МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН, ІНФОРМАЦІЇ ТА
РЕГІОНАЛЬНИХ СТУДІЙ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ Ніна РЖЕВСЬКА
«15» 06 2023 р.

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА
СПЕЦІАЛЬНОСТІ 291 «МІЖНАРОДНІ ВІДНОСИНИ,
СУСПІЛЬНІ КОМУНІКАЦІЇ ТА РЕГІОНАЛЬНІ СТУДІЇ»
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«МІЖНАРОДНА ІНФОРМАЦІЯ»

Тема: «ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ»

Виконавець: здобувач вищої освіти 4 курсу, 409 групи, Кузьмінська Рут Вадимівна

Керівник: к.і.н., доцент кафедри міжнародних відносин, інформації та регіональних студій Дерев'янко Ігор Петрович

Нормоконтролер: _____ Олексій МЕНДРІН
(підпис)

КИЇВ 2023

ЗМІСТ

ВСТУП

Забезпечення національних інтересів держави вимагає створення та забезпечення сприятливих умов для їх реалізації. Це може охоплювати різноманітні сфери, включаючи політичні, економічні, соціальні та безпекові аспекти. Для досягнення мети потребується прийняття стратегічних рішень та здійснення відповідних заходів.

Формування стратегічних та поточних завдань державної політики, спрямованих на гарантування інформаційної безпеки, є ефективним засобом втілення національних інтересів України у сфері інформаційних відносин. Ефективне використання інформаційних ресурсів визначається здатністю держави покращувати свої зусилля для мирного врегулювання кризових ситуацій. Навпаки, ігнорування інформаційних факторів або умисне спотворення інформації може призвести до радикальних настроїв, спалахів ворожості та катастрофічних наслідків.

Використання інформаційних технологій у військовій сфері відкрило нові можливості для забезпечення обороноздатності держави. Володіння інформаційними ресурсами та їх захист стали необхідними компонентами військової сфери, нарівні з озброєнням, боєприпасами та транспортом. Перемога України у інформаційному протистоянні під час війни з Росією сприятиме досягненню стратегічних цілей країни.

У Стратегії інформаційної безпеки України відображено інтереси держави, які полягають у необхідності ефективного захисту конституційного устрою, суверенітету та територіальної цілісності країни, а також у встановленні та підтриманні політичної стабільності, включаючи стабільність державної влади та її інституцій. Аналіз реалізації цілей, визначених у Стратегії, свідчить про продовження процесу досягнення цих цілей, незважаючи на складнощі, пов'язані з воєнним станом.

В умовах воєнного стану країни особливо актуальним стало питання необхідності єдиної інформаційної політики. В цьому контексті Президент України

підписав Указ № 152/2022, яким було запроваджено Рішення Ради національної безпеки та оборони України «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» [1].

Актуальність теми дослідження полягає у висвітлені досвіду України в веденні гібридної війни, до якої 24 лютого 2022-го року не був готовий ніхто. Зміни законодавства України в інформаційній сфері, після початку повномасштабного вторгнення, це відповіді на російську пропаганду, дезінформацію та інформаційні атаки. Забезпечення інформаційної безпеки в умовах війни стає ключовим завданням для України.

Внаслідок російської агресії українське законодавство щодо інформаційної політики виявило ряд недоліків, які призводять до послаблення заходів України у протистоянні зовнішньому (російському) інформаційному впливу в умовах гібридної війни. Правки до концептуальних документів та зміни внесені до законодавства, за останній рік, були прийняті з урахуванням сучасної безпекової ситуації та можливого майбутнього вступу України до військово-політичного союзу НАТО. Сьогодні Україна тісно співпрацює з Європейським Союзом та НАТО у сфері інформаційно-військових питань.

Особлива увага приділяється законодавству, що обмежує або забороняє поширення контенту, створеного країною-агресором, через радіо, телебачення та в Інтернеті на території України.

Стратегічне планування та прогнозування інформаційної та безпекової політики країни стають важливими завданнями в умовах російсько-української війни. Враховуючи недоліки в законодавчій базі, важливо розробити довгострокові стратегії, спрямовані на забезпечення ефективного захисту національного інформаційного простору та інформаційного суверенітету. Це вимагає аналізу поточних тенденцій, прогнозування можливих загроз і визначення пріоритетів для впровадження заходів інформаційної безпеки. Крім того, необхідно здійснити системний підхід до розробки політики, включаючи співпрацю з міжнародними партнерами, такими як Європейський Союз та НАТО, для вироблення спільних стратегій та координації заходів. Це допоможе зміцнити інформаційну безпеку

України, зберегти національну ідентичність та забезпечити її як суверенну та незалежну державу.

В умовах збройного конфлікту органи державної влади та місцевого самоврядування проявляють високий рівень інформаційної взаємодії з суспільством. Систематично, та належним чином, міністерства та відомства надають актуальну інформацію громадськості. Виступи Президента України та голів обласних військових адміністрацій, присвячені аналізу ситуації та звіту про здійснену роботу, стають буденними для громадян.

Формування іміджу України є важливим аспектом зовнішньої комунікації. Посилення позитивного іміджу України, як внутрішнього, так і зовнішнього, має велике значення для політичної, економічної та культурної перспектив розвитку країни. Успішність у зміцненні іміджу держави визначається ефективністю відповідної інформаційної діяльності. Органи влади, що відповідають за зв'язки з громадськістю, засобами масової інформації та іншими структурами громадського суспільства, мають особливу роль у політиці формування іміджу.

З урахуванням вищезазначеної інформації, дослідження теми буде проведено з **метою**: аналіз механізмів та заходів, вжитих для забезпечення інформаційної безпеки України в умовах російсько-української війни. Реалізація мети дослідження умовила розв'язання таких **завдань**:

1. Проаналізувати основні концептуальні підходи до визначення поняття «інформаційна безпека держави»;

2. З'ясувати різновиди забезпечення інформаційної безпеки;

3. Проаналізувати нормативно-правову базу щодо забезпечення інформаційної безпеки України;

4. Описати принципи забезпечення інформаційної безпеки України;

5. Визначити загрози інформаційній безпеці України;

6. Проаналізувати заходи з реалізації стратегії інформаційної безпеки України;

7. Проаналізувати методи й засоби забезпечення інформаційної безпеки України в умовах війни;

8. Описати механізми протидії поширенню російської пропаганди та

дезінформаціїї.

Для кваліфікаційної роботи за темою «Забезпечення інформаційної безпеки України в умовах російсько-української війни» **об'єктом** дослідження є система захисту інформаційних ресурсів та інформаційних процесів України, **предметом** – стратегічні та тактичні аспекти захисту інформаційних систем, кібербезпеки, інформаційної війни, пропаганди та маніпуляційної інформації в контексті російсько-української війни.

Джерельна база теми дослідження є досить розгалуженою та різноманітною. Питання інформаційної безпеки в контексті російсько-української війни досліджують: серед вітчизняних – Георгій Тука, Олександр Даниленко, Віталій Шабунін, Олександр Литвиненко; зарубіжні – Molly McKew, Keir Giles, Margo Gontar та інші. Зокрема, це наукові праці, монографії, статті в наукових журналах, звіти органів державної влади, аналітичні звіти, документи міжнародних організацій, офіційні заяви та комунікати відповідних українських та міжнародних інституцій.

Стан дослідженості проблеми «Забезпечення інформаційної безпеки України в умовах російсько-української війни» можна вважати достатньо розвиненим. За останні роки було проведено значну кількість наукових досліджень та аналізів, присвячених цій проблемі. Вони включають аспекти кібербезпеки, інформаційної війни, впливу дезінформації та пропаганди на суспільство, захисту критично важливих інформаційних інфраструктур та соціального аспекту.

Проте, з урахуванням ситуації яка активно змінюється та постійного розвитку інформаційних технологій, ця проблема залишається актуальною та потребує подальших досліджень. Розширення джерельної бази та поглиблення аналізу наявних даних сприятимуть більш повному розумінню проблеми та розробці ефективних стратегій забезпечення інформаційної безпеки України.

Робота пройшла **апробацію** на 2-х науково-практичних конференціях:

– Круглий стіл з нагоди Дня спротиву окупації Автономної Республіки Крим та міста Севастополя [2];

– XXIII Міжнародна науково-практична конференція здобувачів вищої освіти і

молодих учених «Політ. Сучасні проблеми науки» [3].

Враховуючи мету роботи, поставлені завдання, об’єкт та предмет дослідження, було використано наступні **методи** наукового пізнання:

1) Аналіз літературних джерел: використано для дослідження та узагальнення наявної наукової інформації про проблему;

2) Кейс-стаді: аналіз конкретних ситуацій, виявлення особливостей та недоліків існуючих підходів до забезпечення інформаційної безпеки;

3) Статистичний аналіз: обробки числових даних, таких як статистика пропагандистської діяльності та інших відомостей, що стосуються інформаційної безпеки;

4) Системний аналіз: аналіз взаємодії різних компонентів системи інформаційної безпеки України, виявлення залежності та вплив факторів на її ефективність.

Дипломна робота зосереджена на дослідженні теми «Забезпечення інформаційної безпеки України в умовах російсько-української війни». У першому розділі роботи проаналізовано основні концептуальні підходи до визначення поняття «інформаційна безпека держави» та різновиди забезпечення інформаційної безпеки. Другий розділ присвячений засадам формування інформаційної безпеки України, включаючи нормативно-правову базу, принципи та загрози, що впливають на інформаційну безпеку. Третій розділ розглядає політику України у сфері забезпечення інформаційної безпеки в умовах російської агресії, включаючи заходи реалізації стратегії, методи та засоби забезпечення безпеки та механізми протидії поширенню російської пропаганди та дезінформації.

РОЗДІЛ 1
ТЕОРЕТИКО-КОНЦЕПТУАЛЬНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

1.1. Основні концептуальні підходи до визначення поняття «інформаційна безпека держави»

Нині існує гостра потреба у розв'язанні проблем інформаційної безпеки, оскільки державі необхідно інтегруватись у глобалізоване інформаційне суспільство та забезпечувати своє ефективне функціонування в інформаційній сфері. Часто проблематика пов'язана з неефективністю політики інформаційної безпеки органів державної влади, та необхідністю переглянути доктринальні засади її забезпечення [4]. Тому розуміння та визначення поняття «інформаційна безпека держави» є надзвичайно важливим для розробки ефективних стратегій та заходів, спрямованих на її забезпечення.

Розуміння та тлумачення поняття «інформаційна безпека» має велике значення для розуміння сутності інформаційної безпеки та розробки стратегічних рішень щодо її забезпечення.

Приклади тлумачення поняття вітчизняними діячами: Лібік (2020) вказує, що інформаційна безпека містить систему заходів, спрямованих на захист інформації від незаконного доступу, збереження її конфіденційності, цілісності та доступності. Це означає, що інформаційна безпека забезпечує захист інформаційних ресурсів та запобігає можливим загрозам [5].

Вербицький (2017) розглядає інформаційну безпеку як систему заходів, які включають технічні, організаційні та правові заходи. Він вказує, що інформаційна безпека пов'язана з захистом інформаційних систем, а також з організаційними процедурами та правилами, спрямованими на забезпечення безпеки [6].

Смірнова (2019) акцентує на аспекті криптографічного захисту в контексті інформаційної безпеки. Згідно з її дослідженням, інформаційна безпека охоплює використання криптографічних методів та технологій для захисту конфіденційності, цілісності та доступності інформації [7].

Дослідження різних підходів до тлумачення терміну «інформаційна безпека» відкриває широкий концептуальний простір для подальших роздумів щодо ролі цього поняття у контексті державної безпеки. Розуміння інформаційної безпеки держави має багатоаспектний характер і вимагає окремого розгляду, оскільки враховує специфіку сучасного інформаційно-комунікаційного середовища, що постійно змінюється.

Розглянемо основні концептуальні підходи до визначення поняття «інформаційна безпека держави». Це дозволить зрозуміти різноманітність підходів до розуміння та управління інформаційною безпекою, що важливо для розвитку ефективних стратегій інформаційного захисту та забезпечення стійкості держави у сучасному інформаційному середовищі.

Основні концептуальні підходи до визначення поняття «інформаційна безпека держави» включають:

– концепція цілісності інформаційного простору: За цим підходом інформаційна безпека держави розглядається як забезпечення недоторканості та цілісності інформаційного простору держави. Це означає захист від несанкціонованого доступу, розповсюдження та зміни інформації, а також забезпечення доступності та надійності інформаційних систем [8];

– концепція національної безпеки: Цей підхід вбачає інформаційну безпеку держави як один з ключових елементів загальної національної безпеки. За цим підходом інформаційна безпека розглядається у контексті захисту національних інтересів, суверенітету та безпеки держави у сфері інформаційних технологій та комунікацій [9];

– концепція ризиків та загроз: За цим підходом інформаційна безпека держави розглядається як захист від ризиків та загроз, пов’язаних з використанням інформаційних технологій. Він наголошує на ідентифікації, оцінці та управлінні ризиками, які можуть впливати на інформаційну безпеку держави [10].

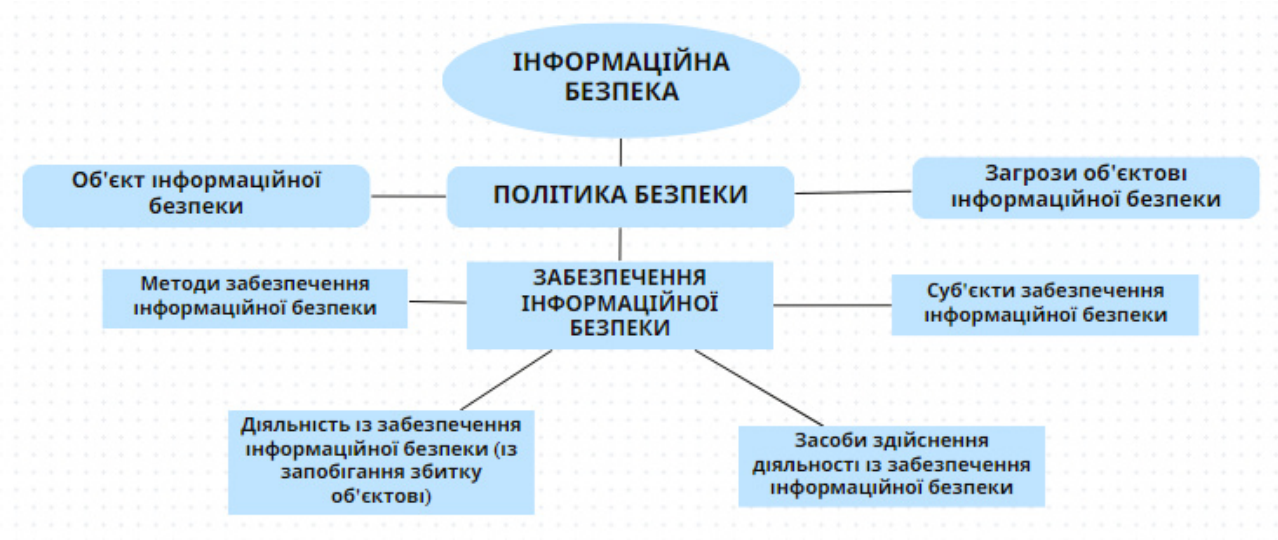
Отже, інформаційна безпека держави, як її визначає Іванова, є складною системою заходів, спрямованих на захист інформаційних ресурсів держави від загроз з боку ворожих суб’єктів, технологічних викликів та інших небезпек [11].

Окремі науковці підкреслюють необхідність комплексного підходу до інформаційної безпеки, який включає технічні, організаційні, правові та соціальні аспекти [12].

Поняття «інформаційна безпека держави» має наступну структуру яка зазначена на діаграмі 1.1.

Діаграма 1.1

«Структура поняття «інформаційна безпека держави»»



Питання інформаційної безпеки держави також пов’язані з глобалізацією та розвитком інформаційно-комунікаційних технологій. Вчені висловлюють думку, що сучасна держава має бути готовою до викликів цифрової епохи та враховувати вплив інформаційного простору на свою безпеку. Це передбачає не лише захист інформації, але й розвиток відповідних стратегій, політик та законодавства [13].

Слід зазначити, що розуміння інформаційної безпеки держави є постійним предметом дискусій та досліджень. Різноманітні підходи та трактування поняття відображають складність і багатогранність цієї проблеми. Продовження досліджень в даній сфері важливо для подальшого розвитку концептуального розуміння інформаційної безпеки держави та розробки ефективних стратегій її забезпечення.

1.2. Різновиди забезпечення інформаційної безпеки

Різновиди забезпечення інформаційної безпеки держави включають широкий спектр заходів, спрямованих на захист інформаційних ресурсів, систем та процесів в державному секторі. Ці заходи охоплюють технічні, організаційні, кадрові та

правові аспекти, що спільно визначають рівень інформаційної безпеки держави. Найпоширенішими різновидами забезпечення інформаційної безпеки держави є:

Кібербезпека. Кібербезпека охоплює широкий спектр заходів для захисту інформаційних систем від кіберзагроз. Вона включає в себе розробку та впровадження сучасних технологій захисту, які здатні виявляти та запобігати хакерським атакам, шкідливим програмам та крадіжці даних. Приклади кібербезпекових заходів включають:

– використання міцних паролів та політик безпеки;

– шифрування даних;

– фаєрволи;

– антивірусні програми та системи виявлення вторгнень.

Країни та організації активно вдосконалюють свої кібербезпекові заходи, враховуючи постійні зміни характеру та складності кіберзагроз.

Фізична безпека. Фізична безпека передбачає заходи для захисту фізичного доступу до інформаційних ресурсів та обладнання, що містять конфіденційну інформацію. Це може включати:

– встановлення контрольованого доступу до приміщень;

– використання систем відеоспостереження та біометричних ідентифікаторів;

– захист серверних кімнат та дата-центрів від несанкціонованого доступу.

Додаткові заходи можуть включати фізичний захист носіїв інформації, які зберігаються в безпечних сейфах або криптографічних пристроях.

Організаційна безпека. Організаційна безпека передбачає розробку та впровадження політик, процедур та стандартів, які регулюють безпекові практики в управлінні інформацією. Це включає:

– встановлення ролей та відповідальності з питань безпеки;

– проведення аудитів безпеки для виявлення вразливостей;

– установлення правил доступу до інформації та забезпечення її конфіденційності.

Організаційні заходи можуть також включати створення аварійних планів та процедур відновлення після інцидентів.

Кадрова безпека. Кадрова безпека передбачає прийняття заходів для забезпечення безпеки інформації, пов'язаної з персоналом державних органів та організацій. Це включає:

– перевірку кваліфікації та надійності працівників перед наданням їм доступу до конфіденційної інформації;

– проведення навчання щодо безпекових політик і процедур;

– забезпечення свідомості персоналу щодо ризиків інформаційної безпеки.

Правова безпека. Правова безпека включає в себе розробку та виконання законодавства, яке регулює захист інформації та кібербезпеку. Це включає:

– створення спеціалізованих правових норм, що стосуються захисту інформації, кримінальної відповідальності за кіберзлочини та незаконну збірку;

– збереження та поширення інформації.

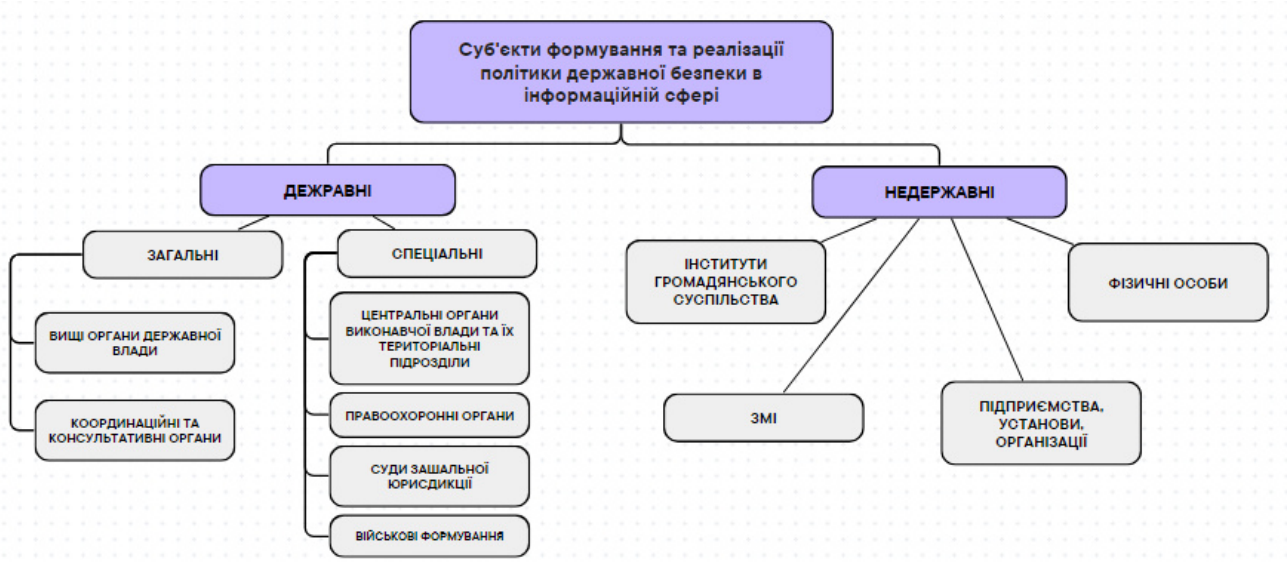
Країни також можуть встановлювати правові рамки для співпраці з міжнародними партнерами у сфері інформаційної безпеки. Різновиди забезпечення інформаційної безпеки мають важливе значення для захисту інформації та забезпечення стійкості інформаційних систем. Комплексний підхід, що об'єднує технічні, організаційні, людські та правові аспекти, є вирішальним для ефективного забезпечення інформаційної безпеки в різних країнах, включаючи Україну.

Система суб'єктів формування та реалізації політики державної безпеки в інформаційній сфері включає не лише внутрішні сили, але й міжнародну співпрацю. Країни усвідомлюють важливість міжнародного партнерства в боротьбі з поширенням дезінформації та пропаганди. Встановлення правових рамок для співпраці з міжнародними партнерами у сфері інформаційної безпеки є одним зі способів забезпечення ефективності заходів протидії.

Система суб'єктів формування та реалізації політики державної безпеки в інформаційній сфері є складною та взаємозалежною структурою, яка включає різні організації, інституції та громадськість. Головними суб'єктами є урядові органи, спеціальні служби, міністерства та відомства, які відповідають за розроблення та впровадження стратегій та програм в області інформаційної безпеки. Взаємодію цих суб'єктів показано на діаграмі 1.2.

Діаграма 1.2

«Система суб’єктів формування та реалізації політики державної безпеки в інформаційній сфері»



Для забезпечення вище наведених різновидів безпеки інформації держави, суб’єкти (рис. 1.2) використовують комплексний підхід, який включає наступні методи, підходи та заходи [14]:

1) Нормативно-правові заходи: Розробка та впровадження відповідних законодавчих актів, положень і норм, які регулюють сферу інформаційної безпеки держави. Це можуть бути закони, постанови, розпорядження, директиви, які визначають правила, обов’язки та відповідальність стосовно інформаційної безпеки.

2) Технічні заходи: Застосування різних технологічних рішень та засобів для захисту інформації. Це можуть бути системи шифрування, брандмауери, системи виявлення вторгнень, контроль доступу до інформаційних ресурсів, а також застосування технічних засобів для захисту мереж та інфраструктури.

3) Організаційні заходи: Впровадження політики інформаційної безпеки в органах державної влади та створення відповідних структур і підрозділів для координації та контролю за заходами інформаційної безпеки. Це включає розробку процедур, стандартів, нормативних актів, проведення навчань та тренінгів, а також організацію моніторингу та аудиту інформаційної безпеки.

4) Соціально-психологічні заходи: Освітня робота, інформаційні кампанії та свідоме формування поведінки та свідомості громадян щодо інформаційної безпеки.

Це можуть бути тренінги, семінари, публічні заходи, поширення інформації про загрози та заходи захисту, а також залучення громадських організацій та ЗМІ до співпраці.

Конкретні заходи можуть варіюватися залежно від країни, політичного контексту та рівня розвитку інформаційних технологій [15].

У ході дослідження теоретико-концептуальних аспектів інформаційної безпеки держави, було з'ясовано що інформаційна безпека є надзвичайно важливим аспектом сучасного світу. Вона включає захист інформації та інформаційних систем від небезпек, пов'язаних зі зловживанням, несанкціонованим доступом, крадіжкою та пошкодженням.

Безпека інформації є складною та багатогранною проблемою, яка вимагає комплексного підходу та взаємодії різних суб'єктів, включаючи державні органи, приватний сектор та громадськість. Для забезпечення інформаційної безпеки держави необхідно використовувати широкий спектр методів та заходів, таких як розробка відповідних законодавчих актів, підвищення кваліфікації фахівців, розвиток кіберзахисту та використання сучасних технологій.

Враховуючи постійні зміни технологій та загроз, держави повинні бути готовими до викликів інформаційної безпеки, посилюючи свої заходи та співпрацюючи на міжнародному рівні. Лише шляхом постійного аналізу, вдосконалення та впровадження ефективних стратегій забезпечення інформаційної безпеки держава може ефективно протистояти сучасним загрозам та зберегти свою національну безпеку й стабільність.

РОЗДІЛ 2
ЗАСАДИ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Нормативно-правова база щодо забезпечення інформаційної безпеки України

Забезпечення інформаційної безпеки України та її громадян – є пріоритетним обов'язком державних органів. Єдина для всіх державна політика у сфері інформаційної безпеки вимагає дотримання конституційних прав і свобод людини в інформаційній сфері. З початком повномасштабного вторгнення росії на територію України було запроваджено воєнний стан [16], метою якого є – створення умов органам державної влади для належного забезпечення безпеки незалежності територіальної цілісності України [17].

Правову основу інформаційної безпеки становлять законодавчі акти, нормативно-правові акти, та нормативні акти щодо інформаційної безпеки в Україні. Відповідно до яких розробляються та затверджуються стратегії, принципи, завдання (тощо) інформаційної політики.

Про Стратегію інформаційної безпеки. В лапках тезово наведе цитування нормативно правового акту, посилання на матеріал міститься у списку використаних джерел на 18-й позиції.

«Забезпечення інформаційної безпеки України є однією з найважливіших функцій держави.»

«Метою Стратегії є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору.»

«Глобальні дезінформаційні кампанії стали повсякденною практикою,(...,) яка загрожує демократичному розвитку держав та міжнародній стабільності.»

«Обмежувальні заходи (санкції) та ефективний механізм моніторингу і відповідальності за їх порушення є одним із дієвих механізмів відповіді на дезінформаційну активність Російської Федерації як держави-агресора.»

«...право на приватність (...) є одним з основних прав людини...»

«Некритичне сприйняття інформації створює загрози політичній та

економічній стабільності демократичних держав.»

«Інформаційне домінування Російської Федерації як держави-агресора на тимчасово окупованих територіях України.»

«Основними напрямами забезпечення інформаційної безпеки України є стійкість та взаємодія, для досягнення яких необхідним є виконання таких стратегічних цілей та завдань.»

Стратегія національної безпеки України [19].

«Для зміцнення позицій у Європі Російська Федерація застосовує енергетичну та інформаційну «зброю», намагається впливати на внутрішньополітичну ситуацію у європейських державах, підживлює тривалі конфлікти, збільшує військову присутність у Східній Європі.»

«Деструктивна пропаганда як ззовні, так і всередині України, використовуючи суспільні протиріччя, розпалює ворожнечу, провокує конфлікти, підриває суспільну єдність. Відсутність цілісної інформаційної політики держави, слабкість системи стратегічних комунікацій ускладнюють нейтралізацію цієї загрози.»

«Основне завдання розвитку системи кібербезпеки – гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації.»

Про захист інформації в інформаційно-комунікаційних системах [20].

«Цей Закон регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах (далі – система).»

«...зберігання державних інформаційних ресурсів та систем з метою забезпечення безперервності їх роботи та подальшого відновлення інформації...»

«Об’єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.»

«Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації.»

«Власник системи на вимогу володільця інформації надає відомості щодо захисту інформації в системі.»

«Розміщення систем та зберігання резервних копій державних інформаційних ресурсів та систем на територіях України...»

«Вимоги до забезпечення захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.»

Про державну таємницю [21].

«Контроль за додержанням законодавства про державну таємницю з метою запобігання її поширенню у пресі та інших засобах масової інформації здійснює центральний орган виконавчої влади з питань інформаційної політики.»

Про інформацію [22].

«Основними напрямами державної інформаційної політики є: забезпечення інформаційної безпеки України.»

Державне регулювання у сфері інформаційної безпеки, обумовлене реалізацією наступних цілей, які чітко сформовані у нормативно-правовому акті «Про Стратегію інформаційної безпеки» [23]:

1. Протидія дезінформації та інформаційним операціям;

2. Забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності;

3. Підвищення рівня медіакультури та медіаграмотності суспільства;

4. Забезпечення дотримання прав особи на збирання, зберігання, використання та поширення інформації;

5. Інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях, та на прилеглих до них територіях України, до загальноукраїнського інформаційного простору;

6. Створення ефективної системи стратегічних комунікацій;

7. Розвиток інформаційного суспільства та підвищення рівня культури діалогу.

При цьому регулювання охоплює, порівняно з управлінням, ширшу сферу організаційної діяльності. Управління означає цілеспрямований вплив саме на об’єкти управління, з використанням методів, що передбачають підпорядкування цих об’єктів управлінському впливу з боку суб’єкта управління. Регулювання ж

пов’язане не стільки з впливом на об’єкти управління, скільки на оточуюче середовище [24].

Крім того, існують інші закони та нормативно-правові акти, спрямовані на забезпечення безпеки інформації. Наприклад, Закон України «Про захист персональних даних», який встановлює правила збирання, обробки та зберігання персональних даних громадян. Також існують закони, які регулюють захист інформації в різних сферах, таких як банківська діяльність, телекомунікації, державна таємниця та інші.

Для ефективного впровадження нормативно-правових актів забезпечення інформаційної безпеки створені відповідні структури та органи, які відповідають за контроль та виконання законодавства. Наприклад, урядова агенція з питань кібербезпеки, органи правопорядку, спеціальні служби та інші організації активно займаються виконанням законів та норм, спрямованих на забезпечення інформаційної безпеки. Вони здійснюють розвідувальну роботу, виявляють загрози та кіберзлочини, ведуть розслідування та приймають заходи щодо притягнення винних осіб до відповідальності.

Для ефективного контролю і нагляду за дотриманням нормативно-правових актів створюються механізми моніторингу та оцінки інформаційної безпеки. Це включає аудит систем безпеки, перевірки на вразливості, аналіз інцидентів та розробку рекомендацій щодо покращення захисту інформації.

Україна також співпрацює з міжнародними організаціями та партнерами з питань інформаційної безпеки. Це включає обмін досвідом, участь у спільних проектах та програмах, координацію заходів щодо боротьби з кіберзагрозами та створення спільних механізмів реагування на них.

Україна розуміє, що безпека інформації є однією з найважливіших складових національної безпеки. Тому країна продовжуватиме активно працювати над покращенням нормативно-правової бази, розвитком кіберзахисту та підвищенням свідомості суспільства щодо інформаційної безпеки. Тільки шляхом постійного удосконалення і злагодженості усіх компонентів можна забезпечити ефективний захист інформаційного простору та відповісти викликам сучасного цифрового світу.

2.2. Принципи забезпечення інформаційної безпеки України

Принципи забезпечення інформаційної безпеки України [25] є фундаментальними принципами, що визначають підходи та принципові положення, необхідні для ефективного захисту інформації в країні. Вони мають вирішальне значення для забезпечення національної безпеки, економічного розвитку та збереження довіри до інформаційних систем.

Основними принципами забезпечення інформаційної безпеки України є:

– верховенство права;

– пріоритетність захисту прав і свобод людини і громадянина в інформаційній сфері;

– своєчасність і адекватність заходів захисту життєво важливих національних інтересів України від реальних і потенційних загроз інформаційній безпеці;

– захист інформаційного суверенітету України;

– свобода думки і слова та вільне вираження своїх поглядів і переконань;

– свобода збирати, зберігати, використовувати та поширювати інформацію;

– захищеність особи від втручання в її особисте та сімейне життя;

– обмеження доступу до інформації виключно на підставі закону;

– гармонізація особистих, суспільних і державних інтересів, відповідальність всього Українського народу за забезпечення інформаційної безпеки;

– розмежування повноважень, взаємодія та відповідальність державних і недержавних суб'єктів забезпечення інформаційної безпеки;

– пріоритетність розвитку та поширення національних інформаційних технологій, ресурсів, продукції та послуг, а також політика постійного поліпшення кількості та технічної якості каналів передачі інформації;

– можливість задіяння в інтересах забезпечення інформаційної безпеки України систем і механізмів міжнародної та колективної безпеки;

– гармонізація інформаційного законодавства з нормами міжнародного права і правовими актами Європейського Союзу;

– захист інформаційного суверенітету, державного суверенітету, конституційного ладу і територіальної цілісності України;

– формування в інформаційному просторі української ідентичності як невід'ємної складової сталого суспільно-політичного дискурсу;

– формування дуальної системи суспільного та комерційного мовлення;

– сприяння розвитку в національному інформаційному просторі контенту, який підтримує збереження і захист загальнолюдських цінностей, інтелектуальний, духовний і культурний розвиток Українського народу.

Один з основних аспектів принципів забезпечення інформаційної безпеки – це усвідомлення того, що це питання є відповідальністю всіх суб'єктів, включаючи державні органи, приватний сектор, громадян та міжнародних партнерів. Дотримання принципів забезпечення інформаційної безпеки є загальнонаціональною задачею, яка потребує спільних зусиль та координації всіх зацікавлених сторін.

Принципи забезпечення інформаційної безпеки регулюються законодавчими актами та нормативно-правовими документами, що стосуються цієї сфери. Найважливішими з них є:

1) Закон України «Про основні засади забезпечення кібербезпеки України», який визначає правові, організаційні та технічні аспекти забезпечення кібербезпеки в Україні. Він встановлює положення про органи державної влади, які відповідають за кібербезпеку, та визначає механізми координації їх дій.

2) Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який визначає правові принципи захисту інформаціції в інформаційно-телекомунікаційних системах, включаючи вимоги до безпеки, захисту персональних даних та конфіденційності інформації. Закон передбачає встановлення відповідальності за порушення вимог щодо захисту інформації та встановлює процедури контролю та нагляду за дотриманням цих вимог.

3) Національна стратегія кібербезпеки України, яка визначає загальну стратегію та пріоритети в галузі кібербезпеки. Вона встановлює основні напрямки розвитку кібербезпекового сектора, механізми координації, розподіл завдань та відповідальності між зацікавленими сторонами.

Дотримання принципів забезпечення інформаційної безпеки контролюється

кількома органами та структурами. Одним з них є Державна служба спеціального зв'язку та захисту інформації, яка відповідає за координацію та реалізацію політики у сфері захисту інформації. Крім того, існують спеціальні відділи та підрозділи у міністерствах, державних органах та інших установах, які забезпечують безпеку інформації у своїх сферах діяльності.

Дотримання принципів забезпечення інформаційної безпеки є основою для ефективного захисту інформаційних ресурсів та інфраструктури країни. Вони сприяють запобіганню втрати конфіденційної інформації, викриттю вразливостей інформаційних систем, а також захисту важливих державних, комерційних та особистих даних.

Забезпечення інформаційної безпеки в Україні здійснюється через систему контролю, координації та співпраці між різними органами та структурами. Основні органи, відповідальні за забезпечення інформаційної безпеки, включають:

а) Державна служба спеціального зв'язку та захисту інформації (далі: ДССЗЗІ): ДССЗЗІ виконує ключову роль у забезпеченні інформаційної безпеки в Україні. Вона координує роботу з питань кібербезпеки, розробляє політику, нормативно-правову базу та стратегії у цій сфері. ДССЗЗІ також здійснює контроль та моніторинг за дотриманням принципів інформаційної безпеки.

б) Міністерство цифрової трансформації: Це відомство відповідає за розвиток та захист інформаційних технологій, забезпечення кібербезпеки в сфері державних інформаційних систем. Воно співпрацює з ДССЗЗІ та іншими зацікавленими органами для впровадження ефективних заходів безпеки.

в) Національна поліція та Служба безпеки України: Ці органи відповідають за розслідування кіберзлочинів, протидію кібершпигунству та кібертероризму. Вони займаються ідентифікацією та припиненням кібератак, забезпечують правоохоронний аспект інформаційної безпеки.

г) Національний банк України (далі: НБУ): НБУ відповідає за захист фінансової системи країни від кіберзагроз. Він розробляє та впроваджує стратегії та політику забезпечення кібербезпеки в банківському секторі, співпрацює з іншими органами та міжнародними партнерами для обміну інформацією та координації

заходів безпеки.

д) Національна комісія з питань регулювання зв'язку та інформатизації (далі: НКРЗІ): Цей орган відповідає за регулювання та контроль за діяльністю операторів зв'язку та постачальників інтернет-послуг. Він забезпечує захист мережі зв'язку та інфраструктури від кібератак, а також встановлює вимоги до захисту персональних даних користувачів.

2.3. Загрози інформаційній безпеці України

Україна, як і багато інших країн, стикається зі значними загрозами інформаційній безпеці, особливо в контексті російсько-української війни, що триває з 2014 року. Кіберпростір став полем битви, де ворог може атакувати невидимо, наносячи значну шкоду державним структурам, критичній інфраструктурі та громадянам. Нижче будуть наведені основні загрози інформаційній безпеці України.

Кібератаки, які спрямовані на державні інституції, критичну інфраструктуру, бізнес-сектор та громадян. Ці атаки можуть бути виконані хакерами, кіберзлочинцями або державними акторами з метою здобуття конфіденційної інформації, викрадення грошей, розповсюдження деструктивного програмного забезпечення тощо.

Кібершпигунство: Україна є об'єктом кібершпигунства, яке виконується іноземними державами або хакерськими групами з метою здобуття та зловживання конфіденційною інформацією, включаючи політичні, військові, економічні та технологічні дані.

Дезінформація та кіберпропаганда: Україна стикається зі значною кількістю дезінформації та кіберпропаганди, які мають на меті впливати на громадську думку, змінювати переконання, роз'єднувати суспільство та порушувати довіру до державних інституцій.

Соціальний інжиніринг: це метод, який використовується зловмисниками для отримання доступу до конфіденційної інформації шляхом маніпулювання людьми. Соціальний інжиніринг може включати фішинг, фармінг, використання шкідливих посилань та інше.

Кібертероризм: Україна стикається з загрозою кібертероризму, який включає кібератаки з метою нанесення шкоди державним інституціям, критичній інфраструктурі, енергетичним системам, транспортним мережам тощо. Кібертерористичні дії можуть призвести до порушення роботи важливих систем і негативно вплинути на економіку та безпеку країни.

Викрадення даних: зловмисники можуть спробувати викрасти конфіденційні дані, такі як персональні дані громадян, банківські дані, комерційну інформацію тощо. Ці дані можуть використовуватися для крадіжок, шахрайства, шпигунства або іншої злочинної діяльності.

Віруси та шкідливе програмне забезпечення: розповсюдження вірусів, шкідливого програмного забезпечення та троянських програм є серйозною загрозою для інформаційної безпеки. Ці програми можуть спричинити виток конфіденційної інформації, пошкодження даних, обмеження доступу до систем та інші негативні наслідки.

Проблему забезпечення інформаційної безпеки необхідно розглядати в загальнодержавному вимірі. У державному механізмі забезпечення інформаційної безпеки мають бути враховані національні інтереси в інформаційному середовищі, внутрішні та зовнішні загрози цим інтересам і передбачена система засобів виявлення та нейтралізації загроз. Він обов'язково має включати двосторонній зв'язок між суспільством, ЗМІ й державою, який допоможе своєчасно сповістити про зміни громадської думки під цілеспрямованим впливом та оцінювати ефективність заходів з протидії [26].

У відповідь на масштабні атаки росії з використанням «інформаційної» зброї, для розповсюдження фейків та пропаганди було прийнято Указ, у 2016 та 2021 роках, Про Національну стратегію кібербезпеки [27]. Україна робить кроки в її реалізації. Створення Національного координаційного центру з кібербезпеки у 2016 році та запропоноване оновлення законодавства про кіберзлочинність відповідно до вимог Будапештської конвенції, зокрема щодо постачальників послуг Інтернету, є двома основними кроками на шляху підвищення кіберстійкості країни. Ця діяльність доповнюється тісною співпрацею з міжнародними партнерами в

кіберсфері, зокрема щодо кіберзлочинності та кіберзахисту.

В умовах воєнного стану важливо бути озброєним та вести боротьбу як на воєнному фронті так і інформаційному. Захист національного інформаційного простору та гарантування інформаційної безпеки є пріоритетними стратегічними завданнями. Збереження інформаційного суверенітету, формування ефективної системи безпеки в інформаційній сфері є актуальною проблемою України.

В Україні триває процес становлення системи стратегічних комунікацій та зміцнення інституційної спроможності у сфері стратегічних комунікацій [28]. Також в процесі створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам.

На сучасному етапі, в умовах російсько-української війни, ситуація наступна: на території України продовжують блокувати російські сайти та канали телебачення; великий акцент поставлено на залучення підтримки міжнародної спільноти та необхідності надання Україні допомоги у вигляді зброї, гумунітарної допомоги тощо; створення і розповсюдження національного інформаційного продукту як на території України, так і за її межами.

Для боротьби з цими загрозами і забезпечення інформаційної безпеки в Україні було впроваджено Механізм забезпечення інформаційної безпеки України. Механізм забезпечення інформаційної безпеки слід розглядати як: систему державно-правових інституцій; систему з власною структурою; систему різних засобів; сукупність державних органів, громадських структур, заходів, важелів і способів дій [29].

Правову основу інформаційної безпеки становлять Конституція України, Закон України «Про основи національної безпеки України» та інші закони України, міжнародні договори, згода на обов’язковість яких надана Верховною Радою України. Правові норми складають базу забезпечення інформаційної безпеки і визначають ефективність діяльності держави, суспільства та окремих громадян із захисту національних інтересів України в інформаційній сфері.

Особливою структурною складовою частиною державного механізму є інституційний механізм забезпечення інформаційної безпеки, що забезпечує

створення норм і правил, які регулюють взаємодію різних економічних суб'єктів в інформаційній сфері щодо запобігання загроз інформаційній безпеці.

Формування, реалізацію та координацію державної інформаційної політики, а також забезпечення інформаційного суверенітету України здійснює спеціально уповноважений центральний орган виконавчої влади відповідно до покладених на нього функцій.

Україна приділяє велику увагу виявленню, відслідковуванню та боротьбі зі загрозами інформаційній безпеці. В сучасному цифровому світі, де кібератаки та кіберзлочини стають все поширенішими, забезпечення безпеки інформації стає необхідністю для збереження стабільності, захисту державних інтересів та захисту прав та свобод громадян.

Загрози інформаційній безпеці українського суспільства невпинно зростають. Російська агресія, яка розпочалася в 2014 році, принесла з собою нову реальність бойових дій в кіберпросторі. Кібератаки на українські державні інституції, енергетичні об'єкти, медіа та приватні компанії стали поширеними явищами. Ці атаки мають на меті зламати критичну інфраструктуру, викрасти конфіденційну інформацію та порушити роботу суспільства в цілому.

Загрози інформаційній безпеці України залишаються важливим викликом, вимагаючи постійного вдосконалення та усунення вразливостей. Уряд України продовжує активно працювати над розвитком кібербезпеки, вдосконаленням законодавства, підвищенням кваліфікації фахівців та співпрацею з іншими країнами. Застосування сучасних технологій, розробка імунітету до кібератак, підвищення кіберсвідомості та ефективне співробітництво є ключовими факторами успішної боротьби зі загрозами інформаційній безпеці.

РОЗДІЛ 3
ПОЛІТИКА УКРАЇНИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ РОСІЙСЬКОЇ АГРЕСІЇ

3.1. Заходи з реалізації стратегії інформаційної безпеки України

Для України пріоритетним є розбудова стійкої кіберекосистеми, яка об'єднує державні інституції, приватний сектор, академічні установи та громадські організації. Це сприяє забезпеченню цілісності і безпеки інформаційного простору, а також забезпечує взаємодію і спільні зусилля для виявлення, відслідковування та протидії загрозам. Крім того, уряд вдосконалює систему реагування на інциденти кібербезпеки та розробляє механізми для оперативного втручання та відновлення роботи після кібератак.

У боротьбі зі загрозами інформаційній безпеці України, велика увага приділяється розвитку законодавства та регулювання в галузі кібербезпеки. Україна активно працює над вдосконаленням нормативно-правової бази, яка ставить цілісні рамки для захисту інформації. Закони та нормативні акти регулюють питання захисту персональних даних, кіберпротиборства, карантинування інформації та відповідальності за кіберзлочини. Це сприяє покращенню координації дій між різними державними органами, спеціалізованими службами та приватними компаніями для ефективної боротьби з кіберзагрозами.

Інформаційні заходи оборони держави – сукупність скоординованих дій, які готуються та здійснюються суб'єктами забезпечення національної безпеки і оборони України щодо:

– прогнозування та виявлення інформаційних загроз у воєнній сфері;

– запобігання, стримування та відсічі збройній агресії проти України;

– протидії інформаційним загрозам з боку держави-агресора;

– здійснення інших необхідних дій в інформаційному протиборстві [30].

Захист інформаційної безпеки є однією з головних складових інформаційної політики України. Україна стикається з викликами сучасного кіберпростору, де кібератаки, кібершпигунство та кіберзагрози є досить розповсюдженими та їх

частота зростає. Для ефективного протидії таким загрозам, Україна розробляє та впроваджує комплексні заходи з кібербезпеки. Відбувається активна співпраця з міжнародними партнерами для обміну досвідом та інформацією щодо кібербезпеки. Також проводяться навчання та тренування фахівців з кібербезпеки для забезпечення надійного захисту державних інформаційних ресурсів.

Україна активно працює над розвитком інформаційного суспільства. З метою створення розвинутої інформаційної інфраструктури та підвищення рівня доступу до інформації, проводяться заходи щодо розвитку широкосмугового Інтернету, електронного урядування та електронних сервісів. Важливим напрямком є забезпечення громадськості доступом до вільного слова та свободи висловлювання, а також зміцнення медійної грамотності інформаційними кампаніями та освітніми заходами.

Формування позитивного іміджу України – ще одна складова інформаційної політики країни. Зусилля спрямовані на просування та пропаганду України в міжнародному масштабі. Інформаційна дипломатія грає важливу роль у встановленні довіри, підтримці національних інтересів та залученні іноземних інвестицій.

Також важливою складовою інформаційної політики є розвиток національних мов і культури. Захист та просування української мови є пріоритетною задачею. Проводяться заходи для зміцнення використання української мови у всіх сферах суспільного життя, розвитку літератури, кіно та мистецтва.

У світі, де інформація стає все більшим ресурсом, Україна активно працює над розвитком своєї інформаційної політики. Забезпечення інформаційної безпеки, створення інформаційного суспільства, просування своїх інтересів та підвищення культурного рівня нації – це головні пріоритети інформаційної політики України.

План заходів з реалізації Стратегії інформаційної безпеки, який був затверджений 30 березня 2023 року, є важливим документом, спрямованим на забезпечення безпеки інформації в Україні. Цей план розрахований на період до 2025 року і включає ряд конкретних заходів, спрямованих на покращення захисту інформації, боротьбу з кіберзагрозами та розвиток інформаційного суспільства.

Основні напрямки та заходи, передбачені в Плані [31], включають:

а) законодавче регулювання та нормативна база забезпечує правовий каркас для захисту інформації, встановлює вимоги щодо кібербезпеки та регламентує діяльність органів та структур, які відповідають за забезпечення безпеки інформації. Детальніше:

1) проведення аналізу та вдосконалення законодавства щодо інформаційної безпеки (проведення комплексного аналізу діючого законодавства та виявлення прогалин, які необхідно заповнити з метою забезпечення ефективного захисту інформації; внесення пропозицій щодо вдосконалення законодавства, враховуючи сучасні виклики та технологічні тренди в галузі інформаційної безпеки; розробка проектів законів та положень, які сприятимуть покращенню захисту інформації та розвитку кібербезпеки в Україні);

2) розробка нових законів, спрямованих на регулювання питань кібербезпеки та захисту персональних даних (розробка та ухвалення нових законів, що регулюють питання кібербезпеки, включаючи захист критично важливих інформаційних систем та критичних інфраструктур; визначення вимог щодо захисту персональних даних громадян, в тому числі відповідно до міжнародних стандартів та норм);

3) забезпечення введення механізмів контролю та відповідальності за порушення законодавства щодо інформаційної безпеки (встановлення системи контролю за дотриманням вимог інформаційної безпеки та кібербезпеки в органах державної влади, державних установах та критичних секторах; розробка механізмів виявлення, розслідування та реагування на кіберінциденти та кіберзлочини; встановлення відповідальності за порушення законодавства щодо інформаційної безпеки, включаючи встановлення адміністративних, цивільних та кримінальних санкцій.)

б) кібербезпека та захист інформації спрямовані на забезпечення захисту інформаційних систем, даних та інфраструктури від кіберзагроз та кібератак. Детальніше:

1) розробка та впровадження системи кібербезпеки (розробка та впровадження комплексних технічних засобів захисту інформаційних систем, включаючи системи

виявлення та запобігання кібератак, моніторингу та аналізу кіберзагроз; створення центрів кібербезпеки та оперативного реагування на кіберінциденти, які забезпечуватимуть постійний моніторинг, виявлення та реагування на кібератаки; вдосконалення системи ідентифікації та автентифікації користувачів, включаючи багатофакторну аутентифікацію та використання сучасних технологій шифрування.)

2) розвиток кадрового потенціалу та підвищення кваліфікації фахівців (проведення навчальних програм та тренінгів з кібербезпеки для працівників державних органів, підприємств та громадських організацій; залучення висококваліфікованих фахівців у галузі кібербезпеки та проведення обміну досвідом з міжнародними партнерами; підтримка освітніх закладів, які надають спеціалізовану підготовку з кібербезпеки та захисту інформації.)

3) проведення аудиту та оцінка ризиків (проведення систематичних аудитів інформаційних систем з метою виявлення потенційних вразливостей та визначення ризиків для інформаційної безпеки; впровадження процесу оцінки ризиків, який дозволить визначити пріоритетні напрямки заходів з кібербезпеки та прийняти відповідні заходи для зниження ризиків.)

4) регулювання та законодавче забезпечення (розробка та прийняття законодавчих актів щодо кібербезпеки та захисту інформації, включаючи створення механізмів реагування на кіберінциденти та встановлення відповідальності за порушення законодавства; забезпечення взаємодії між відповідними органами у сфері кібербезпеки та обміну інформацією про кіберзагрози.)

5) партнерство з міжнародними організаціями та країнами (розробка та укладання міжнародних угод та партнерських відносин з країнами та міжнародними організаціями у сфері кібербезпеки та обміну інформацією про кіберзагрози; участь у міжнародних ініціативах та форумах з метою обміну досвідом та спільного розв’язання кіберпроблем.)

в) забезпечення інформаційної безпеки громадян спрямоване на захист особистих даних громадян, підвищення свідомості щодо кібербезпеки та забезпечення їх безпеки в інформаційному просторі. Детальніше:

1) підвищення свідомості про кібербезпеку (організація інформаційних

кампаній та навчальних заходів для громадян щодо основних принципів кібербезпеки, включаючи захист особистих даних, паролів та використання безпечних онлайн-послуг; розроблення та поширення практичних порад та рекомендацій щодо кібербезпеки, включаючи застосування антивірусного програмного забезпечення, оновлення програм та операційних систем, а також перевірку достовірності посилань та електронних повідомлень);

2) захист особистих даних (забезпечення правового захисту особистих даних громадян та розроблення відповідних нормативно-правових актів щодо зберігання, обробки та передачі особистих даних; застосування технічних засобів захисту особистих даних, таких як шифрування, анонімізація та механізми контролю доступу);

3) попередження шахрайства та кібератак (створення механізмів співпраці з правоохоронними органами та кібербезпековими службами для виявлення та припинення шахрайства та кібератак, спрямованих на громадян; проведення навчальних заходів та поширення інформації про типові шахрайські схеми та методи кібератак, що допомагають громадянам уникнути шахрайства та захистити свою інформацію);

4) забезпечення безпеки від дитячої онлайн-експлуатації (розроблення та впровадження механізмів захисту дітей від шкідливого контенту, онлайн-експлуатації та кіберзагроз; залучення батьків, освітніх закладів та громадських організацій до навчання та популяризації безпечного використання Інтернету серед дітей);

5) підтримка жертв кіберзлочинності (створення механізмів підтримки та захисту жертв кіберзлочинності, включаючи консультування, психологічну підтримку та допомогу відновлення після інциденту).

г) міжнародне співробітництво спрямоване на спільні зусилля з іншими країнами та міжнародними організаціями з метою виявлення, запобігання та реагування на кіберзагрози, обміну інформацією та досвідом, а також встановлення стандартів та правил в галузі кібербезпеки. Детальніше:

1) укладання міжнародних угод та партнерство (укладання двосторонніх та

багатосторонніх угод з іншими країнами щодо спільної боротьби з кіберзагрозами, обміну інформацією про кібератаки та кіберінциденти; підтримка партнерських відносин з міжнародними організаціями, такими як ООН, Європейський Союз, НАТО, Інтерпол та інші, для спільних заходів у сфері кібербезпеки та обміну інформацією);

2) обмін інформацією та досвідом (встановлення механізмів обміну інформацією про виявлені кіберзагрози, нові методи та технології в сфері кібербезпеки; організація міжнародних конференцій, семінарів та тренінгів з питань кібербезпеки з метою обміну досвідом та навчання фахівців з країн-партнерів);

3) спільні оперативні дії та реагування (організація спільних оперативних дій з іншими країнами щодо реагування на кібератаки та кіберінциденти, включаючи обмін інформацією про ідентифікованих злочинців та зловживання в мережі; спільне розроблення та впровадження стратегій і планів надзвичайних ситуацій у випадку масштабних кібератак);

4) створення міжнародних стандартів та правил (участь у розробці міжнародних стандартів та правил в галузі кібербезпеки, включаючи визначення мінімальних вимог до захисту інформації та інформаційних систем; адаптація міжнародних стандартів та правил до національного законодавства та специфіки країни).

Заходи з реалізації стратегії інформаційної безпеки України є важливою складовою частиною загального плану дій, спрямованих на захист інформації та забезпечення кібербезпеки в країні. Вони розроблені з метою зміцнення захисту державних інформаційних ресурсів, протидії кіберзагрозам, забезпечення безпеки персональних даних та підвищення свідомості громадян щодо інформаційної безпеки.

3.2. Методи й засоби забезпечення інформаційної безпеки України в умовах війни

Україна знаходиться в умовах російсько-української війни, яка розпочалася в 2014 році. Цей конфлікт має багатовимірний характер, включаючи збройну агресію,

гібридну війну та інформаційну боротьбу. У цьому контексті роль інформації стає надзвичайно важливою, оскільки вона використовується як засіб впливу на суспільство та формування образу конфлікту.

Російсько-українська війна виникла в результаті комплексу причин, що привели до ескалації конфлікту. Однією з основних причин було анексування росією Криму в 2014 році, що порушило принципи міжнародного права та територіальної цілісності України. Політичні суперечності, етнічні та релігійні конфлікти, економічні труднощі та прагнення росії зміцнити своє впливне становище на пострадянському просторі.

Війна має складний характер, поєднуючи збройні військові операції, гібридну війну та інформаційні маніпуляції. російська сторона використовує тактику хибного вторгнення, що полягає в розгортанні незаконних збройних формувань на території України та постійному наданні військової та іншої допомоги. Зі свого боку, Україна мобілізує власні сили для захисту територіальної цілісності та ведення контрнаступу.

Україна знаходиться у стані гібридної війни, яка негативно впливає на свідомість українського населення. Наша країна, подібно до більшості розвинутих держав, була недостатньо підготовлена до такої форми агресії з боку Росії. Одним із підтверджень цього є відсутність чітких правил поведінки в умовах інформаційної агресії та пропаганди. Особливо відчутним викликом для України стала масштабна російська пропаганда, яка виходить за межі нашої країни. Таким чином, забезпечення інформаційної безпеки стає одним з основних факторів стійкого розвитку національної безпеки.

Для протидії гібридним загрозам та запобігання їх появі Україна змушена використовувати заходи інформаційного захисту держави. В сучасних умовах інформаційні війни охоплюють всі сфери життя, включаючи ідеологію, релігію, історію та освіту. Тому надзвичайно важливо забезпечити інформаційну безпеку, особливо в умовах гібридної війни. Таким чином, основними пріоритетами державної інформаційної політики повинні бути гарантування інформаційної безпеки особистості, захист її психіки та свідомості від шкідливого інформаційного

впливу, дезінформації та маніпуляцій.

Для виявлення та відслідковування кіберзагроз Україна докладає значних зусиль. Країна створила спеціалізовані кібербезпекові служби, які відповідають за виявлення інцидентів, аналіз вразливостей та розробку заходів для протидії кібератакам. Важливу роль у виявленні загроз відіграють також співпраця з міжнародними партнерами та обмін інформацією з іншими країнами. Це дозволяє вчасно реагувати на загрози та ефективно протидіяти їм.

Необхідно зазначити, що російсько-українська війна, яка триває з 2014 року, має суттєвий вплив на інформаційну безпеку України. Російська пропагандистська машина активно використовує кіберпропаганду та дезінформацію з метою маніпулювання громадською думкою, створення розколу та дестаборізацію в українському суспільстві. Це створює значні виклики для інформаційної безпеки, оскільки маніпулювання інформацією та поширення фейкових новин можуть спричинити соціальну нестабільність, збільшення конфліктів та порушення суспільного порядку.

Для ефективного протистояння гібридній війні, Україна повинна ретельно вивчити методи, якими користується ворог у її веденні. Російсько-українська війна є прикладом гібридного конфлікту, в якому використовуються широкий спектр методів, включаючи інформаційну пропаганду, дезінформацію, кібератаки, вплив на масову свідомість та інші.

У цьому контексті велике значення має моніторинг загроз інформаційної безпеки, який здійснюють різні центри та організації. Наприклад, Національний центр кібербезпеки України здійснює постійний моніторинг кіберзагроз, виявляє і аналізує атаки на державні інформаційні системи та реагує на них. Також, Управління з питань інформаційної безпеки та спеціальних технологій Служби безпеки України займається моніторингом загроз інформаційній безпеці, виявленням та припиненням діяльності організацій, які сприяють гібридним загрозам.

Крім того, існують також громадські організації та ініціативи, які займаються моніторингом та аналізом інформаційних загроз. Наприклад, Громадська рада при

Державному агентстві з питань електронного урядування в Україні проводить моніторинг і аналіз інформаційної безпеки, сприяє розробці та впровадженню заходів щодо захисту від кіберзагроз та пропаганди.

Такі центри та організації виконують важливу роль у забезпеченні інформаційної безпеки країни. Їхні дії спрямовані на виявлення, аналіз та протидію загрозам інформаційної безпеки, а також на посилення свідомості громадськості щодо гібридних загроз. Розуміння методів, використованих ворогом, дозволяє ефективніше реагувати на них і розробляти відповідні заходи для захисту національної безпеки та інформаційного простору країни.

Державні та недержавні українські організації що займаються питанням забезпечення інформаційної безпеки:

Служба безпеки України (СБУ): СБУ є головним державним органом забезпечення національної безпеки і виконує функції щодо розкриття, запобігання та припинення діяльності інформаційних загроз та кібератак, які спрямовані на Україну.

Міністерство внутрішніх справ України (МВС): МВС займається контролем і протидією кіберзлочинності, забезпеченням безпеки в інформаційному просторі та викриттям осіб, що сприяють дезінформації та пропаганді.

Міністерство оборони України (МОУ): МОУ відповідає за захист інформаційних систем, комунікацій та інших важливих інфраструктурних об’єктів від кібератак, а також за формування та розвиток кібервійськових сил.

Державна служба спеціального зв’язку та захисту інформації України (ДССЗІ): ДССЗІ відповідає за захист державної інформації, криптографічну безпеку, захист інформаційних систем та виконання інших завдань, пов’язаних із забезпеченням інформаційної безпеки.

Національна поліція України: Національна поліція веде боротьбу з кіберзлочинністю, включаючи розслідування та припинення діяльності кіберзлочинців, які діють у мережі Інтернет з метою пошкодження інтересів України.

Національний кіберцентр України (CERT-UA): CERT-UA є координаційним

центром з виявлення, реагування та врегулювання кіберінцидентів. Вони ведуть моніторинг загроз інформаційної безпеки та надають підтримку організаціям та громадянам в усуненні кіберзагроз.

Для досягнення поставленої мети вище перелічені організації використовують наступні методи та засоби:

– Україна активно розвиває свої кіберзахисні здібності. Це включає захист інформаційних систем, мереж і даних від кібератак, виявлення та розслідування кіберзлочинів, розробку та впровадження кібербезпечних політик та стандартів;

– легіслятивні та нормативні заходи. Україна приділяє велику увагу розробці та впровадженню законодавства, яке регулює сферу інформаційної безпеки. Це включає прийняття законів та нормативних актів, які регулюють захист даних, кібербезпеку, контроль за інформаційними потоками тощо;

– співробітництво з міжнародними партнерами. Україна активно співпрацює з міжнародними партнерами, такими як Європейський Союз, НАТО, Організація з безпеки і співробітництва в Європі (ОБСЄ) тощо. Це сприяє обміну досвідом, координації заходів щодо забезпечення інформаційної безпеки та підтримці в усуненні загроз;

– розвиток кіберрозвідки. Україна розвиває свої кіберрозвідувальні здібності для виявлення та моніторингу кіберзагроз. Це включає аналіз активності ворожих кіберакторів, виявлення нових загроз та розробку стратегій протидії;

– інформаційна освіта та свідомість: Україна надає велику увагу підвищенню рівня інформаційної освіти та свідомості серед населення. Це включає розробку освітніх програм, проведення інформаційних кампаній, тренінгів та семінарів з питань інформаційної безпеки;

– розвиток медійної сфери. Україна сприяє розвитку незалежних та об’єктивних медіа, які грають важливу роль у розповсюдженні правдивої та достовірної інформації. Це сприяє протидії дезінформації та пропаганді;

– розвиток та захист критично важливої інфраструктури. Україна зосереджує зусилля на захисті критично важливої інфраструктури, такої як енергетичні мережі, телекомунікаційні системи, фінансові установи тощо. Це включає застосування

захисних технологій, резервування систем, розробку планів надзвичайних ситуацій.

Ці засоби забезпечення інформаційної безпеки української держави в умовах російсько-української війни спрямовані на забезпечення захисту інформаційних ресурсів, виявлення та протидію загрозам, підвищення інформаційної свідомості та забезпечення стабільності держави.

3.3. Механізми протидії поширенню російської пропаганди та дезінформації

Однією з головних проблем, з якими стикається Україна, є дезінформація та інформаційні операції, зокрема з боку держави-агресора. Ці операції спрямовані на:

– підрив незалежності України, зрушення конституційного ладу;

– порушення суверенітету та територіальної цілісності країни

– поширення пропаганди війни, насильства та жорстокості;

– розпалювання національної, міжетнічної, расової та релігійної ворожнечі та ненависті;

– а також здійснення терористичних актів та порушення прав та свобод людини.

Україна завжди привертала увагу російської пропаганди, яка спотворює події та факти, намагаючись виправдати свої дії. Починаючи з «failed state», що не може зберегти свою незалежність, до спроб мобілізувати населення та створити міжетнічну ворожнечу, російська пропаганда намагалась створити негативне уявлення про Україну. Однак спроба представити окупантів як визволителів не була успішною, а вбивства мирного населення нівелювали їхні сподівання.

Після анексії Криму та подій на Донбасі пропаганда рф зосередилась на натяках про злочини української влади, втручанні США та НАТО та виправданні вторгнення. Вона також використовувала техніку «віддзеркалення», фальсифікувала звинувачення та залучала проросійських експертів та журналістів. Однак підтримка України з боку міжнародного співтовариства та викриття маніпуляцій допомогли зменшити вплив російської пропаганди [32].

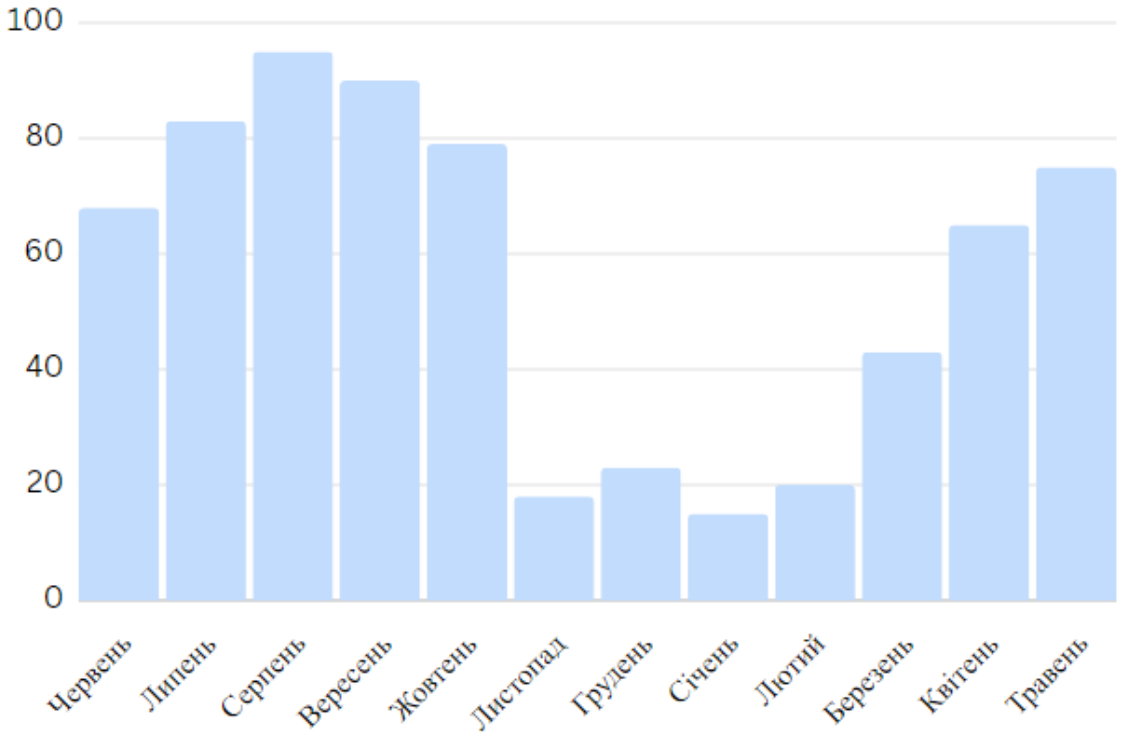
Для того що розуміти як боротися з фейками їх потрібно вміти

відслідковувати та знати їх характер та цільову аудиторію на яку вони направлені. Одним з основних механізмів поширення російської пропаганди є використання проплачених агентів, які просувають російський дискурс через медіа та соціальні мережі. Ці агенти створюють фейкові новини, маніпулюють інформацією та створюють штучні конфлікти з метою посіяти розбрат та неспокій у суспільстві.

Центр протидії дезінформації при РНБО відіграє провідну роль у виявленні і представленні фейкової інформації. Основною метою центру є не розголошення фейків, а скоріше встановлення факту, що конкретна інформація є неправдивою. За період згаданий вище, Центр протидії дезінформації при РНБО виявив 674 випадки фейкових новин. Найбільша кількість фейків припадає на серпень – 95. Загальну кількість фейків по місяцям, виявлених Центром протидії дезінформації, наведено на діаграмі 3.1 [40].

Діаграма 3.1

«Кількість фейків публікованих рф за період червень 2022 р. – травень 2023 р.»



Українські організації та урядові інституції активно працюють над механізмами протидії поширенню російської пропаганди. Для цього використовуються заходи, такі як фактчекінг, розкриття фейків, освітні програми та просування критичного мислення серед населення. Також важливою є співпраця з

міжнародними партнерами та організаціями з метою обміну інформацією та координації зусиль у протидії російській пропаганді.

Наступним кроком є розповсюдження правдивої інформації що є одним із ключових механізмів протидії поширенню російської пропаганди та дезінформації в Україні. Для досягнення цієї мети, українські владні структури, громадські організації та незалежні медіа активно працюють над налагодженням ефективної комунікаційної системи, яка забезпечує поширення достовірної та об'єктивної інформації на різних рівнях.

Одним з найважливіших аспектів розповсюдження правдивої інформації є створення та підтримка незалежних медіаорганізацій. Україна підтримує розвиток незалежних телеканалів, радіостанцій, онлайн-видань та інших джерел інформації, які забезпечують об'єктивне висвітлення подій. Це створює можливість для громадян отримувати різноманітні та достовірні перспективи на події в країні та світі.

Для забезпечення широкого доступу до правдивої інформації, Україна активно розвиває інформаційні технології та мережу Інтернет. Розповсюдження новин, офіційних заяв, фактичних даних та іншої інформації через соціальні мережі, веб-платформи та мобільні додатки стає все більш поширеним. Такий підхід дозволяє швидко та ефективно донести правдиву інформацію до широкої аудиторії, особливо серед молодого покоління, яке активно використовує ці технології.

Крім того, українські владні структури сприяють активному залученню громадськості до процесу розповсюдження правдивої інформації. Залучення громадських організацій, експертів, активістів та журналістів до створення і поширення інформації забезпечує більшу об'єктивність та довіру до наданої інформації. Відкриті публічні дискусії, конференції, тренінги та інші заходи стимулюють обмін ідеями та думками, що сприяє формуванню критичного мислення та вмінню розпізнавати дезінформацію.

Загальна культура медіаграмотності та критичного мислення серед громадян також відіграє важливу роль у розповсюдженні правдивої інформації. Зростаюча увага до медіаосвіти в освітніх програмах та в позашкільних заходах допомагає

формувати у населення навички аналізу інформації, перевірки її достовірності та розуміння основних принципів функціонування ЗМІ.

Не менш важливим кроком є співпраця з іншими країнами та міжнародними організаціями, зокрема Європейським Союзом, НАТО, Організацією з безпеки і співробітництва в Європі (ОБСЄ) та іншими, з метою створення спільної стратегії та координації заходів протидії.

Один з важливих аспектів міжнародного співробітництва полягає в обміні інформацією між різними країнами. Україна активно співпрацює з партнерами, надаючи їм інформацію про російську пропаганду та дезінформацію, що походить з її території. Взаємний обмін інформацією дозволяє країнам отримувати більш повне уявлення про масштаби проблеми та розробляти спільні стратегії протидії.

Крім того, Україна співпрацює з міжнародними організаціями з метою координації заходів протидії російській пропаганді. В рамках цієї співпраці відбуваються зустрічі, конференції та семінари, на яких обговорюються тенденції в сфері розповсюдження дезінформації та виробляються спільні стратегії для її протидії. Такі формати співробітництва сприяють обміну досвідом та виявленню найкращих практик у сфері інформаційної безпеки.

Додатково, Україна здійснює спільні проекти з іншими країнами та міжнародними партнерами з метою підвищення інформаційної безпеки. Ці проекти можуть включати обмін експертами, спільні навчальні програми, створення спільних інформаційних ресурсів та інші заходи, спрямовані на зміцнення інформаційної безпеки в регіоні та світі.

Міжнародне співробітництво грає важливу роль у боротьбі з російською пропагандою та дезінформацією, оскільки це проблема, що перетинає національні кордони. Спільні зусилля країн та міжнародних організацій дозволяють ефективніше протистояти цим загрозам та забезпечити інформаційну безпеку не лише в Україні, але й в масштабах всього світу.

У боротьбі зі загрозами інформаційній безпеці України велику увагу приділяється розвитку законодавства та регулювання в галузі кібербезпеки. Україна активно працює над вдосконаленням нормативно-правової бази, яка ставить цілісні

рамки для захисту інформації. Закони та нормативні акти регулюють питання захисту персональних даних, кіберпротиборства, карантинування інформації та відповідальності за кіберзлочини. Це сприяє покращенню координації дій між різними державними органами, спеціалізованими службами та приватними компаніями для ефективної боротьби з кіберзагрозами.

Україна вживає кроки для протидії загрозам шляхом підвищення обізнаності громадян про механізми поширення дезінформації та фейкових новин. Здійснюються кампанії з медіаграмотності, освітні заходи та навчання молоді та громадськості, щоб забезпечити критичне мислення та вміння розпізнавати дезінформацію.

Крім того, важливою складовою в боротьбі зі загрозами інформаційній безпеці є співпраця з міжнародними партнерами. Україна активно співпрацює з іншими країнами та міжнародними організаціями, обмінюючись інформацією, найкращими практиками та технологіями в галузі кібербезпеки. Це дозволяє підвищити ефективність виявлення та протидії кіберзагрозам шляхом об’єднання зусиль та обміну досвідом.

ВИСНОВКИ

Інформаційна політика, що постійно ведеться Росією щодо України, поступово переросла у інформаційну війну, а згодом стала гібридною. Україна, з метою отримання переваг в цьому конфлікті, активно здійснює постійний моніторинг ситуації на інформаційному фронті та використовує різноманітні інструменти для забезпечення своєї інформаційної безпеки. Одним із найважливіших аспектів є розробка та реалізація стратегічних комунікаційних планів, спрямованих на вплив на громадську думку та формування позитивного іміджу України. Також важливим елементом є підвищення інформаційної грамотності населення, проведення просвітницьких кампаній та антипропагандистської роботи для виявлення та протидії дезінформації та фейкових новин. Крім того, Україна активно співпрацює з міжнародними партнерами та організаціями для обміну досвідом та координації зусиль у сфері інформаційної безпеки.

В рамках дипломної роботи було проведено аналіз механізмів та заходів, спрямованих на забезпечення інформаційної безпеки України в умовах російсько-української війни. В результаті дослідження виявлено, що українська держава вживає широкий спектр заходів для запобігання загрозам у сфері інформаційної безпеки. Серед них варто відзначити розвиток кібербезпеки, криптографічних технологій, контроль за інформаційним простором, сприяння розвитку медіаосвіти та протидії дезінформації. Однак, виявлено й недоліки та проблеми, які потребують подальшого вдосконалення. З метою ефективного забезпечення інформаційної безпеки, ведеться посилена співпраця з міжнародними організаціями, такими як НАТО, ОБСЄ, ЄС та інші. Співпраця відбувається з метою захисту національних інтересів України та можливого приєднання України до безпекових альянсів.

Інформаційна безпека охоплює широкий спектр аспектів, включаючи технічні, соціально-політичні, культурні та економічні складові. Це підтверджує необхідність комплексного підходу до забезпечення ефективного захисту інформації держави. Це означає що потрібно поєднувати різноманітні підходи та заходи, забезпечуючи

конфіденційність, цілісність та доступність інформації. Різновиди забезпечення інформаційної безпеки включають: технічні, організаційні, правові та освітні аспекти.

Провівши аналіз засад формування інформаційної безпеки України, включаючи нормативно-правову базу, принципи забезпечення і загрози інформаційній безпеці країни ми дійшли до наступних висновків:

На сьогоднішній день, у більшості випадків, система протидії загрозам інформаційній безпеці працює в пасивному режимі, хоча наше переконання базується на практиці країн Європейського Союзу і вимагає активного стратегічного мислення. Країною прийняті заходи для захисту цілей, їх утримання та забезпечення безпеки, враховуючи принципи демократії, прав людини, захищеного Інтернету та інше.

Ці аспекти є законодавчо закріплені, адже це дозволяє встановити єдиний понятійний апарат, державну політику щодо забезпечення інформаційної безпеки, об'єкти та суб'єкти забезпечення, правові зони відповідальності відомств, які залучені до цієї сфери. Законодавством визначені механізми координації діяльності відомств (міністерства, інститути, засоби масової інформації тощо) щодо: реагування на виклики та загрози національній безпеці в інформаційній сфері, порядок правового закріплення взаємовідносин між державними структурами безпеки та іншими органами та відомствами які відповідають за національну безпеку України, тощо.

Умови війни не змінили основні напрями інформаційної політики держави. Проте, російська агресія ставить перед Україною виклики, які вимагають посилення дій у сфері інформаційної безпеки. На першому місці - співпраця з громадським суспільством, побудова системи інформування громадян і союзників та захист інформаційного суверенітету. Також важлива активна діяльність на світовій арені для поширення правдивої інформації про події в Україні та розповсюдження спростувань фейків ворога. Особлива увага приділяється взаємодії та координації дій між різними державними органами у формулюванні українських наративів як всередині країни, так і на міжнародній арені. Необхідно також забезпечити належне

інформування населення щодо ситуації на фронті та важливості заходів евакуації та безпеки.

Забезпечення інформаційної безпеки України є складним та багатогранним процесом, що потребує комплексного підходу та поєднання різноманітних заходів. Це включає розвиток технічних, правових, освітніх та організаційних засобів, співпрацю з міжнародними партнерами та залучення всіх секторів суспільства. Такі заходи дозволять забезпечити ефективний захист національної інформації, виконати стратегічні цілі і зберегти національну безпеку.

Україна, знаходячись у складних умовах війни, приділяє велику увагу забезпеченню своєї інформаційної безпеки. Держава активно впроваджує заходи з реалізації стратегії інформаційної безпеки, спрямовані на захист національних інтересів, відстоювання інформаційного суверенітету та протидію поширенню російської пропаганди та дезінформації. Державні органи співпрацюють з громадським суспільством, формуючи єдині українські наративи та поширюючи достовірну інформацію про події в країні. Крім того, з боку України відбуваються активні виступи на світовій арені, залучення партнерів та співробітництво з міжнародними організаціями для зміцнення інформаційної безпеки.

Національна безпека та захист інформації є пріоритетними завданнями, досягнення яких вимагає постійних зусиль та координації зусиль всіх секторів суспільства. Україна виявляє високу готовність в протидії загрозам інформаційної безпеки, забезпечуючи належний захист своїх громадян та національних інтересів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 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. (дата звернення: 05.04.2023).

2. 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.

3. 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.

4. 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, С. 747-756.

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

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

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

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

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

10. 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).

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

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

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

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

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

16. 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. (дата звернення: 18.05.2023).

17. 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. (дата звернення: 17.05.2023).

18. 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. (дата звернення: 25.05.2023).

19. 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. (дата звернення: 13.05.2023).

20. 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. (дата звернення: 16.05.2023).

21. 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. (дата звернення: 01.06.2023).
22. 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. (дата звернення: 27.05.2023).
23. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. URL: http://lsej.org.ua/2_2020/54.pdf.
24. 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&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Mre_2014_1_8.pdf. (дата звернення: 03.04.2023).
25. 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. (дата звернення: 28.05.2023).
26. Антонюк В. В. Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці. URL: http://www.dy.nayka.com.ua/?op=1&z=747. (дата звернення: 27.04.2023).
27. 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. (дата звернення: 04.04.2023).
28. 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. (дата звернення: 04.04.2023).
29. Шевчук В. В. Механізм забезпечення інформаційної безпеки держави: теоретично-методологічні основи. // Періодичні наукові видання НАВС.

URL:http://elar.naiau.kiev.ua/handle/123456789/18709. (дата звернення: 12.04.2023).
30. 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. (дата звернення: 29.04.2023).
31. 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. (дата звернення: 06.05.2023).
32. 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.
33. Gupta M. Cybersecurity: Concepts, methodologies, tools, and applications // IGI Global. 2020.
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. (дата звернення: 29.05.2023).
35. 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. (дата звернення: 31.05.2023).
36. 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. (дата звернення: 31.05.2023).
37. Олійник О. В. Нормативно-правове забезпечення інформаційної безпеки в Україні. URL: http://www.pravoisuspilstvo.org.ua/archive/2012/3_2012/28.pdf.
38. Galeotti M. Russian Political War: Moving Beyond the Hybrid // Hardcover. 18 Feb 2019.

Офіційні вебсайти/портали підприємств, установ, організацій та їхні офіційні сторінки/блоги у соціальних мережах

39. Офіційний сайт Служби безпеки України. URL: https://ssu.gov.ua/. (дата звернення: 13.05.2023).

40. Офіційний сайт Центру протидії дезінформації. URL: https://cpd.gov.ua/. (дата звернення: 25.05.2023).

41. Офіційний сайт інтернет-видання «Українська правда». URL: https://www.pravda.com.ua. (дата звернення: 14.05.2023).

42. Офіційний сайт Центру стратегічних комунікацій та інформаційної безпеки.URL: https://spravdi.gov.ua/. (дата звернення: 01.06.2023).

43. Офіційна сторінка Центру протидії дезінформації у соціальній мережі «Інстаграм».URL: https://instagram.com/cpd.gov.ua. (дата звернення: 20.05.2023).