

Державний торговельно-економічний університет
Кафедра публічного управління та адміністрування

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Студентки 5 курсу, 3 групи,
спеціальності 281 «Публічне
управління та адміністрування»
освітньої програми «Публічне
управління та адміністрування»

Бакай
Альони Григорівни

(підпис
студента)

Науковий керівник
к.економ.наук, доцент

Міняйло
Олександр Іванович

(підпис
керівника)

Гарант освітньої програми
к.держ.упр.

Динник
Ірина Петрівна

(підпис
гаранта)

Київ 2023

Державний торговельно-економічний університет

Факультет економіки, менеджменту та психології

Кафедра публічного управління та адміністрування

Освітній ступінь: бакалавр

Спеціальність: публічне управління та адміністрування

Освітня програма: публічне управління та адміністрування

Затверджую

Зав. кафедри _____

«30» грудня 2022 р.

Завдання на випускню кваліфікаційну роботу студентів

Бакай Альоні Григорівні

(прізвище, ім'я, по батькові)

1. Тема випускної кваліфікаційної роботи: «Державна політика в сфері інформаційної безпеки»

Затверджена наказом ректора від «14» грудня 2022 р. № 3416

2. Строк здачі студентом закінченої роботи: 01.02.2023

3. Цільова установка та вихідні дані до роботи

Мета роботи: дослідження і аналіз сучасного стану та особливостей реалізації державної інформаційної політики та інформаційної безпеки.

Об'єкт дослідження: пов'язані з національними інтересами інформація, інформаційна інфраструктура та правовий статус суб'єкти інформаційної сфери

Предмет дослідження: державна політика у сфері інформаційної безпеки в Україні

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

ЗМІСТ

ВСТУП

РОЗДІЛ 1. ОЦІНЮВАННЯ РІВНЯ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ В УКРАЇНІ

- 1.1. Сучасний стан державної політики у сфері інформаційної безпеки в Україні
- 1.2. Сутність та основні напрями державної політики у сфері забезпечення інформаційної безпеки України на сучасному етапі.

РОЗДІЛ 2. АНАЛІЗ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

- 2.1. Стан інформаційної безпеки України в умовах російської військової агресії
- 2.2. Розроблення заходів удосконалення державної політики у сфері інформаційної безпеки України та обґрунтування її ефективності

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

5. Календарний план виконання роботи

№ по р.	Назва етапів випускної кваліфікаційної роботи	Строк виконання етапів роботи	
		за планом	фактично
1	Визначення напрямку дослідження та затвердження теми випускної кваліфікаційної роботи	До 24.11.2022	24.11.2022
2	Складання плану та підготовка індивідуального завдання для виконання випускної кваліфікаційної роботи	До 30.12.2022	30.12.2022
3	Представлення на рецензування науковому керівнику рукопису першого розділу випускної кваліфікаційної роботи	До 10.01.2023	10.01.2023
4	Представлення на рецензування науковому керівнику рукопису другого розділу випускної кваліфікаційної роботи	До 20.01.2023	20.01.2023

5	Представлення закінченої випускної кваліфікаційної роботи	До 27.01.2023	27.01.2023
6	Підготовка письмового відгуку на випускню кваліфікаційну роботу	До 01.02.2023	01.02.2023
7	Проведення попереднього захисту випускних кваліфікаційних робіт	01-02. 06.2023	01-02. 06.2023
8	Вирішення питання про допуск випускної кваліфікаційної роботи до захисту	До 10.02.2023	До 10.02.2023
9	Направлення випускної кваліфікаційної роботи із зовнішньою рецензією у ЕК для захисту	За графіком	За графіком

5.Дата видачі завдання «30» грудня 2022 р.

6. Науковий керівник випускної кваліфікаційної роботи

(прізвище, ініціали, підпис)

8.Гарант освітньої програми Динник І.П.

9.Завдання прийняв до виконання студент

(прізвище, ініціали, підпис)

10.Відгук наукового керівника випускної кваліфікаційної роботи:

Науковий керівник випускної кваліфікаційної роботи _____

(підпис, дата)

Відмітка про попередній захист Динник Ірина Петрівна _____

(підпис, дата)

11. Висновок про випускну кваліфікаційну роботу:

Випускна кваліфікаційна робота студента Бакай А.Г.

(прізвище, ініціали)

може бути допущена до захисту екзаменаційній комісії.

Гарант освітньої програми: Динник І.П. _____

(підпис)

Завідувач кафедри: Новікова Н.Л. _____

(підпис)

«01» лютого 2023 р.

АНОТАЦІЯ

Бакай А.Г. Державна політика у сфері інформаційної безпеки. Випускна кваліфікаційна робота на здобуття ступеня бакалавра за спеціальністю 281 «Публічне управління та адміністрування» освітньою програмою «Публічне управління та адміністрування». Державний торговельно-економічний університет, 2023.

У випускній кваліфікаційній роботі досліджено сутність державної політики у сфері інформаційної безпеки та її зв'язок з державною інформаційною політикою. Визначено основні напрями, проблеми реалізації державної політики у сфері забезпечення інформаційної безпеки України на сучасному етапі. Досліджено проблему захисту національного інформаційного простору від негативних пропагандистських інформаційно-психологічних впливів, види реальних і потенційних інформаційних загроз для медіапростору України, охарактеризовано особливості загарбницької політики Російської федерації проти України, розробленні рекомендації щодо вдосконалення державної інформаційної політики та створення ефективної системи інформаційної безпеки України.

Проаналізовано рівень інформаційної безпеки України, в умовах воєнного стану. Аргументовано, що застосування інформаційних технологій військовими відкрило нові можливості щодо забезпечення оборони держави. Володіння інформаційними ресурсами у військовій сфері є важливим атрибутом. Аргументовано, що застосування інформаційних технологій військовими відкрило нові можливості щодо забезпечення оборони держави. Запропоновано комплекс заходів по забезпеченню інформаційної безпеки держави.

Ключові слова: інформаційна безпека, національна безпека, державна інформаційна політика, державна політика у сфері забезпечення інформаційної безпеки, інформаційно-психологічні впливи; інформаційна експансія, національні інтереси держави

SUMMARY

Bakai A. **State policy in the field of information security.** Graduation qualification work for obtaining a bachelor's degree in the specialty 281 "Public management and administration" in the educational program "Public management and administration". State University of Trade and Economics, 2023.

The final qualification work examines the essence of the state policy in the field of information security and its connection with the state information policy. The main directions and problems of the implementation of the state policy in the field of information security of Ukraine at the current stage have been determined. The problem of protecting the national information space from negative propagandistic informational and psychological influences, the types of real and potential informational threats to the media space of Ukraine were studied, the peculiarity of the aggressive policy of the Russian Federation against Ukraine was characterized; developed recommendations on improving the state information policy and creating an effective information security system of Ukraine.

The level of information security of Ukraine, in the conditions of martial law, was analyzed. It is argued that the use of information technologies by the military has opened up new opportunities for ensuring the defense of the state. Possession of information resources in the military sphere is an important attribute. It is argued that the use of information technologies by the military has opened up new opportunities for ensuring the defense of the state. A set of measures to ensure information security of the state is proposed.

Key words: information security, national security, state information policy, state policy in the field of information security, information and psychological influences; information expansion, national interests of the state,

ЗМІСТ

ВСТУП	9
РОЗДІЛ 1. ОЦІНЮВАННЯ РІВНЯ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ В УКРАЇНІ	12
1.1 Сучасний стан державної політики у сфері інформаційної безпеки в Україні	12
1.2. Сутність та основні напрями державної політики у сфері забезпечення інформаційної безпеки України на сучасному етапі.	17
РОЗДІЛ 2. АНАЛІЗ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	24
2.1. Стан інформаційної безпеки України в умовах російської військової агресії	24
2.2. Розроблення заходів удосконалення державної політики у сфері інформаційної безпеки України та обґрунтування її ефективності	32
ВИСНОВКИ ТА ПРОПОЗИЦІЇ	38
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	41

ВСТУП

Актуальність теми. На сучасному етапі існування та розвитку суспільства тісно пов'язано з використанням і створенням інформаційних технологій, єдиного інформаційного простору, а саме відбувається накопичення, обробка, зберігання та обмін інформацією, проблеми інформаційної безпеки набувають величезного значення в усіх сферах діяльності, як в суспільстві так і в державі. Головним пріоритетом України є прагнення побудувати відкрите для всіх і спрямоване на розвиток інформаційне суспільство, в якому кожен громадянин міг би вільно володіти інформацією та мати вільний доступ до неї, користуватися і обмінюватися ними, щоб надати можливість кожній людині повною мірою реалізувати свій потенціал, допомагати, сприяти суспільному і особистому розвитку та підвищуючи якість життя.

Сучасний стан розвитку держави характеризується стрімким розвитком інформаційних технологій, які використовуються в усіх сферах життєдіяльності суспільства. В умовах глобалізації процес інформатизації охопив усі країни світу. Сучасні інформаційні технології інтенсивно впроваджуються у процес управління. Разом з цим посилюється небезпека несанкціонованого втручання в роботу інформаційних систем, і вагомість наслідків такого втручання дуже сильно зростає. Неспроможність ефективного управління та невідповідність інформаційної структури новим умовам існування може призвести до втрати власного суверенітету.

Проблема забезпечення інформаційної безпеки України знайшла відображення в законах «Про основи національної безпеки України», «Про концепцію національної програми інформатизації», «Про національну програму інформатизації», а також у Концепції національної безпеки України. Сутність інформаційної безпеки як невід'ємної складової національної безпеки України вперше була зазначена у Законі «Про основи національної безпеки України».

Відповідно до законодавства України під інформаційною безпекою розуміють стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом.

Державна політика у сфері інформаційної безпеки зосереджена на задоволенні та захисті життєво важливих інтересів та потреб громадянина, суспільства і держави в інформаційній сфері щодо: продукування, споживання, розповсюдження і розвитку національного стратегічного контенту та інформації в інтересах громадянина, суспільства і держави.

Головною метою державної політики у сфері інформаційної безпеки є недопущення перешкоджання реалізації життєво важливих інтересів і потреб громадянина, суспільства і держави зовнішніми і внутрішніми загрозами національній безпеці в інформаційній сфері, що є запорукою сталого розвитку національного інформаційного простору[25].

В умовах сучасних інформаційних протистоянь, деструктивних комунікативних впливів, поширення інформаційної експансії та агресії, захист національного інформаційного простору та гарантування інформаційної безпеки стають пріоритетними стратегічними завданнями сучасних держав у системі глобальних інформаційних відносин. Збереження інформаційного суверенітету, формування ефективної системи безпеки в інформаційній сфері є актуальною проблемою для України, яка часто є об'єктом зовнішнього інформаційного загарбання, маніпулятивних пропагандистських технологій та руйнівного інформаційного вторгнення. В умовах російсько-української війни захист національного інформаційного простору від негативних інформаційно-психологічних впливів, операцій та війн, гарантування інформаційної безпеки та інформаційного суверенітету набувають особливого значення і стають чинниками збереження національної ідентичності України та функціонування її як суверенної та незалежної держави.

Мета роботи: дослідження і аналіз сучасного стану та особливостей реалізації державної інформаційної політики та інформаційної безпеки.

Об'єкт дослідження: пов'язані з національними інтересами інформація, інформаційна інфраструктура та правовий статус суб'єкти інформаційної сфери

Предмет дослідження: державна політика у сфері інформаційної безпеки в Україні.

Предметом дослідження відповідно до мети є:

1. Визначити поняття, напрями державної політики в сфері інформаційної безпеки, її проблеми
2. Провести аналіз основних важливих правових документів, законів інформаційного законодавства
3. Провести аналіз державної політики в сфері інформаційної безпеки
4. Запропонувати шляхи вирішення проблем та розробити комплекс заходів

Методи дослідження. Для виконання завдань дослідження використовувалися загальнонаукові та спеціальні методи:

1. Аналіз і синтез – для аналізу об'єкта роботи
2. Порівняльний метод для вивчення поняття, напрямів та нормативно – правової бази інформаційної безпеки
3. Метод моделювання – для проведення пропозицій та розробки певного комплексу заходів
4. Абстрактно-логічний метод – для узагальнення та формування висновків та пропозицій.

Структура роботи. Дипломна робота складається із вступу, основної частини, висновків, списку використаних джерел.

РОЗДІЛ 1.

ОЦІНЮВАННЯ РІВНЯ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ В УКРАЇНІ

1.1.Сучасний стан державної політики у сфері інформаційної безпеки в Україні

Інформаційна безпека є інтегрованою складовою національної безпеки і її розглядають як пріоритетну функцію держави. Інформаційна безпека, з одного боку, передбачає забезпечення якісного всебічного інформування громадян та вільного доступу до різних джерел інформації, а з іншого – це контроль за непоширенням дезінформації, сприяння цілісності суспільства, збереження інформаційного суверенітету, протидія негативним інформаційно-психологічним пропагандистським впливам та захист національного інформаційного простору від маніпуляцій, інформаційних війн та операцій. Рішення комплексної проблеми інформаційної безпеки дасть змогу як захистити інтереси суспільства і держави, так і гарантувати права громадян на отримання всебічної, об'єктивної та якісної інформації. Існує два аспекти трактування інформаційної безпеки у контексті національної безпеки. З одного боку, інформаційну безпеку розглянуто як самостійний елемент національної безпеки будь-якої країни, а з іншого – інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної тощо. Найповнішим є таке визначення: інформаційна безпека – це стан захищеності життєво важливих інтересів особистості, суспільства і держави, за якого зводиться до мінімуму завдання збитків через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [27]. Це визначення є оптимальним та відображає усі аспекти взаємодії суб'єктів інформаційних відносин. Термін «забезпечення інформаційної безпеки» означає діяльність, сукупність заходів і загалом здатність суспільства і держави гарантувати бажаний захищений стан. На думку фахівців,

забезпечення інформаційної безпеки передбачає наявність таких трьох складових: діяльність, засоби та суб'єкти (Рис.1).



Рис.1. Структура забезпечення інформаційної безпеки.

Джерело: розроблено автором за даними [42]

Увага до проблем гарантування інформаційної безпеки України зумовлена антиукраїнськими впливами, які пропагують ідеї сепаратизму, насильства, національної ворожнечі і є спробами руйнування національної ідентичності України, знищення міжнаціональної злагоди, посягання на конституційний лад України, територіальну цілісність держави. Проблема гарантування інформаційної безпеки України актуалізується в умовах війни на Сході, коли з боку Російської Федерації відбувається інформаційна експансія, упереджене та тенденційне висвітлення фактів та явищ, а технології російських інформаційно-психологічних операцій спрямовані на забезпечення домінування в українському (а також у глобальному) інформаційному просторі та на утримання медійної переваги. Через російські пропагандистські інформаційно-психологічні кампанії, акції, медіазаходи відбувається вплив не лише на суспільну свідомість громадян

України, а й на світову громадськість. Представник об'єднання "Інформаційний спротив" В. Гусаров, досліджуючи проблему інформаційної безпеки України, наголошує, що Росія здійснює інформаційно-психологічні атаки, щоб активізувати ескалацію конфлікту на сході України, чинити тиск на українське керівництво з метою змусити його погодитись на московський сценарій урегулювання конфлікту.

В. Гусаров виокремлює напрями інформаційно-психологічних атак проти України:

- 1) нав'язування думок про неспроможність української влади керувати державою та приймати раціональні рішення;
- 2) формування негативних суджень про воєнно-політичне керівництво України та про те, що хаотичні бойові дії призводять до невиправданих жертв серед сил АТО;
- 3) поширення поглядів про те, що українська армія на Сході України деморалізована та неспроможна вести бойові дії, а також про недовіру особового складу до керівництва;
- 4) нав'язування думки про те, що Україна не обійдеться без російського газу та що сторонам необхідно повернутися до перегляду газових контрактів.

Експерт зазначає, що цільовою аудиторією Кремля зараз є населення РФ, російськомовна діаспора за кордоном, населення України, зокрема в окупованих районах Донбасу, громадяни західних країн, а також країн БРІКС та Митного союзу, близькі Росії за політичними поглядами [26]. Україна стала об'єктом інформаційно-психологічних впливів, операцій, війн та її інформаційна безпека опинилась під загрозою. Можна констатувати, що:

- 1) український інформаційний простір є незахищеним від зовнішніх негативних пропагандистсько-маніпулятивних впливів і стає об'єктом інформаційної експансії;
- 2) у світовому медіапросторі відсутній український національний інформаційний продукт, що поширював би об'єктивну, неупереджену та

актуальну інформацію про події в Україні. Як наслідок – світова громадськість відчуває брак інформації або отримує її з інших джерел, які часом дезінформують, надають викривлену, спотворену, неповну інформацію. Водночас проти України активно застосовується потужний медіаресурс, здійснюється експансія іноземних суб'єктів на ринку інформаційних послуг, активізуються негативні інформаційні впливи, які спрямовані на викривлення реальності, заниження міжнародного іміджу держави;

3) діяльність вітчизняних ЗМІ щодо систематичного, об'єктивного висвітлення фактів, подій та явищ є недостатньою та позбавлена стратегічного планування; інформаційно-комунікативна політика України у сфері національної безпеки потребує невідкладного перегляду та удосконалення.

На жаль, як зазначає В. Петрик, низький загальний рівень інформаційної інфраструктури України сприяє експансії іноземними компаніями ринку інформаційних послуг, що створює сприятливі умови для перерозподілу ефірного часу на користь іноземних програм, окремі з яких засмічують український інформаційний простір своїм баченням подій, пропагують спосіб життя та традиції, тим самим деструктивно впливаючи на суспільство і державу, руйнуючи морально-етичні основи генофонду української нації. Недостатній контроль з боку держави за дотриманням законів України політичними силами, ЗМІ та окремими особами, які займаються підприємницькою діяльністю в інформаційній сфері, призводить до того, що нині трапляються непоодинокі випадки надання ефірного часу теле- та радіопрограмам, спрямованим на руйнування моральних цінностей, свідомості української нації[28]

За роки незалежності Україні вдалося напрацювала певну законодавчу базу у сфері національної інформаційної безпеки, яка і діяла до початку збройного вторгнення Росії в Україну, однак, як виявилось вона була не досконалою і відставала від сучасних реалій. Основними концептуальними документами нормативно-правової бази у сфері забезпечення інформаційної безпеки стали Закон України «Про інформацію» (став першим базовим нормативним законом у цій галузі); Закон України «Про друковані засоби масової інформації (пресу в

Україні)» (1992), Закон України «Про авторське право і суміжні права» (1993) [1-3] та ін. Важливим етапом стало прийняття Конституції України, яка гарантувала кожному право на вільне збирання, зберігання, використання і поширення інформації. Конституція стала основним правовим базисом подальшої нормотворчості в інформаційній сфері. Втім ця нормотворчість, поряд з певними позитивами розвитку інформаційного поля, свободи і захисту інформації, не виявила необхідної дієвості в умовах інформаційної війни. Головне, ця нормотворчість не забезпечила реалізацію ст. 17 Конституції, яка ставить інформаційну безпеку до ряду найважливіших функцій держави, таких як захист суверенітету та територіальної цілісності [12]. Однією з причин теперішньої ситуації на Сході України стала нездатність держави дотриматись саме цієї функції у своїй внутрішній політиці. Відповідно, незабезпечення інформаційної безпеки призвело до втрати частини суверенітету та територіальної цілісності нашої держави. З точки зору права, В. Цимбалюк та А. Бабінська справедливо вважають, що ураховуючи різноманіття проблем, досліджених в юридичній науці, слід зазначити, що аспект інформаційної безпеки в умовах глобалізації інформаційного простору ставить завданням вироблення теоретико-правових, методологічних, концептуальних, доктринальних, стратегічних, тактичних та оперативних правових засобів, здатних урегулювати суспільні інформаційні відносини, що здійснюються у взаємозв'язку з міжнародними правовими процесами гармонізації законодавства про інформаційну безпеку як підгалузь законодавства про інформацію [29]. Проте нині ситуація ускладнюється фактичним станом війни на території нашої держави, одним із основних чинників якої стала недостатня увага держави до інформаційної складової безпеки, у тому числі в правовій площині. Тому як, вказує О. Левченко, питання створення та функціонування системи інформаційної безпеки держави необхідно включати до проектів всіх ключових профільних документів і, в першу чергу, концептуальних [11]. З початком російської військової агресії проти України, у якій інформаційний супровід почав відігравати ключову роль, розпочалася трансформація національного інформаційного законодавства. Стартовим

нормативно-правовим актом у цьому напрямку стало рішення РНБО «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 28 квітня 2014 року, введене в дію Указом В. о. Президента України від 1 травня 2014 року № 449/2014. Поворотним твердженням документу стало: «Розглянувши стан забезпечення інформаційної безпеки, Рада національної безпеки і оборони України зазначає, що останнім часом Російська Федерація поширює недостовірну, неповну, упереджену інформацію про Україну, через що намагається маніпулювати суспільною свідомістю в Україні та за її межами» [13]. Документ також поставив завдання розроблення Стратегії кібернетичної безпеки України, Доктрини інформаційної безпеки України, механізму протидії негативному інформаційно-психологічному впливу, в тому числі шляхом заборони ретрансляції телевізійних каналів та ін. Відзначимо, що цей указ розпочав формування якісно іншої нормативноправової бази України у сфері інформаційної безпеки. Так, саме страшні наслідки російського втручання в Україну актуалізували питання інформаційної безпеки України. У цьому документі наголошено на необхідності прийняття основоположних документів в інформаційній сфері та внесення необхідних змін до вже існуючих[21].

1.2. Сутність та основні напрями державної політики у сфері забезпечення інформаційної безпеки України на сучасному етапі.

Інформаційна політика держави в сучасному політичному процесі розглядається як окремий вид політичної діяльності. Основні підходи до проблеми становлення державної інформаційної політики сформувалися ще в ХІХ ст. й отримали новий поштовх до розвитку в 60-х рр. ХХ в. у зв'язку зі вступом розвинених країн у стадію інформаційного суспільства [19, с. 44–45], коли ЗМІ з інструменту відображення реальності перетворились на інструмент створення реальності [2, с. 74]. На думку Г. Почепцова, інформаційну політику необхідно розглядати як сукупність принципів, підходів, визначальних законів функціонування інформаційної сфери [1, с. 12]. С.Бондаренко під державною

інформаційною політикою розуміє цілеспрямовану діяльність центральних органів влади з формування політико-релевантного знання про державу, його поширення та управління в інформаційному просторі з метою досягнення політичних цілей і захисту національних інтересів [3, с. 113]. Інформаційну політику держави також розглядають як діяльність держави в інформаційній сфері, спрямовану на задоволення інформаційних потреб людини і громадянина через формування відкритого інформаційного суспільства на основі розвитку єдиного інформаційного простору цілісної держави та його інтеграції у світовий інформаційний простір з урахуванням національних особливостей і інтересів під час забезпечення інформаційної безпеки на внутрішньодержавному та міжнародному рівнях [20, с. 6].

Основною метою державної політики у сфері забезпечення інформаційної безпеки при цьому є управління реальними та потенційними загрозами з метою створення необхідних умов для задоволення інформаційних потреб людини та громадянина, а також реалізації національних інтересів. Як зазначають Р. Шаповал та В. Ключко, державна політика у сфері забезпечення інформаційної безпеки України – це діяльність державно-правових інституцій щодо управління реальними та потенційними загрозами та небезпеками з метою задоволення інформаційних потреб людини та громадянина, а також реалізації національних інтересів, тож державна інформаційна політика та державна політика у сфері забезпечення інформаційної безпеки співвідносяться як ціле та частина [20, с. 6]. Отже, інформаційна безпека забезпечується проведенням єдиної державної політики в інформаційній сфері, системою заходів економічного, політичного й організаційного характеру, які є адекватними загрозам національній безпеці, а також можливостям держави щодо здійснення управління відповідними ризиками. Головне призначення цієї системи полягає у досягненні цілей національної безпеки в інформаційній сфері, а отже, її основною функцією є забезпечення збалансованого існування інтересів особи, суспільства і держави в інформаційній сфері.



Рис.2. Структура забезпечення інформаційної безпеки.

Джерело: розроблено автором за даними [10, с. 146].

Враховуючи національні інтереси та загрози в інформаційній сфері, Закон України «Про основи національної безпеки України» визначає основні напрями державної політики у сфері забезпечення інформаційної безпеки [14]. Єдність і взаємозв'язок напрямів державної політики у сфері забезпечення інформаційної безпеки має забезпечуватися визначеними на законодавчому рівні правовими механізмами, серед яких: чіткі цілі і завдання державної політики; взаємодія державних і громадських інститутів із реалізації міжвідомчих напрямів державної політики; організація системи інформування суб'єктів, що діють у сфері забезпечення інформаційної безпеки, про актуальні проблеми, виявлення потенційних і реальних загроз та їх джерела, а також доцільні заходи і засоби щодо їх попередження, нейтралізації та ліквідації можливих наслідків; узгоджені і цілеспрямовані дії суб'єктів, що діють у різних сферах життєдіяльності суспільства і держави з питань адекватного реагування на виявлені потенційні і реальні загрози; загальнодержавне керівництво, координація та контроль у сфері забезпечення інформаційної безпеки [4, с. 170].

З огляду на необхідність вдосконалення нормативно-правового забезпечення та попередження й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері, з початком гібридної війни проти України виникла необхідність кардинальних змін у системі забезпечення

інформаційної безпеки України. Основний план заходів запроваджено у рішенні РНБО від 28 квітня 2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України», затвердженого Указом Президента України № 449/2014 від 1 травня 2014 р. [5]. Згідно з рішенням РНБО, Кабінету Міністрів України було доручено розробити і внести на розгляд парламенту законопроекти про внесення змін у закони України щодо протидії інформаційній агресії іноземних держав, передбачивши, зокрема, визначення механізму протидії негативному інформаційно-психологічному впливу, зокрема шляхом заборони ретрансляції телевізійних каналів, а також щодо запровадження для іноземних ЗМІ системи інформування та захисту журналістів, які працюють у місцях збройних конфліктів, вчинення терористичних актів, ліквідації небезпечних злочинних груп. Крім того, необхідно було розробити проект стратегії розвитку інформаційного простору України, розробити і впровадити комплексні заходи організаційного, інформаційного і роз'яснювального характеру щодо всебічного висвітлення заходів із реалізації державної політики у сфері забезпечення інформаційної безпеки, а також посилити контроль за дотриманням законодавства з питань інформаційно-психологічної та кібернетичної безпеки. Відповідно до вказаного плану заходів було розроблено, зокрема, Стратегію кібербезпеки України, за якою розвиток та безпека кіберпростору, запровадження електронного урядування, гарантування безпеки й сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів мають бути складниками державної політики у сфері розвитку інформаційного простору та становлення інформаційного суспільства в Україні [17], та Доктрину інформаційної безпеки України [16]. Необхідність прийняття Доктрини інформаційної безпеки України зумовлена виникненням актуальних загроз національній безпеці в інформаційній сфері, а також потребою визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації. Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії

руйнівному інформаційному впливу РФ в умовах розв'язаної нею гібридної війни. Документ визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформсфері. Його правовою основою є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента від 26 травня 2015 р. № 287 [17], а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України. Із метою реалізації Доктрини РНБО має здійснювати координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері. Зважаючи на особливі умови і ведення проти нашої держави агресивної інформаційної війни не лише на її території, але й у світі, забезпечення реалізації Доктрини можливе лише за умови належної координації заходів, здійснюваних усіма державними органами. Кабінет Міністрів України забезпечуватиме здійснення інформаційної політики держави, фінансування програм, пов'язаних з інформаційною безпекою, спрямовуватиме і координуватиме роботу міністерств, інших органів виконавчої влади у цій сфері. Доктриною також покладається низка завдань на Міністерство інформаційної політики України, Міністерство закордонних справ, Міністерство оборони, Службу безпеки України, Державну службу спеціального зв'язку та захисту інформації, розвідувальні органи, Національний інститут стратегічних досліджень. Участь у забезпеченні захисту українського інформаційного простору від пропагандистської аудіовізуальної та друкованої продукції держави-агресора, розробленні пріоритетів і стимулів розвитку українського кіно, телевізійного контенту, книгодрукування, зокрема, щодо висвітлення героїчного спротиву українського народу російській агресії також беруть Міністерство культури України, Державне агентство України з питань кіно, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України відповідно до їх компетенції.

Сучасна інформаційна інфраструктура в нашій країні перебуває в стадії формування. Не повністю розроблене нормативно-правове підґрунтя відносин у сфері масової інформації. Відсутня конкретна державна політика у сфері

формування національного інформаційного простору, розвитку системи масової інформації, організації міжнародного інформаційного обміну. На фоні цього відзначається й погіршення ситуації із забезпечення безпеки відомостей, що мають державну таємницю. На жаль, під час забезпечення безпеки в інформаційно-психологічній сфері розглядається тільки технічна сторона, а психологічна переважно залишається поза увагою. Це призводить до посилення інформаційної агресії з боку РФ, яка з метою просування своїх інтересів використовує соціально-політичну ситуацію в нашій країні, в т.ч. й за участю українців. Події, що відбуваються в Україні, свідчать про використання іноземними суб'єктами зарубіжних і вітчизняних ЗМІ, соціальних мереж для зміни стану інформаційного простору з метою справляння впливу на хід подій, що завдає нашій країні відчутних політичних і економічних збитків. Відкритість національного інформаційного простору породжує реальну загрозу негативного інформаційно-психологічного впливу на суспільну свідомість населення, що становить особливу соціальну небезпеку. Безконтрольність електронних мас-медіа та соціальних мереж, які використовуються як майданчик для вербування в екстремістські організації, злочинні угруповання, незаконні збройні формування тощо, негативно впливає на користувачів мережі Інтернет, якими переважно є молодь й освічені люди з активною життєвою позицією[22].

Варто також враховувати, що українське суспільство нині розколоте за ставленням до таких фундаментальних цінностей, як демократія, незалежність, приватна власність, ринок тощо. Є розбіжності щодо уявлень про форму державного устрою та правління, кількість мов офіційного спілкування та навчання, напрямки децентралізації, функції і завдання місцевого самоврядування тощо. Існує ціла низка міжрегіональних, міжетнічних, міжконфесійних розбіжностей, різна шкала цінностей та пріоритетів, а тому важко говорити про єдність інформаційного простору та спільні ціннісні орієнтації [16, с. 96–97], що також є джерелом різнопланових внутрішніх загроз. Нині в Україні на законодавчому рівні відсутні достатні гарантії захисту населення від негативних інформаційно-психологічних впливів, результатом яких може стати руйнування

єдиного інформаційного й духовного простору. Тому виникає необхідність формування державної системи забезпечення інформаційно-психологічної безпеки, яка має будуватися на основі тісної взаємодії всіх галузей влади, а також громадських організацій. У процесі реалізації державної політики в області безпеки необхідно звернути увагу на: розроблення й реалізацію комплексних заходів щодо запобігання, нейтралізації й випередження негативних інформаційно-психологічних впливів на суспільство і державу; підготовку суспільства до активної інформаційної протидії; входження національного інформаційного поля у світовий інформаційний простір; удосконалення системи масової інформації й комунікації; формування системи підготовки кадрів для інформаційно-психологічної протидії; духовну консолідацію суспільства і віднайдення всіма верствами населення нової соціальної ідентичності. За сучасних умов інформаційна безпека має визнаватися основою інформаційної складової частини усіх сфер забезпечення національної безпеки¹²²⁴⁵⁵[22].

До головних завдань системи забезпечення інформаційної безпеки належать: прогнозування ризиків реалізації державної внутрішньої і зовнішньої політики, міждержавних та державних програм і проектів; виявлення внутрішніх і зовнішніх потенційних і реальних загроз; розроблення і впровадження адекватних заходів і засобів реагування на виклики як історичного походження, так і сучасного цивілізаційного розвитку; нейтралізація або послаблення дії проявів гібридної війни та інших загроз національній безпеці України. Системний і комплексний підхід до вирішення цих завдань має відповідним чином визначати спрямування державної політики у сфері забезпечення інформаційної безпеки нашої держави[5,с7].

РОЗДІЛ 2

АНАЛІЗ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Стан інформаційної безпеки України в умовах російської військової агресії

Національні інтереси України вимагають забезпечення сприятливих умов політичного розвитку країни. Так, інтереси особи полягають у реальному забезпеченні політичних прав і свобод громадян, суспільство потребує зміцнення демократії, а інтереси держави виражаються у необхідності ефективного захисту конституційного ладу суверенітету та територіальної цілісності країни, встановлення та підтримання політичної стабільності, включаючи стабільність державної влади та її інститутів. В інформаційній сфері на основі національних інтересів України формуються стратегічні та поточні завдання політики держави щодо забезпечення інформаційної безпеки. Ці завдання, зокрема про необхідність протидії спеціальним інформаційним операціям держави-агресора, спрямованих на підлив державного суверенітету, територіальної цілісності України, поставлені у Стратегії інформаційної безпеки України. Цей базовий концептуальний документ про сучасну політику нашої держави у сфері інформаційної безпеки було затверджено Указом Президента України 28 грудня 2021 р. [18]. У ньому визначено сім основних стратегічних цілей у сфері інформаційної безпеки України, можливість реалізації яких в умовах воєнного стану проаналізуємо.

1. Протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету та територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, проведення терористичних актів, посягання на права та свободи людини. На думку директора Українського інституту національної пам'яті Антона Дробовича, «полем бою є не тільки терени України. Такого не було під час Другої світової. Навіть війна в Сирії, де Росія теж свій п'ятак вставила, не було стільки людей, які в зоні військових дій із гаджетами і Інтернетом, які це покажуть. Неймовірна кількість

зафіксованих матеріалів із вебкамер, які стежать, як мародерять росіяни. Такого не було ніколи»[30]. В умовах воєнного стану країни особливо актуальним постало питання необхідності єдиної інформаційної політики. У зв'язку із цим Президент України підписав Указ № 152/2022, яким увів в дію Рішення Ради національної безпеки і оборони України «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану». Раніше РНБО України, «ураховуючи пряму військову агресію з боку Російської Федерації, активне поширення державо-агресором дезінформації, викривлення відомостей, а також виправдовування або заперечення збройної агресії Російської Федерації проти України, з метою донесення правди про війну, забезпечення єдиної інформаційної політики в період дії в Україні правового режиму воєнного стану», вирішила: «Установити, що в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки, забезпечення якої реалізується шляхом об'єднання усіх загальнонаціональних телеканалів, програмне наповнення яких складається переважно з інформаційних та/або інформаційно-аналітичних передач, на єдиній інформаційній платформі стратегічної комунікації – цілодобовому інформаційному марафоні «Єдині новини #UАразом». Таким чином, головним інструментом боротьби України проти російської дезінформації під час воєнного стану є правда, яку потрібно доносити не лише до внутрішньої, а й до закордонної аудиторії. Також велике значення мають медіакультура та медіаграмотність суспільства.

2. Забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності. Однією із цілей окупантів є знищення української культури та української громадянської ідентичності, тому уряд України ухвалив абсолютно правильне рішення, дозволивши установам культури та мистецтв відновити роботу в умовах війни. Як справедливо відзначив міністр культури та інформаційної політики Олександр Ткаченко, «діячі мистецтв готові працювати нон-стоп, аби полегшити страждання людей від пережитих жахів війни, подарувати позитивні емоції дорослим та дітям, а також відродити надію та

віру в краще майбутнє. Культура – це м'яка сила. Вона здатна повернути українців до нормального життя в новій військовій реальності» [31].

Українська культура і мистецтво – це імідж країни у світі. Тому дуже добре, що Міністерство культури та інформаційної політики України спільно з Державним агентством України з питань мистецтв та мистецької освіти та партнерами запускають проєкт *Ukraine Now and Forever*. Основна мета проєкту – спрямування уваги світу до української культури і мистецтва та подальша консолідація міжнародної спільноти у спротиві російській агресії. Проєкт передбачатиме реалізацію двох стратегічних завдань: заклик до світу щодо продовження накладення культурних санкцій на Росію та поглиблення знання зарубіжної аудиторії про українські культурні проєкти та мистецькі заходи [32]. І все ж таки необхідно, щоб таких проєктів та заходів було більше. Можна сказати без перебільшення, що потрібна культурна експансія України. Світ має чути про Україну щодня.

3. Підвищення рівня медіакультури та медіаграмотності суспільства. В умовах інформаційної війни, у ході якої поширюється безліч фейків, важливо, щоб суспільство мало певний рівень медіакультури та медіаграмотності. Щоб люди не панікували до того, як перевіряють інформацію. Щоб уміли відрізнити брехню від правди, виявляти ботів у соціальних мережах. Корисну роботу із цією метою проводить Національна спілка журналістів України [33]. Коли російські агресори завдали ракетного удару по житловому будинку в Одесі, у результаті якого загинуло вісім і поранено 18 людей, вони намагалися зняти з себе відповідальність за скоєне, поширивши спочатку фейк про те, що вразили військовий об'єкт, потім після його викриття військовий об'єкт перетворився на якусь нафтобазу. І цю брехню було викрито Одеською міською владою, яка опублікувала фото з місця трагедії. Тоді російські пропагандисти вигадали новий фейк про те, що житловий будинок став жертвою українських ППО. Однак і цей ворожий фейк був спростований фотографією будинку з характерними руйнуваннями від ракетних ударів [34].

Це вже далеко не перший фейк кремлівської пропаганди, «російська пропаганда вже намагалася неодноразово приховати свою причетність до масової загибелі українців. Яскравий приклад цьому – ракетний обстріл залізничного вокзалу в Краматорську, коли кремль спочатку радів знищенню «військової інфраструктури у Краматорську». Коли ж стала відома правда про вбивство пів сотні цивільних людей, то росіяни негайно видалили всі свої «новини» та звинуватили в усьому нашу державу» [35]. Для того щоб ворожа брехня не мала негативного впливу на населення, необхідно, за можливості, викривати всі фейки, що запускаються в український інформаційний простір. Це дасть змогу громадянам не лише отримувати правдиву інформацію, а й відчувати підтримку влади, яка постійно з ними на зв'язку. Медіакультура суспільства у вітчизняній науковій літературі визначається як «культура сприймання і виробництва соціальними групами та соціумом у цілому сукупності інформаційно-комунікаційних засобів, що функціонують у суспільстві, знакових систем, технологій комунікації, пошуку, збирання, виробництва і передавання інформації. На особистісному рівні медіакультура означає здатність людини ефективно взаємодіяти з мас-медіа, адекватно поводитися в інформаційному середовищі, здійснювати ціннісно-вольову рефлексивну регуляцію інформаційної поведінки» [6,с.71]. Необхідність підвищення медіакультури та медіаграмотності суспільства особливо гостро виявилася в умовах війни. Так, наприклад, несвідомі громадяни публікують у соціальних мережах фото та відео ворожих обстрілів, пересування української військової техніки чи позиції військових, не усвідомлюючи те, що цим полегшують завдання ворогові, створюють загрозу для військових та цивільних людей. Тому органи влади та структури громадянського суспільства мають через засоби масової інформації проводити постійну роз'яснювальну роботу серед населення, а правоохоронні органи – жорстко припиняти такі дії.

4.Забезпечення інформаційних прав особи, захисту прав журналістів. Як ми вже зазначали вище, саме правда є головним інструментом боротьби з ворожими фейками. Цю правду добувають і несуть у маси журналісти. Мужність українських журналістів, які висвітлюють хід війни, ризикуючи своїм життям,

зазначив керівник відділу ЮНЕСКО зі свободи вираження поглядів та безпеки журналістів Гільермо Канела на зустрічі у Центрі журналістської солідарності НСЖУ у Львові: «Вражає, наскільки українські журналісти віддані своїй справі, незважаючи на те, що їх спіткало. Ми підтримуємо вас у цій солідарності і хочемо зрозуміти, що можемо зробити для вас, щоб ви продовжували роботу» [36]. Журналісти, своєю чергою, розповіли про труднощі, з якими їм доводиться стикатися, про викрадення журналістів: «Також серед злочинів росіян – обстріли, погрози, переслідування журналістів, обстріли й захоплення телевеж, хакерські атаки на сайти українських медіа, обстріли офісів медіа, вимкнення українського мовлення, блокування доступу до сайтів українських медіа в РФ та окупованому Криму тощо» [37]. Із кінця березня ІМІ зафіксував погрози на електронні адреси редакцій українських медіа та журналістів. Листи-погрози надходили з російської пошти mail.ru, вони були підписані різними користувачами. Погрожували журналістам допитами, тортурами, ув'язненням, згодом почали слати навіть віршовані погрози. Такі листи отримали редакції «Європейської правди», «Главкому», «Апострофу», «Крим.Реалії», сайту міста «Запоріжжя 061.ua», низка волинських та запорізьких медіа[37].

Свою подяку журналістам, котрі розповідають правду про війну, висловив Президент України Володимир Зеленський під час пресконференції у київському метро. Ураховуючи, що доступ до інформації є одним з основних прав особистості, українська влада має робити все для того, щоб це право ніколи не було порушено. Інтереси особистості в інформаційній сфері полягають у реалізації конституційних прав людини і громадянина на доступ до інформації, на використання інформації на користь здійснення не забороненої законом діяльності, фізичного, духовного та інтелектуального розвитку, а також у захисті інформації, що забезпечує особисту безпеку.

5. Інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та прилеглих до них територіях України, до загальноукраїнського інформаційного простору. умовах воєнного стану воно є ще складнішим. Ситуація посилюється тим, В тимчасово окупованих територій

побільшало і ворог робить все, щоб розірвати інформаційні та культурні зв'язки українців з Україною, які там проживають. Знищують телевежі або захоплюють їх, включаючи російські канали. Також велика роль у вирішенні цієї проблеми має бути відведена гуманітарній освіті. Фахівці справедливо вказують на те, що «інформаційна стратегія не може існувати окремо від комплексної державної стратегії реінтеграції. Інформаційна стратегія – це складова частина загальної стратегії. Одне з головних завдань ЗМІ – просування через інформаційний простір державної стратегії реінтеграції: її роз'яснення і громадське обговорення; донесення проекту спільного майбутнього з чітко визначеними параметрами життя у об'єднаній країні; реалізація через інформаційний простір просвітницьких, освітніх, ціннісно-формуючих завдань» [38].

6. Створення ефективної системи стратегічних комунікацій, метою якої є гарантування ефективної інформаційної взаємодії між органами державної влади, органами місцевого самоврядування та суспільством з питань кризових ситуацій. Зміцнення позитивного іміджу України. У Доктрині НАТО наводиться таке визначення стратегічних комунікацій: скоординоване і належне використання комунікативних можливостей НАТО: публічної дипломатії, зв'язків з громадськістю, PR-служби збройних сил, інформаційних і психологічних операцій для підтримки політики Альянсу і заходів, спрямованих на просування цілей НАТО. Речник Міністерства оборони США у 2008–2009 рр. Роберт Гастінгс-мол. описав стратегічну комунікацію як «синхронізацію образів, дій та слів для досягнення бажаного ефекту» [39]. Можна зробити висновок про те, що якщо стратегічні комунікації – це система внутрішніх і зовнішніх комунікацій, то зв'язки з громадськістю – це один зі складників стратегічних комунікацій. А виступи Президента України, голів обласних військових адміністрацій, присвячені аналізу поточної ситуації, звіту про свою роботу, стали для громадян звичними. Формування іміджу України – це зона відповідальності зовнішніх комунікацій. Зміцнення позитивного іміджу України, як внутрішнього, так і зовнішнього, необхідне тому, що він багато в чому впливає на політичну,

економічну та культурну перспективу розвитку країни. В умовах воєнного стану формувати імідж України можна і потрібно.

7. Розвиток інформаційного суспільства та підвищення рівня культури діалогу. Формування інформаційного суспільства і розвиток інформаційних технологій, що продовжується, чинять значний вплив на відносини у сфері військової безпеки: інформаційні технології активно використовуються не лише в комерційній, а й у військовій галузі. [23].

Інформаційне протистояння є самостійним і принципово новим видом протистояння, здатним вирішувати конфлікт без застосування збройних сил у традиційному розумінні.

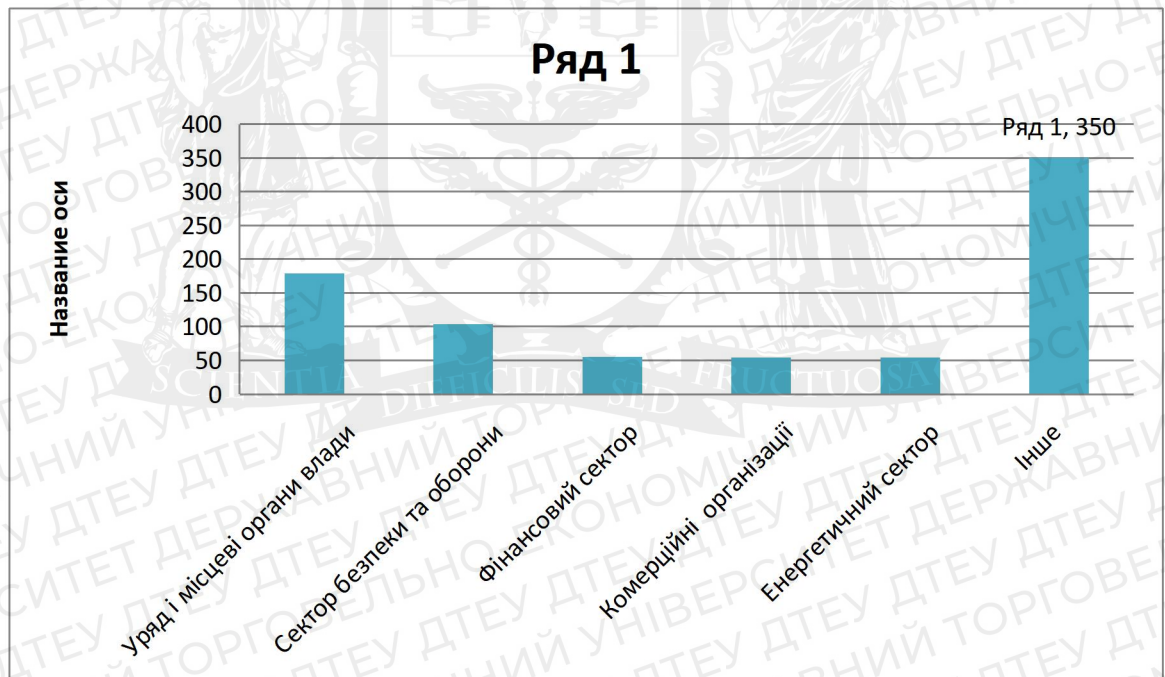


Рис.3 Статистика кібератак за чотири місяці війни розроблено автором на основі статистичних даних [43].

Для вивчення закономірностей інформаційного протистояння та аналізу його кількісних характеристик необхідно формалізувати як поняття рівня інформаційної озброєності держави, так і механізм еволюції ресурсного

потенціалу конкретної держави та вплив зовнішнього оточення. За основу аналізу вибраний інформаційний стан України.

Як базову розглянемо модель вирішення інформаційного конфлікту двох країн, яка складена на основі моделі Річардсона - Каспарова [7]. В основу моделі покладені наступні гіпотези:

- у процесі інформаційних атак кожна з двох країн прагне забезпечити зростання ефективності своєї інформаційної зброї пропорційно рівню інформаційності суперника;
- економічний потенціал кожної з країн надає/обмежує вплив на темп зростання інформаційних потужностей країни;
- держави ініціюють збільшення рівня інформаційних потужностей, керуючись власними прагненнями. Введемо позначення $N_1(t)$, $N_2(t)$ рівнів інформаційних потужностей кожної з сторін конфлікту, де t - час. Тоді перераховані вище умови дії моделі можуть бути формалізовані у вигляді системи двох звичайних диференціальних рівнянь:

$$N_1 = M_2 (L_1 - N_1) [1 - \exp(-p_1 (k_1 N_2 - a_1 N_1 + g_1))] \quad (1)$$

$$N_2 = M_1 (L_2 - N_2) [1 - \exp(-p_2 (k_2 N_1 - a_2 N_2 + g_2))],$$

де $M_1, M_2, L_1, L_2, p_1, p_2, a_1, a_2, k_1, k_2$ є позитивними коефіцієнтами, що не залежать від часу. Параметри моделі (1) за аналогією Т. Сааті [4] визначені наступним чином:

- k_1, k_2 - коефіцієнти реакції на інформаційні атаки;
- a_1, a_2 - показники витрат на генерацію інформаційної зброї;
- g_1, g_2 - коефіцієнти претензії (агресивності), якщо вони позитивні, або коефіцієнти доброї волі, якщо вони негативні;

M_1, M_2 - вартість наявного інформаційного забезпечення; L_1, L_2 - граничні значення рівнів інформаційних потужностей;

p_1, p_2 - коефіцієнти ступеня важливості інформаційних витрат. Модель (1) допускає існування чотирьох особливих розв'язків, що визначають координати положень рівноваги:

$$\begin{aligned}
 \text{а) } N_1^p &= N_1^*, N_2^p = N_2^* \\
 \text{б) } N_1^p &= N_1^*, N_2^p = L_2 \\
 \text{в) } N_1^p &= L_1, N_2^p = N_2^* \\
 \text{г) } N_1^p &= N_2^*, N_2^p = L_2
 \end{aligned} \quad (2)$$

де N_1^*, N_2^* - є рішення системи лінійних алгебраїчних рівнянь.

Нехай функції $u_1 = r_1^o (x_1 - x_2)$ і $u_2 = r_2^o (x_2 - x_1)$ характеризують політику кожної країни в сфері інформаційного протистояння, де змінні $x_1 = N_1 - N_1^*, x_2 = N_2 - N_2^*$ мають значення відхилень від рівноважних рівнів інформаційної потужності. Тут r_1^o, r_2^o - стаціонарні параметри управління.

З врахуванням вигляду функції u_1, u_2 система (1) набуває вигляду:

$$\begin{aligned}
 \dot{x}_1 &= M_1 (\delta_1 - x_1) [1 - \exp(p_1 (a_1 x_1 - k_1 x_2))] + r_1^o (x_1 - x_2) \\
 \dot{x}_2 &= M_2 (\delta_2 - x_2) [1 - \exp(p_2 (a_2 x_2 - k_2 x_1))] + r_2^o (x_2 - x_1)
 \end{aligned} \quad (3)$$

Можна зробити такі висновки: кожна держава, що є частиною світового інформаційного простору, має виробити комплекс заходів для власного сталого інформаційного розвитку в умовах жорсткої конкуренції з урахуванням чинників інформаційної безпеки[9].

2.2. Розроблення заходів удосконалення державної політики у сфері інформаційної безпеки України та обґрунтування її ефективності

Враховуючи цілі та завдання політики інформаційної безпеки України, як правило, виділяють такі основні напрями забезпечення інформаційної безпеки:

- забезпечення інформаційної достатності для прийняття рішень;
- захист інформації, тобто захист інформаційного ресурсу;
- захист та контроль національного інформаційного простору, тобто систем формування масової свідомості;
- присутність у світовому інформаційному просторі.

Головним завданням заходів із забезпечення інформаційної безпеки є зменшення шкоди через неповноту, несвоєчасність або недостовірність інформації чи негативного інформаційного впливу через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації[29] .

Загалом, основні напрямки діяльності по забезпеченню інформаційної безпеки держави являють собою величезний комплекс заходів, до яких відносяться:

- розвиток науково-практичних основ інформаційної безпеки;
- розвиток законодавчої і нормативно-правової бази забезпечення інформаційної безпеки; розробка нормативно-правових і організаційно-методичних документів;
- розробка концепції інформаційної безпеки, спеціальних правових і організаційних заходів, що забезпечують збереження і розвиток інформаційних ресурсів;
- формування правового статусу суб'єктів системи інформаційної безпеки;
- розробка законодавчих і нормативних актів, що регулюють порядок ліквідації наслідків загроз інформаційній безпеці;
- відновлення порушеного права і ресурсів, реалізації компенсаційних мір; вдосконалення організації форм і методів запобігання і нейтралізації загроз інформаційній безпеці;
- розвиток сучасних методів забезпечення інформаційної безпеки[26].

Розвиток науково-практичних основ інформаційної має включати в себе:

- розробку стратегії забезпечення інформаційної безпеки країни;
- обґрунтування державної політики в умовах глобалізації інформаційних процесів, формування світових інформаційних мереж, прагнення деяких країн до домінування в розвитку і використанні світового інформаційного простору;
- розробку науково-практичних основ формування і проведення державної політики в області забезпечення інформаційної безпеки;

-обґрунтування пріоритетів національної безпеки, що відповідають довгостроковим інтересам суспільного розвитку.

Розвиток законодавчої і нормативно-правової бази забезпечення інформаційної безпеки означає визначення порядку розробки законодавчих і нормативно-правових актів, а також механізмів практичної реалізації прийнятого законодавства.

Розробка нормативно-правових і організаційно-методичних документів включає розробку документів, що регламентують:

- діяльність в області інформаційної безпеки органів державної влади; взаємини суб'єктів інформаційної діяльності для забезпечення інформаційної безпеки;

- регулювання державою процесів функціонування і розвитку ринку засобів інформації, інформаційних продуктів і послуг;

- інформаційні відносини в суспільстві і державі в умовах ринкової економіки тощо.

Формування правового статусу суб'єктів системи інформаційної безпеки включає

- формування правового статусу користувачів інформаційних і телекомунікаційних систем;

- визначення їхньої відповідальності за забезпечення інформаційної безпеки процедур застосування законодавства і нормативних актів до суб'єктів, що скоїли злочини при роботі з закритою інформацією, а також правопорушення з використанням незахищених засобів інформації;

- розробку складу правопорушень з урахуванням специфіки карної, цивільної, адміністративної, дисциплінарної відповідальності.

Вдосконалення організації форм і методів запобігання і нейтралізації погроз інформаційної безпеки містить в собі:

-розробку нормативно-правової бази функціонування системи інформаційної безпеки, розмежування повноважень органів державної влади із забезпечення інформаційної безпеки;

-розробку системи моніторингу стану інформаційної безпеки; розробку пропозицій із створення сприятливих умов виходу з критичного стану вітчизняних галузей промисловості, що виробляють засоби інформатизації і захисту інформації;

-аналіз техніко-економічних параметрів вітчизняних і закордонних програмно-технічних засобів забезпечення інформаційної безпеки і вибір перспективних напрямків розвитку вітчизняної техніки;

-розробку системи економічних і статистичних показників, що характеризують ефективність функціонування системи забезпечення інформаційної безпеки;

-дослідження критеріїв і методів оцінки ефективності системи інформаційної безпеки тощо.

Під розвитком сучасних методів забезпечення інформаційної безпеки мається на увазі:

-розробка форм і способів цивілізованого впливу держави на формування суспільної свідомості і практичних рекомендацій з реалізації їх на практиці;

-розробка методів комплексного дослідження діяльності персоналу інформаційних систем, у тому числі методів підвищення мотивації, морально-психологічній стійкості і соціальної захищеності людей, що працюють із секретною і конфіденційною інформацією;

- розробка практичних рекомендацій зі збереження і зміцнення політичної стабільності в суспільстві; забезпеченню прав і свобод громадян;

- зміцненню законності і правопорядку методами інформаційної безпеки;

-формування шляхів і способів забезпечення органів державної влади, підприємств і громадян достовірною, повною і своєчасною інформацією;

- розробка основних напрямків діяльності із запобігання негативних інформаційних впливів на індивідуальну, групову і суспільну свідомість;
- розробка цивілізованих, демократичних форм і методів впливу на засоби масової інформації;
- розробка механізмів розвитку інформаційних відносин у сфері підприємництва і включення інформаційного ресурсу у господарські відношення;
- дослідження основних шляхів послаблення криміногенної обстановки, зниження числа комп'ютерних злочинів, у першу чергу - у кредитно-фінансовій сфері;
- розробка методів і практичних рекомендацій із контролю над експортом вітчизняних наукомістких технологій;
- обґрунтування напрямків протидії інформаційній зброї; удосконалення способів контролю за персоналом у захищених інформаційних системах.

Одним з найважливіших чинників національної безпеки країни є її економічний потенціал, під яким треба розуміти сукупність матеріальних і духовних сил суспільства, а також спроможність держави мобілізувати ці сили для забезпечення своєї безпеки. В свою чергу, інформація охоплює всі сфери людської діяльності і підвищує цей економічний потенціал країни, забезпечуючи зростання матеріальних і духовних сил суспільства і створюючи умови для можливостей, пов'язаних з координацією та мобілізацією. Крім того, вона створює матеріальні і інтелектуальні ресурси країни для ефективного захисту від агресивних в інформаційному відношенні держав[24].

З вищесказаного очевидно, що державна політика в сфері формування інформаційних ресурсів і інформатизації повинна бути спрямована на створення умов для ефективного і якісного інформаційного забезпечення рішення задач соціально-економічного розвитку країни.

Серед основних напрямків державної політики в сфері інформатизації виділяють:

- забезпечення умов для розвитку і захисту всіх форм власності на інформаційні ресурси;

- формування і захист державних інформаційних ресурсів;
- створення і розвиток федеральних і регіональних інформаційних систем і мереж, забезпечення їхньої сумісності і взаємодії в єдиному інформаційному просторі;
- створення умов для якісного й ефективного інформаційного забезпечення громадян, органів державної влади, організацій і суспільних об'єднань на основі державних інформаційних ресурсів;
- забезпечення національної безпеки в сфері інформатизації, а також забезпечення реалізації прав громадян, організацій в умовах інформатизації;
- сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем, технологій, засобів їхнього забезпечення;
- формування і здійснення єдиної науково-технічної і промислової політики в сфері інформатизації з обліком сучасного світового рівня розвитку інформаційних технологій
- підтримка проектів і програм інформатизації;
- створення й удосконалювання системи залучення інвестицій і механізму стимулювання розробки і реалізації проектів інформатизації;
- розвиток законодавства в сфері інформаційних процесів, інформатизації і захисту інформації[27].

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

Державна інформаційна політика в сфері інформаційної безпеки на теперішній час, а особливо в умовах російсько-української війни є стратегічним національним ресурсом, який має особливе значення для економіки, оборони, суверенітету держави. Також інформаційна безпека має невід'ємне значення для безпеки життєво важливих інтересів та потреб громадян України.

Визначено та з'ясовано зміст та види інформаційної безпеки, складовими якими є стан захищеності інтересів суспільства, держави, зберігання інформації. З'ясовано важливість розбору проблем в системі інформаційної безпеки та захисту інтересів суспільства і держави. Проаналізовано сутність та напрями державної політики. Різні підходи поняття «інформаційна політика» на думку Г. Почепцова-сукупність принципів, підходів, визначальних законів функціонування інформаційною політикою. Також бачення В. Цимбалюка та А. Бабинської щодо вирішення проблем в правовій науці інформаційної безпеки є розробка різних правових засобів, що зможуть вирішити та збалансувати суспільні інформаційні відносини за допомогою методологічних, концептуальних, доктринальних, стратегічних правових засобів.

Проаналізовано та вивчено основні важливі документи інформаційного законодавства, що мають важливу роль в безпеці держави. А саме закони «Про основи національної безпеки України», «Про концепцію національної програми інформатизації», «Про національну програму інформатизації», а також у Концепції національної безпеки України. Сутність інформаційної безпеки як невід'ємної складової національної безпеки України вперше була зазначена у Законі «Про основи національної безпеки України». Ці закони мають на увазі стан захищеності інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій.

В інформаційній політиці має приділятися більше уваги для виявлення та усунення проблем, створенню стратегії в цій галузі, удосконалення системи шляхом прийняття додаткових законів, що дозволить уникнути більш складних та глобальних проблем. Покращення та ефективність роботи державно-правових інститутів, відбір максимально компетентних кадрів дозволить задовільнити та вирішити національні інтереси держави і громадян України.

Проблема інформаційної безпеки полягає в удосконаленні нормативно-правової бази при вирішенні якої дозволить створити потужний механізм стримування зовнішньої інформаційної агресії, попередження проблем та якісній протидії та вирішенню наявних проблем, що не дозволить нашому ворогові здійснювати інформаційні атаки та поширювати пропагандистську інформацію.

Державна інформаційна політика відіграє важливу роль для забезпечення прав і свобод людини, зміцнення демократії, для держави - захист суверенітету, територіальної цілісності країни. Та мають вирішуватися завдання, що передбачають гармонійне забезпечення інформаційної безпеки держави, особи і суспільства з одночасним виділенням більш значущих пріоритетів, до яких варто створювати та відновлювати основні точки захисту системи національної безпеки в інформаційній сфері, створення ефективної системи інформаційної безпеки держави, перегляд списку нових інформаційних загроз, усунення реальних проблем для попередження наслідків.

На основі проаналізованих проблем на фоні сучасних інформаційних протистоянь пропагандистської політики Російської федерації, інформаційний простір України є недостатньо захищеним, тому задля захисту інформаційного суверенітету, та створення ефективної і сильної системи інформаційної безпеки України, виділені основні напрямки, які дозволять ефективно забезпечити інформаційну безпеку розробивши певним комплексом заходів, а саме:

- розвиток науково-практичних основ інформаційної безпеки;
- розвиток законодавчої і нормативно-правової бази забезпечення інформаційної безпеки;

- розробка нормативно-правових і організаційно-методичних документів;
- розробка концепції інформаційної безпеки, спеціальних правових і організаційних заходів, що забезпечують збереження і розвиток інформаційних ресурсів;
- формування правового статусу суб'єктів системи інформаційної безпеки;
- розробка законодавчих і нормативних актів, що регулюють порядок ліквідації наслідків загроз інформаційній безпеці;
- відновлення порушеного права і ресурсів, реалізації компенсаційних мір; вдосконалення організації форм і методів запобігання і нейтралізації загроз інформаційній безпеці;
- розвиток сучасних методів забезпечення інформаційної безпеки.
- розробку стратегії забезпечення інформаційної безпеки країни;
- обґрунтування державної політики в умовах глобалізації інформаційних процесів, формування світових інформаційних мереж, прагнення деяких країн до домінування в розвитку і використанні світового інформаційного простору;
- розробку науково-практичних основ формування і проведення державної політики в області забезпечення інформаційної безпеки;
- обґрунтування пріоритетів національної безпеки, що відповідають довгостроковим інтересам суспільного розвитку.

Отже, для вирішення проблем в державній політиці в сфері інформаційної безпеки потрібно підходити комплексно та впевнено проводити якісні та злагоджені дії всіх інститутів та організацій для досягнення мети.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Інформаційна політика: [навчальний посібник] / Г.Почепцов, С. Чукут. – К.: Знання, 2008. – 663 с.
2. Champagne P. 1993. La vision médiatique. – La misère du monde. Paris: Le Seuil. – P. 72–74.
3. Інформаційне право та інформаційне законодавство/Брижко В.М., Фурашев В.М. : наукове видання. – (НДІП НАПрН України). Київ: Видавничий дім “АртЕК”, - 2020. -288 с.
4. Олійник О.В. Інформаційна безпека України: доктрина адміністративно-правового регулювання : дис ... д-ра юрид. наук : 12.00.07 / О.В. Олійник. – Київ, 2013. – 203 с.
5. Руденко Ю.Ю. Плюралізм в Україні як складова інформаційної політики у контексті забезпечення національної безпеки / Ю.Ю. Руденко // Актуальні проблеми управління інформаційною безпекою держави: зб. матер. наук.-практ. конф. – К. : Наук-вид. відділ НА СБ України, 2012. – С. 96–97.
6. Медіакультура особистості: соціально-психологічний підхід : навчальний посібник / за ред. Л.А. Найдьоновой, А.Т. Баришпольця. Київ : Міленіум, 2009. 440 с.
7. Денисюк С. Г. Моделювання політичних процесів / С. Г. Денисюк, А. А. Шиян // Прикладна політологія : навч. посіб. / за ред. В. П. Горбатенка. – К. : ВЦ «Академія», 2008. – 472 с.
8. Деремо В. Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки / В. Н. Деремо // Інформаційна безпека людини, суспільства, держави. – 2015. – № 2. – С. 16-22.
9. І. Р. Боднар, Інформаційна безпека як основа національної безпеки / І. Р. Боднар/ Механізм регулювання економіки. Суми.-2014.-С.1-9

10. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: [монографія] / Б.А. Кормич. – Одеса: Юридична література, 2003. – 472 с.

11. Левченко О. В. Нормативно-правове регулювання інформаційної безпеки України: стан та шляхи вирішення проблем / О. В. Левченко. // Збірник наукових праць Харківського університету Повітряних сил. — 2014. — Випуск 3 (40) — С. 130–135.

12. Конституція України. Прийнята Верховною Радою України 28.06.1996 [Електронний ресурс] — Режим доступу: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>

13. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України. Рішення РНБО від 28.04.2014 [Електронний ресурс] — Режим доступу: <http://zakon2.rada.gov.ua/laws/show/n0004525-14>

14 . Про основи національної безпеки України : Закон України від 19.06.2003 р. № 964 [Електронний ресурс]. — Режим доступу : <http://zakon2.rada.gov.ua/laws/show/964-15>.

15. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» : Указ Президента України від 01.05.2014 р. № 449/2014 [Електронний ресурс]. — Режим доступу : www.president.gov.ua/documents/4492014-17157.

16. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017 [Електронний ресурс]. — Режим доступу : www.president.gov.ua/documents/472017-21374.

17. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України» : Указ Президента України від 15

березня 2016 р. № 96/2016: [Електронний ресурс]. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/96/2016#Text>

18. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: <https://www.president.gov.ua/documents/6852021-41069>

19. Тихомирова О. Інформаційна політика незалежної України: періодизація та вплив на громадянське суспільство / О. Тихомирова // Грані : наук.-теорет. і громад.-політ. альм. – 2020. – Т. 23, № 10. – С. 24–35.

20. Шаповал Р.В., Ключко В.О. Вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України / Р.В. Шаповал, В.О. Ключко // Наше право. – 2014. – № 6. – С. 5–9.

21. Ільницька У, Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним / Ільницька/Політичні науки.-2016.с27-32 [Електронний ресурс]. – Режим доступу <https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf>

22. Ткачук Т.Ю., Державна політика у сфері забезпечення інформаційної безпеки на сучасному етапі/Ткачук Т.Ю/ Науковий вісник Ужгородського національного університету.-2017.-с.29-42 [Електронний ресурс]. – Режим доступу:

<https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/34230/1/%D0%94%D0%95%D0%A0%D0%96%D0%90%D0%92%D0%9D%D0%90%20%D0%9F%D0%9E%D0%9B%D0%86%D0%A2%D0%98%D0%9A%D0%90%20%D0%A3%20%D0%A1%D0%A4%D0%95%D0%A0%D0%86%20%D0%97%D0%90%D0%91%D0%95%D0%97%D0%9F%D0%95%D0%A7%D0%95%D0%9D%D0%9D%D0%AF.pdf>

23. Залєвська І. І., Удренас Г. Інформаційна безпека України в умовах Російської військової агресії/ Залєвська І. І., Удренас Г. І / Південноукраїнський правничий часопис -2022.-№1-2.-С.20-26 [Електронний ресурс]. – Режим доступу: <http://www.sulj.oduvs.od.ua/archive/2022/1-2/6.pdf>

24. Турчак А., Основні складові інформаційної безпеки держави/ Турчак А / Аспекти публічного управління.-2019.-ТОМ7№5.-С.44-56 [Електронний ресурс]. – Режим доступу: <https://core.ac.uk/download/pdf/233892903.pdf>
25. Перевалова Л.В., Державна політика в сфері інформаційної безпеки / Перевалова Л.В. / Інформаційні технології: наука, техніка, технологія, освіта, здоров'я. -2017.- Ч. IV. [Електронний ресурс]. – Режим доступу: https://www.kpi.kharkov.ua/archive/microcad/2017/S24/tez_mic_17_IV_p306-p306.pdf
26. Гусаров В. Кремль розпочав нову інформаційну операцію проти України [Електронний ресурс] / В. Гусаров. – Режим доступу: <http://www.osvita.mediasapiens.ua/material/34281>
27. Захист інформаційної безпеки як функція держави [Електронний ресурс]. – Режим доступу: <http://www.mego.info/матеріал/23-захист-інформаційноїбезпеки-як-функція-держави>
28. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / В. Петрик. – Режим доступу: <http://www.justinian.com.ua/article.php?id=3222>
29. Цимбалюк В.С., Бабінська А. В. Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики [Електронний ресурс] — Режим доступу: <http://applaw.knu.ua/index.php/holovna/item/284-pravove-rehulyuvannya-informatsiynoyibezpeky-v-ukrayini-problemy-teoriyi-ta-praktyky-tsymbaliuk-v-s-babynska-a-v>.
30. «Перша світова медійна війна». З якою назвою напад Росії на Україну увійде в історію і що робити з 9 травня – інтерв'ю з Антоном Дробовичем. URL: <https://nv.ua/ukr/world/geopolitics/viynav-ukrajini-persha-svitova-mediyna-viyna-drobovichnovini-ukrajini-50235840.html>.
31. Уряд дозволив закладам культури відновити роботу в умовах війни. URL: <https://zaxid.net/> [uryad_dozvoliv_zakladam_kulturi_vidnoviti_robotu_v_umovah_viyini_n1539889](https://zaxid.net/uryad_dozvoliv_zakladam_kulturi_vidnoviti_robotu_v_umovah_viyini_n1539889).

32. Ukraine Now and Forever: Держава презентує об'єднаний бренд української культури в світі #StandWithUkraine <https://ck-oda.gov.ua/novyny-cherkaskoyi-oblasti/ukraine-now-and-forever-derzhava-prezentuye-obyednaniy-brend-ukrayinskoyi-kulturi-v-sviti-standwithukraine>

33. Онлайн-лекція «Фактчекінг в умовах війни»: репортерам розкажуть, як об'являти ложь в соцсетях, – НСЖУ. URL: <https://ukranews.com/news/852453-onlajn-lektsiya-faktcheking-v-usloviyahvojny-reporteram-rasskazhut-kak-obnaruzhivat-lozh-v>.

34. Росіяни намагалися видати обстріляний житловий будинок в Одесі за «військовий об'єкт» – Центр стратегічних комунікацій. <https://nv.ua/ukr/odesa/rosiyani-namagalis-vidati-obstrilyaniy-zhitloviy-budinok-v-odesi-za-viyskoviy-ob-yekt-50236728.html>

35. Обстріл житлового будинку в Одесі: окупанти за фейком намагалися приховати свій злочин. URL: <https://armyinform.com.ua/2022/04/25/obstrilzhytlovogo-budynku-v-odesi-okupanty-za-fejkomnamagalysya-pryhovaty-svij-zlochyn/>.

36. В ЮНЕСКО вражені преданністю українських журналістів во время войны своей профессии, – НСЖУ <https://ukranews.com/news/852283-v-yunesko-vpechatleny-predannosti-ukrainskih-zhurnalistov-vo-vremya-vojny-svoej-professii-nszhu>

37. Росія скоїла 243 злочини проти журналістів та медіа в Україні – моніторинг ІМІ. <https://detector.media/infospace/article/198658/2022-04-24-rosiya-skoila-243-zlochyny-proty-zhurnalistiv-ta-media-v-ukraini-monitoryng-imi>

38. Реінтеграція окупованих територій: інформаційна складова. URL: <https://od.org.ua/uk/>.

39. Картки: що таке стратегічна комунікація і кому вона потрібна. URL: <https://cpc.com.ua/articles/kartki-scho-take-strategichna-komunikaciya-ikomu-vona-potribna>

40. Домарев В. В. Безпека інформаційних технологій. Методологія створення систем захисту / В. В. Домарев. – Режим доступу: <http://domarev.kiev.ua>
41. Концепція інформаційної безпеки держав-учасників Співдружності Незалежних Держав у військовій сфері. – Режим доступу: <http://www.ngo.dn.ua>
42. Інформаційна безпека держави: : [навчальний посібник] /Т. Мужанова/ Київ,2019.-131 с.
- 43.Урядовий портал.- – Режим доступу:
<https://www.kmu.gov.ua/news/derzhspeczvyazku-statistika-kiberatak-za-chotiri-misyaci-vijni>



РЕЦЕНЗІЯ

На випускню кваліфікаційну роботу Бакай Альони Григорівни на тему:
«Державна політика в сфері інформаційної безпеки»,
 виконаної на здобуття ОС «Бакалавр»
 за спеціальністю 281 «Публічне управління та адміністрування»
 у Київському національному торговельно-економічному університеті

Представлена на рецензію випускна кваліфікаційна робота носить актуальний характер, вирізняється своєчасністю, популярними методами, поняттями державної політики в інформаційній системі, присвячено питанням сутності, напрямкам, основні важливим документам інформаційного законодавства.

У процесі аналізу автором використовувалися теоретичні методи дослідження відповідно до Закону України «Про інформацію»; Закону України «Про друковані засоби масової інформації (пресу в Україні)» (1992), Закону України «Про авторське право і суміжні права» (1993), загальнонаукові та спеціальні методи, аналізу і синтезу, порівняльний, абстрактно-логічний метод, що дали змогу отримати синтезоване уявлення про досліджуваний об'єкт а також показати складові.

Метою дослідження є аналіз нормативно-правового інформаційного законодавства, змісту та видів інформаційної безпеки, проблем інформаційної безпеки. Робота складається із вступу, двох розділів, висновків, переліку посилань на використані інформаційні джерела та додатків.

Перший розділ висвітлює сутність, напрямки, рівень інформаційної безпеки держави, головні завдання системи забезпечення інформаційної безпеки.

У другому розділі визначено цілі у сфері інформаційної безпеки, виділено основні напрями забезпечення інформаційної безпеки, розроблено заходи по вдосконаленню державної політики в сфері інформаційної системи.

Випускна кваліфікаційна робота відповідає вимогам, виконана в повному обсязі і заслуговує на позитивну оцінку, а її автор Бакай Альона Григорівна на отримання кваліфікації бакалавра відповідно до обраної спеціальності.

Рецензент



Василь ЖИЛА

Завідувачу кафедри публічного
управління та адміністрування
Новіковій Н.Л.



Я, Бакай Альона Григорівна повідомляю, що за результатами проведення самостійної перевірки з використанням програмно-технічних засобів у наданій випускній кваліфікаційній роботі на тему: « Державна політика у сфері інформаційної безпеки» не міститься елементів академічного плагіату. У випадках використання прямих запозичень з друкованих та електронних джерел, вказані відповідні посилання.

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

«24» січня 2023 року

 (підпис)

Згода

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

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

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

«24 січня 2023 року

Підпис

Прізвище, ініціали