

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний аерокосмічний університет
«Харківський авіаційний інститут»

Факультет програмної інженерії та бізнесу

Кафедра економіки та публічного управління

ПОЯСНЮВАЛЬНА ЗАПИСКА ДО КВАЛІФІКАЦІЙНОЇ РОБОТИ

магістра
(освітньо-кваліфікаційний рівень)

на тему: «**ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ІНФОРМАЦІЙНОЇ
БЕЗПЕКИ**»

ХАІ.601.6-96пуа.25О.281.11972153 ПЗ

Виконав: здобувач 2 курсу групи б-69пуа

Спеціальність 281 «Публічне управління та
адміністрування

(код та найменування)

Освітньо-професійна програма:

«Управління та адміністрування регіональних
економічних систем»

(найменування)

Філахтов І.Г.

(прізвище й ініціали здобувача)

Керівник: Дегтяр А.О.

(прізвище й ініціали)

Рецензент: Дзюндзюк В.Б.

(прізвище й ініціали)

Харків – 2025 року

**Міністерство освіти і науки України
Національний аерокосмічний університет
«Харківський авіаційний інститут»**

Факультет програмної інженерії та бізнесу

(повне найменування)

Кафедра економіки та публічного управління

(повне найменування)

Рівень вищої освіти другий (магістерський)

(найменування)

Спеціальність 281 «Публічне управління та адміністрування»

(код та найменування)

Освітня програма «Управління та адміністрування регіональних економічних систем»

(найменування)

**ЗАТВЕРДЖУЮ
Завідувач кафедри**

(підпис)

Вікторія ШВЕДУН

(ім'я та прізвище)

«25» вересня 2025р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

Філахтова Ігоря Геннадійовича

(прізвище, ім'я, по батькові)

Тема кваліфікаційної роботи

ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1. Керівник кваліфікаційної роботи: Дегтяр А.О., д-р. наук держ. упр., професор
затверджені наказом Університету «22» жовтня 2025 року №1681-уч
2. Строк подання студентом кваліфікаційної роботи « 1 2 » грудня 2025 року
3. Вихідні дані до кваліфікаційної роботи: чинне законодавство, матеріали
виробничої практики, періодична література, статистичні дані, інші джерела.
4. Зміст пояснювальної записки: теоретичні засади формування формування та
реалізації державної політики у сфері інформаційної безпеки, аналіз сучасного стану
державної політики України у сфері інформаційної безпеки, напрями вдосконалення
державної політики України у сфері інформаційної безпеки.
5. Перелік графічного матеріалу: Презентація кваліфікаційної роботи в Power Point

5. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Основний	Дегтяр А.О., професор каф. 601	01.10.2025	12.12.2025

Нормоконтроль Дегтяр А.О. «05» грудня 2025 р.
(підпис) (ініціали та прізвище)

6. Дата видачі завдання «01» жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітки
1.	Дослідження основних літературних джерел з теми кваліфікаційної роботи	06.10.2025 - 19.10.2025	виконано
2.	Розділ 1 Теоретичні засади формування та реалізації державної політики у сфері інформаційної безпеки	20.10.2025 – 02.11.2025	виконано
3.	Розділ 2 Аналіз сучасного стану державної політики України у сфері інформаційної безпеки	03.11.2025 – 16.11.2025	виконано
4.	Розділ 3 Напрями вдосконалення державної політики України у сфері інформаційної безпеки	17.11.2025 – 29.11.2025	виконано
5.	Висновки	30.11.2025	виконано
6.	Оформлення пояснювальної записки	01.12.2025 – 02.12.2025	виконано
7.	Оформлення графічного матеріалу	03.12.2025– 04.12.2025	виконано
8.	Нормоконтроль та перевірка на плагіат	05.12.2025 – 07.12.2025	виконано
9.	Одержання відгуку керівника та рецензії	08.12.2025 – 09.12.2025	виконано
10.	Підготовка до передзахисту та передзахист	10.12.2025 – 12.12.2025	виконано
11	Підготовка до захисту	13.12.2025 – 23.12.2025	виконано

Здобувач

(підпис)

Ігор ФІЛАХТОВ

(ім'я та прізвище)

Керівник роботи

(підпис)

Андрій ДЄГТЯР

(ім'я та прізвище)

РЕФЕРАТ

Кваліфікаційна робота магістра: 113 с., 4 таблиці, 113 джерел.

Тема кваліфікаційної роботи «Державна політика у сфері інформаційної безпеки»

Об'єктом дослідження є державна політика у сфері інформаційної безпеки.

Предмет дослідження – державна політика у сфері інформаційної безпеки України в умовах гібридної агресії РФ.

Метою роботи є теоретичне обґрунтування напрямів удосконалення державної політики у сфері інформаційної безпеки України в умовах гібридної агресії РФ.

В першому розділі кваліфікаційної роботи розкриті сутність та зміст державної політики у сфері інформаційної безпеки, розглянуто зарубіжний досвід **В другому розділі** проаналізовано загрози інформаційної безпеки України в умовах гібридної війни та дана оцінка ефективності чинних механізмів державної політики у сфері інформаційної безпеки. **В третьому розділі** розкрито механізми оптимізації державного управління у сфері інформаційної безпеки

Практичне значення роботи полягає у розробці науково обґрунтованих пропозицій та рекомендацій щодо розвитку правових, інституційних, технологічних та кадрових спроможностей держави із протидії загрозам в інформаційній сфері, їх адаптації до специфіки сучасних гібридних конфліктів. Результати дослідження можуть бути використані в діяльності органів державної влади при розробці стратегічних документів, цільових програм, планів заходів у сфері інформаційної безпеки, вдосконаленні чинної нормативно-правової бази, оптимізації інституційного механізму державного управління тощо. Окремі положення роботи доцільно застосовувати в навчальному процесі при викладанні курсів з питань національної та інформаційної безпеки, державної інформаційної політики.

ABSTRACT

Master's qualification work: 110 p., 4 tables, 113 sources.

The topic of the qualification work "State policy in the field of information security"

The object of the study is state policy in the field of information security.

The subject of the study is state policy in the field of information security of Ukraine in the conditions of hybrid aggression of the Russian Federation.

The purpose of the work is the theoretical substantiation of the directions of improvement of state policy in the field of information security of Ukraine in the conditions of hybrid aggression of the Russian Federation.

The first section of the qualification work reveals the essence and content of state policy in the field of information security, considers foreign experience. ***The second section*** analyzes the threats to Ukraine's information security in the conditions of hybrid war and gives an assessment of the effectiveness of the current mechanisms of state policy in the field of information security. ***The third section*** reveals the mechanisms for optimizing public administration in the field of information security.

The practical significance of the work lies in the development of scientifically based proposals and recommendations for the development of legal, institutional, technological and personnel capabilities of the state to counter threats in the information sphere, their adaptation to the specifics of modern hybrid conflicts. The results of the study can be used in the activities of state authorities in the development of strategic documents, target programs, action plans in the field of information security, improvement of the current regulatory and legal framework, optimization of the institutional mechanism of public administration, etc. It is advisable to apply certain provisions of the work in the educational process when teaching courses on national and information security, state information policy.

ЗМІСТ

ВСТУП	7
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ ТА РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.....	10
1.1. Сутність та зміст державної політики у сфері інформаційної безпеки	10
1.2. Зарубіжний досвід формування та реалізації державної політики у сфері інформаційної безпеки	26
РОЗДІЛ 2. АНАЛІЗ СУЧАСНОГО СТАНУ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	41
2.1. Загрози інформаційній безпеці України в умовах гібридної війни	41
2.2. Оцінка ефективності чинних механізмів державної політики у сфері інформаційної безпеки	54
РОЗДІЛ 3. НАПРЯМИ ВДОСКОНАЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	71
3.1. Стратегічні пріоритети державної політики інформаційної безпеки України	71
3.2. Механізми оптимізації державного управління у сфері інформаційної безпеки	83
ВИСНОВКИ.....	97
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ	103

ВСТУП

Актуальність теми. Забезпечення інформаційної безпеки набуває критичного значення для України в умовах повномасштабної збройної агресії Російської Федерації, що триває вже третій рік. Починаючи з 2014 року, коли Росія анексувала Крим та розв'язала гібридну війну на Донбасі, інформаційний простір нашої держави перетворився на поле запеклої битви. Кремль розгорнув проти України безпрецедентну за масштабами та цинізмом кампанію дезінформації, маніпуляцій та пропаганди, намагаючись дестабілізувати ситуацію всередині країни, посіяти розбрат та зневіру в українському суспільстві, делегітимізувати українську владу в очах міжнародної спільноти.

Однак з початком повномасштабного вторгнення 24 лютого 2022 року інформаційна агресія Кремля сягнула небачених раніше масштабів та інтенсивності. Російська пропагандистська машина працює на повну потужність, продукуючи фейки та викривлені наративи про події в Україні, виправдовуючи воєнні злочини окупантів, перекладаючи відповідальність за війну на Київ та Захід. Інформаційні атаки синхронізуються з ракетними ударами по цивільній інфраструктурі та мирних містах, створюючи ефект «інформаційного терору». Російські хакери активно зламують українські урядові сайти та бази даних, поширюють вірусні програми, намагаючись паралізувати роботу критично важливих інформаційних систем. Проти України розгорнуто цілу мережу ботоферм та фейкових акаунтів у соцмережах, які тиражують кремлівські меседжі на глобальну аудиторію.

В цих драматичних умовах перед Україною постали безпрецедентні виклики в інформаційній сфері. Попри героїчні зусилля наших військових, волонтерів, журналістів та блогерів, які на фронті та в тилу борються з російською дезінформацією, гібридна агресія завдає відчутних втрат. Вона не лише руйнує інформаційний суверенітет нашої держави, а й завдає болючих

психологічних травм суспільству, підриває довіру громадян до української влади, сіє розбрат та зневіру, працює на розкол країни. Тож вироблення дієвої та адекватної моделі державної інформаційної політики, здатної ефективно протистояти багатовимірним загрозам в інформаційній сфері, швидко виявляти та нейтралізувати ворожі інформаційні впливи, гарантувати інформаційно-психологічну безпеку суспільства – це питання національного виживання України, збереження її державності та ідентичності.

На жаль, чинна державна політика інформаційної безпеки досі лишається недостатньо ефективною перед лицем «війни нового типу». Вона характеризується інституційною розпорошеністю, браком стратегічного бачення та координації між ключовими суб'єктами, зосередженістю на протидії наслідкам інформаційних атак, а не їх упередженні. Недостатньо уваги приділяється розвитку проактивних спроможностей держави в інформаційній сфері – від стратегічних комунікацій та публічної дипломатії до кіберрозвідки та активних контрзаходів у відповідь на ворожі інформаційні операції. Бракує системної взаємодії з громадянським суспільством, медійною спільнотою та міжнародними партнерами. Тож очевидно є нагальна потреба докорінної трансформації державної інформаційної політики на основі сучасних підходів, кращого світового досвіду та національної специфіки. Лише така оновлена політика дозволить нашій державі вистояти та перемогти в затяжній інформаційній війні, яку розв'язав проти нас підступний ворог. Відтак, обрана тема магістерської роботи є надзвичайно актуальною як з погляду теоретичного осмислення, так і практичного вирішення невідкладних завдань національної безпеки України.

Мета і завдання дослідження. Метою роботи є теоретичне обґрунтування напрямів удосконалення державної політики у сфері інформаційної безпеки України в умовах гібридної агресії РФ.

Для досягнення поставленої мети визначено такі завдання дослідження:

- проаналізувати теоретико-методологічні засади дослідження державної політики у сфері інформаційної безпеки;

- узагальнити зарубіжний досвід формування та реалізації державної політики у сфері інформаційної безпеки;
- охарактеризувати сучасний стан державної політики у сфері інформаційної безпеки України, оцінити її ефективність у протидії актуальним загрозам;
- обґрунтувати стратегічні пріоритети та механізми оптимізації державного управління у сфері інформаційної безпеки України.

Об'єктом дослідження є державна політика у сфері інформаційної безпеки.

Предмет дослідження – державна політика у сфері інформаційної безпеки України в умовах гібридної агресії РФ.

Методи дослідження. Теоретико-методологічною основою дослідження є загальнонаукові та спеціальні методи пізнання. Зокрема, застосовано системний підхід, який дозволив комплексно розглянути інформаційну безпеку у взаємозв'язку її компонентів; порівняльний метод, за допомогою якого узагальнено підходи різних країн до забезпечення інформаційної безпеки; структурно-функціональний аналіз для з'ясування ефективності інституційного механізму інформаційної безпеки України; прогностичний метод для обґрунтування перспектив удосконалення державної інформаційної політики.

Наукова новизна одержаних результатів полягає у вирішенні актуального науково-прикладного завдання – обґрунтування концептуальних засад та практичних рекомендацій щодо вдосконалення державної політики у сфері інформаційної безпеки України в умовах гібридної агресії РФ. Зокрема: комплексно проаналізовано теоретичне підґрунтя забезпечення інформаційної безпеки як функції держави; систематизовано передовий зарубіжний досвід протидії інформаційним загрозам; оцінено стан і дієвість існуючої моделі державної інформаційної політики; визначено ключові напрями та механізми її трансформації в контексті актуальних викликів національній безпеці.