МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет права, публічного управління та національної безпеки
Кафедра економічної теорії, інтелектуальної власності та публічного управління

Кваліфікаційна робота
на правах рукопису

ГУМЕНЮК ДЕНИС МИКОЛАЙОВИЧ
(прізвище, ім'я, по батькові здобувача вищої освіти)

УДК: 351.77.614
(індекс)

КВАЛІФІКАЦІЙНА РОБОТА

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА РЕГІОНАЛЬНОМУ РІВНІ: ДОСВІД УКРАЇНИ ТА ЗАРУБІЖНИХ КРАЇН

(тема роботи)

281 «Публічне управління та адміністрування»
(шифр і назва спеціальності)

Подається на здобуття освітнього ступеня магістр кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Д. М. ГУМЕНЮК
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи
СКИДАН Олег Васильович
(прізвище, ім'я, по батькові)

доктор економічних наук, професор
(науковий ступінь, вчене звання)

Житомир – 2024

Висновок кафедри економічної теорії, інтелектуальної власності та публічного управління
за результатами попереднього захисту: **ГУМЕНЮКА Дениса Миколайовича** допущено до захисту.

Протокол засідання кафедри економічної теорії, інтелектуальної власності та публічного управління № ____ від «____» грудня 2024 р.

Завідувач кафедри економічної теорії, інтелектуальної власності та публічного управління

к.е.н., професор _____ Валентина ЯКОБЧУК
(науковий ступінь, вчене звання) (підпис) (власне ім'я, прізвище)

«___» грудня 2024 р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти **ГУМЕНЮК Денис Миколайович** захистив
(прізвище ,ім'я, по батькові)

кваліфікаційну роботу з оцінкою:
сума балів за 100-бальною шкалою _____
за національною шкалою _____

Секретар ЕК
_____-____ _____ Анастасія ПРУТ
(науковий ступінь, вчене звання) (підпис) (власне ім'я, прізвище)

АНОТАЦІЯ

ГУМЕНЮК Д. М. Забезпечення інформаційної безпеки на регіональному рівні: досвід України та зарубіжних країн. – Кваліфікаційна робота на правах рукопису. Кваліфікаційна робота на здобуття освітнього ступеня магістра за спеціальністю 281 – Публічне управління та адміністрування. – Поліський національний університет, Житомир, 2024.

Кваліфікаційна робота присвячена аналізу та вдосконаленню політики забезпечення інформаційної безпеки України у контексті російської агресії. У дослідженні визначено основні виклики інформаційній безпеці України, зокрема загрози дезінформації, кібератак і пропаганди, які виникають у гібридній війні. Особлива увага приділяється механізмам протидії цим загрозам, що включають нормативно-правові, технічні та організаційні аспекти.

На основі аналізу зарубіжного досвіду, таких країн, як Естонія, США та Великобританія, розроблено рекомендації для покращення системи кібербезпеки в Україні. Робота акцентує на важливості міжнародної співпраці, адаптації українського законодавства до європейських стандартів (наприклад, GDPR), а також підвищенні обізнаності населення про кіберзагрози. У роботі підкреслюється значення формування позитивного іміджу України як інструменту інформаційної дипломатії.

Запропоновані напрями включають розбудову кіберінфраструктури, розвиток національних центрів кіберзахисту та посилення інформаційного суверенітету України. Практична цінність роботи полягає у формуванні цілісного підходу до забезпечення інформаційної безпеки, який може бути інтегрований у державну політику для підвищення стійкості країни до сучасних викликів.

Ключові слова: інформаційна безпека, кібератаки, російська агресія, дезінформація, гібридна війна, інформаційний суверенітет, кібербезпека, нормативно-правова база, міжнародна співпраця, інформаційна політика.

SUMMARY

HUMENIUK D. Ensuring information security at the regional level: experience of ukraine and foreign countries**.** Qualification work on the rights of the manuscript. Qualification work for obtaining a master's degree in specialty 281 «Public management and administration» – Polissia National University, Zhytomyr, 2024.

The qualification thesis is dedicated to analyzing and improving Ukraine's information security policy in the context of Russian aggression. The study identifies key challenges to Ukraine's information security, including threats of disinformation, cyberattacks, and propaganda arising in hybrid warfare. Special attention is paid to countermeasures against these threats, encompassing legal, technical, and organizational aspects.

Based on an analysis of international experience in countries such as Estonia, the USA, and the UK, recommendations are developed to enhance Ukraine's cybersecurity system. The work emphasizes the importance of international cooperation, adapting Ukrainian legislation to European standards (e.g., GDPR), and raising public awareness about cyber threats. The significance of shaping Ukraine's positive image as an instrument of information diplomacy is also highlighted.

The proposed directions include the development of cyber infrastructure, the establishment of national cybersecurity centers, and the strengthening of Ukraine's information sovereignty. The practical value of the study lies in forming a comprehensive approach to ensuring information security that can be integrated into state policy to enhance the country's resilience to modern challenges.

Keywords: information security, cyberattacks, Russian aggression, disinformation, hybrid warfare, information sovereignty, cybersecurity, regulatory framework, international cooperation, information policy.

ЗМІСТ

ВСТУП

Актуальність дослідження. Стратегічне планування і прогнозування інформаційної політики безпеки країни стали важливими завданнями в умовах російсько-української війни. Ураховуючи прогалини в нормативно-правовій базі, актуально розробити довгострокові стратегії забезпечення ефективного та дієвого захисту національного інформаційного простору і інформаційного суверенітету. Це вимагає аналіз щоденних тенденцій, прогнозування потенційних загроз та визначення пріоритетів реалізації заходів інформаційної безпеки. Крім цього, необхідний системний підхід щодо розробки політики, беручи до уваги співпрацю з міжнародними партнерами, такими як Європейський Союз і НАТО, для розробки спільних стратегій і координації дій. Це сприятиме зміцненню інформаційної безпеки України, збереженню та забезпеченню її національної ідентичності як незалежної суверенної держави.

За умов збройного конфлікту органи публічної влади та ОМС мають високий ступінь інформаційної взаємодії з суспільством. Міністерства та відомства систематично та належним чином надають громадськості найсвіжішу інформацію. Офіційні виступи Президента України та голів регіональних військових адміністрацій, мають бути присвячені аналізу ситуації та висвітленню виконаної роботи, є звичайним явищем для громадян.

Важливим аспектом зовнішньої комунікації є формування іміджу України. Зміцнення позитивного іміджу України всередині і за кордоном має велике значення для перспектив економічного, політичного і культурного розвитку країни. Успіх у зміцненні іміджу держави визначається ефективністю відповідної інформаційної діяльності. Особливу роль в іміджевій політиці відіграють органи, що відповідають за зв'язки з громадськістю, ЗМІ та інші структури публічного суспільства.

Метою наукового дослідження: визначення напрямів удосконалення політики інформаційної безпеки України в умовах російської агресії

Для досягнення заявленої мети було поставлено *наступні завдання*:

- вивчити теоретичні та концептуальні аспекти інформаційної безпеки України;
- проаналізувати сучасний стану формування та забезпечення інформаційної безпеки;
- запропонувати напрями удосконалення політика забезпечення інформаційної безпеки України в контексті російської агресії.

Об'єктом дослідження: є *с*истема забезпечення інформаційної безпеки України.

Предмет дослідження: нормативно-правові, технічні та організаційні механізми протидії інформаційним загрозам у контексті російської агресії.

Методи наукового дослідження: аналіз нормативно-правової бази (з метою вивчення чинного законодавства України у сфері інформаційної безпеки, зокрема аналізу таких документів, як Стратегія інформаційної безпеки України та Закон «Про національну безпеку України»); порівняльний аналіз міжнародного досвіду **(**проведено аналізу практик забезпечення інформаційної безпеки в інших країнах (Естонія, США, Великобританія)); системний підхід (дозволив вивчити інформаційну безпеку як цілісну систему, що включає правові, технічні та організаційні компоненти. Метод допоміг інтегрувати різні аспекти забезпечення безпеки в єдину модель); синтез рекомендацій (для формування практичних пропозицій щодо вдосконалення політики інформаційної безпеки. На основі зібраних даних та результатів аналізу були розроблені рекомендації для підвищення стійкості інформаційного простору України); моніторинг та узагальнення фактів (для виявлення ключових загроз, таких як кібератаки, дезінформація та пропаганда. Цей метод дозволив систематизувати актуальну інформацію про стан інформаційної безпеки в Україні).

Перелік публікацій автора за темою дослідження. За темою дослідження опубліковано три тези в збірниках науково-практичних конференцій Поліського національного університету.

Елементи наукової новизни: Систематизовано загрози інформаційній

безпеці в умовах гібридної війни. Запропоновано модель кіберзахисту, яка інтегрує міжнародний досвід і національні особливості. Розроблено рекомендації щодо нормативно-правового вдосконалення політики інформаційної безпеки.

*Практичне значення дослідження: р*езультати можуть бути використані в розробці державної стратегії інформаційної безпеки, вдосконаленні законодавства, навчанні фахівців з кібербезпеки та підвищенні обізнаності населення.

Структура та обсяг дослідження. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел, додатків. Повний обсяг роботи складає 46 сторінок, список використаних джерел налічує 45 найменувань.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ ТА КОНЦЕПТУАЛЬНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

1.1. Основний концептуальний підхід до визначення поняття «д інформаційна безпека держави»

В даний час необхідно терміново вирішити проблеми інформаційної безпеки, оскільки державі потрібно інтегруватися в глобалізоване інформаційне суспільство та забезпечувати його ефективне функціонування в інформаційній сфері. Дуже часто проблема пов'язана з неефективністю політики інформаційної безпеки органів державної влади та необхідністю перегляду застосування догматичних норм [6]. Тому розуміння і визначення поняття «державна інформаційна безпека» вкрай важливо для розробки ефективних стратегій і заходів щодо забезпечення їх безпеки.

Розуміння та сучасна інтерпретація терміну «інформаційна безпека» надзвичайно важливі для розуміння сутності поняття інформаційної безпеки в сучасному контексті та розробки стратегічних рішень для забезпечення її безпеки. Приклади інтерпретації концепції відповідно до національних даних: Лібік Т. (2020) вказує на наявність системи заходів інформаційної безпеки, спрямованих на захист та охорону інформації від незаконного доступу, збереження її конфіденційності, цілісності та доступності. Це значить, що інформаційна безпека захищає інформаційні ресурси та запобігає потенційним загрозам [16].

Вербицький О. (2017) аналізує інформаційну безпеку як цілісну систему заходів, що включає організаційні, технічні та правові заходи. Науковець зазначає, що інформаційна безпека пов'язана із безпосереднім захистом інформаційних систем, а також з організаційними заходами і правилами, що спрямовані на забезпечення безпеки в інформаційній сфері [9].

Смірнова Е. (2019) висвітлює аспект криптографічного захисту в значенні

забезпечення інформаційної безпеки. Згідно до її досліджень, інформаційна безпека передбачає використання методів і технологій шифрування для захисту конфіденційності, доступності та цілісності інформації [37].

Вивчення різних підходів до обґрунтування значення терміну «інформаційна безпека» відкриває великий концептуальний розмах для подальшого осмислення ролі цього поняття в контексті національної безпеки. Розуміння інформаційної безпеки держави носить багатоплановий характер та вимагає окремого розгляду, оскільки враховує особливості постійно мінливого інформаційно-комунікаційного навколишнього середовища, якому притаманна постійна зміна.

Розглянемо основоположні концептуальні підходи до визначення терміну «інформаційна безпека держави». На нашу думку, це дозволить зрозуміти різноманіття підходів до інформаційної безпеки та управління нею, що важливо для розробки ефективних стратегій захисту інформації в її сучасному розумінні та забезпечення стійкого та сталого розвитку держави в сучасному інформаційному середовищі.

Актуальні концептуальні підходи щодо визначення терміну «державна інформаційна безпека» приймають: концепція цілісності (єдності) інформаційного простору: при такому підході інформаційна безпека країни має бути гарантією недоторканного та цілісного (єдиного) інформаційного простору України. Це має на меті захист від шкідливого несанкціонованого (хакерського) доступу до інформації, її розповсюдження та модифікації, а також доступність та надійність інформаційних систем [17]; сучасна концепція національної безпеки: цей підхід розглядає інформаційну безпеку держави як один з ключових компонентів загальної національної безпеки. Цей підхід розглядає інформаційну безпеку в контексті захисту уіх національних інтересів, суверенітету і безпеки держави в області інформаційно-комунікаційних технологій [36]; концепція ризиків і загроз: в даному підході інформаційна безпека держави аналізується як захист від ризиків і загроз, що пов'язані з використанням інформаційних технологій. Вона зосереджена на виявленні,

оцінці та управлінні ризиками, що можуть вплинути на інформаційну безпеку країни [13].

Таким чином, інформаційна безпека держави в розумінні Іванової О. – це складна багаторівнева система заходів, спрямованих на захист всіх існуючих інформаційних ресурсів держави від всіх можливих загроз з боку ворожих суб'єктів, сучасних технологічних викликів та інших ризиків [11]. Окремі дослідники наголошують на необхідності та важливості комплексного підходу до інформаційної безпеки, що охоплює технічні, адміністративно-організаційні, правові та соціальні аспекти [4]. Поняття «інформаційна безпека держави» можна відобразити ту вигляді наступної структури, показану на рис. 1.1.

Рис. 1.1. Структура підходів до визначення сучасного значення терміну «інформаційна безпека держави»

Джерело: [4].

Питання інформаційної безпеки урядів пов'язані з євроінтегацією та глобалізацією і подальшим розвитком інформаційних і комунікаційних технологій. Сучасні дослідники вважають, що сучасна країна повинна бути готова до сучасних викликів цифрової епохи та враховувати вплив інформації на безпеку. Дане визначення включає не лише захист інформації, а й розробку

відповідних стратегій, концепцій, політики, законів та нормативно-правових норм [19].

Варто зробити висновок, що розуміння терміну інформаційної безпеки держави можна вважати предметом постійних дискусій, обговорень та подальших наукових досліджень. Різноманітні підходи та інтерпретації концепції відображають складність та складність проблеми. Важливо продовжити дослідження в цій галузі, щоб надалі розвинути концептуальне розуміння інформаційної безпеки держави та розробити ефективні стратегії її забезпечення.

1.2. Види та форми забезпечення інформаційної безпеки держави

Види державної інформаційної безпеки включають в себе широкий спектр заходів, спрямованих на захист інформаційних ресурсів, їх систем і процесів в державному секторі. Ці заходи включають організаційні, технічні, особисті, кадрові та юридичні аспекти, які в сукупності визначають рівень інформаційної безпеки в країні. Найбільш поширеними способами забезпечення сучасної інформаційної безпеки держави є:

Кібернетична безпека включає багато заходів, спрямованих на захист інформаційних систем від різноманітних кіберзагроз. Це підхід має включає розроблення та подальше впровадження новітніх технологій безпеки, які будуть здатні виявляти та запобігати шпіонських та шкідливих програмам, хакерським нападам та крадіжкам особистих та персональних даних. Ось приклади заходів кібербезпеки, що можуть включають в себе: застосування надійних політик безпеки та паролів; брандмауер; шифрування даних; застосування новіших антивірусного програмного забезпечення та системи виявлення можливих вторгнень. Більшість країн та організацій почали активно вдосконалюють свої вже існуючі заходи кібербезпеки з урахуванням постійних змін, щоденного розвитку та удосконалення та характеру і складності існуючих кіберзагроз [21].

Фізична безпека забезпечує заходи щодо безпосереднього захисту фізичного доступу на пряму до інформаційних ресурсів і пристроїв, на яких містяться бази даних та конфіденційна інформація. Це може передбачати: встановлення контролю доступу до комунальних послуг; використання систем відеоспостереження і біометричних ідентифікаторів; додатковий захист серверних кімнат (бронювання, додаткові способи захисту) і центрів обробки даних для унеможливлювання несанкціонованого доступу. Такі додаткові заходи безпеки також можуть включати фізичний захист носіїв (сейфи, паролі), що зберігаються в захищених сховищах або пристроях шифрування (криптографічних пристроїв).

Організаційна безпека повинна включати розробку та подальше впровадження політики, процедур та стандартів для практик безпеки управління інформацією. Це включає в себе: визначити ролі та обов'язки, пов'язані з питаннями безпеки; проводити аудит безпеки для виявлення вразливих місць; встановлювати правила доступу до інформації та забезпечувати її конфіденційність. Такі організаційні заходи можуть включати розробку планів аварійного відновлення та процедур аварійного відновлення після поломок чи хакерських атак.

Безпека персоналу – це вжиття заходів щодо забезпечення збереження інформації про співробітників державних установ і організацій. Це включає в себе наступні напрями: обов’язкова перевірка кваліфікації та надійності найманих працівників, перш ніж надавати їм доступ до конфіденційної інформації; проведення навчань політикам і процедурам безпеки; переконайтеся, що співробітники обізнані про ризики для інформаційної безпеки [18].

Правова безпека включає розробку і застосування законодавства в області забезпечення інформаційної безпеки та кібербезпеки. Це включає в себе: розробку спеціалізованих правових стандартів в області захисту інформації, передбачення кримінальної відповідальності за кіберзлочини і незаконного збору; записування (збереження), публікація та поширення інформації.

Країни також можуть розробити правову базу для роботи з інтернаціональними партнерами в області забезпечення інформаційної безпеки. Типи інформаційної безпеки мають велике значення для захисту інформації та забезпечення стабільності інформаційних систем. Тому, необхідний комплексний підхід, який і поєднує технічні, людські, юридичні, адміністративно-організаційні аспекти, все це і є ключем до ефективної інформаційної безпеки в багатьох країнах, включаючи Україну.

Контентна система, пов'язана з розробкою і реалізацією політики державної безпеки в інформаційній сфері, повинна включати в себе не лише внутрішні (власні) сили, а й міжнародне співробітництво (зовнішні). Більшість країн усвідомлюють важливість міжнародного партнерства у боротьбі з поширенням пропаганди та дезінформації. Одним із прийомів забезпечення ефективності та дієвості сучасних контрзаходів є створення досконалої правової бази з метою подальшої співпраці з міжнародними (зарубіжними) партнерами в сфері успішного забезпеченя інформаційної безпеки.

Рис. 1.2. Формування та впровадження системи питань політики забезпечення державної безпеки в інформаційній сфері

Джерело: [3].

Контентна система – це складна і узгоджена структура для розробки і реалізації публічної політики державної безпеки в інформаційній сфері, яка містить у собі різні організації, інституції, установи, підприємства та громадськість. Основоположними дійовими особами мають бути державні установи, міністерства, департаменти та відомства, спеціальні служби, що повинні відповідати за розробку і подальшу реалізацію стратегій та програм забезпечення інформаційної безпеки. Взаємодія цих сутностей показано на рис. 1.2.

Для забезпечення вищезазначених форм інформаційної безпеки в державі суб’єкти (рис. 1.2) використовується комплексний підхід, який включає наступні підходи, методи та дії [3]:

1) *організаційно-правові заходи*: розробка і впровадження відповідних законів, нормативних актів і правових норм, що регулюють сферу забезпечення інформаційної безпеки держави. Це можуть бути постанови, закони, накази або інструкції, що визначають правила, зобов’язання, обов'язки та відповідальності, пов'язані з інформаційною безпекою;

2) *технічні заходи:* використання різних технологічних рішень та інструментів забезпечення інформаційної безпеки. До них відносяться системи шифрування, системи виявлення вторгнень, брандмауери, контроль доступу до наявних інформаційних ресурсів та використання технічних засобів з метою захисту мереж та інфраструктури організаційної одиниці;

3) *організаційні заходи:* запровадження політики щодо інформаційної безпеки в органах публічного управління та створення належних структур та департаментів, які б координували та контролювали заходи направлені на забезпечення інформаційної безпеки. Сюди входить розробка процедур, нормативних актів, стандартів, проведення тренінгів та тренінгів, організація моніторингу, контролю та тестування інформаційної безпеки;

4) *соціально-психологічна заходи:* проведення заходів з просвітницької роботи, інформаційних кампаній та усвідомлене та ціле направлене формування поведінки і свідомості громадян у сфері забезпечення

інформаційної безпеки. До них відносяться навчання, публічні заходи, тренінг із залучення спеціалістів у цій сфері, семінари, конференції для обміну думками та досвідом, поширення інформації про загрози і захисні заходи, а також залучення громадських організацій і засобів масової інформації до співпраці. Конкретні дії, способи або методи можуть суттєво відрізнятися залежно від умов країни, дипломатичного контексту та рівня розвитку інформаційних технологій [41].

Під час вивчення теоретичних та концептуальних аспектів забезпечення інформаційної безпеки держави вони виявили, що інформаційна безпека є дуже актуальним аспектом сучасних умов існування світу. Він має містити захист інформації та різноманітних новітніх інформаційних систем, з метою збереження та забезпечення охорони від ризиків зловживання, хакерського (несанкціонованого доступу), крадіжки, пошкодження або використання в злочинних цілях.

Інформаційна безпека – це досить складне і різностороннє питання, що потребує синергетичного, комплексного підходу всіх сферх і взаємодії між усіма зацікавленими сторонами (учасників процесу), включаючи державні інститути, приватний сектор та обов’язково громадськість. Для досягнення поставленої мети, а саме забезпечення інформаційної безпеки урядової інформації необхідно обов’язково застосовувати широкий та різноманітний спектр методів і заходів, таких як розроблення або покращення відповідного законодавства, безперервне та послідовне професійне навчання, розвиток кіберзахисту і використання сучасних технологій.

В умовах безперервного та інтенсивного розвитку технологій і загроз держави повинні бути готові до вирішення проблем інформаційної безпеки шляхом активізації своїх дій і міжнародного співробітництва. Це можливо тільки шляхом постійного аналізу та вдосконалення реалізації ефективних стратегій інформаційної безпеки держави та ефективної протидії сучасних загрози і підтримання національної безпеки і стабільності.

ВИСНОВКИ ДО РОЗДІЛУ 1

Інформаційна безпека є ключовою складовою національної безпеки, оскільки вона захищає інформаційні ресурси, забезпечує стабільність функціонування держави в інформаційному середовищі та запобігає потенційним загрозам. Концептуальне розуміння цього терміну залежить від різних підходів, що охоплюють технічні, організаційні, правові та соціальні аспекти. Це дозволяє інтегрувати інформаційну безпеку в загальну стратегію забезпечення стійкості держави.

Основні підходи до забезпечення інформаційної безпеки держави включають концепцію цілісності інформаційного простору, орієнтацію на національну безпеку, а також управління ризиками й загрозами. Кожен із цих підходів спрямований на побудову системи захисту, що охоплює використання сучасних технологій, розробку відповідного законодавства, вдосконалення організаційних процесів та підвищення обізнаності громадськості.

Інформаційна безпека вимагає комплексного підходу, що поєднує кібернетичні, фізичні, організаційні, кадрові та правові заходи. Успішне забезпечення інформаційної безпеки можливе лише через постійний моніторинг, вдосконалення нормативної бази та міжнародне співробітництво. Розуміння важливості цієї сфери та інтеграція всіх необхідних компонентів дозволяють державі ефективно реагувати на виклики сучасного інформаційного середовища.

РОЗДІЛ 2.
АНАЛІЗ СУЧАСНОГО СТАНУ ФОРМУВАННЯ ТА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Характеристика нормативно-правова база забезпечення інформаційної безпеки в Україні

Досягнення оптимального стану Забезпечення інформаційної безпеки України та всіх її громадян є пріоритетом обов'язком і відповідальністю влади. Формування єдиної державної політики у сфері забезпечення інформаційної безпеки вимагає виконання та дотримання усіх конституційних прав та свобод особистості в інформаційній сфері. В той же час з початком повномасштабних військових дій росією на територію України було введено воєнний стан [25], метою якого було створення умов для органів державної влади для адекватного забезпечення безпеки незалежності, суверенітету та територіальної цілісності України [30].

Правову основу забезпечення інформаційної безпеки складають законодавчі, нормативні та розпорядчі акти України про інформаційну безпеку. Розроблено та затверджено відповідно до стратегій, принципів та цілей їх інформаційної політики (тощо). Стратегія інформаційної безпеки. У цитатах, в роботі згадується нормативно-правовий акт, а посилання на предмет знаходиться в списку використаних джерел в позиції 18.

«Забезпечення інформаційної безпеки в Україні одна з найважливіших завдань держави»; «Мета стратегії – нарощування потенціалу щодо забезпечення інформаційної безпеки держави та її існуючого інформаційного простору»; «Інтернаціональні (глобальн) кампанії з дезінформації стали щоденною практикою, що загрожує існуючому демократичному розвитку більшості сучасних держав та безпосередньо міжнародній стабільності»; «Заходи (санкції) спрямовані на обмеження і ефективний та дієвий механізм нагляду і забезпечення обов'язкової відповідальності за порушення в цій сфері

є одним з ефективних механізмів реагування на спотворену діяльність російської федерації як головному агресору»; «Право на недоторканність приватного життя це основне право людини»; «Сліпе сприйняття інформації, не перевіряючи достовірність та актуальність джерела загрожує політичній, правовій та економічній порушенню стабільності демократичних держав»; «Розвідувальне управління російської федерації, як найбільшого агресора та на тимчасово окупованих територіях України»; «Важливими напрямками забезпечення інформаційної безпеки в Україні є стабільність і взаємодія, необхідні для досягнення цих стратегічних цілей»; «Стратегія національної безпеки України» [39]; «З метою зміцнення своїх позицій в Європі росія використовує інформаційну та енергетичну зброю, та намагається чинити вплив на внутрішньополітичну ситуацію в європейських країнах, розпалює затяжні конфлікти і нарощує свою військову присутність на території Східної Європи»; «Подальша деструктивна та неправдива пропаганда ззовні і зсередини України, що експлуатує соціальні протиріччя, провокує військові дії, провокує конфлікти і завдає шкоди соціальній єдності. Відсутність комплексної державної інформаційної політики та слабка система стратегічних комунікацій значно ускладнюють шляхи нейтралізації цієї загрози»; «Основним завданням подальшого розвитку системи кібербезпеки є досягнення кіберстійкості та кібербезпеки загальнонаціональної інформаційної інфраструктури, особливо в контексті цифрової трансформації»; «Захист інформації в сучасних інформаційно-комунікаційних системах» [28].

Публічне регулювання щодо забезпечення необхіного рівня інформаційної безпеки, обумовлене досягненням наступних цілей, чітко сформульованих у нормативному документі «Стратегія інформаційної безпеки» [10]: боротьба з дезінформацією та розвідувальні операції; забезпечити всебічний розвиток української культури та проголошення української громадянської ідентичності; підвищення медіакультури і медіаосвіти в суспільстві; гарантувати повагу прав людини на збір, використання, зберігання та поширення інформації; реінтеграція інформації для громадян України, які

проживають на окупованих і тимчасово суміжних територіях України, в інформаційний простір України; утворення ефективної систему стратегічних комунікацій.

Розвивати інформаційне суспільство і просувати культуру діалогу. У той же час правила охоплюють більш широкий спектр діяльності організації в порівнянні з управлінням. Менеджмент передбачає конкретний вплив на об'єкти управління з використанням методів, що передбачають опис цих цілей управлінського впливу суб'єкта управління. Регулювання стосується не стільки впливу об'єктів контролю, скільки навколишнього середовища [8].

Крім того, існують певні інші закони та нормативні акти, спрямовані на забезпечення інформаційної безпеки. Як-от, Закон України «Про захист персональних даних» [31], в якому було встановлено правила збору, обробки і зберігання персональних даних громадян. Існують також закони, що регулюють захист інформації в різноманітних сферах, таких як банківська справа, комунікації, державна таємниця та інші.

З метою ефективного виконання нормативних і законодавчих актів, спрямованих на забезпечення інформаційної безпеки, створені відповідні структури та органи з нагляду та виконання законодавства. Наприклад, Національне агентство з кібербезпеки, правоохоронні органи, спецслужби та інші організації беруть активну участь у забезпеченні дотримання законів та нормативних актів, що гарантують інформаційну безпеку. Вони проводять розвідувальну діяльність, виявляють загрози і кіберзлочинності, проводять розслідування і вживають заходів для притягнення винних до відповідальності.

Створено механізми постійного моніторингу та оцінювання інформаційної безпеки для ефективного контролю та моніторингу за дотриманням нормативних актів та законів. До них відносяться аудити безпеки, перевірки на наявність вразливостей, аналіз інцидентів і рекомендації щодо поліпшення захисту інформації. Україна також співпрацює з багатьма міжнародними організаціями та партнерами в області забезпечення інформаційної безпеки. Це може включати обмін досвідом, участь в спільних

проєктах і програмах, координація дій по боротьбі з кіберзагрозами і створення спільних механізмів та заходів реагування на них [38].

Уряд нашої країни розуміє, що інформаційна безпека є одним з найважливіших елементів національної безпеки. Тому країна продовжить активну роботу щодо вдосконалення нормативно-правової бази, розвитку кіберзахисту та підвищення обізнаності суспільства про інформаційну безпеку. Тільки завдяки постійному вдосконаленню і узгодженості всіх компонентів він може забезпечити ефективний та дієвий захист інформаційного простору і відповісти на виклики сучасного цифрового світу.

2.2. Принципи та загрози забезпечення інформаційної безпеки в Україні

Принципи забезпечення інформаційної безпеки в Україні [12] – це основні принципи, які встановлюють методи та принципи, які необхідні для ефективного та дієвого захисту інформації в країні. Вони необхідні для забезпечення загальнонаціональної безпеки, підтримки економічного розвитку і підтримки та підвищення довіри до наявних інформаційних систем.

Головними принципами щодо забезпечення інформаційної безпеки в Україні можна вважати: верховенства права; пріоритетності захисту прав та свобод людини та громадянина в сфері інформаційної безпеки; прийняття відповідних і своєчасних заходів щодо захисту життєво важливих національних інтересів України від конкретних і можливих загроз інформаційній безпеці; охорона інформаційного суверенітету; свобода думок і слова, свобода висловлювати свої думки і переконання; свобода збирати, зберігати, оброблювати, використовувати та поширювати інформацію; захист громадянина від будь-якого втручання в його особисте і сімейне життя; певне обмеження доступу до інформації тільки на підставі Закону; гармонізація індивідуальних, суспільних та національних інтересів, відповідальність усього

українського народу щодо забезпечення інформаційної безпеки; розподіл повноважень, взаємодій та обов'язків державних та недержавних суб'єктів щодо забезпечення інформаційної безпеки; приділяти пріоритетну увагу розвитку і поширенню інформаційних технологій, національних ресурсів, продуктів і послуг і розробляти політику постійного вдосконалення каналів передачі інформації з точки зору кількості і технічної якості; можливість використання міжнародних і колективних систем і механізмів безпеки для забезпечення інформаційної безпеки в Україні; захист інформаційного суверенітету, конституційного ладу, державного суверенітету та територіальної цілісності України; привести інформаційне законодавство у відповідність з нормами міжнародного права та актами Європейського Союзу; формування української ідентичності в сучасному інформаційному просторі як важливої складової частини стабільного політично-суспільно дискурсу; створення подвійної системи комерційного та суспільного мовлення; сприяти розвитку в національному медійному просторі матеріалів, що підтримують збереження і захист загальнолюдських цінностей, духовного, інтелектуального і культурного розвитку українського народу [6].

Однією з основних характеристик принципів інформаційної безпеки є усвідомлення того, що відповідальність за цю проблему несуть усі зацікавлені сторони, приватний сектор, включаючи урядові установи, населення країни та міжнародних партнерів. Обов’язкове дотримання принципів інформаційної безпеки – це національне завдання, яке вимагає спільних зусиль і координації функціонування всіх зацікавлених сторін.

Важливі принципи забезпечення інформаційної безпеки налагоджують законодавчими актами та нормативними документами в цій галузі. Основними з них є:

1) Закон України «Про основні засади захисту від кібератак в Україні», що визначає правові, технічні та організаційні аспекти захисту від кібератак в Україні. Він встановлює правила для органів, відповідальних за кібербезпеку, і має встановлювати конкретні механізми координації їх дій [44].

2) Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», в якому характеризуються правові засади захисту інформації в більшості інформаційно-телекомунікаційних системах, у тому числі встановлено вимоги до безпеки, захисту особистих (персональних) даних та конфіденційності персональних даних. Закон має на меті встановлення відповідальності щодо недотримання вимог захисту інформації та визначає чіткі процедури моніторингу, контролю та нагляду щодо дотриманням встановленихвимог[40] .

3) Національна стратегія кібербезпеки України, що визначає загально прийняту стратегію та подальші пріоритети в сфері кібербезпеки. Він встановлює головні керівні принципи розвитку сектору кібербезпеки, механізми координації, розподілу завдань та обов'язків між зацікавленими сторонами [21].

Дотримання головних принципів щодо забезпечення інформаційної безпеки контролюється рядом органів і структур. Одним з таких можна вважати є Державну службу спеціального захисту зв'язку та інформації, що відповідає за керівництво, управління та подальшу реалізацію політики захисту інформації. Проте, також сформовано спеціальні відділи та департаменти міністерств, державних установ та інших організацій, що забезпечують інформаційну безпеку у своїх сферах діяльності.

Контроль за дотриманням принципів інформаційної безпеки є засадою ефективного захисту інформаційних ресурсів і інфраструктури в країні. Вони допомагають запобігти втраті конфіденційної інформації, виявити вразливості в інформаційній системі та захистити важливу урядову, ділову та особисту інформацію.

Інформаційна безпека в Україні забезпечується системою контролю, координації і співпраці різних відомств і структур. До основних органів, що відповідають за забезпечення інформаційної безпеки, відносяться:

1) Державна служба спеціального захисту комунікацій та інформації (далі ДССЗЗІ): яка відіграє ключову роль щодо забезпечення інформаційної безпеки

в Україні. Координує та моніторить роботу з питань кібербезпеки, формує політику, нормативно-правове забезпечення і стратегії в цій області. Служба здійснює моніторинг та нагляд щодо дотримання принципів інформаційної безпеки»;

2) Міністерство цифрової трансформації: цей департамент відповідає за розробку і захист інформаційних технологій та забезпечує кібербезпеку в галузі державних інформаційних систем. Мінцифра співпрацює з ДССЗЗІ та з деякими іншими зацікавленими сторонами, відомствами для прийняття ефективних заходів безпеки та їх дотримання;

3) Національна поліція та СБУ: відповідають за рослідування кіберзлочинів, боротьбу з кібершпигунством та кібертероризмом. Вони виявляють і зупиняють кібератаки, забезпечують умовний аспект сучасної інформаційної безпеки.

4) Національний банк України (НБУ) відповідальний за захист фінансово-економічної системи країни від кіберзагроз. Розробляти та впроваджувати стратегії і політики кібербезпеки в з точки зору банківської системи, співпрацювати з іншими зацікавленими органами влади та міжнародними партнерами щодо обміну інформацією та на пряму координації заходів безпеки.

5) Національна комісія з регулювання телекомунікацій та інформації (НКРЗІ): даний орган відповідає за безпосереднє регулювання та нагляд за операторами та постачальниками послуг Інтернету. Він захищає мережу зв'язку та інфраструктуру від кібератак і встановлює вимоги для захисту особистих даних користувачів.

Україна, як і певні інші країни, стикається зі серйозними загрозами інформаційній безпеці, особливо зважаючи на російсько-українську війну, яка триває ще з 2014 року. Кіберпростір теж став майже полем битви, де вороги можуть нападати та атакувати непомітно, завдаючи серйозної шкоди урядовим структурами, критичної інфраструктури та громадян [27].

Кібератаки на урядові установи, критично важливу інфраструктуру, корпоративний сектор та громадян. Такі атаки можуть проводитися хакерами,

кіберзлочинцями або державами з метою отримання конфіденційної інформації, крадіжки грошей, поширення шкідливого програмного забезпечення і багато чого іншого.

Кібершпигунство: Україна зазнає кібершпигунства з боку іноземних держав або хакерських груп з метою отримання та зловживання секретною інформацією, включаючи економічні, політичні, військові та технологічні дані.

Кіберпропаганда та дезінформація: Україна постійно стикається з величезною кількістю дезінформації та кіберпропаганди, спрямований на вплив на громадську думку, зміну переконань, розкол суспільства та підрив довіри до державних інституцій.

Соціальний інжиніринг: це техніка, яку зловмисники використовують для доступу до конфіденційної інформації через маніпуляції людьми. Соціальний інженіринг може включати фармінг, фішинг, підробку, використання шкідливих посилань тощо.

Кібертероризм: країна стикається із загрозою кібертероризму, включаючи кібератаки, спрямовані на руйнування державних установ, критично важливої інфраструктури, енергетичних систем, транспортних мереж і т.д. Кібертерористична діяльність може порушити роботу важливих систем та негативно впливати на економіку і безпеку країни.

Крадіжка даних: правопорушники можуть намагатися викрасти конфіденційні (особисті) дані, такі як особисті дані громадян, банківські реквізити, ділову інформацію тощо. Такі дані можуть бути використані для крадіжки, шахрайства, шпигунства або іншої злочинної діяльності.

Віруси та шкідливі програми: поширення вірусів, шкідливих програм та троянських програм становить серйозну загрозу інформаційній безпеці. Такі програми можуть призвести до втрати конфіденційної інформації, пошкодження наявних даних, обмежень доступу до системи та інших негативних наслідків.

Проблему інформаційної безпеки слід розглядати в національному вимірі. Державний механізм забезпечення інформаційної безпеки повинен враховувати

національні інтереси щодо інформаційного середовища, внутрішні і зовнішні загрози цим інтересам та забезпечувати систему методів виявлення і нейтралізації загроз. Він повинен включати двосторонній зв'язок між ЗМІ, суспільством та державою, що допоможе своєчасно повідомляти про зміни в громадській думці щодо навмисних наслідків та оцінювати ефективність контрзаходів [7].

В даний час в умовах російсько-української війни ситуація така: на території України як і раніше блокуються російські сайти і телеканали; велика увага приділяється отриманню підтримки з боку міжнародного співтовариства і надання фінансової допомоги Україні у вигляді зброї, створення та розповсюдження національного інформаційного продукту на території України та за її межами.

Для протидії цим загрозам та забезпечення інформаційної безпеки в Україні створено механізм забезпечення інформаційної безпеки в Україні. Цей механізм забезпечення інформаційної безпеки варто розглядати таким чином: система державно-правових інститутів; система зі своєю структурою; система різними способами; сукупність державних органів, соціальних структур, важелів, заходів і способів діяльності [42].

Правовою основою інформаційної безпеки є Конституція України, Закон України «Про національну безпеку України» та деякі закони України, згода, дана Верховною Радою, міжнародні договори, яка є обов'язковою для України. Правові норми є основою забезпечення інформаційної безпеки та визначення ефективності діяльності держави, суспільства і окремих громадян щодо захисту національних інтересів країни в інформаційній сфері.

Особливим структурним елементом державного механізму є інституційний механізм щодо забезпечення інформаційної безпеки, який забезпечує встановлення правил і положень взаємодії різних господарюючих суб'єктів в інформаційній сфері з метою запобігання загроз інформаційній безпеці.

Розробку, реалізацію та пряму координацію державної інформаційної

політики, що також забезпечення інформаційного державного суверенітету України реалізує центральний орган виконавчої влади, що володіє особливою компетенцією відповідно до покладених на нього завдань. В Україні приділяється велика увага виявленню, моніторингу та протидії загрозам інформаційній безпеці. У сучасному цифровому світі, в якому кібератаки та кіберзлочинність стають дедалі все більш поширенішими, інформаційна безпека стала необхідною для підтримки стабільності, захисту суспільних інтересів та захисту прав і свобод громадян [39].

Загрози інформаційній безпеці в українському суспільстві постійно зростають. Російська агресія, що почалася в 2014 році, принесла з собою нові реалії боротьби в кіберпросторі. Кібератаки на державні установи України, енергетичні об'єкти, засоби масової інформації та приватні компанії є широко поширеним явищем. Ці атаки спрямовані на проникнення в критично важливу інфраструктуру, крадіжку конфіденційної інформації та порушення функціонування суспільства в цілому.

Загрози інформаційній безпеці України залишаються серйозною проблемою, яка потребує постійного вдосконалення та усунення вразливих місць. Уряд України продовжує активно працювати на удосконаленням кібербезпеки, удосконалювати законодавство, підвищувати якість фахівців і співпрацювати з іншими країнами. Використання сучасних технологій для підвищення імунітету до кібератак, підвищення рівня кібер-знань і ефективне співробітництво є основними факторами в боротьбі з загрозами інформаційної безпеки.

2.3. Вивчення зарубіжного досвіду забезпечення інформаційної безпеки

Зарубіжний досвід забезпечення інформаційної безпеки має велике значення для України, оскільки дозволяє не лише запозичити ефективні моделі

захисту, але й адаптувати їх до місцевих умов. Вивчення підходів інших країн допоможе створити комплексну стратегію, здатну протистояти сучасним загрозам у цифровому середовищі. Ось деякі конкретні приклади зарубіжних підходів, які заслуговують на особливу увагу

Естонія є лідером у сфері кібербезпеки завдяки своєму інноваційному підходу до інформаційної безпеки. У 2007 році країна зазнала масованих кібератак, які вразили урядові, банківські та медійні системи. У відповідь на це Естонія створила потужну систему кіберзахисту, яка включає: національний центр кібербезпеки для координації виявлення та реагування на загрози; систему резервного копіювання даних: урядові дані зберігаються у захищених центрах як у країні, так і за її межами; кіберполігон для тренувань фахівців у сфері кібербезпеки [27].

Ключовою особливістю естонської стратегії є інтеграція державного і приватного секторів та тісна співпраця з міжнародними організаціями, такими як НАТО. Цей підхід може бути корисним для України, особливо в розбудові національного центру кіберзахисту та розробці систем резервних копій критичних даних.

США мають одну з найбільш розвинених систем забезпечення інформаційної безпеки. Національна стратегія кібербезпеки США включає наступні елементи: моніторинг ризиків: постійний аналіз вразливостей у державних та приватних системах; інноваційні технології: використання штучного інтелекту та машинного навчання для виявлення та запобігання кібератакам; партнерство між державою та приватним сектором: залучення приватних компаній до розробки захисних рішень; міжнародне співробітництво: підтримка глобальних ініціатив, спрямованих на боротьбу з кіберзлочинністю [2].

Для України цей досвід може бути корисним у створенні взаємодії між державними структурами та IT-компаніями, а також у впровадженні сучасних технологій для виявлення загроз.

ЄС впровадив Загальний регламент про захист даних (GDPR), який став

прикладом для багатьох країн світу. Регламент: встановлює жорсткі вимоги до обробки персональних даних; забезпечує право громадян на доступ до своїх даних і контроль над їх використанням; передбачає суворі штрафи за порушення правил обробки даних [1].

Для України, яка прагне інтеграції з ЄС, важливо адаптувати положення GDPR до національного законодавства. Це сприятиме підвищенню рівня довіри з боку міжнародних партнерів і забезпеченню захисту прав громадян у цифровому просторі.

Великобританія створила Національний центр кібербезпеки (NCSC), який забезпечує централізований підхід до кіберзахисту. Центр: моніторить кіберзагрози у режимі реального часу; проводить навчання для урядових установ та приватних компаній; розробляє рекомендації для підвищення стійкості до атак [1].

Особливість британського підходу полягає в акценті на освіті та обізнаності громадян. Це важливо і для України, оскільки підвищення кіберграмотності населення є ключовим елементом захисту від інформаційних загроз.

Південна Корея активно інвестує у розвиток технологій для забезпечення інформаційної безпеки. В країні створені передові системи штучного інтелекту, які: виявляють аномалії у мережевому трафіку; автоматично реагують на потенційні загрози. Також уряд Південної Кореї підтримує стартапи у сфері кібербезпеки, що сприяє розвитку інноваційних рішень. Україна може перейняти цей досвід для підтримки місцевих розробників та впровадження інноваційних технологій [9].

Зарубіжний досвід демонструє важливість комплексного підходу до забезпечення інформаційної безпеки. Ключовими уроками для України є: створення національного центру кібербезпеки за прикладом Естонії та Великобританії; інтеграція сучасних технологій, таких як штучний інтелект і автоматизовані системи моніторингу, за прикладом США та Південної Кореї; адаптація законодавства до міжнародних стандартів, включаючи елементи

GDPR для захисту персональних даних; підвищення кіберграмотності населення через освітні кампанії, як у Великобританії. Застосування цих практик дозволить Україні не лише ефективно захищати свої інформаційні ресурси, але й посилити свої позиції на міжнародній арені у сфері кібербезпеки.

ВИСНОВКИ ДО РОЗДІЛУ 2

Забезпечення інформаційної безпеки є одним із пріоритетних завдань держави, особливо в умовах воєнного стану. В Україні сформована нормативно-правова база, яка визначає принципи, засоби та механізми захисту інформаційного простору. Основними завданнями є протидія дезінформації, захист прав громадян на конфіденційність, розвиток медіакультури та медіаосвіти, а також інтеграція тимчасово окупованих територій до українського інформаційного простору.

Національна система забезпечення інформаційної безпеки передбачає тісну взаємодію органів державної влади, таких як Державна служба спеціального зв’язку, Міністерство цифрової трансформації, СБУ та Національний банк. Разом із міжнародними партнерами ці органи реалізують заходи для боротьби з кіберзагрозами, зокрема з кібератаками, шпигунством і тероризмом. Важливим елементом є розробка та впровадження стратегій і політик, що сприяють захисту національного інформаційного простору.

Водночас Україна стикається з низкою загроз, серед яких кібератаки, дезінформація, крадіжка даних і поширення шкідливих програм. Ефективна протидія цим загрозам потребує вдосконалення законодавства, розвитку кіберзахисту, підвищення обізнаності населення про інформаційну безпеку, а також координації дій усіх залучених сторін. Тільки комплексний підхід дозволить зберегти стабільність та захистити інформаційний суверенітет України в умовах сучасних викликів.

РОЗДІЛ 3.
НАПРЯМИ УДОСКОНАЛЕННЯ ПОЛІТИКА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В КОНТЕКСТІ РОСІЙСЬКОЇ АГРЕСІЇ

3.1. Заходи спрямовані на реалізацію стратегії забезпечення інформаційної безпеки України

Для України пріоритетом є послідовний розвиток стійкої електронної екосистеми, що об'єднує державний сектор, приватні підприємства, академічні (освітні) установи та громадянське суспільство. Це сприяє дотриманню безпеки інформаційного простору, а також забезпеченню взаємодії, комунікації та спільних зусиль щодо виявлення, відстеження та протидії існуючим загрозам. Крім цього, уряд вдосконалює систему реакцій на інциденти, пов'язані з кібербезпекою, і розробляє механізми негайного реагування, захист та відновлення роботи після кібератак та усунення їх наслідків.

В ході боротьби з загрозами інформаційній безпеці в Україні велика увага приділяється розробці, удосконаленню та усуненню прогалин в законодавстві і нормативних актів, якими регулюється сфера кібербезпеки. Україна активно вдосконалює правову базу, яка створює всеосяжну основу для захисту інформації. Нормативні акти та закони, які регулюють питання, пов'язані із захистом персональних даних, кіберзлочинністю, інформаційним карантином та відповідальністю за кіберзлочинність. Це допомагає покращити координацію між різними державними установами, службами які вузько направлені і займаються цими питаннями та проблемами та приватними організаціями для ефективної та дієвої боротьби з кіберзлочинністю [2].

Інформаційні заходи щодо захисту держави – це комплекс скоординованих заходів, які готують і розробляють матеріали для забезпечення національної безпеки та борони України в поєднанні з: прогнозуванням і виявленням розвідувальних загроз у військовій області; запобігати, утримувати

та протистояти збройній агресії проти України; боротьба з розвідувальними погрозами з боку атакуючої держави; вжити інших необхідних заходів у світлі отриманої інформації [31].

Захист інформаційної безпеки головною основних складових інформаційної політики України. Нині Україна стикається з викликами нинішнього сучасного кіберпростору, в якому де кібершпигунство, кібератаки і кіберзагрози дуже поширені, а їх частота та масштаби постійно зростає. Для ефективної протидії цим загрозам Україна розробляє та запроваджує комплексні методи та заходи кібербезпеки. Ведеться активна співпраця з міжнародними партнерами по обміну досвідом і інформацією в області кібербезпеки. Фахівці з кібербезпеки також проводять навчання та тренінги з метою забезпечення захисту державних інформаційних ресурсів.

В Україні активно розвивається інформаційне суспільство. Для створення сучасної цивілізованої інформаційної інфраструктури та подальшого поліпшення доступу до інформації вживаються заходи з запровадження широкосмугового інтернету, подальший розвиток електронного публічного управління (держава в смартфоні) та розширення електронних послуг. Це важлива сфера, яка дозволяє громадськості отримати доступ та втілювати свої права, такі як свободи слова та вільне вираження поглядів, а також сприяти освіті ЗМІ за допомогою медіа-кампаній та різних форм та видів освітніх заходів [26].

Ще одна складова інформаційної політики країни – запровадження та підтримка позитивного іміджу України. Ці зусилля спрямовані на зміцнення і розповсюдження України на міжнародному рівні. Саме, інформаційна дипломатія відіграє ключову роль у зміцненні довіри, підтриманні національних інтересів та сприяння залученню іноземних інвестицій. Піднесення національної мови і культури теж є важливим елементом сучасної інформаційної політики. Захист і просування української мови в умовах сучасності є пріоритетом. Активно проводяться заходи, спрямовані на сприяння

використанню України в усіх сферах суспільного життя розвитку, саме літератури, мистецтва та кіно.

У сучасних умовах, коли інформація відіграє дедалі важливішу роль, Україна активно розвиває свою інформаційну політику. Ключовими напрямами цієї політики є забезпечення інформаційної безпеки, формування інформаційного суспільства та сприяння культурному зростанню нації через підтримку індивідуальних інтересів. 30 березня 2023 року було затверджено план дій для реалізації стратегії інформаційної безпеки. Цей документ має стратегічне значення для захисту інформаційного простору країни. Розрахований на період до 2025 року, він містить низку конкретних заходів, спрямованих на підвищення рівня інформаційної безпеки, протидію кіберзагрозам та стимулювання розвитку інформаційного суспільства [27].

Головні напрямки та заходи, передбачені Планом [27], охоплюють такі аспекти:

1. *Нормативно-правове забезпечення* створює основу для захисту інформації, визначає вимоги в сфері кібербезпеки та регулює діяльність органів і структур, відповідальних за її забезпечення. Зокрема:

а) аналіз чинного законодавства в галузі інформаційної безпеки та його вдосконалення (оцінка наявних правових норм, виявлення прогалин і підготовка пропозицій щодо їх усунення з урахуванням сучасних викликів та технологій);

б) розробка нових законодавчих актів з питань кібербезпеки та захисту персональних даних (запровадження нормативних положень для захисту інформаційних систем, інфраструктур і персональних даних відповідно до міжнародних стандартів);

в) створення механізмів моніторингу порушень законодавства у сфері інформаційної безпеки (впровадження системи обліку порушень та реагування на кіберінциденти, а також визначення відповідальності за такі порушення).

2. *Кібербезпека та захист інформації* спрямовані на захист інформаційних систем, баз даних та інфраструктур від кіберзагроз. Зокрема:

а) впровадження систем кібербезпеки (розробка засобів виявлення та запобігання кіберзагрозам, створення центрів швидкого реагування на інциденти);

б) підвищення кваліфікації персоналу (навчання працівників, що займаються кібербезпекою, та обмін досвідом із міжнародними партнерами);

в) проведення аудитів і оцінки ризиків (регулярні перевірки інформаційних систем для виявлення вразливостей);

г) нормативно-організаційна підтримка (розробка законодавчих механізмів реагування на кіберінциденти);

д) партнерство з міжнародними організаціями (співпраця з країнами та міжнародними установами для обміну інформацією і досвідом у сфері кібербезпеки) [26].

3. *Інформаційна безпека громадян* передбачає захист персональних даних, підвищення обізнаності та захист від кіберзагроз. Зокрема:

а) інформаційна просвіта (кампанії з підвищення обізнаності про кібербезпеку, поширення рекомендацій щодо захисту персональних даних);

б) забезпечення захисту персональних даних (впровадження технічних рішень, як-от шифрування та анонімізація);

в) боротьба з шахрайством (співпраця з правоохоронними органами для виявлення та запобігання злочинам у кіберсфері);

г) захист дітей в Інтернеті (розробка механізмів для протидії шкідливому контенту та забезпечення безпечного використання Інтернету дітьми);

д) підтримка постраждалих від кіберзлочинів (психологічна допомога та консультування жертв) [26].

4. *Міжнародне співробітництво* зосереджується на об’єднанні зусиль з іншими країнами та організаціями для запобігання кіберзагрозам. Зокрема:

а) укладення міжнародних угод (партнерство з іншими країнами для боротьби з кіберзагрозами);

б) обмін інформацією (створення механізмів для передачі даних про нові загрози та технології у сфері кібербезпеки);

в) спільні оперативні дії (реагування на великомасштабні кіберінциденти);

г) розробка міжнародних стандартів (участь у створенні норм для забезпечення кібербезпеки).

Ключовими елементами цього плану є заходи, спрямовані на захист державних ресурсів, боротьбу з кіберзагрозами, забезпечення безпеки персональних даних і підвищення рівня поінформованості громадян.

3.2. Методи та способи забезпечення інформаційної безпеки України в умовах військового стану

Російсько-український конфлікт є багатогранним явищем, що включає військові дії, інформаційну боротьбу та елементи гібридної війни. У цьому контексті інформація відіграє ключову роль як засіб впливу на суспільство та формування сприйняття конфлікту.

Початок війни був спричинений низкою факторів, серед яких анексія Росією Криму в 2014 році, що порушила міжнародні норми та територіальну цілісність України. Причинами конфлікту також стали політичні протиріччя, етнічні та релігійні розбіжності, економічні труднощі та прагнення Росії посилити вплив у пострадянському просторі.

Ця війна є складною і багатовимірною, охоплюючи як безпосередні військові дії, так і використання елементів гібридної війни та інформаційних маніпуляцій. Росія використовує нелегальні збройні формування на території України, надаючи їм військову та іншу допомогу. Україна, зі свого боку, мобілізує свої сили для захисту території та здійснення контрнаступальних операцій [38].

Інформаційна війна є одним із головних викликів для України, адже країна зіштовхнулася з масштабною пропагандою та дезінформацією. Недостатня підготовленість до таких викликів проявляється у відсутності

чітких механізмів протидії інформаційній агресії. Російська пропаганда, що виходить за межі України, ставить під загрозу стабільність та єдність суспільства. У таких умовах забезпечення інформаційної безпеки стає невід'ємною частиною національної безпеки.

Заходи протидії інформаційним загрозам Україна активно працює над посиленням інформаційної безпеки, впроваджуючи державні програми захисту інформаційного простору. З огляду на гібридний характер війни, інформаційна безпека охоплює всі аспекти суспільного життя: мислення, освіту, історію та культуру. Основними напрямами роботи в цій сфері є захист психіки громадян від маніпуляцій, спотворень та шкідливого впливу пропаганди.

Держава приділяє значну увагу кіберзахисту. Було створено спеціалізовані органи, які займаються моніторингом та аналізом кіберзагроз, розробляють стратегії протидії та забезпечують захист державних інформаційних систем. Співпраця з міжнародними партнерами, такими як НАТО та ЄС, сприяє ефективному реагуванню на кіберзагрози [36].

Служби кібербезпеки, зокрема Національний центр кібербезпеки та Управління інформаційної безпеки СБУ, аналізують та реагують на атаки, які спрямовані на дестабілізацію ситуації в країні. Діяльність громадських організацій та ініціатив також відіграє важливу роль у забезпеченні інформаційної стабільності.

Основні напрями забезпечення інформаційної безпеки

1. Кіберзахист. Включає захист інформаційних систем, боротьбу з кіберзлочинами, впровадження стандартів безпеки та дослідження новітніх кіберзагроз.

2. Розвиток законодавства. Україна активно вдосконалює нормативно-правову базу в сфері інформаційної безпеки.

3. Міжнародна співпраця. Обмін досвідом з міжнародними партнерами сприяє розробці ефективних заходів протидії кіберзагрозам.

4. Кіберрозвідка. Розвиток розвідувальних можливостей дозволяє виявляти та попереджати кібератаки.

5. Освіта та інформованість. Реалізуються освітні програми та інформаційні кампанії для підвищення рівня медіаграмотності громадян.

6. Розвиток ЗМІ. Підтримка незалежних та об’єктивних медіа сприяє протидії дезінформації та пропаганді.

7. Захист критично важливої інфраструктури. Впроваджуються технології безпеки для телекомунікацій, енергетичних систем та фінансових інституцій [18].

Зазначені кроки спрямовані на підвищення інформаційної безпеки, збереження стабільності та захист національних інтересів України в умовах триваючого конфлікту.

3.3. Механізми протидії щодо поширення російської пропаганди та дезінформації

Однією з ключових проблем, з якими стикається Україна, є маніпуляція фактами та проведення розвідувальних операцій з боку агресора. Ці дії мають на меті: підрив незалежності та конституційного ладу країни, порушення суверенітету і територіальної цілісності, а також розповсюдження пропаганди війни, насильства і жорстокості. Вони спрямовані на провокування міжнаціональної, релігійної, етнічної і расової ненависті, а також на вчинення терористичних актів і порушення основних прав і свобод людини.

Україна вже давно є мішенню російської пропагандистської машини, яка спотворює реальні події і факти, намагаючись обґрунтувати свої агресивні дії. Від наративу про «державу, що не відбулася», до тверджень про неспроможність України зберегти свою незалежність – російська пропаганда прагне створити негативний імідж країни. Також поширюються спроби мобілізувати населення агресора через розпалювання міжетнічних конфліктів. Попри це, спроби представити окупантів як визволителів зазнали краху, адже масові злочини проти цивільних осіб розвінчали ці міфи.

Після анексії Криму та початку військових дій на Донбасі російська пропаганда зосередилася на дискредитації українського уряду. Вона наголошувала на нібито злочинах української влади, втручанні США та НАТО у внутрішні справи України, намагаючись виправдати свої дії. Застосовуючи метод «дзеркального відображення», пропагандисти маніпулювали звинуваченнями, вводячи в оману проросійськи налаштованих експертів і журналістів. Проте міжнародна підтримка України та систематичне викриття маніпуляцій значно послабили вплив цієї пропаганди [38].

Для ефективної протидії дезінформації необхідно вміти ідентифікувати фейковий контент, аналізувати його типи та визначати цільову аудиторію. Одним із найефективніших механізмів російської пропаганди є залучення платних агентів, які через ЗМІ та соціальні мережі поширюють проросійські наративи. Ці агенти займаються створенням фейкових новин, маніпуляцією фактами та інсценуванням конфліктів з метою посіяти недовіру та страх серед населення [38].

Центр протидії дезінформації, що функціонує при Раді національної безпеки і оборони України, відіграє провідну роль у виявленні та боротьбі з фейковою інформацією. Основна задача центру полягає не лише у виявленні фейків, але й у розкритті конкретних прикладів недостовірної інформації. За аналізований період Центром було зафіксовано 674 випадки поширення неправдивих новин, причому найбільша кількість таких інцидентів сталася у серпні – близько 95 випадків. Графічне зображення (рис. 3.1) демонструє щомісячну статистику виявлених підроблених матеріалів [20].

Українські державні установи та організації активно працюють над розробкою ефективних механізмів для боротьби з російською пропагандою. З цією метою застосовуються такі заходи, як фактчекінг (перевірка інформації), викриття фейків, інформаційна протидія та запровадження освітніх програм для розвитку критичного мислення серед громадян. Крім цього, важливим напрямом є співпраця з міжнародними організаціями та партнерами, що дає

змогу обмінюватися інформацією і координувати зусилля у сфері протидії пропаганді.

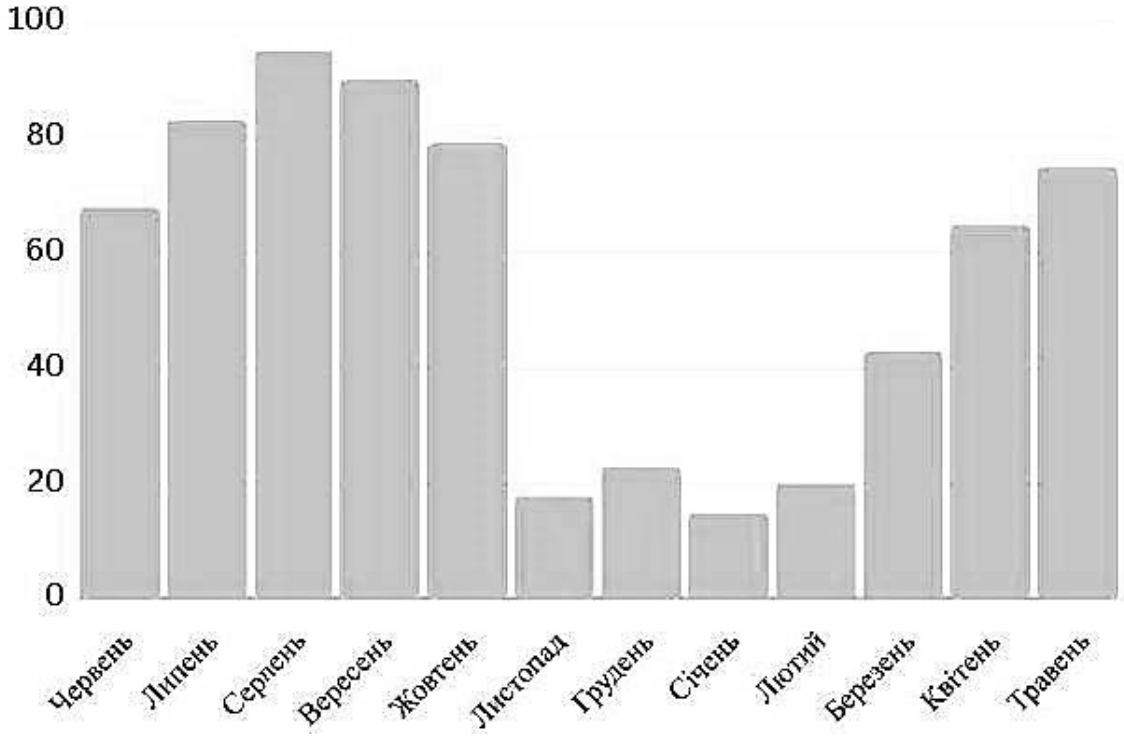

Рис. 3.1. Загальна кількість опублікованих рф фейкових-новин з а червень 2022 р. – травень 2024 р.

Джерело: [20].

Одним з ключових способів протидії російській дезінформації є поширення правдивої інформації. Цей підхід передбачає активну діяльність української влади, громадських організацій і незалежних ЗМІ, які спільно працюють над створенням ефективної системи комунікацій. Вона спрямована на забезпечення об’єктивного і достовірного інформування громадян на різних рівнях. Важливу роль у цьому процесі відіграє розвиток незалежних медіа, зокрема телеканалів, радіостанцій, інтернет-видань та інших платформ. Завдяки таким джерелам населення отримує доступ до різних точок зору на події в Україні та світі, що сприяє формуванню збалансованого уявлення про реальність [21].

Україна також активно використовує сучасні інформаційні технології для забезпечення широкого доступу до достовірної інформації. Через соціальні

мережі, веб-платформи та мобільні додатки поширюються офіційні заяви, фактичні дані та новини. Такий підхід забезпечує оперативність і ефективність донесення інформації до різних аудиторій, особливо серед молоді, яка активно користується цифровими технологіями. Окрім того, до поширення правдивої інформації залучаються громадські організації, експерти, журналісти та активісти, що додає довіри та об'єктивності до повідомлень. Відкриті дискусії, тренінги, конференції та інші заходи сприяють формуванню критичного мислення серед громадян, навчаючи їх розпізнавати дезінформацію [22].

Розвиток медіаосвіти та критичного мислення серед населення є важливим кроком у протидії інформаційним загрозам. Зростаючий інтерес до впровадження медіаграмотності в освітні програми та позакласну діяльність допомагає громадянам здобувати навички аналізу та перевірки інформації, а також краще розуміти принципи роботи сучасних ЗМІ. Також важливим елементом є співпраця з міжнародними організаціями та іншими країнами, такими як Європейський Союз, ОБСЄ, НАТО тощо, для розробки спільних стратегій і узгоджених дій у протидії дезінформації.

Особливу роль у міжнародному співробітництві відіграє обмін інформацією. Україна активно взаємодіє зі своїми партнерами, надаючи їм дані про російську пропаганду і дезінформацію, що поширюється з території агресора. Це дозволяє міжнародній спільноті краще розуміти масштаби проблеми і виробляти ефективні стратегії реагування.

Крім того, Україна проводить спільну роботу з міжнародними організаціями для координації дій у боротьбі з пропагандою. У рамках цього співробітництва організовуються зустрічі, семінари та конференції, на яких аналізуються нові тенденції дезінформаційних кампаній і обговорюються способи протидії. Такі заходи сприяють обміну досвідом і визначенню найкращих практик у сфері інформаційної безпеки. Україна також реалізує спільні проєкти зі своїми партнерами, які охоплюють обмін експертами, створення спільних інформаційних платформ, проведення навчальних програм

та інші ініціативи, спрямовані на підвищення рівня інформаційної безпеки в регіоні та світі [40].

Міжнародна співпраця є критично важливою для подолання викликів, пов’язаних із російською пропагандою та дезінформацією, оскільки ця проблема має глобальний характер. Спільні зусилля держав та організацій допомагають забезпечувати інформаційну безпеку не лише в Україні, а й на міжнародному рівні.

ВИСНОВКИ ДО РОЗДІЛУ 3

В умовах гібридної війни, розв'язаної росією, Україна стикається з низкою викликів у сфері інформаційної безпеки. Реалізація заходів, спрямованих на вдосконалення нормативно-правової бази, зміцнення кіберзахисту, підвищення поінформованості громадян і посилення міжнародного співробітництва, є ключовими для ефективної протидії кіберзагрозам і пропаганді. Особливого значення набуває адаптація національних стратегій до сучасних викликів, що забезпечує ефективний захист державних інформаційних ресурсів і приватних даних громадян.

Зміцнення позицій України у глобальному інформаційному просторі через формування позитивного іміджу, активну інформаційну дипломатію та просування національної культури є важливими складовими державної політики. Підвищення рівня громадської обізнаності про кіберзагрози та навички безпечного користування цифровими технологіями сприяє посиленню інформаційної стійкості суспільства. Такі дії дозволяють зменшити вплив дезінформації та маніпуляцій, що використовуються ворожими силами для дестабілізації країни.

Успішна протидія інформаційній агресії можлива лише через активну взаємодію з міжнародними партнерами. Спільні оперативні дії, обмін досвідом та розробка єдиних стандартів у сфері кібербезпеки підсилюють національні

зусилля України. Укладення міжнародних угод та участь у глобальних ініціативах забезпечують доступ до передових технологій і дозволяють ефективно реагувати на сучасні виклики в інформаційній сфері.

ВИСНОВКИ

Інформаційна безпека є ключовою складовою національної безпеки, оскільки вона захищає інформаційні ресурси, забезпечує стабільність функціонування держави в інформаційному середовищі та запобігає потенційним загрозам. Концептуальне розуміння цього терміну залежить від різних підходів, що охоплюють технічні, організаційні, правові та соціальні аспекти. Це дозволяє інтегрувати інформаційну безпеку в загальну стратегію забезпечення стійкості держави.

Основні підходи до забезпечення інформаційної безпеки держави включають концепцію цілісності інформаційного простору, орієнтацію на національну безпеку, а також управління ризиками й загрозами. Кожен із цих підходів спрямований на побудову системи захисту, що охоплює використання сучасних технологій, розробку відповідного законодавства, вдосконалення організаційних процесів та підвищення обізнаності громадськості.

Інформаційна безпека вимагає комплексного підходу, що поєднує кібернетичні, фізичні, організаційні, кадрові та правові заходи. Успішне забезпечення інформаційної безпеки можливе лише через постійний моніторинг, вдосконалення нормативної бази та міжнародне співробітництво. Розуміння важливості цієї сфери та інтеграція всіх необхідних компонентів дозволяють державі ефективно реагувати на виклики сучасного інформаційного середовища.

Забезпечення інформаційної безпеки є одним із пріоритетних завдань держави, особливо в умовах воєнного стану. В Україні сформована нормативно-правова база, яка визначає принципи, засоби та механізми захисту інформаційного простору. Основними завданнями є протидія дезінформації, захист прав громадян на конфіденційність, розвиток медіакультури та медіаосвіти, а також інтеграція тимчасово окупованих територій до українського інформаційного простору.

Національна система забезпечення інформаційної безпеки передбачає тісну взаємодію органів державної влади, таких як Державна служба спеціального зв’язку, Міністерство цифрової трансформації, СБУ та Національний банк. Разом із міжнародними партнерами ці органи реалізують заходи для боротьби з кіберзагрозами, зокрема з кібератаками, шпигунством і тероризмом. Важливим елементом є розробка та впровадження стратегій і політик, що сприяють захисту національного інформаційного простору.

Водночас Україна стикається з низкою загроз, серед яких кібератаки, дезінформація, крадіжка даних і поширення шкідливих програм. Ефективна протидія цим загрозам потребує вдосконалення законодавства, розвитку кіберзахисту, підвищення обізнаності населення про інформаційну безпеку, а також координації дій усіх залучених сторін. Тільки комплексний підхід дозволить зберегти стабільність та захистити інформаційний суверенітет України в умовах сучасних викликів.

В умовах гібридної війни, розв'язаної росією, Україна стикається з низкою викликів у сфері інформаційної безпеки. Реалізація заходів, спрямованих на вдосконалення нормативно-правової бази, зміцнення кіберзахисту, підвищення поінформованості громадян і посилення міжнародного співробітництва, є ключовими для ефективної протидії кіберзагрозам і пропаганді. Особливого значення набуває адаптація національних стратегій до сучасних викликів, що забезпечує ефективний захист державних інформаційних ресурсів і приватних даних громадян.

Зміцнення позицій України у глобальному інформаційному просторі через формування позитивного іміджу, активну інформаційну дипломатію та просування національної культури є важливими складовими державної політики. Підвищення рівня громадської обізнаності про кіберзагрози та навички безпечного користування цифровими технологіями сприяє посиленню інформаційної стійкості суспільства. Такі дії дозволяють зменшити вплив дезінформації та маніпуляцій, що використовуються ворожими силами для дестабілізації країни.

Успішна протидія інформаційній агресії можлива лише через активну взаємодію з міжнародними партнерами. Спільні оперативні дії, обмін досвідом та розробка єдиних стандартів у сфері кібербезпеки підсилюють національні зусилля України. Укладення міжнародних угод та участь у глобальних ініціативах забезпечують доступ до передових технологій і дозволяють ефективно реагувати на сучасні виклики в інформаційній сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Galeotti M. Russian Political War: Moving Beyond the Hybrid // Hardcover. 18 Feb 2019.

2. Gupta M. Cybersecurity: Concepts, methodologies, tools, and applications // IGI Global. 2020.

3. National Institute of Standards and Technology (NIST). Security and Privacy Controls for Federal Information Systems and Organizations // NIST Special Publication. 2018. № 800-53.

4. Petrov A., Smith J. Information security in the digital age: A comprehensive guide to current and emerging threats // Butterworth-Heinemann. 2019.

5. Yakobchuk V., Ivaniuk O., Krut V. THE PUBLIC ADMINISTRATION OF INFORMATION TECHNOLOGIES IN HEALTH CARE FIELD UNDER THE CONDITIONS OF MARTIAL STATE. *Economic scope*. 2024. No. 195. P. 193–200. URL: https://doi.org/10.30838/ep.195.193-200.

6. Zozulia I. Ensuring Information Security as a Function of the Modern State: the Experience of Ukraine: International Journal of Computer Science and Network Security, May 2022. VOL.22 No.5, C. 747–756.

7. Антонюк В. В. Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці. URL: http://www.dy.nayka.com.ua/?op=1&z=747.

8. Бондар І. Р. Інформаційна безпека як основа національної безпеки. URL:http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAG E_FILE_DOWNLOAD=1&Image_file_name=PDF/Mre_2014_1_8.pdf.

9. Вербицький О. Організаційно-правові засади інформаційної безпеки // Юридичний журнал «Право України». 2017.

10. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. URL: http://lsej.org.ua/2_2020/54.pdf.

11. Іванова О. В. Інформаційна безпека держави в умовах глобалізації // Гуманітарний вісник Запорізької державної інженерної академії. 2018. № 74(3). С. 120–126.

12. Концепція інформаційної безпеки України: Проект. // Organization for Security and Co-operation in Europe. URL: https://www.osce.org/files/f/documents/0/2/175056.pdf.

13. Концепція національної безпеки України: Затверджено Указом Президента України від 26.06.2015 р. № 287/2015. URL: https://www.president.gov.ua/documents/2872015-19070. (дата звернення: 05.04.2023).

14. Кузьмінська Р. В. Мережеве суспільство і психологія натовпу // Матеріали круглого столу з нагоди дня спротиву окупації Автономної Республіки Крим та міста Севастополя. 2023. С. 74–75.

15. Кузьмінська Р. В. Національна безпека в умовах розвитку індустрії штучного інтелекту // Тези доповідей / XXIII Міжнародна науково-практична конференція здобувачів вищої освіти і молодих учених. 2023. С. 90–92.

16. Лібік О. Основні засади інформаційної безпеки // Вісник Національного університету «Львівська політехніка». 2020.

17. Марущак А. І., Панченко В. М. До визначення поняття «Інформаційна безпека» // Збірник наукових праць «Правчий вісник університету «КРОК»». 2010. № 5 (1). С. 122–127.

18. Олійник О. В. Нормативно-правове забезпечення інформаційної безпеки в Україні. URL: http://www.pravoisuspilstvo.org.ua/archive/2012/3_2012/28.pdf.

19. Омельченко В. В. Концепція національної безпеки та інформаційна безпека держави // Правові проблеми інформаційної безпеки. 2017. № 2. С. 39-46.

20. Офіційна сторінка Центру протидії дезінформації у соціальній мережі «Інстаграм».URL: https://instagram.com/cpd.gov.ua.

21. Офіційний сайт інтернет-видання «Українська правда». URL: https://www.pravda.com.ua.

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

23. Офіційний сайт Центру протидії дезінформації. URL: https://cpd.gov.ua/.

24. Офіційний сайт Центру стратегічних комунікацій та інформаційної безпеки.URL: https://spravdi.gov.ua/.

25. Про введення воєнного стану: Указ Президента України від 24.02.2022 р. № 64/2022 (з усіма змінами та правками) // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text..

26. Про державну таємницю: Закон України від 1994 р. № 3856-XII (з усіма змінами та правками) // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

27. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: Розпорядження Кабінету Міністрів України № 272-р // Урядовий портал / Єдиний веб-портал органів виконавчої влади України. URL: https://www.kmu.gov.ua/news/uriad-zatverdyv-plan-zakhodiv-z-realizatsii-stratehii- informatsiinoi-bezpeky-do-2025-roku.

28. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 16.12.2020 р. № 1089-IX // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

29. Про інформацію: Закон України від 1992 р. № 2658-XII. Поточна редакція - Редакція від 31.03.2023, підстава - 2849-IX // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

30. Про правовий режим воєнного стану: Закон України № 389-VIII. Поточна редакція - Редакція від 31.03.2023, підстава - 2849-IX // База даних «Законодавство України» / ВР України. URL:

https://zakon.rada.gov.ua/laws/show/389-19#Text..

31. Про Сратегію інформаційної безпеки: Указ Президента України від 15.10.2021 р. № 685/2021 // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

32. Про стратегію інформаційної безпеки: Указ Президента України від 15.10.2021 р. № 685/2021 // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

33. Про Стратегію кібербезпеки України: Указ Президента України від 14.05.2021 р. № 447/2021 // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

34. Про Стратегію кібербезпеки України: Указ Президента України від 26.01.2016 р. № 96/2016 // Офіційний веб-портал Ради національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/ua/Ukazy/417.html?PRINT.

35. Про стратегію кібербезпеки: Указ Президента України від 14.05.2021 р. № 447/2021 // Офіційне інтернет-представництво Президента України Володимира Зеленського. URL: https://www.president.gov.ua/documents/4472021-40013.

36. Розумна А. Інформаційна безпека держави: підходи та принципи визначення // Наукові записки Національного університету «Острозька академія». Серія «Філософія». 2017. № 32. С. 166–171.

37. Смірнова Е. Криптографічний захист інформації: аспекти інформаційної безпеки // Збірник наукових праць КНУ імені Тараса Шевченка. 2017.

38. Соломін Є. Телепроєкти «Єдині новини» та «FreeДом» як спосіб інформаційного спротиву російській агресії та засіб регулювання медіасферою під час війни // Наукові праці Міжрегіональної Академії управління персоналом. Філологія. 2023. № 3. С. 62–71.

39. Стратегія національної безпеки України: Указ Президента України від 14 вересня 2020 року № 392/2020 // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/392/2020#n12.

40. Стратегія національної безпеки України: Указ Президента України від 14.09.2020 р. № 392/2020 // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/392/2020#n12.

41. Ткачук В. М., Косолапов В. Г. Інформаційна безпека держави в сучасних умовах // Економіка та держава. 2018. № 9. С. 97–101.

42. Шевчук В. В. Механізм забезпечення інформаційної безпеки держави: теоретично-методологічні основи. // Періодичні наукові видання НАВС. URL:http://elar.naiau.kiev.ua/handle/123456789/18709.

43. Щодо реалізації єдиної інформаційної політики в умовах воєнного стану: Рішення Ради національної безпеки і оборони України від 19.03.2022 р. № 152/2022 // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/n0004525-22.

44. Якобчук В.П., Скидан О.В., Дацій Н.В., Данкевич В. Є., Данкевич Є. М., Данкевич А. Є., Литвинчук І.Л., Першко Л.О., Симоненко Л.І., Довженко В.А., Войтенко А.Б., Захаріна О.В., Іванюк О.В., Мосієнко О.В. Публічне управління та адміністрування: навч. посіб. / за заг. Ред. В.П. Якобчук. Київ: Видавництво Ліра-К, 2024. 476 с.

45. Яременко О.О. Державне регулювання і державне управління: співвідношення понять у контексті трансформації вищої освіти в Україні. URL: https://lib.chmnu.edu.ua/pdf/naukpraci/govermgmt/2012/186-174-10.pdf.

ДОДАТКИ