаційної безпеки / О. В. Олійник // Юридичний вісник. Повітряне і космічне право. - 2015. - № 1. - С. 65-69.

23. Деякі питання діяльності Міністерства культури та інформаційної політики: Постанова Кабінету Міністрів України від 16.10.2019 № 885 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/885-2019-%D0%BF

24. Про перелік, кількісний склад і предмети відання комітетів Верховної Ради України дев'ятого скликання: Постанова Верховної Ради України від 29.08.2019 № 19-IX//Відом. Верхов. Ради України. – 2019р. -№35

25. Про Кабінет Міністрів України: Закон України від від 27.02.2014 № 794-VII//Відом. Верхов. Ради України. – 1992р. -№27

26. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16.11.1992 № 2782-XII//Відом. Верхов. Ради України. – 1993р. -№1

27. Про телебачення і радіомовлення: Закон України від 21.12.1993 № 3759-XII//Відом. Верхов. Ради України. – 1994р. -№10

28. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII//Відом. Верхов. Ради України. – 2018р. -№31

29. Про Службу безпеки України: Закон України від 25.03.1992 № 2229-XII//Відом. Верхов. Ради України. – 1992р. -№27

30. Про Державну службу спеціального зв’язку та захисту інформації України: Закон України від 23.02.2006 № 3475-IV//Відом. Верхов. Ради України. – 2006р. -№30

31. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України; Доктрина від 25.02.2017 № 47/2017

32. The National Security Act of 1947 – July 26, 1947 Public Law 253, 80th Congress; Chapter 343, 1st Session; S. 758. [Електронний ресурс]. – Режим доступу: https://www.cia.gov/library/readingroom/docs/1947-07-26.pdf

33. Central Intelligence Agency [Електронний ресурс]. – Режим доступу: https://www.cia.gov/index.html

34. The National Strategy to Secure Cyberspace – February 2003 [Електронний ресурс]. – Режим доступу: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

35. National Cyber Strategy of the United States of America – September 2018 [Електронний ресурс]. – Режим доступу: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

36. Захаренко К.В. До питання про розвиток національної системи інформаційної безпеки: досвід сусідів / К. В. Захаренко // Науковий вісник. Серія «Філософія». – Харків: ХНПУ, 2018. – Вип.50 – С. 176-189

37. The National People's Congress of the People's Republic of China [Електронний ресурс]. – Режим доступу: http://www.npc.gov.cn/npc/index.shtml

38. China Cybersecurity Review Technology and Certification Center [Електронний ресурс]. – Режим доступу: http://www.isccc.gov.cn/index.shtml

39. European Convention on Human Rights [Електронний ресурс]. – Режим доступу: https://www.echr.coe.int/Pages/home.aspx?p=basictexts

40. Про ратифікація Конвенції про захист прав людини і основоположних свобод 1950 року, Першого протоколу та протоколів N 2, 4, 7 та 11 до Конвенції: Закон України від 17.07.1997 № 475/97-ВР//Відом. Верхов. Ради України. – 1997р. -№40

41. Про внесення змін до деяких законів України щодо захисту інформації телерадіопростору України: Закон України від 05.02.2015 № 159-VIII//Відом. Верхов. Ради України. – 2015р. -№18

42. Національна рада України з питань телебачення і радіомовлення [Електронний ресурс]. – Режим доступу: https://www.nrada.gov.ua/

43. Перелік осіб, які створюють загрозу нацбезпеці – 19/03/2020 [Електронний ресурс]. – Режим доступу: http://mkms.gov.ua/content/perelik-osib-yaki-stvoryuyut-zagrozu-nacbezpeci.html

44. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: Указ Президента України №133/2017 від 15.05.2017 [Електронний ресурс]. – Режим доступу: https://www.president.gov.ua/documents/1332017-21850

45. Про рішення Ради національної безпеки і оборони України від 14-го травня 2020-го року «Про застосування, скасування і внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: Указ Президента України №184/2020 від 14.05.2020 [Електронний ресурс]. – Режим доступу: https://www.president.gov.ua/documents/1842020-33629

46. Перелік іноземних програм, зміст яких відповідає вимогам Європейської конвенції про транскордонне телебачення і законодавства України [Електронний ресурс]. – Режим доступу: https://www.nrada.gov.ua/dlya-zarubizhnyh-movnykiv/

47. Російські телеканали, розповсюдження яких обмежено на території України у 2014-2017 рр. [Електронний ресурс]. – Режим доступу: https://www.nrada.gov.ua/infographics/rosijski-telekanaly-rozpovsyudzhennya-yakyh-obmezheno-na-terytoriyi-ukrayiny-u-2014-2017-rr/

48. Про забезпечення функціонування української мови як державної: Закон України від від 25.04.2019 № 2704-VIII//Відом. Верхов. Ради України. – 2019р. -№21

49. Про звільнення Монахової Т.В. з посади Уповноваженого із захисту державної мови: Розпорядження Кабінету Міністрів України від 06.05.2020 № 491-р [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/491-2020-%D1%80

50. План розвитку цифрового телебачення на територіях з особливим режимом мовлення 2019-2020 [Електронний ресурс]. – Режим доступу: https://www.nrada.gov.ua/wp-content/uploads/2019/09/Plan-rozvytku-tsyfrovogo-telebachennya_2019-2020.pdf

ДОДАТКИ

Додаток А

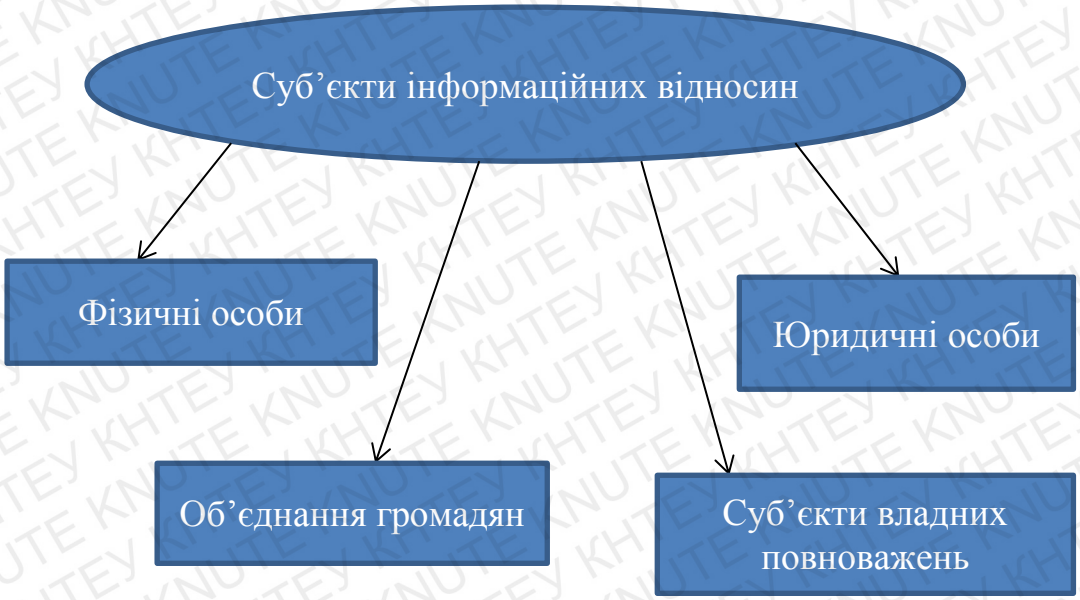


Рис. А.1 Суб'єкти інформаційних відносин

Джерело: Розроблено автором на основі даних [3]

Додаток Б

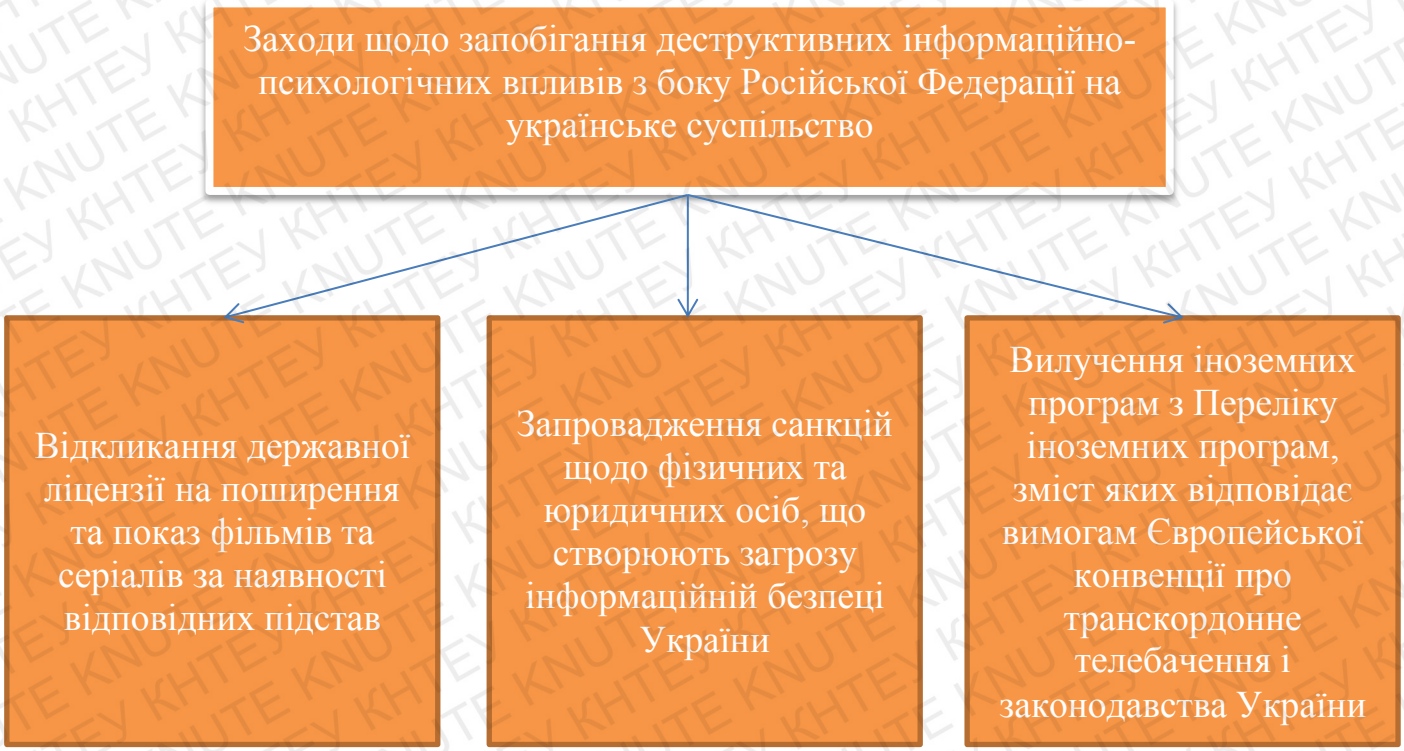


Рис. Б.1 Заходи щодо запобігання деструктивних інформаційно-психологічних впливів з боку Російської Федерації на українське суспільство

Джерело: Розроблено автором на основі даних [41-46]

Київський національний торговельно-економічний університет
Кафедра публічного управління та адміністрування

РЕФЕРАТ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на тему:

ДЕРЖАВНА ПОЛІТИКА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Студента 4 курсу, 12 групи,
спеціальності 074 «Публічне управління та адміністрування»
спеціалізації «Публічне управління та адміністрування» Шилов Максим Андрійович
(підпис студента)

Науковий керівник
доктор економічних наук,
доцент Ладонько Людмила Степанівна
(підпис керівника)

Гарант освітньої програми
кандидат економічних наук,
доцент Головня Юлія Ігорівна
(підпис гаранта)

Київ 2020

Випускна кваліфікаційна робота складається зі вступу, двох розділів, висновків, списку використаних джерел (50 найменувань), двох додатків. Основний зміст роботи викладено на 40 сторінках комп'ютерного тексту. Робота містить 4 рисунки, 6 таблиць.

Метою роботи є дослідженні теоретичних і практичних засад та розробці практичних рекомендацій щодо вдосконалення державної політики у сфері інформаційної безпеки в Україні.

Досягнення мети роботи передбачало вирішення наступних завдань:

1) визначити теоретичні аспекти державної політики забезпечення інформаційної безпеки;

2) дослідити досвід іноземних держав щодо забезпечення інформаційної безпеки;

3) провести аналіз вітчизняного законодавчого забезпечення інформаційної безпеки та практичних заходів державної політики щодо її реалізації;

4) визначити існуючі загрози інформаційної безпеки України та практичні рекомендації щодо їх усунення.

Об'єктом дослідження є процес реалізації державного управління у сфері забезпечення інформаційної безпеки України, діяльність органів державної влади щодо забезпечення інформаційної безпеки.

Предметом дослідження є теоретико-методологічні підходи та практичний інструментарій здійснення державної політики у сфері інформаційної безпеки в Україні.

Для теоретичного осмислення різних аспектів проблеми застосовуються аналіз і синтез (можливості адаптації світових зразків в Україні із організації інформаційної безпеки держави та її забезпечення, дослідження стану вітчизняної теоретико-методологічної бази інформаційної безпеки), абстрагування й узагальнення (визначення шляхів удосконалення організаційно-правового забезпечення державної політики у сфері інформаційної безпеки України, порівняння й уточнення новітніх функціоналів системи державного управління нею), дедукція та індукція (розклад об'єкту дослідження на складові та оцінка його

стану) та графічний метод (використання схем та таблиць).

У першому розділі представлена теоретична та нормативно-правова основа державної політики забезпечення інформаційної безпеки в Україні. Розглянуті наявні механізми забезпечення інформаційної безпеки. Досліджений досвід зарубіжних країн, а саме Сполучених Штатів Америки та Китайської Народної Республіки.

У другому розділі здійснюється аналіз реалізації державної політики інформаційної безпеки в Україні та викладено практичні рекомендації щодо усунення існуючих загроз та вдосконалення інформаційної безпеки в Україні.

Одержані результати можуть бути використані при удосконаленні нормативно-правової основи державної політики забезпечення інформаційної безпеки в Україні та практичних заходів щодо її забезпечення.

Анотація

У випускній кваліфікаційній роботі висвітлені теоретичні аспекти та нормативно-правова основа інформаційної безпеки в Україні, закордонний досвід інформаційної безпеки в провідних країнах світу, проаналізована реалізація інформаційної безпеки в Україні та існуючі загрози, викладено практичні рекомендації щодо вдосконалення нормативно-правової бази інформаційної безпеки в Україні та нейтралізації існуючих загроз.

Ключові слова: інформаційна безпека, національна безпека, інформаційна політика, національні інтереси, інформація.

Annotation

The graduation work covers theoretical aspects and the legal and regulatory basis of information security in Ukraine, the foreign experience of information security in the leading world countries, analyzes the implementation of information security in Ukraine and actual threats, provides practical recommendations for the improvement of the legal and regulatory basis of information security in Ukraine and neutralization of actual threats.

Keywords: information security, national security, information policy, national interests, information.

Рецензія

на випускну кваліфікаційну роботу студента
Шилова Максима Андрійовича
тема роботи «Державна політика забезпечення інформаційної безпеки в Україні»

В наш час забезпечення інформаційної безпеки є однією з головних складових політики кожної держави в сфері національної безпеки. Неефективна політика забезпечення інформаційної безпеки знаходить своє відображення в усіх сферах життя країни. Інформаційна галузь є однією із складових національних інтересів сучасних держав, а отже заслуговує особливої уваги. Розробка даного проекту є актуальною в контексті подій, що відбуваються в нашій державі.

Метою роботи є дослідженні теоретичних і практичних засад та розробці практичних рекомендацій щодо вдосконалення державної політики у сфері інформаційної безпеки в Україні.

В випускній кваліфікаційній роботі визначено теоретичні аспекти державної політики забезпечення інформаційної безпеки, досліджено досвід забезпечення інформаційної безпеки іноземних держав, проведено аналіз вітчизняного законодавчого забезпечення інформаційної безпеки та практичних заходів державної політики щодо її реалізації, визначені існуючі загрози інформаційної безпеки України та практичні рекомендації щодо їх усунення.

Робота складається із вступу, двох розділів, висновків, списку використаних джерел та додатків.

Завдання визначені метою дослідження були виконані в повному обсязі. Зміст роботи та її виконання свідчать про високий рівень підготовки бакалавра. Загалом робота виконана відповідно до методичних рекомендацій. Робота заслуговує на високу позитивну оцінку, рекомендована до захисту, а її автор, Шилов Максим Андрійович, на присвоєння ступеня бакалавра зі спеціальності 281 «Публічне управління та адміністрування».

Начальник Головного управління
державної казначейської служби
України у Чернігівській області А.ЛІТОШ

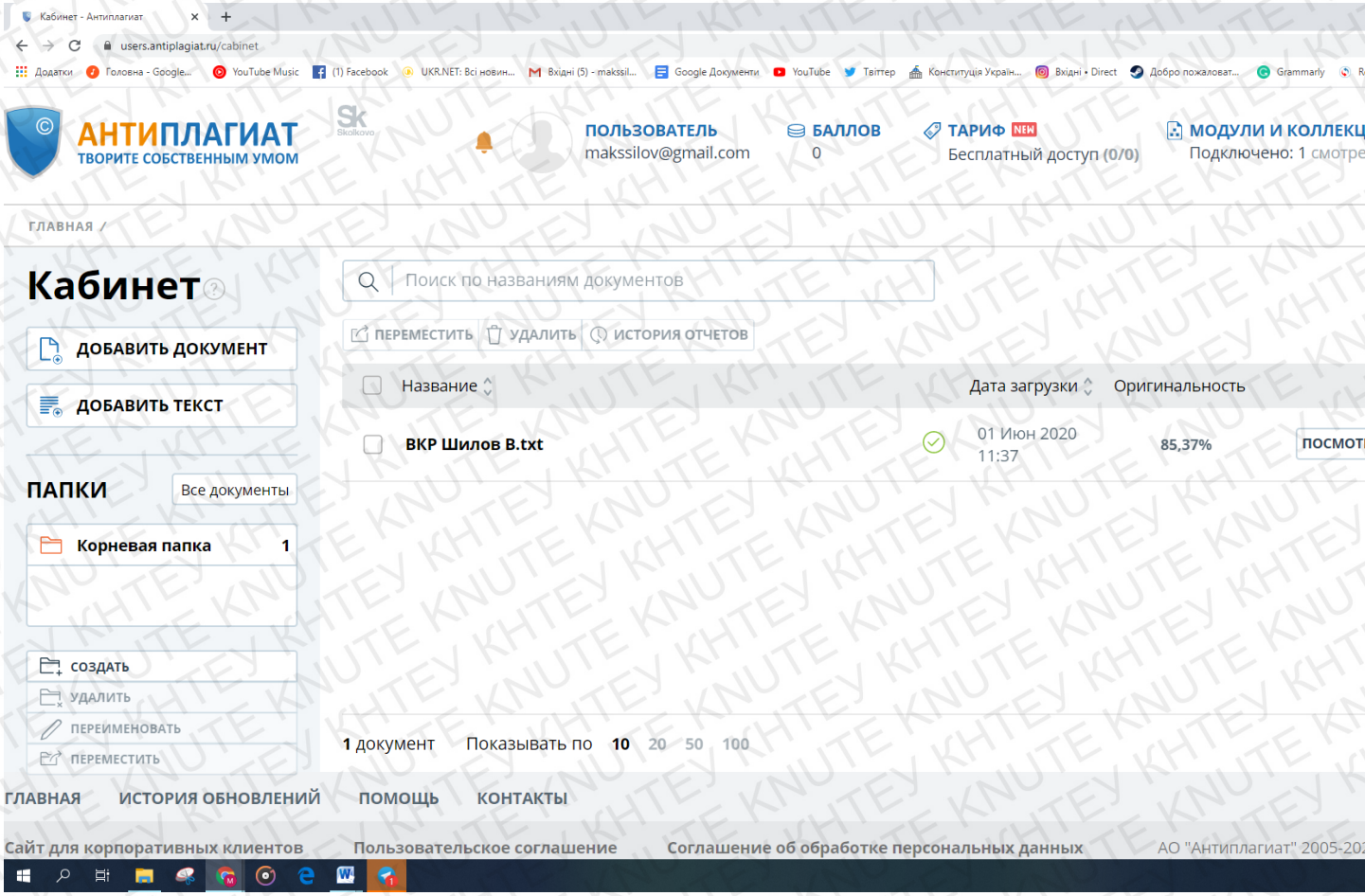
Завідувачу кафедри публічного
управління та адміністрування
Новіковій Н.Л.

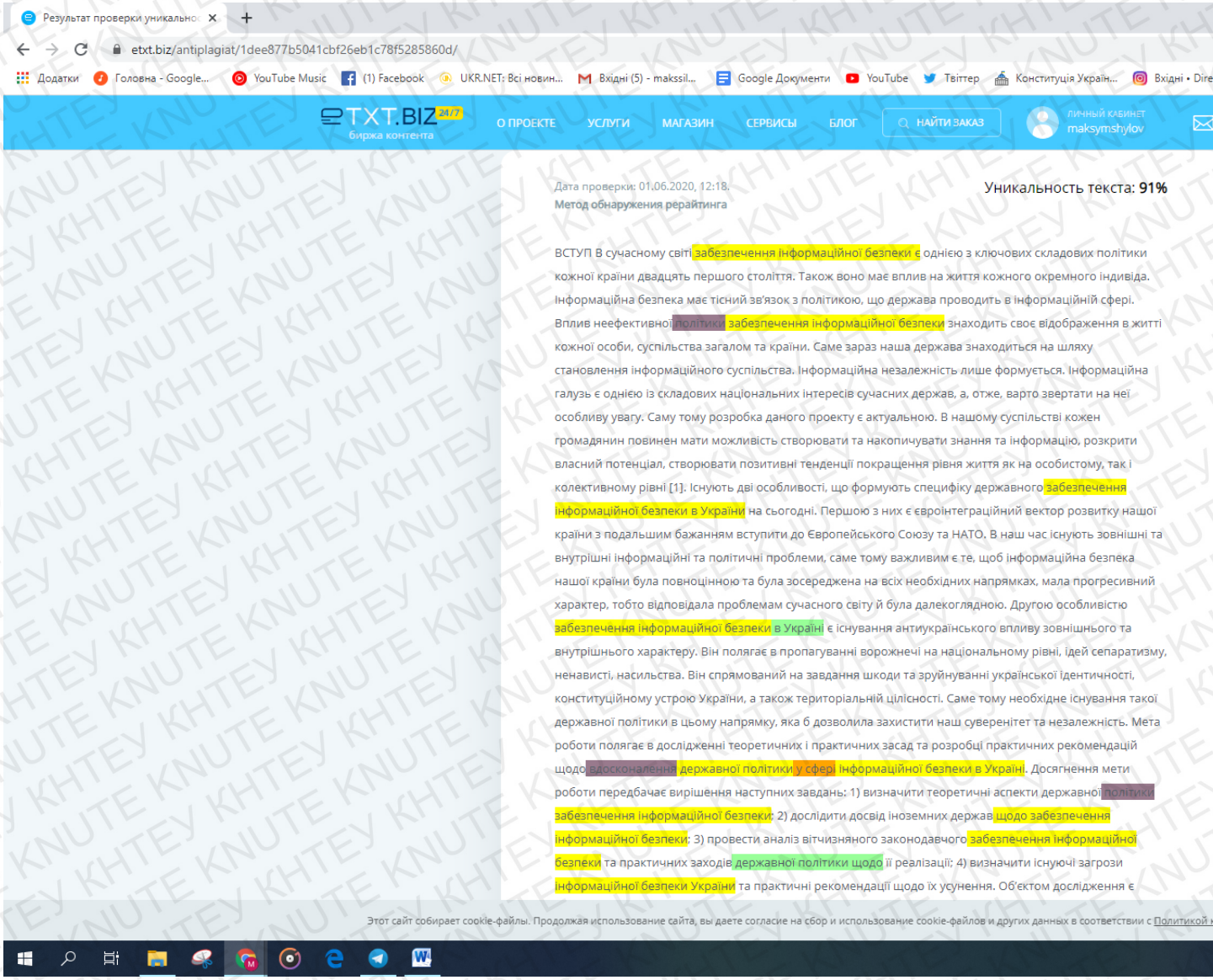
Заява

Я, Шилов Максим Андрійович (ПІБ), повідомляю, що за результатами проведення самостійної перевірки з використанням програмно-технічних засобів у наданій випускній кваліфікаційній роботі на тему: «Державна політика забезпечення інформаційної безпеки в Україні» не міститься елементів академічного плагіату. У випадках використання прямих запозичень з друкованих та електронних джерел, вказані відповідні посилання.

Робота для перевірки надається у друкованому та електронному варіантах. Електронна версія моєї роботи ідентична з друкованою.

«1» червня 2020 року _____ (підпис)


Кабинет - Антиплагиат
users.antiplagiat.ru/cabinet
АНТИПЛАГИАТ
ТВОРИТЕ СОБСТВЕННЫМ УМОМ
ПОЛЬЗОВАТЕЛЬ
maksslov@gmail.com
БАЛЛОВ
0
ТАРИФ NEW
Бесплатный доступ (0/0)
МОДУЛИ И КОЛЛЕКЦ
Подключено: 1 смотре
ГЛАВНАЯ /
Кабинет
ДОБАВИТЬ ДОКУМЕНТ
ДОБАВИТЬ ТЕКСТ
ПАПКИ
Все документы
Корневая папка 1
СОЗДАТЬ
УДАЛИТЬ
ПЕРЕИМЕНОВАТЬ
ПЕРЕМЕСТИТЬ
Поиск по названиям документов
ПЕРЕМЕСТИТЬ
УДАЛИТЬ
ИСТОРИЯ ОТЧЕТОВ
Название
Дата загрузки
Оригинальность
ВКР Шилов В.txt
01 Июн 2020 11:37
85,37%
ПОСМОТ
1 документ
Показывать по 10 20 50 100
ГЛАВНАЯ
ИСТОРИЯ ОБНОВЛЕНИЙ
ПОМОЩЬ
КОНТАКТЫ
Сайт для корпоративных клиентов
Пользовательское соглашение
Соглашение об обработке персональных данных
АО "Антиплагиат" 2005-202


Результат проверки уникальнос
etxt.biz/antiplagiat/1dee877b5041cbf26eb1c78f5285860d/
Додатки
Головна - Google...
YouTube Music
(1) Facebook
UKR.NET: Всі новин...
Вхідні (5) - maksil...
Google Документи
YouTube
Твіттер
Конституція Україн...
Вхідні • Dire
TXT.BIZ 24/7
биржа контента
О ПРОЕКТЕ
УСЛУГИ
МАГАЗИН
СЕРВИСЫ
БЛОГ
НАЙТИ ЗАКАЗ
ЛИЧНЫЙ КАБИНЕТ
maksymshylov
Дата проверки: 01.06.2020, 12:18.
Метод обнаружения рерайтинга
Уникальность текста: 91%
ВСТУП В сучасному світі забезпечення інформаційної безпеки є однією з ключових складових політики кожної країни двадцять першого століття. Також воно має вплив на життя кожного окремого індивіда. Інформаційна безпека має тісний зв'язок з політикою, що держава проводить в інформаційній сфері. Вплив неефективної політики забезпечення інформаційної безпеки знаходить своє відображення в житті кожної особи, суспільства загалом та країни. Саме зараз наша держава знаходиться на шляху становлення інформаційного суспільства. Інформаційна незалежність лише формується. Інформаційна галузь є однією із складових національних інтересів сучасних держав, а, отже, варто звертати на неї особливу увагу. Саму тому розробка даного проекту є актуальною. В нашому суспільстві кожен громадянин повинен мати можливість створювати та накопичувати знання та інформацію, розкрити власний потенціал, створювати позитивні тенденції покращення рівня життя як на особистому, так і колективному рівні [1]. Існують дві особливості, що формують специфіку державного забезпечення інформаційної безпеки в Україні на сьогодні. Першою з них є євроінтеграційний вектор розвитку нашої країни з подальшим бажанням вступити до Європейського Союзу та НАТО. В наш час існують зовнішні та внутрішні інформаційні та політичні проблеми, саме тому важливим є те, щоб інформаційна безпека нашої країни була повноцінною та була зосереджена на всіх необхідних напрямках, мала прогресивний характер, тобто відповідала проблемам сучасного світу й була далекоглядною. Другою особливістю забезпечення інформаційної безпеки в Україні є існування антиукраїнського впливу зовнішнього та внутрішнього характеру. Він полягає в пропагуванні ворожнечі на національному рівні, ідей сепаратизму, ненависті, насильства. Він спрямований на завдання шкоди та зруйнуванні української ідентичності, конституційному устрою України, а також територіальній цілісності. Саме тому необхідне існування такої державної політики в цьому напрямку, яка б дозволила захистити наш суверенітет та незалежність. Мета роботи полягає в дослідженні теоретичних і практичних засад та розробці практичних рекомендацій щодо вдосконалення державної політики у сфері інформаційної безпеки в Україні. Досягнення мети роботи передбачає вирішення наступних завдань: 1) визначити теоретичні аспекти державної політики забезпечення інформаційної безпеки; 2) дослідити досвід іноземних держав щодо забезпечення інформаційної безпеки; 3) провести аналіз вітчизняного законодавчого забезпечення інформаційної безпеки та практичних заходів державної політики щодо її реалізації; 4) визначити існуючі загрози інформаційної безпеки України та практичні рекомендації щодо їх усунення. Об'єктом дослідження є
Этот сайт собирает cookie-файлы. Продолжая использование сайта, вы даете согласие на сбор и использование cookie-файлов и других данных в соответствии с Политикой