Київський національний торговельно-економічний університет
Кафедра публічного управління та адміністрування

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Студента 5 курсу, 7 групи,
спеціальності 074 «Публічне управління та адміністрування»
спеціалізації «Публічне управління та адміністрування» Мажари Романа Володимировича

(підпис студента)

Науковий керівник
к.держ.упр. Динник Ірина Петрівна

(підпис керівника)

Гарант освітньої програми
канд. екон. наук,
доцент Головня Юлія Ігорівна

(підпис гаранта)

Київ 2022

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 _____
«11» грудня 2021 р.

Завдання
на випускну кваліфікаційну роботу (проект)
студентові

Мажарі Роману Володимировичу

---

1. Тема випускної кваліфікаційної роботи (проекту): «Державна політика у сфері інформаційної безпеки»

Затверджена наказом ректора від «08» грудня 2021 р. № 4067

2.Строк здачі студентом закінченого проекту (роботи)

24.01.2022 р.

3. Цільова установка та вихідні дані до роботи (проекту)

Метою роботи (проекту) є обґрунтування й розробка пропозицій щодо напрямів удосконалення державної політики у сфері інформаційної безпеки.

Об'єктом дослідження є суспільні відносини, які виникають у процесі державної політики у сфері інформаційної безпеки.

Предметом дослідження є теоретико-методичні та прикладні основи державної політики у сфері інформаційної безпеки.

4. Зміст випускного кваліфікаційного проекту (роботи) (перелік питань за кожним розділом) :

ВСТУП

РОЗДІЛ 1. ОЦІНЮВАННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

1.1. Сучасний стан та тенденції розвитку інформаційної безпеки в Україні

1.2. Аналіз факторів впливу на забезпечення інформаційної безпеки в Україні

Розділ 2. УДОСКОНАЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Інформаційна безпека в умовах поширення пандемії COVID-19

2.2. Напрями удосконалення державної політики у сфері інформаційної безпеки

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

ДОДАТКИ

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 10.12.2021	10.12.2021
2	Складання плану та підготовка індивідуального завдання для виконання випускної кваліфікаційної роботи	До 20.12.2021	20.12.2021
3	Представлення на рецензування науковому керівнику рукопису першого розділу випускної кваліфікаційної роботи	До 10.01.2022	10.01.2022
4	Представлення на рецензування науковому керівнику рукопису другого розділу випускної кваліфікаційної роботи	До 20.01.2022	20.01.2022
5	Представлення закінченої випускної кваліфікаційної роботи на кафедру	До 21.01.2022	21.01.2022
6	Підготовка письмового відгуку на випускну кваліфікаційну роботу	До 22.01.2022	22.01.2022
7	Зовнішнє рецензування ВКР	До 22.01.2022	22.01.2022
8	Проведення попереднього захисту випускних кваліфікаційних робіт	21-23. 01.2022	21-23. 01.2022

9	Вирішення питання про допуск випускної кваліфікаційної роботи до захисту	До 25.01.2022	До 25.01.2022
10	Направлення випускної кваліфікаційної роботи із зовнішньою рецензією у ЕК для захисту	За графіком	За графіком

6. Дата видачі завдання «11» грудня 2021р.

7. Науковий керівник випускної кваліфікаційної роботи (проекту)

Динник І.П.

(прізвище, ініціали, підпис)

8. Гарант освітньої програми

Головня Ю.І.

(прізвище, ініціали, підпис)

9. Завдання прийняв до виконання студент

Мажара Р. В.

(прізвище, ініціали, підпис)

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

Випускна кваліфікаційна робота написана на актуальну тему.

Інформаційна безпека є невід'ємною складовою у забезпеченні національної безпеки держави, а створення розвинутого та захищеного середовища – основна умова розвитку суспільства та конкурентоспроможної держави. Ефективна система заходів по забезпеченню інформаційної безпеки громадян, суспільства та держави дозволить своєчасно попереджувати та виявляти усі потенційні та реальні загрози національним інтересам і запобігати збиткам в соціально-економічній сфері.

У випускній кваліфікаційній роботі студентом розглянуто сучасний стан та тенденції розвитку інформаційної безпеки в Україні; проаналізовано фактори впливу на забезпечення інформаційної безпеки в Україні; охарактеризовано особливості інформаційної безпеки в умовах поширення пандемії COVID-19 та сформульовано пропозиції щодо напрямів удосконалення державної політики у сфері інформаційної безпеки.

Зміст випускної кваліфікаційної роботи підпорядкований поставленій у роботі меті. Проведений аналіз дозволив визначити проблемні питання у

здійсненні державної політики у сфері інформаційної безпеки. Завдання поставлені в роботі виконані в повному обсязі, що підтверджено висновками.

Випускна кваліфікаційна робота має досить логічну структуру та відповідає вимогам оформлення. Робота написана на достатньому науковому рівні, є самостійним дослідженням студента, повністю розкриває обрану тему. Вважаю, що випускна кваліфікаційна робота заслуговує позитивної оцінки, а її автор, Мажара Роман Володимирович на отримання кваліфікації бакалавра зі спеціальності 074 «Публічне управління та адміністрування».

Науковий керівник випускної кваліфікаційної роботи (проекту)
(підпис, дата)
Відмітка про попередній захист Головня Юлія Ігорівна
(ПІБ, підпис, дата)

11.Висновок про випускну кваліфікаційну роботу (проект):
Випускна кваліфікаційна робота (проект) студента Мажари Р.В.
(прізвище, ініціали)
може бути допущена до захисту екзаменаційній комісії.
Гарант освітньої програми): Головня Юлія Ігорівна
(прізвище, ініціали, підпис)
Завідувач кафедри: Новікова Наталія Леонідівна
(підпис, прізвище, ініціали)

«25» січня 2022 р.

ЗМІСТ

ВСТУП

Актуальність теми. На початку XXI ст. інформація для будь-якої цивілізованої держави є стратегічним ресурсом, ефективне використання якого забезпечує безпеку країни та перспективу формування демократичного суспільства, у якому реалізуються всі конституційні права та свободи громадян, включно з правом вільного пошуку, отримання, передачі та розповсюдження інформації усіма можливими законними способами. З розвитком різноманітних засобів інформації суспільство мимоволі підключається до глобальних інформаційних систем, стаючи при цьому суб'єктом цих систем. Соціальні умови життя населення конкретної країни у багатьох аспектах визначаються досконалістю доступних інформаційних технологій, а у політичній сфері все більшого значення набувають не силові, а інформаційні чинники. А основним є те, що через глобальну інформатизацію стався якісний стрибок в управлінні на всіх рівнях.

Актуальність обраної теми полягає також в тому, що тенденції до збільшення відкритості суспільства, масове використання інформаційно-комунікаційних технологій створили передумови для потенційних протиправних дій стосовно інформації, тих хто її використовує та інформаційних систем зв'язку, що має наслідком зниження рівня забезпечення інформаційної безпеки держави.

Питанням інформаційної безпеки України, її стану і перспективам розвитку, методологічне та теоретичне підґрунтя досліджуваної проблеми висвітлюється в наукових працях вітчизняних і зарубіжних авторів, таких як: В. Антонов, С. Бєлай, О. Власюк, В. Горбулін, О. Золотар, Д. Золотухін, Д. М. В. Циганов та інші [19; 21; 23; 26; 35; 49].

Інформаційна безпека є невід'ємною складовою у забезпеченні національної безпеки держави, а створення розвинутого та захищеного середовища – основна умова розвитку суспільства та конкурентоспроможної держави. Ефективна система заходів по забезпеченню інформаційної безпеки громадян, суспільства та держави дозволить своєчасно попереджувати та виявляти усі потенційні та

реальні загрози національним інтересам і запобігати збиткам в соціально-економічній сфері. Гостроти цій проблематиці додає також те, що інформаційна складова частина є об'єктом маніпулювання за умов гібридної війни яка ведеться Російською Федерацією проти України, адже складна політична ситуація, в якій вона Україна протягом останніх восьми років, постійне погіршення іміджу держави на міжнародній арені, обумовлюється низкою факторів, серед яких важливим є неналежний стан системи інформаційної безпеки.

Метою випускної кваліфікаційної роботи є обґрунтування й розробка пропозицій щодо напрямів удосконалення державної політики у сфері інформаційної безпеки.

Поставлена мета зумовила необхідність вирішення таких дослідницьких завдань:

- розглянути сучасний стан та тенденції розвитку інформаційної безпеки в Україні;

- проаналізувати фактори впливу на забезпечення інформаційної безпеки в Україні;

- охарактеризувати особливості інформаційної безпеки в умовах поширення пандемії COVID-19;

- сформулювати пропозиції щодо напрямів удосконалення державної політики у сфері інформаційної безпеки.

Об’єктом дослідження є суспільні відносини, які виникають у процесі державної політики у сфері інформаційної безпеки.

Предметом дослідження є теоретико-методичні та прикладні основи державної політики у сфері інформаційної безпеки.

Методи дослідження. Для вирішення окреслених завдань, у процесі дослідження використано загальнонаукові та спеціальні методи дослідження. Для аналізу сучасного стану та тенденції розвитку інформаційної безпеки в Україні та визначення стану інформаційної безпеки в умовах поширення пандемії COVID-19 було використано такі методи, як: аналітичний, описовий, структурного аналізу,

порівняння. Для оцінки факторів впливу на інформаційну безпеку основними методами були – структурний аналіз, узагальнення, синтез, аналогія. Метод порівняльного аналізу - з метою узагальнення наукових поглядів вітчизняних та зарубіжних авторів стосовно поняття інформаційної безпеки. Прогностичний метод, що передбачає узагальнення незалежних характеристик опрацьованих матеріалів для формулювання висновків, пропозицій щодо напрямів удосконалення державної політики у сфері інформаційної безпеки.

Структура роботи. Випускна кваліфікаційна робота складається зі вступу, двох розділів, висновків та списку використаних джерел. Повний обсяг роботи становить 46 сторінки, з них 35 сторінок основного тексту. Робота включає 3 таблиці та 1 рисунок. Список використаних джерел налічує 57 найменувань.

РОЗДІЛ 1

ОЦІНЮВАННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

1.1. Сучасний стан та тенденції розвитку інформаційної безпеки в Україні

Інформаційна сфера є тим системотворчим фактором життя будь-якого суспільства який впливає на політичну, економічну, оборонну та інших види безпеки України. Тому важливим є, при оперуванні інформацією, мати впевненість у тому, що використовувана нами інформація якісна і, що в процесі її поширення вона не була спотворена, адже питання інформаційної безпеки є важливим компонентом усієї системи безпеки України [19, с. 65].

Відомим фактом є те, що специфіка категорій в будь-якій галузі науки випливає з об'єкту досліджень останньої. А тому важливе значення для з'ясування сутності категорій, які визначають зміст і сутність державної політики у сфері інформаційної безпеки України, має систематизація, доповнення та взаємоузгодження понятійного апарату [21, с. 53].

Розпочнемо з сучасного наукового знання про безпеку, яке включає певні уявлення про цей феномен в межах юридичної, воєнної, політичної, соціальної та інших наук, які взаємозв'язані. Вітчизняні дослідники Т. Ткачук, Д. Корнієнко, М. Криштанович та В. Циганов вважають, що «безпека» це категорія, що характеризує ступінь (міру, рівень) захищеності життєво важливих інтересів, прав та свобод особи, суспільства і держави від зовнішніх і внутрішніх загроз або ступінь від- сутності загроз правам і свободам людини, базовим інтересам і цінностям суспільства та держави [49, с.121]. Зокрема В. Циганов під поняттям «безпека» розуміє «діяльність людей, суспільства, держави по виявленню, запобіганню, послабленню, відверненню загрози, яка здатна загубити їх, позбавити матеріальних і духовних цінностей, завдати невідшкодованих збитків, заблокувати шляхи для прогресивного розвитку» [49, с. 32]. Тобто «безпека»

набуває значення філософської категорії, оскільки охоплює всі аспекти життєдіяльності особи, суспільства і держави, а також безпосередньо відіграє в ній визначальну роль.

Безпека буквально завжди означає відсутність небезпеки. Потреба в безпеці є одним з основних мотиваційних механізмів у житті людини і мало чим відрізняється від інших живих істот. Більше того, безпека є незаперечною загальнолюдською цінністю, оскільки її визнають усі люди незалежно від расового, національного чи соціального походження [20, с. 45].

Що ж до поняття «інформація» то воно законодавчо закріплено у законі України «Про інформацію», де у ст. 1 вказується, що: «Інформація це будь-які дані та/або дані, які можуть зберігатися на матеріальних носіях або відображатися в електронному вигляді» [10]. Аналогічне визначення містить ч. 1 статті 200 Цивільного кодексу України [5]. А от детальне визначення поняття «інформація» є у іншому законодавчому акті – законі України «Про захист економічної конкуренції» (стаття 1), де під інформацією розуміють відомості які в будь-якій формі і у будь якому вигляді зберігаються на будь-яких носіях (до прикладу листи, книги, позначки, ілюстрації (тобто на картах, діаграмах, органіграмах, малюнках, схемах тощо), фотографії, кіно-, відео-, мікрофільми, голограми, бази даних комп'ютерних систем або повне або часткове відтворення їх елементів, звукові записи,), усні пояснення осіб або будь-які публічно виголошені чи задокументовані відомості [9].

А от така категорія як «інформаційна безпека» є досить багатоплановою, тому з цього приводу у науці існує величезна кількість думок. Нами було проведено порівняльний аналіз даної категорії, результати якого систематизовано і подано нижче у табл. 1.1.

Відповідно до проведеного аналізу під інформаційною безпекою розуміють стан захищеності інформаційного середовища, суспільні відносини та захищеність установлених законом правил. Також слід наголосити на тому, що в умовах глобалізації інформаційна безпека це інтегрований складник процесу

забезпечення захисту інформації від усіх внутрішніх і зовнішніх загроз, а також створення сприятливих умов для ефективного функціонування системи інформаційної безпеки.

Таблиця 1.1

Підходи авторів до визначення змісту поняття «інформаційна безпека»

Автори	Визначення
Д.М. Корнієнко [21, с.123]	Суспільні правовідносини щодо процесу організації створення, підтримки, охорони та захисту необхідних для особи (людини чи юридичної особи, установи, підприємства, організації), суспільства і держави безпечних умов їх життєдіяльності; суспільні правовідносини пов'язані з організацією технологій створення, поширення, зберігання та використанням інформації (відомостей, даних, знань) для забезпечення функціонування і розвитку інформаційних ресурсів людини, суспільства, держави
М.А. Дмитренко [29, с.237]	Стан інформації, за якого забезпечується збереження визначених політикою безпеки властивостей інформації
О.О. Золотар [35, с.154]	Стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави
О.С. Зозуля [34, с.108]	Стан захищеності потреб в інформації особистості, суспільства і держави, за якого забезпечується їх існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз
О.С. Власюк [23, с.74]	Один із аспектів розгляду інформаційних відносин у межах інформаційного законодавства

Джерело: узагальнено автором [21, с. 123; 29, с. 237; 35, с. 154; 34, с. 108; 23, с. 74].

Інформаційна безпека – це складне, системне, багаторівневе явище, на стан і перспективи якого безпосередньо впливають зовнішні та внутрішні фактори, найважливішими з яких є: 1) політична ситуація у світі; 2) наявність потенційних зовнішніх і внутрішніх загроз; 3) стан і рівень інформаційно-комунікаційного розвитку в країні; 4) внутрішньополітична ситуація в країні. Водночас інформаційна безпека - це складна, динамічна, цілісна соціальна система, складовими якої є підсистеми безпеки особистості, держави та суспільства.

Взаємозалежна, системна інформаційна єдність останнього - це якісна визначеність, спрямована на захист життєво важливих інтересів людини, суспільства і держави, забезпечення їх конкурентоспроможного, поступального розвитку [35, с. 154-155].

З точки зору права, інформаційна безпека базується на державній інформаційній політиці, відповідних законах, які врегульовують основні аспекти та гарантують інформаційну свободу громадян та їх доступ до інформації [19, с. 97].

Насамперед забезпечення інформаційної безпеки гарантується Конституцією України в якій окреслюється основні принципи під час здійснення діяльності в інформаційній сфері, а саме «створення, отримання, використання, поширення та зберігання інформації і захисту прав суб'єктів інформаційних відносин», містяться у 32 і 34, а також низці інших (10, 15, 17, 23. 28, 29, 31, 32, 40, 50, 53, 54, 55, 57) її статей [1]. Стаття 2 Закону України «Про національну безпеку України», правовою основою в сфері національної безпеки, окрім Конституції, визначає «закони України, міжнародні договори, згода на обов'язковість яких надана ВРУ України» [13], а також видані заради виконання Конституції та законів України інші нормативно-правові акти. Крім того, основою галузевого законодавства є більш ніж п'ятнадцять основних законів і значна кількість пов'язаних нормативних актів. До найважливіших відносять закони: «Про інформацію» [10], «Про доступ до публічної інформації» [7], «Про захист персональних даних» [9], «Про друковані засоби масової інформації (пресу) в Україні» [10], «Про телебачення і радіомовлення» [15], «Про основні засади інформаційного суспільства» [14], «Про державну таємницю» [6] та деякі інші.

Крім того, є нормативні акти які у тій чи іншій мірі розглядають питання інформаційної безпеки, до прикладу, Податковий та Митний кодекси України, регулюють питання пов'язані зі створенням, збором, використанням специфічної податкової, митної інформації [3; 4]. Окремі аспекти розповсюдження інформації та забезпечення її безпеки регулюються адміністративним та цивільним

кодифікованим законодавством [2; 5]. Важливою правовою основою інформаційної безпеки виступають підзаконні нормативно-правові акти, такі як: Концепції, Стратегії, Доктрини. Зокрема була розроблена Стратегія національної безпеки України, Стратегія інформаційної безпеки, Стратегія розвитку інформаційного суспільства в Україні [17; 16; 18]. В цих актах закріплюються основні пріоритети розвитку певної сфери, і вони є базовими при прийнятті нових норм та при усуненні колізій в існуючих.

Забезпечення інформаційної безпеки шляхом послідовної реалізації чітко сформульованої національної інформаційної стратегії може суттєво сприяти успіху у вирішенні проблем у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах діяльності держави. Таким чином, реалізація ефективної інформаційної політики може суттєво вплинути на вирішення внутрішніх, зовнішніх та військових конфліктів [28, с. 203].

В останні роки, на жаль, пріоритетним завданням соціальних і державних інституцій стала розробка невідкладних та ефективних заходів щодо нейтралізації інформаційно-диверсійної діяльності Російської Федерації проти України та недопущення її подальшого розгортання. Вирішення цієї складної проблеми забезпечить захист інтересів суспільства та держави, сприятиме реалізації права громадян на отримання вичерпної та якісної інформації [40, с. 38].

У гібридній війні з державою-агресор друга сторона неминуче піддається низці інформаційних загроз, нейтралізація яких, з одного боку, потребує спеціальних правових та адміністративних заходів, а, з іншого боку, може супроводжуватися значними обмеженнями демократичних прав і свобод. Пошук балансу між інтересами національної безпеки та верховенства права є, в даному випадку, стратегічно важливим завданням держави [25].

Чи не найважливішим знаряддям гібридної війни яке застосовується як стороною-агресором (для поширення недостовірної інформації заради паніки та деморалізації противника та інших агресивних дій), та другою стороною (підняття патріотичного духу, закликів до боротьби, спростування недостовірної інформації

та ін.) є засоби масової інформації (далі – ЗМІ) різного роду. Вони є найефективнішою зброєю, яка використовується в сучасних гібридних війнах. З огляду на це, державна політика у сфері інформаційної безпеки має зосередитися на вибірковому застосуванні обмежень до конкретних мас-медіа, які виявилися ворожими, упередженими та маніпулятивними. Такий підхід вимагає максимальної юридичної визначеності щодо обмежувальних критеріїв, оскільки в разі їх недотримання існує ризик заборони неупереджених та політично нейтральних (наприклад, у разі ненавмисного поширення недостовірної інформації). При цьому велика група людей та громадських організацій можуть наголошувати на тому, що введені заборони позбавлені будь-яких фактичних підстав, не мають правових підстав, суперечать Конституції, обмежують демократичні права і свободи. Тому всі обмеження в інформаційному середовищі мають бути точковими і застосовуватись лише до тих ресурсів, які були скомпрометовані конкретними діями або є джерелом загроз державі та суспільству [27, с. 21-22].

Нормативно-правове регулювання створення єдиного інформаційного простору України має сприяти гармонійному розвитку інформаційних ресурсів, інформаційних послуг та інформаційних продуктів в країні. Значення розвитку законодавства у сфері інформаційної та інформаційної безпеки та формування інформаційного суспільства визначається тим, що закони цієї сфери істотно впливають на законодавче регулювання відносин у всіх сферах життя [34, с. 106].

31.03.2021 року при Міністерстві культури та інформаційної політики було створено Центр стратегічних комунікацій та інформаційної безпеки (далі – ЦСКІБ) [41] з метою протидії дезінформації. ЦСКІБ об’єднав зусилля громадських організацій та влади у боротьбі із дезінформацією, швидкого реагування на фейки, а також на промоцію українських наративів. Робота Центру сфокусована на протидії зовнішнім загрозам, об’єднанні зусиль держави та громадських організацій у боротьбі з дезінформацією, оперативному реагуванні на фейки, а також на промоцію українських наративів.

Ключові завдання Центру [41]:

- розбудова стратегічних комунікацій (розробка контрнаративів РФ, проведення інформкампаній, включення українських наративів у щоденну комунікацію Уряду);

- протидія дезінформації та формування стійкості до неї. Постійне сповіщення про інформаційні атаки проти України на ресурсах Центру, зокрема на web-порталі , FB-сторінці , та Telegram-каналі;

- підвищення обізнаності про гібридні загрози (розробка та проведення тренінгів для державних службовців, зокрема для представників комунікаційних підрозділів);

- регулярне інформування про гібридну агресію з боку Росії на міжнародному рівні, напрацювання механізмів протидії дезінформації спільно з міжнародними партнерами.

Основними напрямками діяльності ЦСКІБ передбачено такі [41]:

1. Стратегічні комунікації: розроблення контрнаративів РФ; проведення інформаційних кампаній; включення українських наративів у щоденну комунікацію уряду

2. Онлайн ресурс: створенням онлайн-ресурсу, який активно реагуватиме на інформаційної атаки

3. Співробітництво з міжнародними партнерами: систематичне сповіщення про гібридну агресію з боку Росії на міжнародному рівні; спільне напрацювання механізмів з протидії дезінформації з міжнародними партнерами.

Розглянувши сучасний стан та тенденції розвитку інформаційної безпеки в Україні, приходимо до висновку, що інформаційна безпека є комплексною категорією, яка включає внутрішньо- та зовнішньополітичні, економічні, технологічні, військові та інші елементи. Система інформаційної безпеки входить до загальної системи національної безпеки держави і її ефективне функціонування врегульоване низкою нормативно-правових актів. Діяльність держави в особі органів державної влади, громадських організацій, засобів масової інформації та

громадян, які координують свої дії по здійсненню діяльності у сфері інформаційної безпеки на основі єдиних правових стандартів має бути спрямована на ефективну протидію інформаційним загрозам в сучасних умовах.

1.2. Аналіз факторів впливу на забезпечення інформаційної безпеки в Україні

Розуміння та виявлення факторів, відповідальних за підвищення загроз інформаційній безпеці, має системний характер, а отже, охоплює всі без винятку сфери діяльності людини, суспільства та держави. Насправді аналіз викликів – це завжди суб'єктивний процес, що складається зі сприйняття суб'єктом певних факторів через призму власних інтересів і професіоналізму. Фахівці відзначають важливий елемент гібридної війни – вторгнення до інформаційно-комунікаційного простору країни з метою придушення опору та формування глобальної політичної картини відповідно до інтересів агресора. Для цього використовуються різні інструменти маніпулювання суспільною думкою: втручання у функціонування інформаційно-комунікаційного простору та телекомунікаційних систем та мереж; розвиток кіберзлочинності; вплив на ЗМІ та маніпулювання громадською думкою [27, с. 18].

Як зазначає Н. Дмитренко: «Характер та особливості російсько-української війни вказують на те, що її метою є зміна самоідентифікації населення та перетворення східного регіону нашої країни на «сіру зону», яка залишить Російській Федерації важіль тиску через постійну загрозу поширення нестабільності на всю Україну. Це війна не за територію, а за світогляд, думки та душі людей. А оскільки контроль над інформаційною інфраструктурою забезпечує основу для формування громадської думки, що завжди виявляється спочатку у певних переконаннях, а потім у конкретних діях, у конкурентній боротьбі контроль над інформаційною інфраструктурою сферою стає одним із головних ресурсів влади» [29, с. 40-41].

Разом з воєнними засобами агресії (окупація і анексія Криму, збройне вторгнення на Донбас), Росія використовує весь наявний арсенал засобів «гібридної» війни – від інформаційно-пропагандистської експансії, економічного, енергетичного тиску та дискредитації Києва на світовій арені до підривних, шпигунсько-диверсійних дій на українській території, підбурювання сепаратистських настроїв в регіонах і масованих кібератак на державні електронні мережі. На думку українських експертів, саме експансія в інформаційному просторі є однією з найнебезпечніших складових «гібридної» війни Росії проти України (табл. 1.2). [31]

Таблиця 1.2

Оцінка рівня небезпеки засобів, що використовує Росія проти України (Оцінки за п'ятибальною шкалою – «5» – максимальна небезпека, «1» – мінімальна небезпека).

Засоби	Оцінка
Інформаційно-пропагандистська експансія (диверсії, провокації) в українському медіа-просторі.	4,4
Ведення інтенсивних бойових дій в зоні АТО з загрозою їх ескалації	4,3
Шпигунська, агентуро-розвідувальна діяльність російських спецслужб на території України	4,3
Мілітаризація Криму і ОРДЛО	4,3
Підтримка «п'ятої колони» в органах влади, ЗМІ, громадських організаціях в Україні	4,2
Дискредитація України в Європі і світі політико-дипломатичними, інформаційними та ін. засобами	4,2
Диверсійно-терористичні акції на території України	4,0
Підбурювання сепаратистських настроїв в регіонах	4,0
Захоплення українських заручників за сфабрикованими звинуваченнями у шпигунстві, тероризмі тощо.	4,0
Інспірування акцій соціального протесту	3,9
Введення і поширення економічних санкцій проти України	3,4
Кібератаки на українські комп'ютерні мережі	4,0
Використання «енергетичних» засобів тиску	3,4

Джерело: складено автором на основі [31]

Загрози інформаційній безпеці України переважно узгоджуються та якісно доповнюють перелік загроз національній безпеці в цілому. У Стратегії національної безпеки України, затвердженій Указом Президента України від 14.09.2020 № 392/2020 визначено сучасні загрози національній безпеці України в інформаційній сфері [17]:

– стрімка технологічна зміна та зміцнення ролі інформаційних технологій в всіх сферах суспільного життя (п. 9);

– застосування Російською Федерацією інформаційної «зброї» в поєднанні з енергетичною заради зміцнення позиції у Європі, її спроби вплинути на внутрішньополітичну ситуацію в європейських державах, та підтримка триваючих конфліктів, збільшення своєї військової присутності у Східній Європі (п. 16);

– продовження Російською Федерацією гібридної війни проти України через системне застосування інформаційно-психологічних, кібернетичних, політичних, економічних і воєнних засобів для ефективного впливу на неї (п. 17);

– внутрішня і зовнішня деструктивна пропаганда, яка розпалює ворожнечу, провокує конфлікти, підриває суспільну єдність, використовуючи при цьому суспільні протиріччя за умов відсутньої цілісної інформаційної політики нашої держави, слабої системи стратегічних комунікацій (п. 20);

– недостатньо ефективна діяльність державних органів, що тягне за собою труднощі у виробленні і реалізації ефективної державної політики (у т.ч. в інформаційній сфері), що в свою чергу, є основним джерелом загроз незалежності України, її суверенітету і демократії (п. 22);

– посилення загроз для критичної інфраструктури (у т.ч. її інформаційної складової), що пов’язане з погіршенням технічного стану, недостатньою кількістю інвестицій заради її оновлення та розвитку, несанкціоноване втручання у її функціонування, зокрема завдяки фізичним і кібернетичним атакам, а також тимчасова окупація частини території України (п. 27).

Президент України 28 грудня 2021 р. затвердив Стратегію інформаційної безпеки, яка була схвалена Радою національної безпеки і оборони та відповідним рішенням РНБО [16]. Вона є одним з низки документів, які розробляються заради реалізації Стратегії національної безпеки України. Цей документ прийнятий заради створення умов для забезпечення інформаційної безпеки України, яка в свою чергу допоможе захистити життєво важливі інтереси громадянина, суспільства та держави під час протидії внутрішнім та зовнішнім загрозам, забезпечить захист державного суверенітету і територіальної цілісності України, підтримає соціальну та політичну стабільність, оборону держави, забезпечить права та свободи кожного громадянина. Реалізація поставлених окреслених у Стратегії цілей розрахована на період до 2025 р. [16].

Ключовими загрозами для інформаційної безпеки, які окреслені в Стратегії є [16]:

- велика кількість глобальних дезінформаційних кампаній які інспіровані авторитарними урядами та радикальними рухами для маніпулювання свідомістю окремих людей та груп населення;

- вплив на внутрішню і зовнішню суспільно-політичну ситуацію соціальних мереж, адже специфіка організації всесвітньої мережі Інтернет ставить під загрозу гарантії права особи на приватність;

- низький рівень медіаграмотності (медіакультури) українського населення в умовах стрімкого розвитку цифрових технологій, що супроводжується зменшенням критичності сприйняття інформації і створює підґрунтя для можливих маніпуляцій громадською думкою, що, в свою чергу сприяє зростанню впливу дезінформації та деструктивної пропаганди, популярності конспірологічних теорій;

- масований інформаційний вплив Російської Федерації на населення України завдяки спеціальним інформаційним операціям, які спрямовані на підрив національної безпеки України, її національних інтересів, ліквідацію української державності та знищення української ідентичності, провокування проявів

екстремізму, панічних настроїв у суспільстві, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації в Україні;

- домінування на інформаційному просторі Російської Федерації як держави-агресора на тимчасово окупованих територіях України;

- наявність обмежених можливостей реагувати на дезінформаційну кампанію через відсутність ефективної системи реагування на такі виклики;

- відсутність сформованої системи стратегічних комунікацій адже в Україні досі триває процес становлення системи стратегічних комунікацій;

- недосконале регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів;

- маніпуляція свідомістю громадян України стосовно європейської та євроатлантичної інтеграції України.

Не менш гостро стоїть питання кібербезпеки в умовах гібридної війни. У світі кіберпростір все частіше використовується для широкого кола небезпечних операцій: від крадіжки цінної інформації до актів кібертероризму [27, с. 18]. Насамперед, мережі та інформаційні системи містять конфіденційні дані та економічно цінну інформацію, що підвищує мотивацію до атаки. Атаки на інформаційні системи можуть мати серйозні наслідки в національному масштабі, наприклад, збої в системах зв'язку, витік конфіденційної інформації тощо [24, с. 28]. Зрозуміло, що сьогодні українському суспільству загрожує постійне отримання недостовірної, часом шкідливої інформації, її несвоєчасне отримання, шпигунство, комп'ютерна злочинність тощо.

У 2014-2021 рр. було дуже важко забезпечити інформаційну безпеку України. Українська держава роками бореться з використанням системи пропаганди, яка будується в Росії. Дії ворога спрямовані на розбрат в українському суспільстві та знищення української політичної нації, уславлення сепаратизму, штучне загострення реальних та уявних внутрішніх протиріч, створення атмосфери громадянської недовіри до дій і намірів влади, провокування актів громадянської непокори, та формування у громадян України та міжнародної спільноти

негативного ставлення до подій в Українській державі, спроби спотворення української історії та маніпулювання історичними фактами [34]. До прикладу Російські ЗМІ заради створення образу України як «фашистської» держави використовують фейкові новини про появу символів нацистської Німеччини в найбільш неочікуваних контекстах. 12 січня 2015 року журналісти федерального каналу «Россия1-» в ефірі програми «Вести» повідомили: партія «Свобода» розробила проект 1000 гривневої купюри, яка виражає цінності нових українських еліт». На цій «купюрі» на розмитому фоні був зображений Адольф Гітлер. Сайт «StopFake» розвінчав цю брехню, вказавши, що фотографія була узята з російського гумористичного сайту pikabu.ru, а на оригінальній презентаційні купюрі НБУ зразка 2008 року був зображений Пантелеймон Куліш [36, с. 324].

Війни такого типу є досить поширеними в глобальному інформаційному просторі і ретельно досліджуються вченими та фахівцями. Зокрема, Інститут національних стратегічних досліджень США та деякі західні експерти та вчені виділяють декілька елементів інформаційної війни. Одним з них є психологічна війна. Головне завдання психологічної війни – маніпулювання масами. Метою такої маніпуляції є: впровадження ворожих ідей та поглядів у суспільну та індивідуальну свідомість; дезорієнтація та дезінформація мас; послаблення певних вірувань, залякування народу через образ ворога; залякування противника власними силами [25].

Крім того, Україна посідає третє місце в рейтингу країн з найбільшим ризиком зараження через Інтернет: 35,7% користувачів зіткнулися з онлайн-загрозами, а Україна посіла 9 місце в рейтингу країн з найбільшим ризиком зараження мобільними вірусами (8,39 %). Ризик зіткнення з локальними загрозами також дуже високий для українців (54,5%) [54]. Сюди входять об’єкти, які проникли на комп’ютери шляхом зараження файлів або знімних носіїв, або які вперше з’явилися на комп’ютері невідкритими (наприклад, складні програми встановлення, зашифровані файли тощо). За цим показником країна посідає передостаннє місце в двадцятці топ у світі, але перше в Європі [54].

В Україні зафіксовано велику кількість антивірусних програм, пов’язаних із прикладними програмами та програмами шифрування – шкідливими програмами, призначеними для блокування пристрою чи браузера чи шифрування файлів користувача, роблячи їх недоступними без спеціального ключа, який вимагає викупу. На думку експертів, ситуація загалом характеризується такими тенденціями у сфері загроз інформаційної безпеки: неконтрольовані загрози, пов’язані з т. зв. «інтернетом речей» і поширенням мережевих з'єднань; стрімкий розвиток «кіберзлочинності як послуги» – надання цифрових послуг злочинними синдикатами; підвищений юридичний ризик у сфері регулювання мережевого зв'язку; хакерські атаки, спрямовані на підрив репутації брендів і політичних сил [24]. Національна система кібербезпеки формується за мінімальної участі громадськості та експертної підтримки (громадські ради малоефективні, а Національний координаційний центр кібербезпеки (НКЦК) не має у своєму складі представників відповідних структур). Міністерство цифрової трансформації України, хоча і має завдання у сфері кібербезпеки (кіберзахисту), однак обмежене у можливостях для їх реалізації (передусім – кадрових). Відтак важливим є посилення його потенціалу, щонайменше в аналітичному супроводі прийняття рішень у зазначеній сфері [22].

Заради протидії новим загрозам та викликам на фоні активної агресії Російської Федерації у кіберпросторі Україна намагається створити повноцінну систему національної кібернетичної безпеки. Указом президента України від 26 серпня 2021 року № 447/2021, було затверджено Стратегію кібербезпеки України на 2021-2025 рр., яка була внесена Національним координаційним центром кібербезпеки та схвалена Радою національної безпеки і оборони України [47]. В стратегії зазначається, що необхідно створити умови для безпечного функціонування кіберпростору, заради можливості його використання в інтересах особи, суспільства, держави. Стратегія безпосередньо визначає механізми її реалізації та критерії вимірювання успіху на цьому шляху [47].

Проаналізувавши основні фактори впливу на забезпечення інформаційної безпеки в Україні розуміємо, що ключовим залишається стратегічне інформаційне протистояння яке є небезпечним компонентом гібридної війни, розгорнутої РФ проти України, причому головна загроза інформаційній безпеці нашої держави є можливість впливу ворога на інформаційну інфраструктуру, інформаційні ресурси, на суспільство, свідомість і підсвідомість особистості заради нав'язування власної системи цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності.

РОЗДІЛ 2

УДОСКОНАЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Інформаційна безпека в умовах поширення пандемії COVID-19

В умовах надзвичайних ситуацій, зокрема таких масштабних як епідемії/пандемії, для адекватної відповіді на породжені ними виклики, крім належного рівня медицини, налагодженої системи охорони здоров'я та санітарно-епідеміологічної служби, важливе значення мають такі фактори, як інформація та інформаційна безпека, призначення яких є забезпечення поінформованості населення про перебіг пандемії та її наслідки, з одночасним уникненням панічних настроїв, істеричності чи байдужості. У свою чергу, вимоги дотримання інформаційної безпеки можуть стати фактором обмеження інформації, усунення неправдивої інформації тощо, внаслідок чого виникає колізія права приватної особи на інформацію та права на безпечну інформацію (безпеку інформації) [47, с. 183].

У період поширення вірусу COVID-19 набуває великого значення захист інформаційної безпеки держави від цілої низки загроз. Сучасне інформаційне суспільство вкрай уразливе до зловмисних дій окремих елементів в інформаційному просторі мережі Інтернет та медіапросторі. Насамперед, йдеться про хибні повідомлення, які можуть розміщуватися як з метою заподіяння негативних наслідків, так і для задоволення потреб певних елементів у відомості чи громадському резонансі. До таких загроз можна віднести поширення неправдивої інформації щодо самої хвороби (фейкова інформація про кількість загиблих/хворих, симптоматика, кількість ускладнень після хвороби тощо), лікування (фейкова інформація про ефективність певних ліків або методик лікування, ефективність та небезпека певних видів щеплень тощо), джерела хвороби (вже відомі фейкові повідомлення про поширення COVID-19 завдяки

використанню веж 5G, непідтверджені витоки штучного розповсюдження вірусу певними державами або іншими суб'єктами, релігійний контекст поширення вірусу та ін.) та інших факторів, пов'язаних з протидією пандемії (фейні новини про умови лікування в лікарнях, умови у місцях примусової обсервації та ряд різних факторів) [56].

Для вдалої протидії зазначеним загрозам інформаційній безпеці у цій сфері необхідно створити механізм чинних правових засобів протидії та законодавчо його закріпити. Слід зазначити, що є позитивний закордонний досвід протидії певним загрозам. Так, на одному з інформаційних ресурсів Європолу йдеться про те, що «злочинці швидко адаптували свої методи, щоб використовувати наші страхи навколо пандемії COVID-19, головна мета отримання прибутку будь-якими коштами». У той самий час, цьому ж ресурсі вказується ряд засобів протидії такий злочинної діяльності [56].

Слід зазначити, що пропонується розширити визначення, яке дане Європолом, оскільки головною метою поширення помилкової інформації COVID-19 не завжди є отримання прибутку. Це може бути стимулювання панічних настроїв, недовіри до існуючої влади (як один із методів гібридної війни) та просто отримання позитивних емоцій від популярності постів злочинця у мережі Інтернет. Також дуже важливою частиною механізму протидії загрозам національній інформаційній безпеці під час пандемії COVID-19 має стати планування. Так, у Європейському Союзі було прийнято Кодекс практики проти дезінформації [51] та План дій проти дезінформації [52]. На основі цих документів пропонується розробити загальнодержавний план протидії інформаційним загрозам під час пандемії COVID-19.Законодавство майже не передбачає відповідальності за поширення неправдивої інформації про пандемію COVID-19. У той же час, враховуючи його велику небезпеку для національних інтересів, слід посилити відповідальність за розміщення неправдивої інформації про COVID-19, яка може призвести до несприятливих наслідків [37, с. 36].

Слід зазначити, що правоохоронні органи нашої держави вже активно діють у цьому напрямку – так, ще навесні 2020 р. Служба Безпеки України почала активно притягувати до відповідальності осіб, які розповсюджували свідомо неправдиву інформацію про пандемію COVID-19 (зокрема, про кількість хворих, кількість померлих, кількості ліжко-місць у лікарнях тощо) [46].

Крім того, під час пандемії COVID-19 багато суб'єктів перейшли на дистанційний режим роботи (зокрема навчальні заклади). Наприклад, всі освітні заняття перейшли у відеоформат із широким використанням таких сервісів, як Moodle, Discord, Zoom та Skype. У той же час всі послуги можуть стати метою хакерських атак з метою отримання доступу до персональних даних, саботування діяльності користувачів, крадіжки електронних облікових записів і т.д. Тому важливою складовою правового механізму засобів забезпечення національної інформаційної безпеки має стати особливий режим захисту таких сервісів від атак під час пандемії COVID-19 [50]. Також важливим є запровадження державних програм з підвищення інформаційної грамотності як серед громадян, так і серед суб’єктів господарювання, які функціонують у сфері медіа. Для цього необхідно проводити спеціальні масові заходи (у формі лекцій, онлайн-семінарів, каналів на YouTube, постів у соціальних мережах та меседжерах). Доцільно залучати до участі у таких заходах як представників наукової спільноти, і фахівців правоохоронних органів. Тим більше, що пандемія коронавірусу та заходи карантину помітно вплинули на структуру споживання інформації громадянами України. Насамперед серед українців загалом виріс попит на інформацію, оскільки за багатьма позиціями помітне зростання часток аудиторії без падіння за іншими позиціями [50].

Хоча центральні українські телеканали залишаються найпопулярнішим джерелом – їх дивляться 75% респондентів, на – друге місце вирвалися соціальні мережі – їхня частка зросла з 24% [30] у 2019 до 44% у 2020. Значно зросла частка тих, хто отримує інформацію від родичів та друзів – з 11% до 23% [30]. Поки що

ця позиція конкурує за третє місце з українськими інтернет-ЗМІ, з яких інформацію про Україну та світ отримували не менше 27% респондентів [30].

Далі йдуть меседжери (Viber, Telegram, WhatsApp та ін.) з часткою 11%, українські загальнонаціональні радіостанції та місцеве телебачення, про які згадали майже по 9% респондентів, українські загальнонаціональні друковані видання (8%) та місцеві інтернет-ЗМІ (6%) [50].

Російське телебачення залишається одним із основних джерел інформації майже для 6% респондентів. Аналіз даних опитування показав, що російські телеканали частіше дивляться респонденти віком від 50 років, які проживають у східних областях України (де частка глядачів сягає 12% серед опитаних респондентів) [50] .

Також пандемія COVID-19 призвела до більшого попиту на місцеві друковані видання. Якщо 2019 року їх згадали трохи менше 2% респондентів [53], то 2020 року їхня частка зросла до 4%.

Проаналізуємо рис. 2.1, на якому зображено результати дослідження, проведеного фондом «Демократичні ініціативи» ім. Ілька Кучера спільно з соціологічною службою центру Разумкова з 14 по 19 серпня 2020 р. щодо джерел отримання інформації різними верствами населення [50]. Окремим кіберінформаційним аспектом пандемії стало посилення кіберзлочинності. Почастішали кібератаки на системи охорони здоров'я. Під час пандемії зросла кількість кіберзлочинів, пов’язаних з електронним банкінгом та онлайн-комерцією. Збільшення обсягів онлайн-платежів з використанням різноманітних електронних банківських послуг призвело до збільшення кількості крадіжок із рахунків клієнтів банку [26]. Тільки за підсумками першого півріччя 2020 року Служба безпеки України [42] нейтралізувала 300 кібератак та кіберінцидентів. Тому сьогодні пріоритетним є забезпечення інформаційної та кібербезпеки кожного окремого громадянина, суспільства та держави загалом і набуває стратегічного значення. Проте загалом, враховуючи необхідність зменшення руйнівних кіберінформаційних впливів та загроз в умовах пандемії COVID-19,

нормативна інформаційна безпека потребує вдосконалення. Пандемія COVID-19 наголосила на необхідності зміцнення національної безпеки України та необхідності зменшення негативних наслідків руйнівного впливу кіберінформації [24, с. 27].

Також дослідники виділяють поширення злочинності, спричиненої поширенням COVID-19 у різних сферах життя людини та суспільства.

1) стрімке збільшення кількості кримінально-кримінальних порушень санітарних правил та норм щодо запобігання інфекційним хворобам, а також масовим отруєнням;

2) зростання шахрайств та обманів, насамперед обумовлених продажем, а також придбанням медичних засобів або засобів індивідуального захисту та продуктів харчування, а також індивідуальних речей, зокрема продажів у мережі «Інтернет» ліків для лікування COVID-19;

3) збільшення випадків мародерства та вандалізму через недостатню охорону приміщень;

4) поширення кіберзлочинності, обумовлене шахрайством у вигляді дзвінків та смс-розсилок про фінансові компенсації державою витрачених на лікування коштів або інших виплат, що мають на меті поширення паніки серед населення;

5) збільшення випадків домашнього насильства у всіх можливих його проявах (сексуальний, економічний, психологічний, фізичний) [37, с. 37].

Ще однією загрозою, пов'язаною із застосуванням карантинних заходів COVID-19, є витік персональних даних громадян, які перебувають на лікуванні, карантині або самоізоляції. Також держава зобов'язана забезпечувати достовірність та оперативність інформування товариства COVID-19. Особливо важливим є недопущення поширення помилкової та некоректної інформації про COVID-19. З метою нівелювання цих процесів МОЗ України опубліковує інформацію про COVID-19, крім офіційних сайтів, на спеціально створених каналах, таких як Telegram та Viber [21, с. 313].

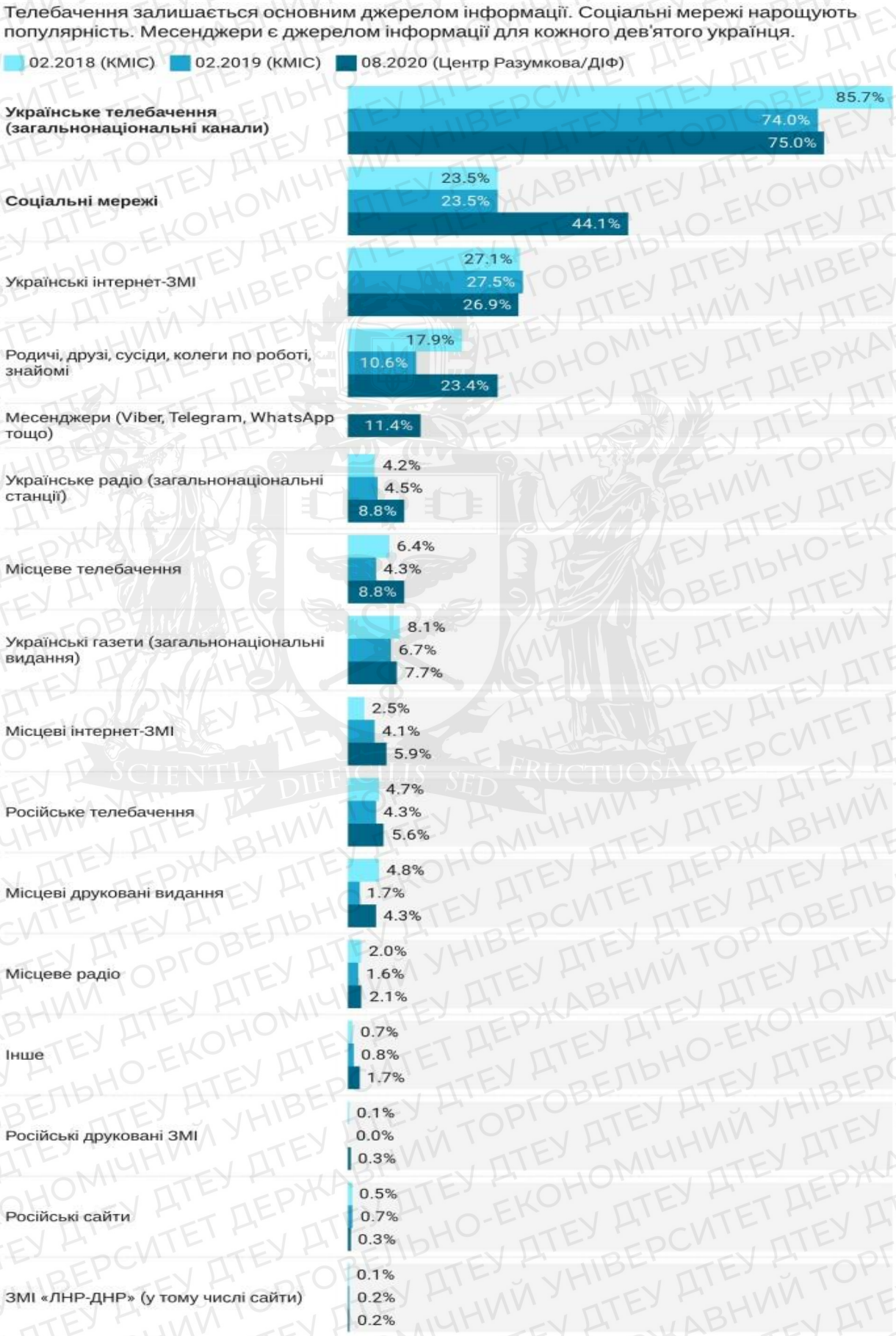

Рис. 2.1 Джерела отримання інформації різними верствами населення

Зазначимо, що ЄС серед заходів запобігання та протидії поширенню фейків щодо COVID-19 реалізується План дій проти дезінформації [53], а також запроваджено кодекс практики проти дезінформації [51]. Наведені вище документи та програми доцільно впровадити в національне законодавство.

Аналіз стану інформаційної безпеки в умовах поширення пандемії COVID-19 дозволяє стверджувати, що пандемія COVID-19 стала найбільшим викликом для людства за останні десятиліття. Її руйнівний вплив поширився на всі сфери суспільства. У той же час пандемія не спричинила за собою, а лише наголосила на небезпеці, які неминуче виникають у сучасному глобалізованому світі. Враховуючи періодичність виникнення нових пандемій, необхідно створити оптимальний механізм захисту національної інформаційної безпеки вже зараз, оскільки невідомі як наслідки пандемії COVID-19, що триває, так і наслідки майбутніх захворювань.

2.2. Напрями удосконалення державної політики у сфері інформаційної безпеки

Окреслений нами в попередньому розділі сучасний стан та тенденції розвитку інформаційної безпеки, а також аналіз факторів впливу на забезпечення інформаційної безпеки та видів інформаційних загроз визначає предметне поле діяльності, в якому повинні працювати спеціальні державні служби та інституції, що вповноважені державою виявляти та нівелювати ці загрози. На наш погляд, важливим елементом технології реагування на ці загрози є створення загальнодержавної системи інформаційної безпеки України, її наступальної спрямованості, як важливої умови захисту національного суверенітету, яка передбачає:

- розробку й удосконалення нормативно-правової бази в сфері інформаційної безпеки, яка нині є фрагментарною та не повною мірою відповідає нагальним потребам;

- створення (визначення) керівного та координаційного органу системи інформаційної безпеки України в структурі органів виконавчої влади;

- визначення (уточнення) переліку суб'єктів, які відповідають за стан інформаційної безпеки;

- проведення досліджень та визначення потреб у технічному, фінансовому й кадровому забезпеченні функціонування системи;

- активізація заходів у Міністерстві оборони та Генеральному штабі Збройних Сил України зі створення власної системи інформаційної безпеки як складової національної системи інформбезпеки [32].

На сьогодні розглядати будь-які загрози в інформаційній сфері необхідно з урахуванням того контексту, в якому вони виникають і знаходять свій вияв [38, с. 143]. Зміст і специфіка технології виявлення і усунення інформаційних загроз, ризиків та викликів залежать від розвиненості й цивілізованості суспільства, його міжнародних зв'язків. При цьому рівень інформаційної безпеки має визначатися здатністю технології до реальної оцінки й оптимальної протидії цим загрозам. Тому основним пріоритетними напрямами технології із виявлення й усунення інформаційних загроз та важливими кроками її здійснення з боку владних органів України мають бути:

- створення власної національної моделі інформаційного простору та забезпечення необхідних заходів щодо запобігання інформаційним загрозам;

- модернізації усієї системи інформаційної безпеки держави та формування й реалізація ефективної інформаційної політики;

- удосконалення законодавства з питань інформаційної безпеки, узгодження національного законодавства з міжнародними стандартами та дієве правове регулювання інформаційних процесів; - розвиток сучасної інформаційної інфраструктури;

- впровадження новітніх інформаційно-комунікативних технологій у процеси державного управління;

- ефективна взаємодія органів державної влади з усіма інститутами громадянського суспільства під час формування, реалізації та коригуванні необхідної технології, яка має спрямовуватися на виявлення та ліквідацію інформаційних загроз, недопущення інформаційної експансії [57, с. 30].

Така технологія має здійснюватись за такими напрямами:

- реалізація упереджувальної стратегії та тактики (превентивні заходи);

- здійснення реагувальної стратегії (оперативне реагування на інформаційні атаки супротивника та активний наступ);

- захист національного інформаційного простору [28, с. 31-32].

Комплексний характер актуальних загроз національній безпеці в інформаційній сфері насамперед потребує визначення ефективних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації. Для цього потрібна ефективна управлінська діяльність, яку доцільно розглядати в двох аспектах: управління технічними системами та вплив на соціальні процеси з метою досягнення поставлених цілей [20].

Шляхами вдосконалення організаційних засад державної політики у сфері інформаційної безпеки України передбачається адаптація в Україні світового досвіду (зокрема, США) щодо створення єдиної державної інформаційно-комунікаційної інфраструктури [28, с. 201]. Вона, з одного боку, сприятиме формуванню стійкої організаційно-інформаційної мережі, а з другого покликана забезпечити захист інформаційних і комунікаційних засобів від потенційних загроз. При цьому важливе значення набуває модель міжсекторної взаємодії щодо забезпечення інформаційної безпеки [32, с. 31].

В умовах нових інформаційних викликів Україна має бути готова до забезпечення своєї інформаційної безпеки, при цьому нашій державі необхідно розробити всеосяжну і чітку стратегію інформаційного захисту, що має сприяти

досягненню поставлених цілей, а не перешкоджати їх досягненню. А в майбутньому цю систему необхідно розвивати, враховуючи правові, технологічні, матеріально-фінансові та інші аспекти. Адже сьогодні, коли ресурсні можливості держави обмежені, необхідний пошук нових шляхів і напрямів забезпечення інформаційної безпеки України в умовах зростання інформаційних викликів та загроз.

Вирішення та розв'язання даної проблеми полягає в [48, с. 182]:

- чіткій державній інформаційній політиці України, тому що інформаційні ресурси держави значною мірою перебувають під зовнішнім впливом;

- інформаційному забезпеченні внутрішньої і зовнішньої політики держави, що створює передумови для її підтримки громадянами, сприяє формуванню об'єктивного іміджу України в світі;

- наявності цілісної ідеології щодо ефективного функціонування інформаційної владної вертикалі, що виходить з історичного досвіду розвитку України, свого географічного простору і населення, традиційних національних інтересів, сучасних глобальних викликів та загроз;

- узгодженні та координуванні діяльності різних силових відомств під час здійснення як розслідування злочинів у інформаційному просторі так і створенні ефективної системи захисту вітчизняного інформаційного простору України; - контролі і використанні інформаційного простору України, захисті при цьому своїх інформаційних функцій від ворожих дій супротивника тощо [48, с. 182].

Серед напрямів, якими доцільно характеризувати зазначені питання, можна визначити щонайменше трьох. Перший напрямок (прикладний) – розробка та впровадження стандартів та алгоритмів ведення мережевих інформаційних воєн, які допоможуть швидко реагувати на певні виклики та компенсувати за певних обставин брак досвіду та власних інструментів. Другий напрямок (кадровий) – налагодження системної роботи з підготовки відповідних фахівців, яка базуватиметься на чіткій методологічній базі та практичних методиках навчання. Третій напрямок – створення мережі незалежних наукових центрів та

стимулювання роботи окремих учених, які зможуть дослідити проблематику інформаційних загроз та шляхів їх виявлення та усунення [32, с. 28].

Як показали події останніх років – Євромайдан, анексія Росією Автономної республіки Крим та її гібридна агресія на Сході України, вітчизняна інформаційна сфера у її аспекті безпеки потребує суттєвих структурних змін. Зазначені зміни мають бути спрямовані на:

- удосконалення систем моніторингу та контролю інформаційних потоків, як усередині країни, так і в міжнародному масштабі;

- уніфікацію та модернізацію засобів та методів управління інформаційними потоками, які мають ґрунтуватися на гнучких схемах роботи;

- розробку та практичне впровадження національної стратегії інформаційно-комунікаційної безпеки, що відповідає сучасним викликам гібридної та інформаційно-психологічної війн другого покоління;

- формування профільної нормативно-правової бази, що дозволяє оперативно реагувати на сучасні виклики та загрози у контексті інформаційно-психологічних воєн у соціальних онлайн-мережах;

- створення та широке застосування ефективної системи підготовки фахівців у галузі інформаційно-психологічних воєн із знаннями та рівнем практичної підготовки;

- активне залучення широких верств громадськості у питаннях національної безпеки на волонтерських засадах;

- Формування ефективного ментального бар'єру свідомості громадськості проти іноземних впливів;

- створення національного конкурентоспроможного середовища медіапроектів;

- вивчення іноземного досвіду, стратегій, тактики ведення інформаційно-психологічних воєн [32, с. 29].

Цілі реалізації державної політики забезпечення інформаційної безпеки можуть бути досягнуті лише шляхом послідовного та випереджаючого розвитку

вітчизняного законодавства, за умов обов'язкового дотримання європейських конституційних принципів. Оскільки нормативно-правова база не охоплює всі основні елементи, необхідні для ефективної протидії реальним інформаційним загрозам, певною мірою застаріла, це потребує удосконалення системи нормативно-правового регулювання державної політики у сфері розвитку інформаційної безпеки в сучасних умовах. Крім цього одним із шляхів комплексного вирішення проблем у сфері забезпечення інформаційної безпеки України може стати кодифікація інформаційного законодавства, яка підтримується багатьма науковцями-юристами та дослідниками національного інформаційного простору [38, с. 125].

На нашу думку, важливим є створення сучасної правової бази на основі безпосереднього поєднання основоположних ідей правового регулювання інформаційної сфери та принципів забезпечення національної безпеки. Оскільки нормами вітчизняного законодавства не визначені стандарти та вимоги, способи та заходи щодо створення цілісної системи національної інформаційної безпеки, то ця проблема є головною у питаннях забезпечення інформаційної безпеки країни. Система правових стандартів має стати системоутворюючим чинником для системної та ефективної реалізації державної інформаційної політики, а також надійної протидії деструктивному іноземному інформаційному впливу та інформаційним загрозам у цілому [57, с. 688].

Все це потребує цілеспрямованої скоординованої діяльності органів державного управління, які мають характеризуватися: планомірністю, конкретністю, активністю; надійністю, універсальністю, комплексністю. Зарубіжний досвід забезпечення інформаційної безпеки, свідчить, що значна кількість держав світу приділяє особливу увагу інформаційній безпеці, шляхом створення спеціальних органів і підрозділів для боротьби з інформаційними загрозами. На жаль в Україні поки що немає можливості протиставити достатню кількість кваліфікованих фахівців, які б могли на належному рівні протидіяти зростаючим інформаційним загрозам іноземних держав щодо українського

інформаційного простору. Саме тому Україна має використовувати досвід розвинутих країн, що певною мірою мають напрацювання у сфері забезпечення інформаційної безпеки, зокрема досвід Європейського Союзу. З метою розгляду державної інформаційної політики розвинених країн світу та заради переймання кращих світових практик з реалізації інформаційної політики Україною наводимо порівняльну таблицю 2.1 [55; 45].

Таблиця 2.1

Порівняльна характеристика державної інформаційної політики розвинених країн світу

Країна	Характеристика інформаційної політики
Великобританія	Основною метою функціонування інформаційної політики є удосконалення існуючих умов в інформаційній сфері; посилення ефективності надання інформаційних послуг та реалізації інформаційних технологій у системі державного управління. Важливими пріоритетами інформаційної політики є освіта, охорона здоров'я, приватний бізнес. Головними засадами визначають технологічну нейтральність нормативних документів, активізацію міжнародного співробітництва, захист інтересів споживача в інформаційній мережі.
Німеччина	Головною метою інформаційної політики визначається надання безперешкодного міжнародного обміну інформацією та свободою слова. До того ж, основними завданнями є розвиток та функціонування інформаційно-комп'ютерних технологій та інформаційних мереж; активізація конкуренції у інформаційній сфері; розробка сучасних політико-економічних умов становлення принципів правового регулювання інформаційної діяльності у німецькому суспільстві. Інформаційна політика спрямовано трансформацію державного управління у процесі міжнародного обміну інформацією; пропагування ідеалів європейської демократії; створення надійної законодавчої бази; удосконалення технічного оснащення інформаційного сектора тощо.
Франція	Метою інформаційної політики є: активізація інформаційних магістралей, електронного ринку та банківської сфери; лібералізація різних комунікаційних технологій; оновлення інформаційного законодавства; посилення науково-дослідних робіт у сфері створення систем захисту інформації та запобігання комп'ютерним злочинам. Також важливим є той факт, що урядом країни було відкрито Фонд допомоги та співпраці для підтримки реалізації вітчизняних інформаційних технологій.
США	Головною метою інформаційної політики США є впорядкування інформаційних потоків у різних галузях для підтримки балансу між державним контролем та свободою підприємницької діяльності. До основних пріоритетів належать: підтримка наукових розробок у сфері інформатизації та телекомунікацій; посилення діалогу та обміну різними технологіями між університетами та організаціями; формування та покращення глобальної інформаційної інфраструктури; підтримання балансу між важливими інформаційними цінностями та затвердженням нових інформаційних технологій; удосконалення державної політики у інформаційній сфері.

Продовження таблиці 2.1

Країна	Характеристика інформаційної політики
Японія	Інформаційна політика спрямовано створення найефективнішого інформаційного суспільства. Таке завдання реалізується за допомогою застосування низки засобів волоконно-оптичного зв'язку, що дало змогу урядовим інститутам, державним організаціям та приватним підприємствам отримати доступ до необхідного програмного забезпечення.
Європейський Союз (ЄС)	Інформаційна політика Європейського Союзу реалізується відповідно до концепції єдиної загальної інформаційної політики, розробленої та впровадженої ідеологією європейської співпраці у сфері масової комунікації. До того ж інформаційна політика ЄС розробляється та забезпечується на місцевому, регіональному, державному та міжнародному рівнях, що об'єднуються в одну цілісну систему.
Скандинавські країни (Данія, Швеція, Норвегія, Фінляндія)	Основними завданнями інформаційної політики є: запровадження сучасних оновлених технологій у систему державного управління; ефективна реалізація політичної влади; поширення роботи «інфоцентрів» серед населення для задоволення потреб та запитів в інформаційній сфері; активізація та поширення інформаційної економіки та бізнесу; підтримка національних виробників інформаційних продуктів; Формування інформаційно-довідкових центрів 68 Проаналізувавши загальні аспекти розвитку інформаційної політики найбільш розвинених країн світу, можна констатувати, що даний вид політики спрямований на формування єдиного інформаційного простору та впроваджується шляхом реалізації програм та проектів різних міжнародних організацій. Крім того, у рамках міжнародних стратегій розглядаються питання розвитку інформаційного суспільства та телекомунікаційних мереж у Європейських країнах. Важливо зазначити, що Україні доцільно запозичити найкращі світові практики та намагатися їх запровадити на українську практику. Так, інформаційна політика Польщі функціонує та розвивається відповідно до Законів «Про пошту та телекомунікації» та «Про телебачення та радіомовлення» та орієнтована на лібералізацію інформаційної політики та врегулювання норм державного контролю над розповсюдженням інформаційних продуктів. До того ж, польська інформаційна політика спрямована на побудову власного розвиненого інформаційного простору для впровадження тематичними базами даних про інформаційні компанії, фірми тощо; поширення комп'ютерних технологій у соціальній сфері; активізацію роботи електронних бібліотек; вільний доступ до інформаційних ресурсів у мережах та системах для соціально незахищених верств населення – молоді, людей з обмеженими можливостями, малозабезпечених осіб тощо; створення та поширення громадського телерадіомовлення.
Італія	Головними цілями функціонування інформаційної політики є: - моніторинг та координація сфери надання онлайн-послуг; - Підвищення внутрішньомережевої якості; - Створення електронного управління на базі програми «Електронний уряд для ефективного федералізму: одне бачення - спільна реалізація»; - поширення культури електронної комунікації у співпраці з Державною адміністрацією та громадянами у діяльності регіональних та місцевих органів управління.

Джерело : узагальнено автором на основі [55; 45].

Проаналізувавши загальні засади розвитку інформаційної політики розвинених країн світу, констатуємо, що даний вид політики спрямований на формування єдиного інформаційного простору та реалізовується на практиці

шляхом втілення програм та проектів різних міжнародних організацій. Окрім того, у межах міжнародних стратегій розглядають питання розвитку інформаційного суспільства та телекомунікаційних мереж в Європейських країнах. Важливо зазначити, що Україні доцільно запозичати найкращі світові практики та намагатися їх впровадити в українські реалії [45, с. 98].

Крім цього, слід визначити основні завдання, виконання яких, на нашу думку, сприятиме ефективній реалізації політики інформаційної безпеки. Зокрема це:

- формулювання чітких, зрозумілих стратегічних цілей інформаційної політики, заснованих на обґрунтованій програмі державного управління, які має ґрунтуватися на реальних програмах і є частиною необхідної, виваженої інформаційної політики;

- діяльність інформаційних служб повинна здійснюватися в рамках виробленої інформаційної політики держави, мета й завдання якої має узгоджуватися з державним політичним й економічним управлінням;

- важливо безпосередньо здійснювати ефективний моніторинг інформаційного простору, ретельний контроль змісту, вірогідності отриманої інформації;

- державним інформаційним службам у своїй діяльності необхідно використовувати новітні інформаційні технології, методи й спеціальні інструменти виявлення загроз інформаційній безпеці країни [43, с. 88].

Постала також необхідність розробити нові інструменти, передусім аналітично оцінного спрямування, що можуть на ранніх етапах прогнозувати та запобігати негативним наслідкам загроз інформаційній безпеці і відповідно можливим збиткам для суспільства й держави. Таку функцію має виконувати державна система моніторингу стану національної безпеки як комплекс заходів щодо спостережень, збирання, опрацювання, передавання, збереження та аналізу інформації про стан національної безпеки, прогнозування його змін і розроблення науково обґрунтованих рекомендацій для прийняття рішень про запобігання можливим негативним наслідкам [48, с. 89].

Вкрай важливим є підвищення рівня інформаційної культури всіх суб'єктів інформаційних відносин та налагодження їх якісної взаємодії, що створить підґрунтя для забезпечення високого рівня інформаційної безпеки.

Необхідно також проаналізувати стратегічні цілі та напрями вдосконалення інформаційної безпеки які передбачені Стратегії інформаційної безпеки прийнятої 28 грудня 2021р. [16]. Вони в основному відображають плани уряду у сфері інформаційної безпеки, а саме:

- забезпечити всебічний розвиток української культури та утвердження загальнонаціональної ідентичності;

- підвищити рівень медіакультури та медіаграмотності;

- забезпечити дотримання конституційних прав особи на свободу вираження та захист приватного життя, захист прав журналістів і протидіяти поширенню незаконного контенту;

- створити ефективну систему стратегічних комунікацій;

- провести інформаційну реінтеграцію;

- здійснювати розвиток інформаційного суспільства та підвищувати рівень культури діалогу;

- протидіяти дезінформації [28, с. 221].

Очікуваним результатом реалізації Стратегії є забезпечення захищеного інформаційного простору в Україні, включаючи ефективну протидію незаконному контенту, сприяння створенню ефективної системи стратегічних комунікацій та суттєвому підвищенню медіакультури та медіаграмотності населення. Втім, відповідний розділ стратегії містить лише загальні визначення бажаного стану при імплементації Стратегії. Більш детальний опис стану справ у сфері інформаційної безпеки, певні кількісні та якісні показники могли б кращим чином розкрити питання, як виміряти ефективність впровадження цієї Стратегії [16].

Проаналізувавши пропоновані науковцями напрями удосконалення державної політики у сфері інформаційної безпеки, розуміємо, що проблема

гарантування інформаційної безпеки держави, суспільства та особистості має комплексний характер і для її розв'язання потрібна ефективна державна політика, спрямована на системне об'єднання на державному рівні законодавчих, організаційних та програмно-технічних засобів. Створення потужної та ефективної системи інформаційної безпеки України, а також розроблення дієвих стратегій реалізація існуючої повинні стати пріоритетними завданнями органів державної влади та недержавних інститутів.

Для забезпечення ефективності і результативності формування та реалізації державної політики у сфері інформаційної безпеки України потрібно комплексно використовувати інструменти правового, економічного, фінансового, організаційного, інформаційного, освітнього характеру. Інструменти та механізми, що застосовуються у сфері фінансово-економічного забезпечення мають враховувати довгострокове бюджетне планування, здійснювати аналіз бюджетних запитів розпорядників бюджетних коштів із залученням органів влади в процесі підготовки проекту державного бюджету України на поточний рік тощо; у сфері інституційного забезпечення: запроваджувати електронне урядування та системи документообігу; надавати державну підтримку програм та проектів стосовно національної безпеки і оборони України, узгоджувати стратегічні плани з цілями та напрямами державної політики, продовжувати курс України до членства в Євроатлантичному Альянсі.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

У випускній кваліфікаційній роботі досліджено сучасний стан та тенденції розвитку інформаційної безпеки в Україні. Проаналізовано фактори впливу на забезпечення інформаційної безпеки в Україні та охарактеризовано особливості інформаційної безпеки в умовах поширення пандемії COVID-19 та сформульовано пропозиції щодо напрямів удосконалення державної політики у сфері інформаційної безпеки.

Результати проведеного дослідження стану інформаційної безпеки в Україні та розробка пропозицій щодо напрямків удосконалення державної політики у сфері інформаційної безпеки в Україні, дозволили відповідно до мети та завдань зробити такі висновки та узагальнення.

1. Розглянувши сучасний стан та тенденції розвитку інформаційної безпеки в Україні, приходимо до висновку, що інформаційна безпека є комплексною категорією, яка включає внутрішньо- та зовнішньополітичні, економічні, технологічні, військові та інші елементи. Система інформаційної безпеки входить до загальної системи національної безпеки держави і її ефективне функціонування врегульоване низкою нормативно-правових актів. Діяльність держави в особі органів державної влади, громадських організацій, засобів масової інформації та громадян, які координують свої дії по здійсненню діяльності у сфері інформаційної безпеки на основі єдиних правових стандартів має бути спрямована на ефективну протидію інформаційним загрозам в сучасних умовах.

2. Проаналізувавши основні фактори впливу на забезпечення інформаційної безпеки в Україні розуміємо, що ключовим залишається стратегічне інформаційне протистояння яке є небезпечним компонентом гібридної війни, розгорнутої РФ проти України, причому головна загроза інформаційній безпеці нашої держави є можливість впливу ворога на інформаційну інфраструктуру, інформаційні ресурси, на суспільство, свідомість і підсвідомість особистості заради

нав'язування власної системи цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності.

3. Аналіз стану інформаційної безпеки в умовах поширення пандемії COVID-19 дозволяє стверджувати, що пандемія COVID-19 стала найбільшим викликом для людства за останні десятиліття. Її руйнівний вплив поширився на всі сфери суспільства.

Визначено проблеми реалізації державної політики у сфері інформаційної безпеки, що виникли через поширення COVID-19. Проаналізовано заходи політики, які застосовуються для боротьби з поширенням COVID-19 та підтримки систем охорони здоров'я в Україні та світі. Досліджено основні інформаційні загрози у сфері національної безпеки, що пов'язані з поширенням COVID-19, такі як: зростання правопорушень в сфері кіберзлочинності.

Визначено, що ще однією загрозою, яка пов'язана із застосуванням карантинних заходів COVID-19, є витік персональних даних громадян, які перебувають на лікуванні, карантині або самоізоляції. Також, наголошено, що держава зобов'язана забезпечувати достовірне інформування суспільства про COVID-19. Враховуючи періодичність виникнення нових пандемій, необхідно створити оптимальний механізм захисту національної інформаційної безпеки вже зараз, оскільки невідомі як наслідки пандемії COVID-19, що триває, так і наслідки майбутніх захворювань.

4. Для забезпечення ефективності і результативності формування та реалізації державної політики інформаційної безпеки України потрібно комплексно використовувати інструменти правового, економічного, фінансового, організаційного, інформаційного, освітнього характеру.

Основні напрямки удосконалення державної політики у сфері інформаційної безпеки України:

– розробка критеріїв та методів оцінки ефективності систем захисту інформаційної безпеки держави;

– ідентифікація та попередження появи дестабілізуючих чинників та інформаційних загроз, проведення їх моніторингу;

– організація проведення фундаментальних та прикладних наукових досліджень в галузі забезпечення інформаційної безпеки;

– розробка та прийняття відповідних нормативно правових актів;

– впровадження єдиної системи ліцензування та сертифікації в даній сфері;

– протистояння загрозі інформаційної війни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України від 28 червня 1996 р. URL: http://zakon5.rada.gov.ua/laws/show/254к/96-вр.

2. Кодекс України про адміністративні правопорушення від 07 грудня 1988 р. № 80731-10. URL: http://zakon2.rada.gov.ua/laws/show/ 80731-10.

3. Митний кодекс України від 13 березня 2012 р. № 4495-VI URL: https://zakon.rada.gov.ua/laws/show/4495-17#Text

4. Податковий кодекс України від 2 грудня 2010 р. № 2755-VI URL: https://zakon.rada.gov.ua/laws/show/2755-17#Text

5. Цивільний кодекс України від 16.01.2003 № 435-IV URL: https://zakon.rada.gov.ua/laws/show/435-15#Text.

6. Про державну таємницю: Закон України від 21 січня 1994 р. № 3855-XII. URL: http://zakon.rada.gov.ua/laws/show/3855-12.

7. Про доступ до публічної інформації: Закон України від 13 січня 2011 р. № 2939-VI. URL: http://zakon.rada.gov.ua/laws/show/2939-17.

8. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16 листопада 1992 р. № 2782-XII. URL: http://zakon. rada.gov.ua/ laws/show/2782-12.

9. Про захист персональних даних: Закон України від 1 червня 2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#top

10. Про інформацію: Закон України від 02 жовтня 1992 р. № 2657-XII. URL: http://zakon.rada.gov.ua/laws/show/2657-12.

11. Про Кабінет Міністрів України: Закон України від 27 лютого 2014 р. № 794-18. URL: http://zakon2.rada.gov.ua/laws/show/794-18.

12. Про Концепцію Національної програми інформатизації: Закон України від 04 лютого 1998 р. № 75/98-ВР. URL: http://zakon.rada. gov.ua/laws/ show/75/98-%D0%B2%D1%80.

13. Про національну безпеку України: Закон України від 21 червня 2018 р. № 2469-VIII. URL: http://zakon.rada.gov.ua/laws/ show/2469-19#n355.

14. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.: Закон України від 09 січня 2007 р. № 537-V. URL: http://zakon.rada.gov.ua/laws/show/537-16?find=1&text=%E1%E5%E7%E.

15. Про телебачення і радіомовлення: Закон України від 21 грудня 1993 р. № 3759-XII. URL: http://zakon.rada.gov.ua/laws/show/3759-12.

16. Стратегія інформаційної безпеки України: затверджено Указом Президента України від 28 грудня 2021 р. №685/2021 URL: https://www.president.gov.ua/documents/6852021-41069

17. Стратегія національної безпеки України: указ Президента України від 14 вересня 2020 року № 392/2020 URL: https://www.president.gov.ua/documents/3922020-35037

18. Стратегія розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України від 15 травня 2013 р. № 386-р URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text

19. Антонов В.О. Конституційно-правові засади національної безпеки України: монографія / В. О. Антонов; наук. ред. Ю.С. Шемшученко. Київ: ТАЛКОМ, 2017. 576 с.

20. Беззубов Д.О. Проблеми теорії публічного адміністрування в сфері забезпечення національної безпеки. Наукові записки. Серія «Право». 2018. Вип. 5. С. 45–49.

21. 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.

22. Бойко В. О. Залучення громадськості до вирішення питань цифровізації та кібербезпекової політики. Аналітична записка. URL:

https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/zaluchennya-gromadskosti-do-virishennya-pitan-cifrovizacii-ta.

23. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики: Вибр. наук. праці К.: НІСД, 2016. 528 с.

24. Войціховський А.В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. Журнал східноєвропейського права. 2018. № 53. С. 26–37.

25. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення URL: http://www.visnyk.academy. gov.ua/wpcontent/uploads/2015/04/20.pdf/

26. Горбулін В.П., Данюк Ю.Г. Національна безпека України: фокус пріоритетів в умовах пандемії // Вісник національної академії наук України. 2020. № 5. С. 3-18.

27. Гуржій Т. Інформаційне право: виклики гібридної війни. Зовнішня торгівля: економіка, фінанси, право. 2018. № 4. С. 16–26.

28. Державна політика забезпечення національної безпеки України: основні напрямки та особливості здійснення.: монографія / Криштанович М.Ф., Пушак Я.Я., Флейчук М.І., Франчук В.І. Львів: Сполом, 2020. 418 с.

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

30. Джерела інформації, медіаграмотність і російська пропаганда: результати всеукраїнського опитування громадської думки. URL: https://detector.media/infospace/article/164308/2019-03-21-dzherela-informatsii-mediagramotnist-i-rosiyska-propaganda-rezultaty-vseukrainskogo-opytuvannya-gromadskoi-dumky/.

31. Експертне опитування проведене Центром Разумкова з 17 по 28 листопада 2020 р. URL: https://razumkov.org.ua/vydannia/zhurnal-natsionalna-bezpeka-i-oborona?showall=1

32. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам / Уляна Ільницька // Політичні науки. 2016. № 1. С.27-32.

33. Інститут інформаційного суспільства. Інтернет-платформа. URL: http://e-ukraine.org.ua.

34. Зозуля О.С. Періодизація розбудови системи державного управління забезпеченням інформаційної безпеки України. Інвестиції: практика та досвід. К., 2016. №8. С. 106-114.

35. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

36. Золотухін Д. Ю. Біла книга спеціальних інформаційних операцій проти України. За підтримки Міністерства інформаційної політики України 2014-2018. К., 2018. 384 с.

37. Калініна А.В. Вплив світової пандемії коронавірусу на стан злочинності. Держава і злочинність. Нові виклики в епоху постмодерну: збірник тез доп. наук.-практ. конф. / МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНАДУ 2020. С. 36-38.

38. Кобко Є.В. Моніторринг загроз наувональної безпеці держави: зарубіжний досвід та українські реалії // Науковий вісник Національної академії внутрішніх справ. 2018. № 1 (106). С.123-134.

39. Косогов О.М., Сірик А.О. Завдання захисту національного інформаційного простору за досвідом ведення гібридної війни РФ на Сході України. Системи озброєння і військова техніка. 2017. С. 38–41.

40. 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.

41. Офіційний сайт Міністерства культури та інформаційної політики. Презентовано Центр стратегічних комунікацій та інформаційної безпеки. URL: https://mkip.gov.ua/news/5234.html

42. Офіційний сайт Служби безпеки України. URL: https://ssu.gov.ua/.

43. Пасічник В. Російський фактор як загроза національній безпеці України // Матеріали міжнародної конференції "Політична праксеологія: безпека, технології, комунікації" / за ред. В. Бебика. К.: ВАПН, 2016. 117 с.

44. Платоненко А. В. Сучасні загрози інформаційної безпеки для державних та приватних установ України. Сучасний захист інформації. 2015. № 4. С. 86-90.

45. Рябоконь О. Державна інформаційна політика формування інформаційного суспільства: зарубіжний досвід / О. Рябоконь // Наукові праці Національної бібліотеки України імені В. І. Вернадського. 2016. Вип. 43. С. 97-114. URL: http://nbuv.gov.ua/UJRN/npnbuimviv_2016_43_9.

46. СБУ притягає до відповідальності осіб, які поширюють фейки про коронавірус // Служба безпеки України : офіц. сайт. URL: https://ssu.gov.ua/-novyny/7300 (дата звернення: 01.02.2021).

47. Стратегія кібербезпеки України на 2021-2025 рр.: указ Президента України від 26 серпня 2021 р. № 447/2021 URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

48. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз Т. Ткачук // Інформаційне право. 2017. № 10. С.182-186.

49. Циганов В.П. Політична безпека і безпечна політика: складові, ознаки, стан, тенденції.К.: Ніка центр, 2018. 112 с.

50. Як змінились уподобання та інтереси українців до засобів масової інформації після виборів 2019р. та початку пандемії COVID-19 (серпень 2020р.). URL: https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/yak-zminylys-upodobannia-ta-interesy-ukraintsiv-do-zasobiv-masovoi-informatsii-pislia-vyboriv-2019r-ta-pochatku-pandemii-covid19-serpen-2020r

51. Code of Practice on Disinformation // European Commission : сайт. 18.01.2021. URL: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation (дата звернення: 01.12.2021).

52. Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Action Plan against Disinformation. Brussels, 05.12.2018. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56166 (дата звернення: 01.02.2021).

53. Action Plan against Disinformation. Joint Communication To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions. URL: https://ec.europa.eu/newsroom/dae/document. cfm?doc id=56166 (дата звернення: 28.12.2021).

54. Olavsrud T. Information security threats that will dominate 2017. CIO (December 29, 2016) URL: https:// cio.com/article/ 3153706/security/4-information-security-threats-thatwill-dominate-2017.html.

55. Savich, A.C. (2018), "European programs for the formation of the EU information space", Problems of international relations, available at: http://vmv.kymu.edu.ua/v/p09/12.pdf (Accessed 20 December 2021).

56. Staying Safe During COVID-19: What You Need to Know // Europol : сайт. 12.11.2020. URL: https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know (дата звернення: 01.12.2021).

57. Zolotar O. System prawnej ochrony bezpieczeństwa informacyjnego Ukrainy // Rocznik Towarzystwa Naukowego Płockiego. 2017. S. 687-702.

Київський національний торговельно-економічний університет
Кафедра публічного управління та адміністрування

РЕФЕРАТ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на тему:

«ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Студента 5 курсу, 7 групи,
спеціальності 074 «Публічне управління та адміністрування»
спеціалізації «Публічне управління та адміністрування» Мажари Романа Володимировича

_____
(підпис студента)

Науковий керівник
к.держ.упр. Динник Ірина Петрівна

_____
(підпис керівника)

Гарант освітньої програми
канд. екон. наук,
доцент Головня Юлія Ігорівна

_____
(підпис гаранта)

Київ 2022

Випускна кваліфікаційна робота складається зі вступу, двох розділів, висновків та списку використаних джерел. Повний обсяг роботи становить 46 сторінки, з них 35 сторінок основного тексту. Робота включає 3 таблиці та 1 рисунок. Список використаних джерел налічує 57 найменувань.

Метою роботи є обґрунтування й розробка пропозицій щодо напрямів удосконалення державної політики у сфері інформаційної безпеки.

Поставлена мета зумовила необхідність вирішення таких дослідницьких завдань:

- розглянути сучасний стан та тенденції розвитку інформаційної безпеки в Україні;

- проаналізувати фактори впливу на забезпечення інформаційної безпеки в Україні;

- охарактеризувати особливості інформаційної безпеки в умовах поширення пандемії COVID-19;

- сформулювати пропозиції щодо напрямів удосконалення державної політики у сфері інформаційної безпеки.

Об’єктом дослідження є суспільні відносини, які виникають у процесі державної політики у сфері інформаційної безпеки.

Предметом дослідження є теоретико-методичні та прикладні основи державної політики у сфері інформаційної безпеки.

Для вирішення визначених завдань, у процесі дослідження використано загальнонаукові та спеціальні методи дослідження: аналітичний, описовий, структурного аналізу, виокремлення статистичних даних, порівняння, узагальнення, аналогія.

У першому розділі проведено аналіз сучасного стану та аналіз факторів впливу на забезпечення інформаційної безпеки в Україні у процесі якого зроблено висновок щодо правового регулювання державної інформаційної політики у сфері національної безпеки.

У другому розділі розглянуто шляхи та напрямки вдосконалення державної політики у сфері інформаційної безпеки. Зроблено висновок щодо ефективності та результативності реалізації державної політики у сфері інформаційної безпеки потрібно комплексно використовувати інструменти правового, економічного, фінансового, інформаційного характеру.

Одержані результати дослідження знайшла своє відображення в конкретних пропозиціях, спрямованих на удосконалення державної політики у сфері інформаційної безпеки.

АНОТАЦІЯ

У випускній кваліфікаційній роботі обґрунтовано й розроблено пропозиції щодо напрямів удосконалення державної політики у сфері інформаційної безпеки.

Проаналізовано сучасний стан та фактори впливу на забезпечення інформаційної безпеки в Україні. Визначено проблеми реалізації державної політики у сфері інформаційної безпеки, що виникли через поширення COVID-19. Досліджено основні інформаційні загрози у сфері національної безпеки, що пов'язані з пандемією, такі як, зростання правопорушень в сфері кіберзлочинності. Надано пропозиції щодо удосконалення державної політики у сфері інформаційної безпеки.

Ключові слова: державна політика, інформаційна безпека, національна безпека, кібербезпека, інформація.

SUMMARY

In the final qualification work the proposals on the directions of improvement of the state policy in the field of information security are substantiated and developed.

The current state and factors influencing the provision of information security in Ukraine are analyzed. The problems of realization of the state policy in the field of information security which have arisen because of distribution of COVID-19 are

defined. The main information threats in the field of national security related to the pandemic, such as the growth of cybercrime offenses, have been studied. Suggestions for improving the state policy in the field of information security are given.

Key words: public policy, information security, national security, cybersecurity, information.

РЕЦЕНЗІЯ

на випускну кваліфікаційну роботу студента 5-го курсу
7 групи заочної форми навчання освітнього ступеня "бакалавр"
спеціальності 074 "Публічне управління та адміністрування"
Київського національного торговельно-економічного університету
Мажари Романа Володимировича
на тему: **"Державна політика у сфері інформаційної безпеки"**

Актуальність обраної теми полягає в тому, що тенденції до збільшення відкритості суспільства, масове використання інформаційно-комунікаційних технологій створили передумови для потенційних протиправних дій стосовно інформації, тих хто її використовує та інформаційних систем зв'язку, що має наслідком зниження рівня забезпечення інформаційної безпеки держави.

Інформаційна безпека є невід'ємною складовою у забезпеченні національної безпеки держави, а створення розвинутого та захищеного середовища – основна умова розвитку суспільства та конкурентоспроможної держави. Ефективна система заходів по забезпеченню інформаційної безпеки громадян, суспільства та держави дозволить своєчасно попереджувати та виявляти усі потенційні та реальні загрози національним інтересам і запобігати збиткам в соціально-економічній сфері. Гостроти цій проблематиці додає також те, що інформаційна складова частина є об'єктом маніпулювання за умов гібридної війни яка ведеться Російською Федерацією проти України, адже складна політична ситуація, в якій вона Україна протягом останніх восьми років, постійне погіршення іміджу держави на міжнародній арені, обумовлюється низкою факторів, серед яких важливим є неналежний стан системи інформаційної безпеки.

В роботі розглянуто сучасний стан та тенденції розвитку інформаційної безпеки в Україні; проаналізовано фактори впливу на забезпечення інформаційної безпеки в Україні; охарактеризовано особливості інформаційної безпеки в умовах поширення пандемії COVID-19; сформульовано пропозиції щодо напрямів удосконалення державної політики у сфері інформаційної безпеки.

Тема широко розкрита, особливо детально проаналізовано фактори впливу на забезпечення інформаційної безпеки в Україні. Автор констатує, що особливу групу важливих для України загроз інформаційній безпеці становлять загрози, пов'язані з віртуалізацією – соціальним відчуженням людини, зміненими станами свідомості, перехід до персонального віртуального світу. З прискореними темпами інформаційного прогресу і особливо з розвитком Інтернету речей люди зазвичай ризикують стати додатком до технологій та інформаційних ресурсів.

Поряд із загальною позитивною оцінкою необхідно звернути увагу на наступне: графічне або схематичне представлення окремих підсумкових положень могли б значно посилити та унаочнити основні наукові результати, які студентом виносяться на захист.

Варто додатково перевірити коректність посилання на джерела. Разом з тим вважаємо, що висловлені зауваження не применшують наукового значення та цінності роботи і мають рекомендаційний характер.

Випускна кваліфікаційна робота Мажари Романа Володимировича за змістом та оформленням відповідає поставленим вимогам, мета та завдання розкриті.

Враховуючи вищевикладене випускна кваліфікаційна робота рекомендується до захисту та заслуговує на позитивну оцінку.

Рецензент,
к.держ.упр.,
начальник відділу аспірантури
Інституту підготовки наукових кадрів
ПрАТ «Вищий навчальний заклад
«Міжрегіональна академія управління персоналом» Щур Н.О.

ВІДДІЛ УПРАВЛІННЯ ПЕРСОНАЛОМ
Ідентифікаційний код 00127522

Приватне акціонерне товариство «Вищий навчальний заклад «Міжрегіональна академія управління персоналом»
Власноручний підпис Щур Н. О.
СТВЕРДЖУЮ
Відділ управління персоналом
«20» січня 2022
Підпис

Завідувачу кафедри публічного управління та адміністрування Новіковій Н.Л.

Заява

Я, Мажара Роман Володимирович (ПІБ), повідомляю, що за результатами проведення самостійної перевірки з використанням програмно-технічних засобів у наданій випускній кваліфікаційній роботі на тему: «Державна політика у сфері інформаційної безпеки» 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.

«24» січня 2022 року _____ (підпис)

Згода

Я, Мажора Роман Володимирович,

цим засвідчую, що є автором випускної кваліфікаційної роботи на тему: "Державна політика у сфері інформаційної безпеки" несу повну відповідальність за достовірність, точність та повноту поданої у роботі інформації, жодна частина роботи не була скопійована, за винятком випадків, коли робиться належне підтвердження в присвоєнні. Я підтверджую, що у роботі не міститься державної таємниці або інформації для службового користування.

Цим засвідчую, що жодна частина цієї роботи не була опублікована мною раніше.

Я даю дозвіл на те, що моя робота буде направлена в інституційний депозитарій Київського національного торговельно-економічного університету і збережена в базі даних для майбутньої перевірки плагіату.

« 24 » січня 2022 року

Підпис

(Мажора Р. В.)

Прізвище, ініціали