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

ГРУШЕВСЬКА ПОЛІНА ЮРІЇВНА
(прізвище, ім'я, по батькові здобувача вищої освіти)

УДК: 004.056:35.077:32.019.5.
(індекс)

КВАЛІФІКАЦІЙНА РОБОТА

ДЕРЖАВНА ПОЛІТИКА В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

(тема роботи)

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

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

_____П. Ю. ГРУШЕВСЬКА
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи:
ДАНКЕВИЧ Євген Михайлович
(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: **ГРУШЕВСЬКА Поліна Юріївна** допущена до захисту

Протокол засідання кафедри економічної теорії, інтелектуальної власності та публічного управління № ____ від «____» травня 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)

«___» травня 2024 р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти _ **ГРУШЕВСЬКА Поліна Юріївна** захистила
(прізвище ,ім'я, по батькові)

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

Секретар ЕК

_____-_____	_____	Настасія ПУГАЧОВА
(науковий ступінь, вчене звання)	(підпис)	(власне ім'я, прізвище)

АНОТАЦІЯ

ГРУШЕВСЬКА П. Ю. Державна політика в сфері інформаційної безпеки. – Кваліфікаційна робота на правах рукопису. Кваліфікаційна робота на здобуття освітнього ступеня бакалавра за спеціальністю 281 «Публічне управління та адміністрування» – Поліський національний університет, Житомир, 2024.

На початку XXI століття інформація стала стратегічним ресурсом для будь-якої цивілізованої країни. Ефективне використання інформаційних ресурсів гарантує безпеку держави та перспективу побудови демократичного суспільства, де реалізовані всі конституційні права та свободи громадян. В умовах глобальної комп'ютеризації та швидкого розвитку інформаційно-комунікаційних технологій, суспільство занурюється в світові інформаційні системи, що створює нові виклики для інформаційної безпеки. Актуальність дослідження зумовлена необхідністю вдосконалення державної політики у сфері інформаційної безпеки, особливо в контексті російсько-української війни.

Мета даного дослідження полягає в обґрунтуванні та розробці пропозицій щодо покращення державної політики в галузі інформаційної безпеки України. Використовуючи методи аналізу та синтезу, індукції та дедукції, а також системний підхід, було проведено всебічне дослідження сучасного рівня інформаційної безпеки, визначено фактори, що на нього впливають, та запропоновано напрями вдосконалення політики у цій сфері. Практичне значення результатів полягає у розробці конкретних рекомендацій, які сприятимуть підвищенню рівня захищеності інформаційного простору та зміцненню національної безпеки України.

Ключові слова: інформаційна безпека, державна політика, національна безпека, інформаційні технології, російсько-українська війна, загрози, захист інформації, рекомендації, інформаційний простір.

SUMMARY

HRUSHEVSKA P. State policy in the field of information security. – Qualification work for the degree of bachelor in specialty 281 «Public Administration and Management». Polissia National University, Zhytomyr, 2024.

At the beginning of the 21st century, information has become a strategic resource for any civilized country. Effective use of information resources ensures the security of the state and the prospect of building a democratic society where all constitutional rights and freedoms of citizens are realized. In the context of global computerization and rapid development of information and communication technologies, society is immersed in global information systems, creating new challenges for information security. The relevance of this study is due to the need to improve state policy in the field of information security, especially in the context of the Russian-Ukrainian war.

The aim of this study is to substantiate and develop proposals for improving state policy in the field of information security of Ukraine. Using methods of analysis and synthesis, induction and deduction, as well as a systematic approach, a comprehensive study of the current level of information security was conducted, factors influencing it were identified, and directions for improving policy in this area were proposed. The practical significance of the results lies in the development of specific recommendations that will help enhance the level of protection of the information space and strengthen the national security of Ukraine.

Keywords: information security, state policy, national security, information technologies, Russian-Ukrainian war, threats, information protection, recommendations, information space.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. На початку XXI століття інформація є стратегічним ресурсом для будь-якої цивілізованої країни, ефективне використання якого гарантує безпеку країни і перспективу побудови демократичного суспільства, в якому будуть реалізовані всі конституційні права і свободи громадян, в тому числі право на вільний пошук, отримання, передачу і поширення інформацію всіма можливими законними методами та способами. З бурхливим розвитком різних засобів масової інформації суспільство поневолі втягується в світові інформаційні системи і в той же час стає суб'єктом цих систем. Умови соціального життя населення конкретної країни багато в чому визначаються досконалістю доступних інформаційних технологій, а в політичній сфері все більшого значення набувають інформаційні фактори, а не владні і силові. А суть в тому, що глобальна комп'ютеризація привела до якісного стрибка в управлінні на всіх щаблях.

Актуальність теми кваліфікаційної роботи полягає ще й у тому, що тенденції до більшої відкритості суспільства та таке масове використання інформаційно-комунікаційних технологій створили умови для можливих протиправних дій щодо інформації, користувачів та систем передачі інформації, що, у свою чергу, може призвести до подальшого погіршення ситуації, що призводить до зниження інформаційної безпеки держави.

Тема інформаційної безпеки в Україні, її стан та перспективи розвитку, методологічні та теоретичні засади досліджуваної проблематики розглядаються в наукових працях вітчизняних та зарубіжних авторів, у тому числі: Антонова В., Бєлайя С., Власюка О., Булуя О., Горбуліна В., Золотар Д., Золотухіна Д., Циганова В. та інші [4; 6; 9; 12; 17; 55].

Інформаційна безпека є невід'ємною частиною національної безпеки держави, а створення розвиненого і захищеного середовища є основною умовою розвитку суспільства і конкурентоспроможної держави. Діюча система заходів щодо забезпечення інформаційної безпеки індивід, громадськості і

держави дозволить своєчасно запобігати і виявляти всі можливі і реальні загрози національним інтересам, а також запобігати втратам в соціально-економічній сфері. Актуальність цієї проблеми посилюється ще й тим, що інформаційна складова маніпулюється в контексті повномасштабного втрогення рф в Україну, оскільки складна політична ситуація, в якій Україна перебуває протягом останніх тринадцяти років, постійне погіршення іміджу та становлення держави на міжнародному рівні і триваюче погіршення політичної ситуації в країні, обумовлена рядом причин, серед яких основним є неналежний стан систем інформаційної безпеки.

Мета і завдання дослідження. Метою роботи є обґрунтування та розробка пропозицій щодо вдосконалення державної політики в галузі інформаційної безпеки. Реалізація заявленої мети дослідження вимагає розв'язання таких *завдань:*

- дослідити теоретичні та концептуальні засади інформаційної безпеки України;
- провести оцінку сучасного рівня інформаційної безпеки та визначити фактори, що впливають на сучасну інформаційну безпеку в Україні;
- запропонувати напрями покращення політики інформаційної безпеки України в контексті російської агресії.

Предмет та об'єкт дослідження. Об'єктом дослідження є суспільні відносини, що формуються в процесі реалізації державної політики у галузі інформаційної безпеки. *Предметом дослідження* є теоретичні, методичні та прикладні аспекти державної політики в галузі інформаційної безпеки.

Методи дослідження (із зазначенням конкретного застосування кожного методу). Для проведення досліджень кваліфікаційної роботи було використано наступні методи дослідження: аналіз та синтез (використання для аналізу наукових праць, законодавчих актів, політичних документів, а також синтезу отриманих знань для створення цілісного уявлення про стан та перспективи політики в сфері інформаційної безпеки); індукція та дедукція (застосування індуктивного методу для узагальнення конкретних даних та

випадків і дедуктивного для перевірки гіпотез та формування висновків); системний підхід (розгляд проблеми інформаційної безпеки як частини загальної системи національної безпеки, що дозволяє виявити взаємозв'язки та взаємозалежності). Використання цих методів дозволило забезпечити комплексний та всебічний підхід до дослідження проблем інформаційної безпеки та розробки ефективних рекомендацій для вдосконалення державної політики у цій сфері.

Перелік публікацій автора за темою дослідження. Результати дослідження публікувались на конференціях поліського національного університету.

Практичне значення отриманих результатів полягає у розробці конкретних рекомендацій щодо вдосконалення державної політики в галузі інформаційної безпеки України. Це сприятиме підвищенню рівня захищеності інформаційного простору, своєчасному виявленню та нейтралізації загроз, що, в свою чергу, зміцнить національну безпеку та стабільність держави.

Структура та обсяг роботи. Випускна кваліфікаційна робота містить вступ, три розділи основної частини та висновки до них, висновки та пропозиції, список використаних джерел, додатки. Основний текст роботи викладено на 45 сторінках. Список використаних джерел включає 55 найменувань.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ ТА КОНЦЕПТУАЛЬНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

1.1. Базові підходи до визначення поняття «державна інформаційна безпека»

На даний час існує гостра необхідність у вирішенні існуючих проблем інформаційної безпеки, оскільки сучасній державі необхідно інтегруватися в глобалізоване інформаційне суспільство і забезпечити його належне функціонування в існуючій інформаційній сфері. Неодноразово проблеми пов'язана з неефективністю політики інформаційної безпеки органів публічної влади та необхідністю перегляду наукових принципів щодо її забезпечення [3]. Отже розуміння і визначення терміну «інформаційна безпека держави» вкрай важлива для розробки ефективних та дієвих стратегій і заходів щодо її забезпечення. Розуміння та інтерпретація поняття «інформаційна безпека» надзвичайно важливі для розуміння суті інформаційної безпеки та розроблення стратегічних рішень щодо її забезпечення.

Розглянемо приклади інтерпретації терміну «інформаційна безпека» вітчизняними дослідниками: Лібік О. підкреслює, що поняття «інформаційна безпека» включає систему заходів, які спрямовані на захист інформації від незаконного доступу та підтримку її конфіденційності, доступності та цілісності. Так, інформаційна безпека гарантує захист інформаційних ресурсів та запобігає потенційним загрозам [26].

Вербицький О. досліджує поняття «інформаційної безпеки», як систему заходів, що включають технічні, правові та організаційні заходи. В його дослідженнях підкреслюється, що інформаційна безпека безпосередньо пов'язана із захистом інформаційних систем, і також з певними організаційними процедурами і правилами забезпечення безпеки [8].

Смірнова Є. зосереджується вивченні аспектів криптографічного захисту

з врахуванням інформаційної безпеки. Відповідно до її досліджень, інформаційна безпека включає застосування криптографічних методів і технологій з метою захисту конфіденційності, доступності та цілісності інформації [47].

Вивчення різних підходів щодо тлумачення поняття «інформаційна безпека» розкриває широкий концептуальний простір для подальшого вивчення та дослідження ролі даного поняття в контексті забезпечення безпеки держави. Погляди на визначення терміну інформаційної безпеки держави багатовимірне та має розглядатися окремо, оскільки саме специфіка сучасного інформаційно-комунікаційного середовища полягає у постійній зміні.

Дослідимо фундаментальні концептуальні підходи щодо визначення терміну «інформаційна безпека держави». Це дозволить нам зрозуміти всю різноманітність підходів щодо розуміння та управління сучасною інформаційною безпекою, що актуально для розробки ефективних стратегій інформаційної безпеки та забезпечення стійкості держави в сучасному IT-середовищі.

Можемо виділити такі основні концептуальні підходи щодо визначення терміну «державна інформаційна безпека»:

- концепція національної безпеки: такий підхід розглядає інформаційну безпеку держави, як один з основних елементів національної безпеки в цілому. Відповідно до цього підходу, інформаційна безпека оцінюється в контексті захисту існуючих національних інтересів, безпеки та суверенітету держави в галузі інформаційно-комунікаційних технологій [45];

- концепція цілісності загального інформаційного простору: згідно з цим підходом передбачається, що інформаційна безпека держави гарантує недоторканність і цілісність інформаційного простору держави. Це значить захист від несанкціонованого доступу, зміни та розповсюдження інформації, а також гарантію надійності та доступності інформаційних систем [30];

- концепція ризиків і загроз: згідно з цим підходом, інформаційна безпека держави розглядається як захист від загроз та ризиків, які пов'язані з

застосуванням сучасних інформаційних технологій. Основна увага приділяється виявленню, управлінню та оцінці наявних ризиків, що можуть вплинути на інформаційну безпеку держави [26].

Таким чином, згідно з визначенням О. В. Іванової, інформаційна безпека держави – це складна система заходів, що спрямовані на захист інформаційних ресурсів держави від всіх загроз з боку підрозділів противника, технологічних викликів та інших існуючих небезпек [19].

Деякі вчені наголошують на необхідності саме комплексного підходу до визначення поняття «інформаційної безпеки», що має включати технічні, правові, організаційні та соціальні аспекти [2]. Визначення терміну «інформаційна безпека держави» має певну структуру, що зображено на рисунку 1.1.

Рис. 1.1. Конструкція поняття «інформаційна безпека держави»

Джерело: побудовано автором за [18].

Проблеми інформаційної безпеки держави в той же час пов'язані з глобалізацією та безперервним розвитком інформаційно-комунікаційних технологій. Вчені вважають, що сучасна держава повинна бути готова до викликів цифрової епохи і враховувати вплив існуючого інформаційного простору на свою безпеку. Це включає не лише захист інформації, а й розробку відповідних стратегій, політики та законодавства [33].

Варто зазначити, що розуміння терміну «інформаційної безпеки держави» є предметом постійних дискусій та досліджень. Різні підходи та інтерпретації концепції демонструють складність та універсальність цієї проблематики. Поточні дослідження в цій галузі важливі для подальшого розвитку концептуального поняття та розуміння сучасної інформаційної безпеки держави та розроблення ефективних стратегій щодо її забезпечення.

1.2. Види заходів забезпечення інформаційної безпеки

Види забезпечення інформаційної безпеки держави включають в себе широкий спектр заходів, які спрямовані на захист інформаційних ресурсів, процесів і систем в державному секторі. Такі заходи включають організаційні, технічні, кадрові, особисті та юридичні аспекти, які в сукупності визначають сучасний рівень інформаційної безпеки держави. Найбільш поширеними видами забезпечення інформаційної безпеки держави вважаються:

1. *Кібернетична безпека* включає широкий спектр заходів щодо захисту інформаційних систем від кіберзагроз, що стало особливо актуально з початком повномасштабного вторгнення росії в Україну. Він включає розробку та впровадження передових технологій безпеки, здатних виявляти та запобігати різноманітним шкідливим програмам, хакерським атакам та крадіжкам даних. Нижче можемо навести приклади заходів кібербезпеки, які найчастіше засовуються: шифрування (подвійне шифрування) даних; застосування надійних паролів та впровадження політики безпеки; використання брандмауерів та фаєрвовів; встановлення сучасних антивірусних програм та систем виявлення та запобігання вторгнень. Розвинуті країни та організації, що турбують про свою репутацію та діяльність активно вдосконалюють свої заходи у сфері кібербезпеки з врахуванням постійних змін складності та характеру сучасних кіберзагроз [46].

2. Фізична безпека включає заходи щодо захисту фізичного доступу до

наявних інформаційних ресурсів, пристроїв та обладнання, що містять конфіденційну інформацію. Це здійснюється наступними методами та способами: забезпечення контрольованого доступу до приміщення; захист наявних серверних кімнат і центрів обробки даних від несанкціонованого проникнення та доступу; застосування системи відеоспостереження та різноманітних біометричних ідентифікаторів. Одним з додаткових заходів можна вважати також і фізичний захист носіїв даних, що зберігаються в захищених сейфах, захищених шафках або криптографічних пристроях.

3. *Організаційна безпека* включає розробку та впровадження політики, стандартів та процедур, що регулюють практику безпеки управління інформацією. Що включає в себе: визначення ролі і обов'язків в області безпеки; необхідність встановлення правил доступу до інформації та забезпечувати її конфіденційність; проводити аудит безпеки з метою виявлення її вразливостей. Організаційні заходи можуть включати підготовку планів та процедур в умовах надзвичайних ситуацій для усунення інцидентів.

4. *Безпека персоналу* включає заходи, спрямовані на забезпечення інформаційної безпеки персоналу державних установ і організацій. Що передбачає: навчання, підготовку та перепідготовку у сфері політики і процедур безпеки; проведення постійних перевірок кваліфікації і надійності співробітників, перш ніж надавати їм необхідний доступ до конфіденційної інформації; забезпечення обізнаності співробітників про існуючі ризики інформаційної безпеки.

5. *Правова безпека* залучає розробку та застосування законодавства в сфері інформаційної безпеки та кібербезпеки. Це відбувається через наступні методи та способи: зберігання та поширення наявної інформації; створення спеціалізованих правових норм, які конкретно стосуються захисту інформації, передбачають кримінальну відповідальність за кіберзлочини і незаконний збір інформації [46].

Уряди країн також можуть створити правову основу для співпраці з міжнародними партнерами в області інформаційної безпеки. Форми

забезпечення інформаційної безпеки важливі для захисту інформації та забезпечення стійкості інформаційних систем. Комплексний підхід, що поєднує організаційні, технічні, кадрові та юридичні аспекти, є ключем до ефективної інформаційної безпеки в певних країнах, включаючи й Україну.

Контекстна система розробки та реалізації політики державної безпеки в сфері інформаційної безпеки включає в себе не тільки внутрішні сили, а й міжнародне співробітництво. Уряди переважної більшості країни визнають важливість міжнародного співробітництва у боротьбі з розповсюдженням пропаганди та дезінформації, що є особливо актуальним для України в умовах війни, і особливо війни інформаційної. Одним із способів забезпечення ефективності контрзаходів є створення правової основи для співпраці з міжнародними партнерами в області інформаційної безпеки [6].

Контекстна система формування і реалізації політики державної безпеки в сфері інформаційної безпеки являє собою складну і взаємозалежну структуру, в яку входять різні організації, установи та громадськість. Основними дійовими особами є державні установи, спеціальні служби, відомства та міністерства, що відповідають за розробку і реалізацію стратегій і програм інформаційної безпеки. Взаємодія згаданих суб'єктів зображено на рис. 1.2 .

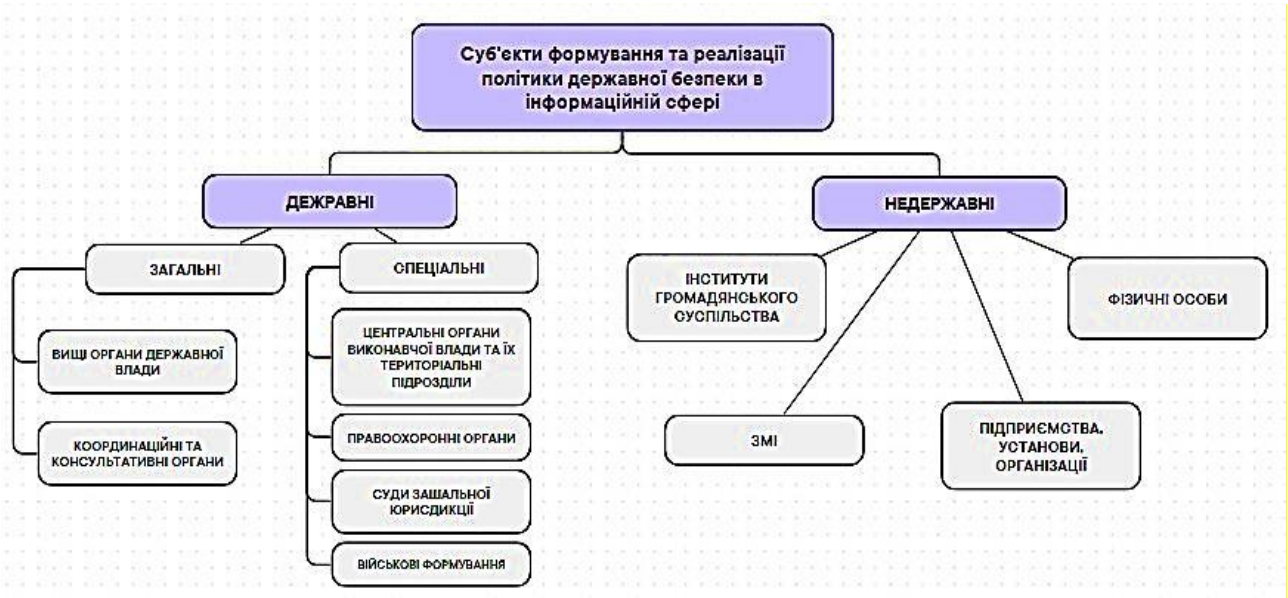

Рис. 1.2. Схематисте зображення формування і реалізації політики інформаційної безпеки держави

Джерело: адаптовано автором за [17].

З метою забезпечення вищевказаних видів інформаційної безпеки держави, всі суб'єкти (рис. 1.2) застосовують комплексний підхід, що включає наступні методи, заходи та підходи [1]:

1) нормативні заходи – розробка та реалізація відповідних законодавчих актів, нормативних актів, стандартів, норм та положень у галузі державної інформаційної безпеки. Вони можуть включати закони, нормативні акти, положення, постанови та інструкції, які встановлюють правила, відповідальність та обов'язки у сфері інформаційної безпеки;

2) організаційні заходи: реалізація політики інформаційної безпеки в органах публічного управління та утворення відповідних структур та департаментів для координації і контролю заходів інформаційної безпеки. Це включає в себе розробку процедур, правил, стандартів, проведення навчань і тренінгів, і теж організація постійного моніторингу та тестування інформаційної безпеки;

3) технічні заходи: застосування різноманітних технологічних рішень та інструментів щодо захисту інформаційної безпеки. Вони можуть включати брандмауери, системи шифрування, системи виявлення вторгнень, контролювання доступу до інформаційних ресурсів та використання технічних засобів для захисту мереж та інфраструктур;

4) соціально-психологічні заходи: просвітницька робота, інформаційні кампанії та умисне формування свідомості та поведінки громадян та підвищення обізнаності про інформаційну безпеку. Вони можуть включати семінари, тренінги, публічні заходи, поширення інформації про загрози та безпосередньо заходи безпеки, а також участь громадських організацій та засобів масової інформації у співпраці з органами державної влади. Конкретні дії або методи можуть відрізнятися залежно від країни, політичного устрою та ступеня розвитку інформаційних технологій [52].

ВИСНОВКИ ДО РОЗДІЛУ 1

Вивчаючи теоретичні та концептуальні аспекти поняття «інформаційної безпеки держави», було встановлено, що інформаційна безпека є надзвичайно важливим аспектом сучасного життя. Він включає захист інформації та сучасних інформаційних систем від ризиків зловживання, несанкціонованого доступу, крадіжки та пошкодження.

Інформаційна безпека – це складне і багатогранне питання, яке вимагає комплексного підходу і взаємодії між різними зацікавленими сторонами, включаючи урядові установи, приватний сектор і громадськість. З метою забезпечення інформаційної безпеки держави варто застосовувати широкий спектр різноманітних методів і заходів, таких як розробка належних законодавчих актів, безперервне професійне навчання, розвиток кіберзахисту і застосування сучасних технологій.

В умовах поступового та постійного розвитку технологій і загроз уряди держав повинні бути готові до викликів та загроз інформаційній безпеці шляхом активізації своїх дій і співпраці на міжнародному рівні. Лише аналізуючи, вдосконалюючи та постійно впроваджуючи ефективні стратегії інформаційної безпеки, уряд держава створює методи ефективно протистояти сучасним загрозам та підтримувати свою національну безпеку та стабільність.

РОЗДІЛ 2.
ОЦІНКА СУЧАСНОГО РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

2.1. Стан і тенденції розвитку сучасної інформаційної безпеки держави

Інформаційне поле є системоутворюючим фактором у житті будь-якого суспільства, що впливає на економічну, політичну, оборонну та іншу безпеку України. Тому при обробці інформації важливо щоб інформація, яку ми використовуємо, має високу якість і не була фальсифікована при її поширенні, оскільки питання інформаційної безпеки є важливою складовою всієї системи національної безпеки України [4, с. 65].

Загальновідомо, що дані категорій в будь-якій галузі науки отримані з об'єкта дослідження останньої. Тому важливо уточнити сутність категорій, що визначають зміст і сутність державної політики у сфері інформаційної безпеки України, а саме систематизацію, взаємодоповнюваність і взаємоузгодженість понятійного апарату [16, с. 109].

Почнемо з сучасних наукових знань про безпеку, які включають деякі уявлення про це явище в юридичних, військових, політичних, соціальних та інших взаємопов'язаних науках. Вітчизняні науковці Ткачук Т., Корнієнко Д., Циганов В. та Криштанович М. визначали поняття «безпека», як категорію, що характеризується ступенем (мірою, рівнем) захисту життєвих інтересів, прав і свобод людини, суспільства та держави від зовнішніх та внутрішніх загроз або ступенем відсутності загрози правам і свободам людини, основним інтересам і цінностям індивіда та держави [55, С. 121]. На думку Циганова В. термін «безпека» означає «діяльність особистості, суспільства і держави з виявлення, запобігання, послаблення і відвернення загрози, що може знищити їх, позбавити матеріальних та духовних цінностей, завдати небажаних втрат і заблокувати шляхи поступального розвитку» [55, С. 32]. Іншими словами, «безпека» приймає значення філософської категорії, адже охоплює всі аспекти

життя індивіда, суспільства та стану людини, держави і це також безпосередньо відіграє вирішальну роль.

Безпека завжди буквально означає, що небезпеки немає. Потреба в безпеці є одним з найважливіших мотиваційних механізмів в житті індивіда і не сильно відрізняється від других живих істот. Крім того, безпека є незаперечною універсальною цінністю, оскільки вона визнана всіма, незалежно від їх національного, расового чи соціального походження [15, с. 112].

Термін «інформація» юридично закріплений в Законі України «Про інформацію», в статті 1 якого говориться: «інформація – це всі дані та / або дані, які можуть зберігатися на апаратному носії або відтворюватись в електронному вигляді» [41]. Схоже визначення можна знайти в частині 1 статті Цивільного кодексу України [54]. Однак детальне визначення терміна «інформація» можна знайти в іншому законодавчому акті, а саме законі України «Про захист економічної конкуренції», в якому під інформацією розуміється інформація, що зберігається в будь-якій формі та на будь-якому носії (наприклад, листи, марки, книги, ілюстрації, такі як у картах, схемах, блок-схемах, кресленнях, діаграмах тощо), фотографіях, фільмах, відео, мікрофільмах, голограмах, базах даних комп'ютерних систем або повних або часткових відтвореннях їх елементів, аудіозаписах), усних заявах осіб або усній або документованій публічній інформації (ст. 1 Закону) [40].

Згідно з аналізом, під інформаційною безпекою розуміється стан захищеності інформаційного середовища, суспільних відносин і захищеність норм, встановлених законом. Слід також підкреслити, що в умовах глобалізації інформаційна безпека є невід'ємною частиною процесу забезпечення захисту інформації від усіх внутрішніх і зовнішніх загроз і створення сприятливих умов для ефективного функціонування системи інформаційної безпеки.

З юридичної точки зору інформаційна безпека повинна ґрунтуватися на інформаційній політиці держави, відповідних законах, що регулюють основні аспекти і гарантують громадянам свободу інформації та їх доступ до інформації [17, С. 155].

Перш за все, інформаційна безпека гарантується Конституцією України, яка встановлює основні засади ведення діяльності в інформаційній сфері, а саме «отримання, створення, поширення, використання і зберігання інформації та права суб'єктів інформаційних відносин», які містяться в 32 та 34, а також деяких інших її статей [25]. Закон України «Про національну безпеку України» а саме стаття 2, правова основа в галузі національної безпеки, визначає, крім Конституції, зазначає «закони України, міжнародні договори, згоду на обов'язковість для виконання Верховною Радою України» [42], а також інші нормативні правові акти, прийняті з метою реалізації Конституції і законів України. Окрім того, більше п'ятнадцяти основних законів і досить значна кількість пов'язаних з ними нормативних актів складають основу галузевого законодавства. Основні закони включають: «Про інформацію» [41], «Про захист персональних даних» [40], «Про доступ до публічної інформації» [38], «Про телевізійне мовлення і радіо» [44], «Про друковані засоби масової інформації (пресу) в Україні» [39], «Про державну таємницю» [37], «Про основи інформаційного суспільства» [43] та деякі інші.

Крім того, існують нормативні акти, які так чи інакше враховують питання інформаційної безпеки, наприклад, податкове і митне регулювання України, яке регулює питання, пов'язані з підготовкою, збором і використанням певної податкової та митної інформації [31; 36]. Деякі аспекти поширення інформації та забезпечення її безпеки регулюються нормативними актами, що кодифікують адміністративне та цивільне право [24; 54]. Цінними правовими засадами інформаційної безпеки є статути, такі як концепції, стратегії та вчення. Зокрема, були розроблені Стратегія інформаційної безпеки, Стратегія національної безпеки України та Стратегія розвитку інформаційного суспільства України [48; 50; 51]. Ці заходи визначають основні пріоритети розвитку конкретної області і є основними для прийняття нових стандартів і усунення колізій в існуючих стандартах.

Забезпечення інформаційної безпеки за допомогою логічної реалізації чітко сформульованої інформаційної національної стратегії може внести

значний внесок в успішне вирішення завдань у військово-політичній, політичній, військовій, економічній, соціальній та інших сферах діяльності держави. Отже, реалізація ефективної інформаційної політики зможе суттєво вплинути на вирішення зовнішніх, внутрішніх та військових конфліктів [28, С. 39].

На жаль, в останні роки пріоритетним завданням громадських та державних інститутів стала розробка термінових і ефективних заходів з нейтралізації розвідувально-диверсійної діяльності Російської Федерації проти України та запобігання їх подальшого використання. Рішення цієї складної проблеми убезпечить захист інтересів суспільства і держави та сприятиме реалізації прав громадян на повну та якісну інформацію [28, С. 38].

В гібридній війні з державою-агресором інша сторона неминуче піддається ряду інформаційних небезпек, нейтралізація яких, з одного боку, вимагає спеціальних правових і адміністративних заходів, а з іншого – може супроводжуватися істотними обмеженнями існуючих демократичних прав і свобод. У цьому випадку для держави стратегічно важливо знайти баланс між інтересами національної безпеки і верховенством закону [28, С. 39].

Мабуть, найважливіший інструмент гібридної війни використовується як агресором (з метою поширення неправдивої інформації заради паніки та наклепу на ворога та інших агресивних дій), так і як друга сторона (з метою підняття патріотичного духу, заклику до боротьби, спростування фактів тощо) ЗМІ різних типів – це найефективніша зброя, що використовується в сучасній гібридній війні. Ось чому державна політика в області інформаційної безпеки повинна бути орієнтована на вибіркове застосування обмежень до конкретних ворожих, упереджених і маніпулятивних ЗМІ. Зазначений підхід вимагає найвищого ступеня правової визначеності щодо обмежуючих критеріїв, оскільки недотримання може призвести до заборони неупереджених і політично нейтральних критеріїв (тик як, ненавмисне поширення неправдивої інформації). У той же час велика кількість людей і громадських організацій можуть вказувати на те, що запроваджувані заборони не мають фактичної

основи, не мають правової основи, суперечать Конституції і обмежують демократичні права і свободи. Отже, всі обмеження в інформаційному середовищі повинні бути сконцентровані і застосовуватися тільки до ресурсів, на які негативно вплинули певні заходи або які становлять загрозу для держави і суспільства [13, С. 21–22].

Регулювання створення єдиного інформаційного простору в Україні має сприяти гармонійному розвитку наявних інформаційних ресурсів, інформаційних продуктів та інформаційних послуг в країні. Важливість розвитку законодавства в галузі інформації та інформаційної безпеки та формування інформаційного суспільства визначається тим, що закони в цій галузі роблять істотний вплив на правове регулювання відносин в усіх сферах життя [13, С. 22].

Вивчивши поточну ситуацію і тенденції розвитку інформаційної безпеки в Україні, ми прийшли до висновку, що інформаційна безпека – це складна категорія, яка включає в себе елементи внутрішньої і зовнішньої політики, технологічні, економічні, військові та інші. Система інформаційної безпеки є частиною загальної системи національної безпеки держави, та її ефективне функціонування регулюється низкою законодавчих актів. Функціонування держави в особі органів публічної влади, громадських організацій, засобів масової інформації і громадян, що координують свої дії щодо здійснення діяльності у сфері інформаційної безпеки на основі єдиних правових норм, має бути направлена на ефективну протидію всім інформаційним загрозам у сучасних умовах.

2.2. Фактори, що впливають на сучасну інформаційну безпеку в Україні

Фактори, відповідальні за розуміння і виявлення зростаючих загроз інформаційній безпеці, носять системний характер і, отже, охоплюють всі без

винятку сфери людської, соціальної та державної діяльності. Дійсно аналіз проблем – це завжди досить суб'єктивний процес, який полягає в тому, що випробуваний сприймає певні фактори через призму особистих інтересів та професіоналізму. Експерти підкреслюють серйозний аспект гібридної війни – вторгнення в інформаційно-комунікаційний простір країни з метою придушення опору і формування глобального політичного іміджу, відповідного інтересам агресора. З метою досягнення цього використовуються різноманітні інструменти маніпулювання громадською думкою: порушення функціонування інформаційно-комунікаційного простору, а також телекомунікаційних систем і мереж; вплив на ЗМІ та маніпулювання громадською думкою; розвиток кіберзлочинності [13, С. 18].

Як зазначив Дмитренко Н.: «характер і особливості російсько-української війни дозволяють припустити, що її мета – змінити самоідентифікацію населення і перетворити східний регіон нашої країни в «сіру зону», що залишить Російську Федерацію в якості важеля тиску в Європі, а саме як причина в постійній небезпеці нестабільності по всій Україні. Дана війна не за безпосередню територію, а за думки, світогляд і душі людей. І оскільки контроль над інформаційною інфраструктурою є засадами формування громадської думки, яка завжди проявляється спочатку в певних переконаннях, а потім у конкретних діях, контроль над сферою інформаційної інфраструктури стає одним з основних владних ресурсів у конкурентній боротьбі» [29, С. 40-41].

Крім військових засобів нападу (окупація значної території країни і анексія Криму, повномасштабне вторгнення), росія застосовує весь арсенал доступних ресурсів «гібридної» війна: починаючи інформаційно-пропагандистською експансією, економічного та енергетичного тиску і дискредитації влади України на світовій арені до безпосередньо підривних актів шпигунства і диверсій на території України, провокацій, розділових настроїв в регіонах і масованих кібератак на мережі. На думку деяких українських експертів, експансія в інформаційний простір є однією з найбільш

небезпечних складових війни росії проти України [15].

Сучасні загрози інформаційній безпеці України значною мірою скоординовані та якісно доповнюють список загроз національній безпеці в цілому. В Стратегії національної безпеки України, яка затверджена Указом Президента України №392/2020 станом на 14.09.2020 р. визначено загрози національній безпеці України в сфері інформаційної безпеки [50]:

- використання країною-агеросором інформаційної «зброїпоєднуючи з енергетичним та погрозами ядерного удару для зміцнення своїх позицій в Європі, такі спроби впливати на внутрішньополітичну ситуацію в певних європейських державах і її підтримка триваючих конфліктів, посилення її військової присутності в Східній Європі та країнах Азії (пункт 16);

- швидкий технологічний розвиток і посилення ролі інформаційних технологій у всіх сферах суспільного життя (пункт 9);

- деструктивна внутрішня і зовнішня пропаганда, що провокує ворожнечу, підриває суспільну єдність, провокує конфлікти і експлуатує суспільні протиріччя (так звані мовні питання) в умовах відсутності цілісної інформаційної політики української держави, слабкої системи стратегічних комунікацій (пункт 20);

- збільшені загрози критично важливим об'єктам інфраструктури (включаючи їх інформаційну складову), пов'язані з погіршенням технічного стану, недостатніми інвестиціями в їх реконструкцію і розвиток, несанкціонованими зброями в їх роботі, в тому числі через фізичні атаки і кібератаки, а також тимчасовою окупацією частини території України (пункт 27);

- ведення рф гібридної війни проти України шляхом систематичного використання інформації: психологічні, кібернетичні, політичні, економічні та військові методи ефективного впливу на неї (пункт 17);

- не досить ефективна діяльність державних органів, які зазнають труднощів з розробкою та реалізацією ефективної державної політики (у тому числі в інформаційній сфері), які є основним джерелом загроз незалежності,

суверенітету та демократії України (пункт 22).

28 грудня 2021 року президент України затвердив Стратегію інформаційної безпеки, схвалену відповідним рішенням РНБО [48]. Це один з багатьох документів, які розробляються для реалізації Стратегії національної безпеки України. Даний документ був прийнятий з метою створення необхідних умов для забезпечення інформаційної безпеки України, що, в свою чергу, сприятиме захисту життєво важливих інтересів громадян, суспільства і держави в боротьбі з внутрішніми і зовнішніми загрозами, надасть захист інформації, суверенітету та територіальній цілісності України, буде підтримувати соціальну і політичну стабільність, захист держави, а також права і свободи кожного. Виконання цілей, поставлених в стратегії, розрахована до 2025 року [4].

Основними загрозами інформаційної безпеки, описаними в стратегії, є:

- вплив на внутрішню та зовнішню суспільну, політичну ситуацію соціальних мереж, оскільки особливості організації Всесвітньої павутини загрожують забезпеченню права людини на недоторканність приватного життя;

- значна кількість глобальних кампаній з дезінформації, що проводяться авторитарними урядами країн та радикальними рухами з метою маніпулювання свідомістю окремих осіб та груп населення;

- низький рівень медіаосвіти (медіакультури) населення України в умовах стрімкого розвитку цифрових технологій, що супроводжується зниженням критичного сприйняття інформації та створює основу для можливого маніпулювання громадською думкою, що, в свою чергу, сприяє посиленню впливу спотворень і деструктивної пропаганди, популяризації конспірологічних теорій;

- переваги в інформаційному просторі рф, як держави-агресора на тимчасово окупованих територіях України;

- величезний вплив спецслужби рф на українське населення через спеціальні операції спецслужб з підриву національної безпеки України, національних інтересів країни, ліквідації української держави та знищення

української ідентичності, внаслідок чого прояви екстремізму, паніки в суспільстві, загострення та дестабілізації соціально-економічної ситуація в Україні;

- обмежена здатність реагувати на спотворюючу кампанію через відсутність ефективної системи для вирішення таких завдань;

- недосконале регулювання відносин в сфері інформаційної діяльності та охорони професійної діяльності журналістів;

- відсутність усталеної системи стратегічних комунікацій, оскільки Україна все ще перебуває в процесі розробки системи стратегічних комунікацій;

- маніпулювання свідомістю українських громадян з приводу європейської та євроатлантичної інтеграції України [48].

Ще однією серйозною є проблема кібербезпеки в умовах війни. У всьому світі кіберпростір все частіше застосовується для різних небезпечних операцій: починаючи крадіжками цінної інформації до актів кібертероризму [13, С. 18]. По-перше, мережі та інформаційні системи поміщають конфіденційні дані та економічно важливу інформацію, що значно підвищує мотивацію до нападу. Напад на інформаційні системи на національному рівні можуть мати серйозні наслідки, такі як, зброї в системах зв'язку, втрата конфіденційної інформації тощо [10, С. 28]. Очевидно, що сьогоднішньому українському суспільству загрожує отримання недостовірної, іноді шкідливої інформації, передчасні зізнання, комп'ютерні злочини, шпигунство тощо.

Протягом 2014-2024 років забезпечити інформаційну безпеку України було дуже складно. Українська держава роками боролася з використанням різноманітних систем пропаганди, створюваної в Росії. Дії противника спрямовані на розпалювання ворожнечі в українському суспільстві і руйнування української політичної нації, прославляння сепаратизму, штучне нагнітання реальних і уявних внутрішніх протиріч, створення атмосфери громадянської недовіри до дій та намірів влади, провокація масових акцій протесту, громадянська непокора та формування негативного ставлення

українців та міжнародного співтовариства до подій в середині країни, створення «фашистської» держави та спотворення українсько-російської історії [16]. Так от, російські ЗМІ використовують неправдиву інформацію про появу символів нацистської Німеччини в найнесподіваніших контекстах. Ось, як ще 12 січня 2015 року журналісти популярного федерального телеканалу «Росія1» повідомили в ефірі програми «Вести», що партія «Свобода» розробила проєкт щодо вигляду 1000 гривеневої купюри, що виражає цінності нової української еліти. В цьому проєкті Адольф Гітлер був зображений на розмитому тлі на купюрі. Сайт StopFake представив цю брехню, вказавши, що фотографія була зроблена на російському гумористичному сайті. pikabu.ru, а в оригіналі накладної НБУ зразка 2008 року було зображено Пантелеймона Куліша та ще купа різноманітних фейкових та подекуди абсурдних новин [18, С. 324].

Соціальні мережі також є важливим інструментом спотворення, оскільки, згідно з результатами дослідження «ставлення до історій проти дезінформації», що було проведено на основі онлайн-опитування в кінці липня 2021 року, 86 % опитаних читають Facebook щодня або кілька разів на тиждень, Telegram – 68 %, Твіттер – 9 %. Соціальна мережа Facebook є джерелом інформації про політику і поточні події для 70 % населення, Telegram – для 36 % та Twitter – для 7 % респондентів. Онлайн-дослідження не вважається статистично репрезентативним для населення України в цілому, але воно може пролити світло на загальну картину [5].

Війни такого роду широко поширені в світовому інформаційному просторі та ретельно вивчаються вченими і фахівцями. Зокрема, деякі аспекти інформаційної війни виявлені Національним інститутом стратегічних досліджень США і ряд західних експертів і вчених. Один з них – психологічна війна. Основне завдання психологічної війни-маніпулювати масами. Основною метою такої маніпуляції є: впровадження ворожих ідей і точок зору в суспільну та індивідуальну свідомість; дезорієнтація і дезінформація мас; ослаблення певних переконань, які залякують людей чином ворога; залякати ворога своїми власними силами [11].

Також, Україна посідає третє місце в рейтингу країн щодо найвищого ризику зараження особистих пристроїв через Інтернет: 35,7 % користувачів стикалися з онлайн-загрозами, а Україна посідає дев'яте місце в рейтингу країн з найвищим ризиком зараження мобільними вірусами (8,39 %). Ризик зіткнутися з місцевими загрозами дуже високий для українців (54,5 %) [2]. До них відносяться об'єкти, які потрапили на комп'ютери в результаті зараження файлів або знімних носіїв або які вперше з'явилися на комп'ютері без відкриття (наприклад, у випадку комп'ютерного вірусу), складні інсталятори, зашифровані файли тощо. За цим показником країна займає передостаннє місце в двадцятці кращих в світі, але перше в Європі [2].

В Україні зареєстровано значну кількість антивірусних програм, що пов'язані з прикладними програмами і програмами шифрування, шкідливих програм, які блокують пристрій або браузер або шифрують файли користувача, щоб до них можна було отримати доступ без спеціального ключа, що вимагає оплати. Деякі експерти вважають, що ситуація в цілому характеризується наступними тенденціями в області загроз інформаційної безпеки: неконтрольовані загрози, пов'язані з так званим «інтернетом речей», та поширення мережевих підключень; регулювання підвищеного правового ризику у сфері мережевих комунікацій; швидкий розвиток «кіберзлочинності як послуги» – надавання цифрових послуг злочинними синдикатами; хакерські атаки, що спрямовані на створення підрив репутації брендів і політичних сил [10]. Існуюча національна система кібербезпеки з мінімальною участю громадськості та експертної підтримки у тому числі з боку правоохоронних органів, громадських рад неефективні, а Національний координаційний центр кібербезпеки (НКЦК) виключає представників відповідних структур. Міністерство цифрової трансформації України, незважаючи на те, що у нього є завдання в сфері кібербезпеки (кіберзахисту), має обмежені можливості для їх реалізації (в першу чергу особистої). Тому важливо зміцнити його потенціал, принаймні, в аналітичній допомозі у прийнятті рішень у цій галузі [7].

ВИСНОВКИ ДО РОЗДІЛУ 2

З метою протидії новим загрозам і викликам, пов'язаним з активною агресією рф в кіберпросторі, Україна прагне створити цілу національну систему кібербезпеки. 26 серпня 2021 р. було затверджено Стратегію кібербезпеки України на період 2021-2025 рр., представлену Національним координаційним центром кібербезпеки України і затверджена Радою національної безпеки і оборони України [49]. Стратегія передбачає, що необхідно створити умови для безпечного використання кіберпростору, щоб використовувати його в інтересах особистості, суспільства і держави. Стратегія безпосередньо визначає механізми її реалізації та критерії оцінки успіху на цьому шляху [49].

Провівши аналіз основних чинників, що впливають на забезпечення інформаційної безпеки в Україні, ми можемо зробити висновок, що ключовим залишається стратегічне інформаційне протистояння, що є небезпечною складовою гібридної війни, розв'язаної рф проти України, і головною загрозою інформаційній безпеці від нашої держави виходить можливість впливу ворога, що нав'язує свою систему цінностей, свої погляди, інтереси та рішення в життєво важливих сферах суспільної та державної діяльності.

РОЗДІЛ 3.
НАПРЯМИ ПОКРАЩЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В КОНТЕКСТІ РОСІЙСЬКОЇ АГРЕСІЇ

3.1. Заходи щодо реалізації стратегії інформаційної безпеки України

Для України пріоритетом є розвиток стійкої кіберсистеми, що об'єднує всі державні установи, приватний сектор, академічні (навчальні) установи та громадські організації. Це підтримує забезпечення цілісності та безпеки інформаційного простору, а також забезпеченню взаємодії та спільних зусиль з виявлення, відстеження та протидії загрозам. Крім того, уряд країни постійно удосконалює системи реагування на інциденти, пов'язані з кібербезпекою, і розробляє механізми оперативного реагування та відновлення роботи після кібератак.

В боротьбі з загрозами інформаційній безпеці в Україні значна увага приділяється розробці законів і нормативних актів у галузі кібербезпеки. Україна завзято працює над вдосконаленням існуючої нормативно-правової бази, що створює цілісну основу для захисту інформації. Нормативні акти та закони регулюють питання захисту особистих даних, кіберзлочинності та кіберпротиборства, переведення інформації на карантин та введення відповідальності за кіберзлочинність. Це дозволяє покращити координацію між різними урядовими установами, спеціалізованими службами і приватними компаніями для ефективної та дієвої боротьби з кіберзагрозами.

Заходи державної оборонної – це комплекс скоординованих дій, які готуються і здійснюються суб'єктами з метою забезпечення національної безпеки та оборони України з метою: запобігати, стримувати і відбивати збройну агресію проти України; прогнозувати та виявляти інформаційні загрози у військовій галузі; боротися з інформаційними загрозами з боку держави-агресора; здійснення інших важливих та необхідних заходів в інформаційному протистоянні [48].

Захист інформаційної безпеки держави є однією з основних складових сучасної інформаційної політики України. Наша країна стикається з викликами сучасного кіберпростору, широко поширені та їх частота зростають такі види: кібершпигунство, кібератаки і кіберзагрози. Для результативної протидії цим загрозам Україна розробляє і впроваджує комплекси заходів кібербезпеки. Ведеться активне налагодження співпраці з міжнародними партнерами по обміну інформацією та досвідом по темі кібербезпеки. Фахівці з кібербезпеки також проходять навчання та підготовку з метою забезпечення надійної охорони та захисту державних інформаційних ресурсів.

Україна активно працює над розвитком сучасного інформаційного суспільства. З цією метою утворення розвиненої інформаційної інфраструктури та поліпшення доступу до інформації вживаються заходи з розвитку широкосмугового інтернету, введення електронного державного управління та електронних послуг. Важливою сферою є надання громадськості доступу до свободи слова та вираження поглядів, а також посилення медіаосвіти за допомогою інформаційних кампаній, тренінгів та освітніх заходів.

Ще одним елементом інформаційної політики країни є формування позитивного іміджу України. Зусилля, які спрямовані на просування і поширення України на міжнародному рівні. Інформаційна дипломатія відіграє важливу роль у зміцненні довіри, підтримці національних інтересів та залученні іноземних інвестицій. Розвиток національних мов і культур також є важливим елементом інформаційної політики. Захист і популяризація української мови є пріоритетом. Проводяться заходи щодо зміцнення використання України в усіх сферах суспільного життя, розвитку кіно, літератури і мистецтва [17].

У світі, в якому інформація стає все більш важливою, Україна активно працює над розвитком та удосконаленням своєї інформаційної політики. Основними пріоритетами інформаційної політики України є забезпечення інформаційної безпеки, просування особистих інтересів та підвищення культурного рівня нації та створення інформаційного суспільства.

План дій щодо реалізації Стратегії інформаційної безпеки, прийнятий 30 березня 2023 року, є основоположним документом для забезпечення інформаційної безпеки в Україні. Цей план дій розрахований на період до 2025 року та включає в себе ряд конкретних заходів, які спрямовані на підвищення інформаційної безпеки, протидію кіберзагрозам і розвиток інформаційного суспільства. Головні напрямки та заходи, які передбачені планом [48], включають:

1) нормативно-правова база і законодавче регулювання забезпечує правову базу захисту інформації, установлює вимоги в галузі кібербезпеки і регулює діяльність організацій і структур, що відповідають за забезпечення інформаційної безпеки. А саме:

а) аналіз та вдосконалення існуючого законодавства в галузі інформаційної безпеки (проведення поглибленого аналізу чинного законодавства та виявлення прогалин, що необхідно усунути для забезпечення ефективного захисту інформації; внесення пропозицій для вдосконалення законодавства з урахуванням сучасних викликів та технологічних тенденцій у цій галузі інформаційної безпеки; розробляти проєкти законів і нормативних актів, що забезпечують ефективний захист інформації;

б) розроблення нових законів, що регулюють кібербезпеку і захист персональних даних (розробка і прийняття нових законів, що унормовують питання кібербезпеки, в тому числі захист критично важливих інформаційних систем та інфраструктур; встановлення вимог до захисту персональних даних громадян, в тому числі відповідно до міжнародних норм і стандартів);

в) забезпечити створення механізмів контролю та підзвітності у разі порушення законів про інформаційну безпеку (створити систему моніторингу дотримання усіх вимог інформаційної безпеки та кібератак у державних органах, державних установах та критичних секторах; розробити механізми контролю та підзвітності у разі порушення законів про інформаційну безпеку; виявляти, розслідувати та реагувати на кібер-інциденти та кіберзлочини; встановлювати відповідальність за порушення законів про інформаційну

безпеку, включаючи встановлення цивільної, адміністративної та кримінальної відповідальності) [48].

2) захист інформації та кібербезпека спрямовані на забезпечення захисту всіх інформаційних систем, інфраструктури та даних від кіберзагроз і кібератак. А саме:

а) розробка та запровадження системи кібербезпеки (розроблення та впровадження комплексу технічних засобів захисту інформаційних систем, що включають системи запобігання та виявлення кібератак, постійного моніторингу та аналізу кіберзагроз; утворення центрів кібербезпеки та результативного реагування на кіберінциденти; удосконалена система аутентифікації та ідентифікації користувачів, включаючи багатофакторну аутентифікацію і використання новітніх технологій шифрування);

б) розвиток людських ресурсів і професійний розвиток фахівців (організація програм навчання і перепідготовки по темі кібербезпеки для співробітників державних установ, підприємств і громадських організацій; залучення висококваліфікованих фахівців в області кібербезпеки і обмін досвідом з міжнародними партнерами; підтримувати освітні установи, які проводять спеціалізоване навчання по темі кібербезпеки і захисту інформації);

в) проводити аудити та оцінки ризиків (проводити систематичні аудити інформаційних систем для виявлення вразливостей та можливих ризиків інформаційної безпеки; впроваджувати процес оцінки ризиків, який визначає пріоритетні сфери заходів кібербезпеки та вживає відповідних заходів для зниження ризиків);

г) нормативно-правова підтримка (розроблення та прийняття законодавчих актів у галузі кібербезпеки та захисту інформації, що включає створення механізмів реагування на кіберінциденти і встановлення відповідальності у разі порушення закону; забезпечення взаємодії компетентних органів у галузі кібербезпеки та захисту інформації);

д) взаємодія з країнами та міжнародними організаціями (розробка та вкладення міжнародних угод та налагодження партнерських відносин з

міжнародними організаціями та країнами в галузі кібербезпеки та обмін інформацією про кіберзагрози; участь у міжнародних ініціативах і форумах з обміну досвідом та спільного вирішення кібернетичних проблем) [48].

3) інформаційна безпека громадян спрямована на захист персональних даних громадян, підвищення обізнаності про кібератаки та забезпечення їх безпеки в інформаційному просторі. А саме через:

а) підвищення обізнаності в області кібербезпеки (організація інформаційних кампаній і навчальних заходів для громадян з основних принципів кібербезпеки, включаючи захист персональних даних, логінів, паролів і використання безпечних онлайн-сервісів; розробка і поширення практичних порад і рекомендацій з кібербезпеки, включаючи використання антивірусного програмного забезпечення, періодичне оновлення програм та операційних систем, а також автентифікацію посилань та повідомлень електронної пошти);

б) Захист персональних даних (забезпечення юридичного захисту персональних даних громадян та розробка відповідних правових актів про зберігання, передачу та обробку персональних даних; впровадження технічних засобів захисту персональних даних, а саме анонімізація, шифрування та механізми контролювання доступу);

в) запобігання шахрайству та кібератакам (утворення механізмів щодо співпраці з правоохоронними органами та службами кібербезпеки з метою виявлення та припинення шахрайства та кібератак проти громадян; організація навчальних заходів та поширення інформації про традиційні шахрайські системи та методи кібератак, які допомагають запобігти шахрайству та кібератакам на громадян);

г) забезпечення безпеки від експлуатації дітей в Інтернеті (розробка та впровадження механізмів захисту дітей від шкідливого контенту, експлуатації в Інтернеті та кіберзагроз; участь батьків, освітніх установ та громадських організацій у навчанні та популяризації безпечного застосування мережі Інтернет у дітей);

д) допомога жертвам кіберзлочинів (утворення механізмів щодо підтримки та захисту жертв кіберзлочинів, включаючи психологічну підтримку, консультування та допомогу у відновленні після інциденту) [48].

4) налагодження міжнародного співробітництва, яке має на меті розгорнути спільні зусилля з іншими країнами та міжнародними організаціями щодо виявлення, запобігання та реагування на кіберзагрози, обміну інформацією та досвідом, і також встановлення норм та стандартів кібербезпеки. Досягається через :

а) підписання міжнародних угод і налагодження партнерських відносин (укладення двосторонніх і багатосторонніх угод з іншими країнами про протидію кіберзагрозам, обмін інформацією щодо кібератак і кіберінцидентів, підтримування партнерських відносин з міжнародними організаціями, а саме Європейський Союз, ООН, НАТО, Інтерпол та деякі інші, для спільної діяльності в області кібербезпеки та обміном інформацією);

б) обмін досвідом та інформацією (створення механізмів з метою обміну інформацією про відомі кіберзагрози, нові методи і технології в галузі кібербезпеки; організація міжнародних тренінгів, конференцій, семінарів з тем кібербезпеки для обміну досвідом і підготовки фахівців з країн, в яких існує кібербезпека);

в) проведення спільної оперативної діяльності та реагування (організація спільної оперативної діяльності з іншими країнами у відповідь на кібератаки та кіберінциденти, включаючи обмін інформацією про виявлених злочинців та зловживання в Інтернеті; спільна розробка та реалізація стратегій та планів дій у надзвичайних ситуаціях при великих масштабах кібератаках та кіберінцидентах;

г) розробка міжнародних норм і стандартів (брати участь у розробці міжнародних норм і стандартів у галузі кібербезпеки, приймаючи визначення мінімальних вимог захисту інформації та інформаційних систем; адаптація та гармонізація міжнародних норм і стандартів до національного українського законодавства та специфіки України) [48].

Важливим елементом загального плану дій є заходи щодо реалізації стратегії інформаційної безпеки України щодо захисту інформації та забезпечення кібербезпеки в країні. Вони призначені для посилення захисту інформаційних ресурсів держави, протидії кіберзагрозам, забезпечення безумовної безпеки персональних даних та підвищення та популяризація обізнаності громадян про інформаційну безпеку.

3.2. Способи і методи забезпечення інформаційної безпеки України в контексті війни

Україна знаходиться в контексті російсько-української війни, яка почалася в 2014 році. Даний конфлікт має багатоплановий характер, включаючи гібридну війну, збройну агресію та інформаційну війну. В цьому сенсі роль інформації надзвичайно важлива, оскільки вона впливає на суспільство і формує картину конфліктів.

Російсько-українська війна розпочалась в результаті сукупності причин, які призвели до ескалації збройного конфлікту. Однією з головних причин була анексія росією Криму в 2014 році, яка порушила принципи міжнародного права і територіальну цілісність України. Сукупність політичних протиріч, етнічні та релігійні конфлікти, економічні складності і прагнення росії зміцнила свої впливові позиції на пострадянському просторі [5].

Війна має досить складний характер і поєднує в собі збройні військові операції, гібридну війну та маніпулювання інформацією. Російською стороною використовується тактика помилкового вторгнення, яка полягає у розміщенні незаконних збройних формувань на території України та постійному надавані військової та іншої допомоги. Україна, зі свого боку, мобілізує свої власні сили для захисту своєї територіальної цілісності і ведення контрнаступу.

Україна перебуває у стані гібридної війни, що негативно позначається на свідомості українського населення. Наша країна, як і більшість розвинених

країн, була недостатньо підготовлена до такого роду агресії з боку росії. Одним з підтверджень цього є відсутність твердих правил поведінки в умовах інформаційно-пропагандистської атаки. Дуже важливою проблемою для України була широкомасштабна російська пропаганда, яка виходить за межі нашої країни. Отже, забезпечення інформаційної безпеки є одним з ключових факторів сталого розвитку національної безпеки.

Щоб протистояти гібридним загрозам і запобігти їх виникненню, Україна зобов'язана вжити заходів щодо захисту державної інформації. У сучасних умовах інформаційні війни проникло у всі сфери життя, включаючи ідеологію, історію, релігію та освіту. Тому вкрай важливо забезпечити інформаційну безпеку, особливо в умовах гібридної війни. Тому основними пріоритетами інформаційної політики держави повинні бути забезпечення інформаційної безпеки особистості, захист її психіки і свідомості від шкідливого впливу інформації, від спотворення і маніпулювання [10].

Україна докладає значних зусиль для виявлення та відстеження кіберзагроз. У країні створені спеціалізовані служби кібербезпеки, які відповідають за виявлення інцидентів, моніторинг вразливостей і розробку заходів захисту від кібератак. Співпраця з міжнародними партнерами та обмін інформацією з іншими країнами відіграють важливу роль у виявленні загроз. Це дозволяє своєчасно реагувати на загрози і ефективно їм протистояти.

Щоб ефективно протистояти гібридній війні, Україна має ретельно вивчити засоби, які противник використовує у своїй поведінці. Російсько-українська війна є яскравим прикладом гібридного конфлікту, в якому застосовується широкий спектр методів, беручи до уваги і інформаційну пропаганду, кібератаки, дезінформацію, вплив на масову свідомість та інші.

У зв'язку з цим вкрай важливо відстежувати загрози інформаційної безпеки, які виходять від різних центрів і організацій. Такі як Національний центр кібербезпеки України постійно відстежує кіберзагрози, виявляє та аналізує атаки на державні інформаційні системи та реагує на них. Крім того, Департамент інформаційної безпеки та спеціальних технологій Служби безпеки

України проводить моніторинг загроз інформаційній безпеці, виявлення та припинення діяльності організацій, що сприяють виникненню гібридних загроз.

Крім того, є також громадські організації та ініціативи, що відстежують та аналізують інформаційні загрози. Наприклад, Громадська рада Державного агентства з електронного урядування в Україні здійснює моніторинг та аналіз інформаційної безпеки, сприяє розробці та запровадженню заходів захисту від кіберзагроз і пропаганди [32].

Ці центри та організації відіграють важливу роль в забезпеченні інформаційної безпеки країни. Його дії спрямовані на виявлення, боротьбу та аналіз загрозам інформаційної безпеки, і в той же час на підвищення обізнаності громадськості про гібридні загрози. Оцінка методів, що використовуються противником, дозволяє нам більш ефективно реагувати на них та розробляти відповідні заходи щодо захисту національної безпек і та інформаційного простору країни.

Для досягнення цієї мети перераховані вище організації використовують наступні методи та інструменти:

- законодавчі та нормативні заходи. Уряд країни приділяє чималу увагу розробці та застосуванню законодавства, що регулює сферу інформаційної безпеки. Що включає прийняття нормативних актів та законів щодо захисту даних, кібербезпеки, контролю інформаційних потоків тощо;

- Україна досить активно розвиває свої можливості в області кіберзахисту. Включає в себе захист інформаційних систем, мереж та даних від кібератак, виявлення і розслідування кіберзлочинів, розроблення та запровадження політики та стандартів кібербезпеки;

- співпраця з міжнародними партнерами. Україна активно співпрацює з такими міжнародними партнерами, як НАТО, Європейський Союз, Організація з безпеки і співробітництва в Європі (ОБСЄ) та ін. Це створює умови обміну досвідом, координації методів та заходів інформаційної безпеки та сприянню в усуненні загроз;

- інформаційна освіта та підвищення обізнаності: Україна надає великого значення вдосконаленню інформаційної освіти та підвищенню обізнаності населення. Це включає розроблення освітніх програм, проведення тренінгів, семінарів та інформаційних кампаній, з питань інформаційної безпеки;

- розвиток кіберрозвідки. Україна продовжує розвивати свої можливості кіберрозвідки для виявлення та моніторингу кіберзагроз. Включаючи аналіз діяльності ворожих кіберакторів, виявлення нових загроз і розроблення контрстратегій;

- розвиток і захист критично важливої інфраструктури. Україна концентрує свої зусилля на захисті критично важливої інфраструктури, я-от енергетичні мережі, фінансові установи, телекомунікаційні системи і т.д. До них відносяться використання оборонних технологій, резервування систем і розробка планів дій у надзвичайних ситуаціях;

- розвиток медійної сфери. Україна строює умови для розвитку об'єктивних незалежних засобів масової інформації, які відіграють важливу роль у поширенні правдивої та достовірної інформації. Це допомагає протистояти спотворенню та пропаганді [28].

Ці заходи забезпечення інформаційної безпеки України в умовах російсько-української війни спрямовані на захист інформаційних ресурсів, виявлення та нейтралізацію загроз, підвищення інформаційної обізнаності та забезпечення стабільності держави.

3.3. Механізми боротьби з поширенням і спотворенням російської пропаганди

Однією з важливих проблем України є деформація інформації і ведення інформаційних операцій, особливо з боку атакуючої держави. Дані операції направлені на: підірвання незалежності України, зміну конституційного ладу; поширювати пропаганду війни, насильства і жорстокості; порушення

суверенітету і територіальної цілісності України; розпалювання національної, расової, міжетнічної, мовної та релігійної ненависті та ворожнечі; здійснювати терористичні акти і порушення прав і свобод людини [1].

Україна постійно привертала увагу російської пропаганди, спотворюючи події і факти, намагаючись таким чином виправдати свої дії. Починаючи з «failed state», нездатної зберегти свою незалежність, і закінчуючи спробою мобілізувати населення і розв'язати міжетнічну війну, російська пропаганда намагалася сфабрикувати негативне уявлення про Україну. Проте спроба зобразити загарбників визволителями провалилася, а вбивство мирних жителів зруйнувало їхні надії.

Після анексії Криму і подій на Донбасі російська пропаганда зосередилася на інсинуаціях про злочини української влади, втручання НАТО іта США та виправдовувала вторгнення. Вони також використовували техніку «віддзеркалення», сфальсифікував звинувачення і найняв проросійських експертів і журналістів. Проте підтримка України міжнародним співтовариством та виявлення маніпуляцій допомогли знизити вплив російської пропаганди [53].

Щоб зрозуміти, як боротися з підробками, необхідно вміти відстежувати їх і знати їх природу і цільову аудиторію, якій вони адресовані. Одним з основних механізмів поширення російської пропаганди є використання платних агентів, які просувають російську мову через ЗМІ та соціальні мережі. Такі агенти створюють фальшиві новини, маніпулюють інформацією та провокують штучні конфлікти, щоб викликати розлад і заворушення в суспільстві.

Центр Ради національної безпеки і оборони по боротьбі з дезінформацією відіграє провідну роль щодо виявлення та поданні неправдивої інформації. Основна мета центру – не виявлення підробок, а встановлення того, що певна інформація є невірною. За вказаний період Центр по боротьбі з дезінформацією РНБО виявив 674 випадків поширення неправдивої інформації. Найбільша кількість підробок припадає на серпень майже 100 випадків. Загальна кількість підробок, виявлених центром дезінформації на місяць, показана на рис. 3.1 [33].

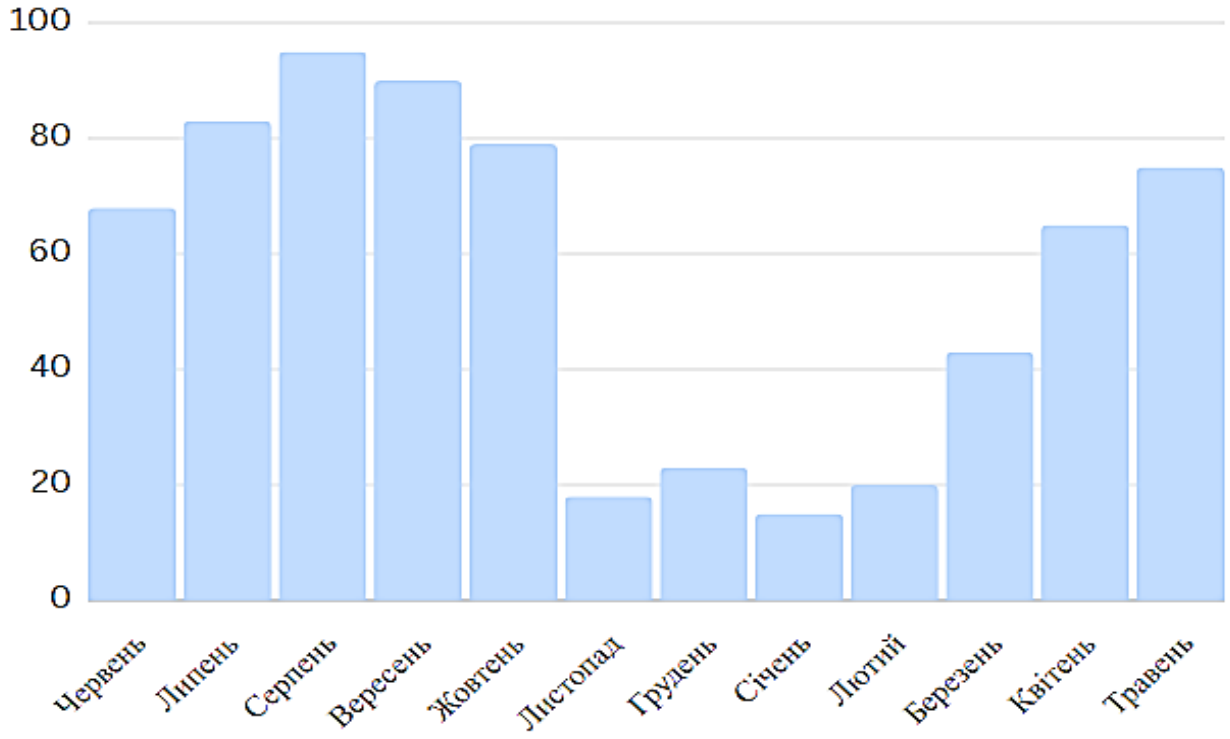

Рис. 3.1. Кількість опублікованих рф фейків з червня 2022 року по травень 2023 року

Джерело: [33].

Українські громадські організації та урядові установи активно працюють над розробкою механізмів протидії поширенню російської пропаганди. З цією метою використовуються такі заходи, як перевірка фактів, виявлення підробок, просування освітніх програм та критичне мислення серед населення. Також важливо співпрацювати з міжнародними партнерами та організаціями для обміну інформацією і координації зусиль по боротьбі з російською пропагандою.

Наступним етапом є поширення правдивої інформації, яка є одним з основних механізмів протидії поширенню російської пропаганди і дезінформації на Україні. Щоб досягнути цю мету українська влада, неурядові організації та незалежні ЗМІ активно працюють над створенням ефективної комунікаційної системи, що забезпечує поширення достовірної та об'єктивної інформації на різних рівнях.

Одним з головних аспектів поширення правдивої інформації є створення і підтримка незалежних медіа-організацій. Україна підтримує розвиток самостійних та незалежних телеканалів, інтернет-видань, радіостанцій та інших джерел інформації, що забезпечують об'єктивне висвітлення подій. Це дає можливість для громадян мати різні і достовірні погляди на події в країні і в світі.

З метою забезпечення широкого доступу до достовірної інформації Україна сприяє активному розвитку інформаційних технології та інтернет. Поширення новин, фактів, офіційних заяв та іншої інформації через соціальні мережі, веб-платформи та різноманітті мобільні додатки стає дедалі все більш поширеним явищем. Такий підхід дозволяє досить швидко і ефективно донести правдиву інформацію до більш широкої аудиторії, особливо молоді, яке активно користується цими технологіями.

Також, українська влада сприяє активній участі громадськості в поширенні правдивої інформації. Участь громадських організацій, активістів, експертів та журналістів у створенні та поширенні інформації забезпечує більшу об'єктивність і довіру до отриманої інформації. Відкриті конференції, публічні дебати, тренінги та інші заходи заохочують обмін ідеями та думками, що строює сприятливі умови для формування критичного мислення та здатності виявляти недостовірну інформацію [37].

Загальна культура медіаосвіти та критичного мислення громадян відіграє важливу роль у поширенні правдивої інформації. Зростаюча увага, що приділяється медіаосвіті в освітніх програмах і позакласних заходах, сприяє розвитку у населення навичок аналізу інформації, перевірки її достовірності та розумінні основних принципів функціонування засобів масової інформації.

Не менш актуальним кроком є співпраця з іншими міжнародними організаціями та країнами, зокрема з НАТО, Європейським союзом, Організацією з безпеки і співробітництва в Європі (ОБСЄ) та багатьма іншими, з метою розробки спільної стратегії та координації контрзаходів.

Одним з найважливіших аспектів міжнародного співробітництва є обмін

інформацією між різними країнами. Україна активно співпрацює зі своїми партнерами, надаючи їм інформацію про російську пропаганду і дезінформацію, що виходить зі своєї території. Взаємний обмін інформацією дозволяє країнам краще зрозуміти масштаби проблеми і виробити загальні контрстратегії.

Також, Україна співпрацює з міжнародними організаціями для координації заходів по боротьбі з російською пропагандою. У рамках цієї співпраці проводяться зустрічі, конференції та семінари для обговорення тенденцій поширення дезінформації та розробки спільних стратегій боротьби з ними. Ці формати співпраці сприяють обміну досвідом і виявленню передового досвіду в області інформаційної безпеки.

Крім того, Україна реалізує спільні проєкти з іншими країнами і міжнародними партнерами щодо підвищення інформаційної безпеки. Такі проєкти можуть включати обмін спільні програми навчання, експертами, створення спільних інформаційних ресурсів та деякі інші заходи, що спрямовані на зміцнення інформаційної безпеки в конкретному регіоні та в усьому світі в цілому.

Міжнародне співробітництво відіграє важливу роль в боротьбі з російською пропагандою та дезінформацією, адже це транскордонна проблема. Спільні зусилля країн і міжнародних організацій дозволяють більш ефективно протистояти цим загрозам і забезпечувати інформаційну безпеку не тільки в Україні, а й у всьому світі.

ВИСНОВКИ ДО РОЗДІЛУ 3

У боротьбі з загрозами інформаційній безпеці в Україні значна увага приділяється розробці законів і нормативних актів у галузі кібербезпеки. Україна активно працює над удосконаленням нормативно-правової бази, що створює цілісну основу для захисту інформації. Закони та нормативні акти

регулюють захист персональних даних, кібервійну, карантин інформації та відповідальність у разі кіберзлочинів. Це дозволяє покращити координацію між різними урядовими установами, спеціалізованими службами та приватними компаніями з метою ефективної боротьби з кіберзагрозами.

Україна вживає заходів з протидії загрозам, підвищуючи обізнаність громадян про механізми дезінформації та поширення неправдивих новин. Кампанії з просвітництва в засобах масової інформації, освітні та навчальні заходи для молоді та громадськості проводяться для забезпечення критичного мислення та здатності виявляти дезінформацію.

Крім того, співпраця з міжнародними партнерами є важливим елементом у боротьбі з загрозами інформаційній безпеці. Україна активно розвиває співпрацю з іншими країнами та міжнародними організаціями, при цьому обмінюючись передовим досвідом, інформацією і технологіями в галузі кібербезпеки. Це дозволяє виявляти кіберзагрози і ефективно боротися з ними, приєднуючись до них і обмінюючись досвідом.

ВИСНОВКИ

Інформаційна політика, яку росія постійно проводить щодо України, поступово перетворилася на інформаційну війну, а потім на гібридну війну. Щоб отримати переваги в цьому конфлікті, Україна активно стежить за ситуацією з інформаційної точки зору і застосовує різні інструменти з метою забезпечення своєї інформаційної безпеки. Одним з найбільш важливих планів є розробка і реалізація стратегічних комунікаційних аспектів, що направлені на вплив громадської думки і створення позитивного іміджу України. Це також важливий аспект підвищення інформаційної грамотності населення, постійне проведення антипропагандистської роботи та інформаційних кампаній з виявлення та протидії дезінформації і фейковим новинам. Також, Україна активно розвиває співпрацю з міжнародними організаціями та партнерами з метою обміну досвідом та координації зусиль в сфері забезпечення інформаційної безпеки.

Інформаційна безпека охоплює досить широкий спектр аспектів, залучаючи соціально-політичні, технічні, економічні та культурні компоненти. Це підкреслює необхідність комплексного підходу щодо забезпечення ефективного захисту державної інформації. Це значить, що необхідно поєднувати різні підходи і заходи з метою забезпечення конфіденційності, доступності та цілісності інформації. До видів інформаційної безпеки відносяться: організаційні, технічні, освітні та правові аспекти.

Проаналізувавши основні концепції навчання інформаційної безпеки в Україні, приймаючи нормативно-правову базу, принципи забезпечення інформаційної безпеки країни та загрози, з якими вона стикається, ми дійшли наступних висновків:

В даний час система управління загрозами інформаційної безпеки в більшості випадків працює пасивно, в той час як наші переконання засновані на практиці країн Європейського Союзу і вимагають активного стратегічного мислення. Країна вжила заходів для захисту цілей та їх вмісту, а також для

забезпечення безпеки з урахуванням принципів демократії, прав людини, безпечного Інтернету тощо.

В умовах війни не було змінено основні напрямки інформаційної політики держави. Однак російська агресія створює для України проблеми, які вимагають більш рішучих заходів в області інформаційної безпеки. Першим пріоритетом є співпраця з громадськістю, створення інформаційної системи для громадян та союзників та захист інформаційного суверенітету. Також важливо активно працювати на світовій арені, щоб поширювати правдиву інформацію про події в Україні та поширювати спростування ворожих фальсифікацій. Особлива увага приділяється взаємодії і координації дій різних державних органів у формулюванні української історії всередині країни та за кордоном. Також необхідно забезпечити, щоб населення було належним чином поінформоване про ситуацію на фронті та ознайомлене з важливістю заходів з евакуації та безпеки.

Забезпечення інформаційної безпеки в Україні – складний і багатогранний процес, що вимагає комплексного підходу і поєднання декількох заходів. Це має на мені розробку технічних, юридичних, освітніх та організаційних інструментів, співпрацю з міжнародними партнерами та участь усіх верств суспільства. Ці заходи гарантують ефективний захист національної інформації, досягнення стратегічних цілей та підтримку національної безпеки.

Україна перебуває в складних військових умовах і приділяє особливу увагу інформаційній безпеці. Держава активно реалізує заходи щодо реалізації стратегії інформаційної безпеки, спрямованої на захист національних інтересів, збереження інформаційного суверенітету та протидію розповсюдження російської пропаганди та дезінформації. Державні установи співпрацюють з громадським товариством, створюють єдину історію України та поширюють достовірну інформацію про події, що відбуваються в країні. Крім того, Україна активно виступає на світовій арені, залучає партнерів і співпрацює з міжнародними організаціями в зміцненні інформаційної безпеки.

Національна безпека і захист інформації – це пріоритети, реалізація яких вимагає постійних зусиль і координації зусиль усіх сфер життя суспільства. Україна демонструє високий рівень готовності до протидії загрозам інформаційній безпеці та забезпеченню належного захисту своїх громадян та національних інтересів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

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

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

3. 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.

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

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

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

7. Бойко В. О. Залучення громадськості до вирішення питань цифровізації та кібербезпекової політики. Аналітична записка. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/zaluchennya-gromadskosti-do-virishennya-pitan-cifrovizacii-ta.

8. Вербицький О. Організаційно-правові засади інформаційної безпеки. Юридичний журнал «Право України». 2017. С. 36–57.

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

10. Войціховський А. В. Кібербезпека як важлива складова системи

захисту національної безпеки європейських країн. Журнал східноєвропейського права. 2018. № 53. С. 26–37.

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

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

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

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

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

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

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

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

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

20. Ільницька У. Інформаційна безпека України: сучасні виклики,

загрози та механізми протидії негативним інформаційно-психологічним впливам. Політичні науки. 2016. № 1. С.27–32.

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

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

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

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

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

26. Концепція національної безпеки України: Затверджено Указом Президента України від 26.06.2015 р. № 287/2015. URL: https://www.president.gov.ua/documents/2872015-19070.

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

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

29. Лібік О. Основні засади інформаційної безпеки // Вісник Національного університету «Львівська політехніка». 2020. № 2. С. 45–52.

30. Марущак А. І., Панченко В. М. До визначення поняття «Інформаційна безпека» // Збірник наукових праць «Правчий вісник

університету «КРОК»». 2010. № 5 (1). С. 122–127.

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

32. Михайлюк Т. Розвиток інформаційного суспільства в Скандинавських країнах URL: http://www.viche.info/journal/1784.

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

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

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

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

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

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

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

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

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

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

43. Про Основні засади розвитку інформаційного суспільства в Україні

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

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

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

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

47. Смірнова Е. Криптографічний захист інформації: аспекти інформаційної безпеки // Збірник наукових праць КНУ імені Тараса Шевченка. 2017. С. 147–159.

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

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

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

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

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

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

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

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