Прим. № 1

**НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ**

Кафедра інформаційної безпеки держави

# РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

## Інформаційне протиборство

| | |
|---|---|
| Освітня програма | «Кіберзахист у сфері інформаційних технологій та кіберпросторі» |
| Рівень вищої освіти | другий (магістерський) |
| Форма здобуття вищої освіти | заочна |
| Статус навчальної дисципліни | обов'язкова |
| Мова викладання | українська |

КИЇВ – 2025

обл. 877
по пс 401

Робочу програму навчальної дисципліни розглянуто та схвалено на засіданні кафедри КІБД ННІ ІБ СК НА СБ України від «30» 09 2025 року, протокол № 11.

Робочу програму навчальної дисципліни погоджено з гарантом освітньої програми:

Структура робочої програми навчальної дисципліни відповідає встановленій формі, навчальному плану (схвалено Вченою радою НА СБ України від 26.06.2025р., протокол №6), робочому плану на 2025/2026 навчальний рік.

## Опис навчальної дисципліни

| Показник | Значення показника |
|---|---|
| **Курс (и)** | 1 |
| **Семестр (и)** | 1, 2 |
| **Обсяг *(кредити ЄКТС/години)*** | 5 /150 |
| **Кількість змістових модулів** | 3 |
| **Розподіл годин за видами навчальної діяльності:** | |
| **лекції (Л)** | 8 |
| **семінарські заняття (СЗ)** | 8 |
| **практичні заняття (ПЗ)** | |
| **лабораторні заняття (ЛЗ)** | |
| **індивідуальні завдання (ІЗ)** | |
| самостійна робота (СР) | 134 |
| **форма підсумкового контролю *(семестр)*** | екзамен |

## 2. Мета та завдання навчальної дисципліни

2.1. Мета та основні завдання навчальної дисципліни

Мета: формування у студентів сучасного рівня інформаційно-психологічної та комп'ютерної культури, набуття знань про організаційно-правові основи, принципи, методи та засоби інформаційного протиборства, набуття практичних навичок підготовки та ведення інформаційних операцій, використання новітніх інформаційно-психологічних, інформаційно-комунікаційних технологій для вирішення різноманітних завдань у професійній діяльності.

Завдання:

Основними завданнями вивчення дисципліни «Інформаційне протиборство» є:

вивчення нормативних документів в сфері інформаційного протиборства;

вивчення основних понять, які пов'язані з інформаційним протиборством;

вивчення принципів та методів інформаційного протиборства;

вивчення рефлексивного управління як теоретичної основи інформаційного протиборства;

вивчення основ використання можливостей глобальної мережі Internet в інтересах інформаційного протиборства;

проведення моніторингу соціально-орієнтованих ресурсів мережі Internet як складової національного інформаційного простору;

вивчення використання відкритих даних у веденні інформаційного протиборства;

надбання вмінь та навичок ефективного використання сучасних комп'ютерних інформаційних технологій при вирішенні практичних завдань інформаційного протиборства, освоєння нових програмних продуктів;

вивчення основ автоматизації обробки документів в ході інформаційного протиборства.

2.2. Результати навчання

Обов'язкова навчальна дисципліна «Інформаційне протиборство» спрямована на досягнення програмних результатів навчання, які в інтегрованому (синтезованому) вигляді визначені у профілі освітньо-професійної програми «Кіберзахист у сфері інформаційних технологій та кіберпросторі» *(від 26.06.2025 № 6)*, а саме:

| | |
|---|---|
| ПРН 2. | Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності. |
| ПРН 3. | Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог |
| ПРН 5. | Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів |
| ПРН 8. | Забезпечувати дотримання принципу гендерної рівності під час здійснення професійної діяльності. |
| ПРН 11. | Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності . |
| ПРН 13. | Організовувати та здійснювати керівництво територіальною обороною, мобілізаційною підготовкою та мобілізацією у межах професійної компетентності. |
| ПРН 15. | Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів. |
| ПРН 16. | Організовувати та спрямовувати діяльність фахівців з кіберзахисту у сфері інформаційних технологій та кіберпросторі; розробляти та впроваджувати заходи із кіберзахисту у сфері інформаційних технологій та кіберпросторі, самостійно та у взаємодії з контролюючими органами. |
| ПРН 20. | Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. |
| ПРН 24. | Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. |

## 3. Програма та структура навчальної дисципліни

| Назви змістових модулів, тем навчальних занять | Кількість годин | | | | | |
|---|---|---|---|---|---|---|
| | Усього | Л | СЗ | ПЗ | ЛЗ | СР |
| *1* | *2* | *3* | *4* | *5* | *6* | *7* |
| **Семестр 1** | | | | | | |
| **Змістовий модуль 1. Інформаційне протиборство як механізм забезпечення національної безпеки в інформаційній сфері** | | | | | | |
| **Тема 1. Генезис інформаційного протиборства** | **16** | **2** | **2** | | | **12** |
| Лекція 1. Сутність та зміст інформаційного протиборства | | 2 | | | | |
| Семінар 1. Еволюція інформаційного протиборства | | | 2 | | | |
| Самостійна робота 1. Загрози національним інтересам в сфері інформаційного протиборства | | | | | | 12 |
| **Тема 2. Сучасні стратегії та концепції інформаційного протиборства** | **26** | **2** | | | | **24** |
| Лекція 1. Стратегія інформаційного протиборства держави | | 2 | | | | 24 |
| Самостійна робота 1. Стратегія національної безпеки України: інформаційний аспект | | | | | | 12 |
| Самостійна робота 2. Концепції інформаційного протиборства провідних країн світу | | | | | | 12 |
| Модульна контрольна робота 1. | | | | | | |
| **Всього годин за модуль 1** | **42** | **4** | **2** | | | **36** |
| **Модуль 2. Теоретичні та технологічні основи інформаційного протиборства** | | | | | | |
| **Тема. 3 Теоретичні основи інформаційного протиборства** | **16** | **2** | **2** | | | **12** |
| Лекція 1. Рефлексивне управління як теоретична основа інформаційного протиборства | | 2 | | | | |
| Семінар 1. Когнітивне моделювання інформаційного протиборства | | | 2 | | | |
| Самостійна робота 1. Теоретичний доробок Володимира Лефевра | | | | | | 12 |
| **Тема 4. Технології та засоби інформаційного протиборства** | **26** | | | | | **26** |
| Самостійна робота 2. Технології та засоби захисту у сфері інформаційної безпеки та кіберсфері | | | | | | 12 |
| Самостійна робота 3. Технології та засоби інформаційного протиборства в сфері кібербезпеки | | | | | | 14 |
| Модульна контрольна робота 2. | | | | | | |
| **Всього годин за модуль 2** | **42** | **2** | **2** | | | **38** |
| **Модуль 3. Організаційні аспекти підготовки та ведення інформаційного протиборства** | | | | | | |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| **Тема 5. Форми ведення інформаційного протиборства** | **14** | **2** | **2** | | | **10** |
| Лекція 1. Форми ведення інформаційного протиборства | | 2 | | | | |
| Семінар 1. «Використання відкритих даних у веденні інформаційного протиборства» | | | 2 | | | |
| Самостійна робота 1. Особливості ведення інформаційно-психологічної операції на державному та військовому рівнях | | | | | | 10 |
| **Тема 6. Підготовка та ведення інформаційного протиборства з використанням соціально-орієнтованих ресурсів мережі Internet та відкритих даних** | **32** | | **2** | | | **30** |
| Самостійна робота 1. Система інформаційного протиборства держави | | | | | | 10 |
| Семінар 1. «Моніторинг соціально-орієнтованих ресурсів мережі Internet як складової національного інформаційного простору» | | | 2 | | | |
| Самостійна робота 1 «Моніторинг початку спеціальної інформаційної операції» | | | | | | 10 |
| Самостійна робота 2. «Спеціальна інформаційна операція у протидії загрозам національній безпеці» | | | | | | 10 |
| **Тема 7. Перспективи ведення інформаційного протиборства в соціальних мережах** | **20** | | | | | **20** |
| Самостійна робота 1. Технології використання сервісів та прикладних програмних засобів для ведення інформаційного протиборства в соціальних мережах | | | | | | 10 |
| Самостійна робота 2. Інформаційне протиборство в соціальних мережах в системі стратегічних комунікацій | | | | | | 10 |
| Модульна контрольна робота 3 | | | | | | |
| **Всього годин за модуль 3.** | **66** | **2** | **4** | | | **60** |
| **Підсумковий контроль (екзамен)** | | | | | | |
| **Всього годин за навчальну дисципліну** | **150** | **8** | **8** | | | **134** |

## 4. Основні методи навчання

Методи організації та здійснення навчально-пізнавальної діяльності:

1. За джерелом інформації:

словесні: лекція (традиційна, проблемна) із застосуванням комп'ютерних інформаційних технологій, семінари, пояснення, розповідь, бесіда;

наочні: спостереження, ілюстрація, демонстрація.

2. За логікою передачі і сприймання навчальної інформації: індуктивні, дедуктивні, аналітичні, синтетичні.

3. За ступенем самостійності мислення: репродуктивні, пошукові, дослідницькі.

4. За ступенем керування навчальною діяльністю: під керівництвом викладача; самостійна робота студентів: з книгою; виконання індивідуальних навчальних проектів.

Методи стимулювання інтересу до навчання і мотивації навчально-пізнавальної діяльності:

навчальні дискусії;

створення ситуації пізнавальної новизни;

створення ситуацій зацікавленості (метод цікавих аналогій тощо).

## 5. Оцінювання результатів навчання

5.1 Результати навчання здобувача вищої освіти з навчальної дисципліни оцінюються за 100-бальною шкалою як сума балів поточного та підсумкового контролю із застосуванням наступних вагових коефіцієнтів, загальна сума яких дорівнює 1:

| Вид контролю | Ваговий коефіцієнт |
|---|---|
| Поточний контроль (К) | **0,6** |
| Підсумковий контроль (ПК) | **0,4** |

**Підсумкова семестрова оцінка (ПСО) обчислюється за формулою: ПСО=К+ПК**

5.2. Складниками для обчислення балу поточного контролю здобувача вищої освіти є:

| Види навчальної діяльності | Кількість балів (максимальна) |
|---|---|
| Робота на лекціях (ведення конспекту лекцій або інше) | 1 |
| Робота на семінарських заняттях | 5 |
| Робота на практичних заняттях | - |
| Робота на лабораторних заняттях | - |
| Виконання завдань для самостійної роботи | 1 |
| Виконання індивідуальних та/або групових завдань | - |
| Виконання модульної контрольної роботи | 5 |

**Мінімальна кількість балів для допуску до підсумкового контролю 36**

5.3. Шкала оцінювання здобувача вищої освіти

| Оцінка за шкалою ЄКТС | Оцінка за 100-бальною шкалою | Значення оцінки |
|---|---|---|
| A | 90-100 | *Відмінно – відмінне виконання лише з незначною кількістю помилок.* Здобувач вищої освіти виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування і нахили. |
| B | 84-89 | *Дуже добре – вище середнього рівня, але з кількома помилками.* Здобувач вищої освіти вільно володіє вивченим обсягом матеріалу, застосовує |

| | | |
|---|---|---|
| | | його на практиці, вільно розв'язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна. |
| C | 75-83 | *Добре – загалом правильна робота, але з певною кількістю помилок.* Здобувач вищої освіти вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, серед яких є суттєві, добирати аргументи для підтвердження думок. |
| D | 65-74 | *Задовільно – непогано, але зі значною кількістю недоліків.* Здобувач вищої освіти відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих. |
| E | 60-64 | *Достатньо – виконання задовольняє мінімальні вимоги.* Здобувач вищої освіти володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні. |
| FX | 35-59 | *Незадовільно – потрібна додаткова робота.* Здобувач вищої освіти володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу |
| F | 1-34 | *Незадовільно – потрібна значна додаткова робота.* Здобувач вищої освіти володіє матеріалом на рівні елементарного розпізнання і відтворення окремих фактів, елементів, об'єктів. |

## 6. Ресурсне забезпечення навчальної дисципліни

**Основна література:**


1. Актуальні проблеми інформаційної безпеки: навч. посіб./ О.О. Тихомиров, А.В. Ватраль, Д.С. Мельник та ін. Київ: НА СБУ, 2024. 264 с.
2. Інформаційна безпека: підручник / [В. В. Остроухов, М. М. Присяжнюк, О.І.Фармагей, М.М.Чеховська та ін.]; під ред. В.В.Остроухова. – К.: Ліра-К, 2021. – 412 с.
3. Інформаційне протиборство: навчальний посібник / І.М. Ничитайло, Л.В. Єрьоміна, В.Л. Тиква, Г.М. Чіпуріна, В.М. Шемаєв; – К.: Наук.-вид. відділ НА СБ України, 2023. – 263 с.
4. Сугестивні технології маніпулятивного впливу: навчальний посібник / [В. М. Петрик, М. М. Присяжнюк, Л. Ф. Компанцева, Є. Д. Скулиш, О. Д. Бойко, В. В. Остроухов]; за заг. ред. Є. Д. Скулиша. — 2-ге вид.— Київ: Вид. Дім. «СКІФ», 2023. —248 с.
5. Забезпечення інформаційної та кібербезпеки в умовах військової агресії рф проти України: аналітичний огляд/ Л.М. Стрельбицька, М.П. Стрельбицький, М.Л. Пальчик. – Київ: НА СБУ, 2022. – 56 с.


**Допоміжна література:**


1. Горбулін В.П. Як перемогти росію у війні майбутнього / В.Горбулін – Київ: Брайт Букс, 2021. – 248 с.
2. Почепцов Г. Г. Токсичний інфопростір / Г. Почепцов - Харків: Віват, 2022. - 384 с.
3. Почепцов Г.Г. Когнітивні війни у соцмедіа, масовій культурі та масових комунікаціях/ Г. Почепцов – Харків: Фоліо, 2019. – 314 с.
4. Кулеба Д.І. Війна за реальність. Як перемагати у світі фейків, правд і спільнот/ Д.Кулеба – Київ: Книголав, 2023. – 480 с.
5. Деструктивні впливи та негативні наративи: інструменти виявлення та протидії: метод.мат. / Д.В. Дубов, А.В. Баровська, Ю.К. Каздобіна. – К.:УФБС,

2020. – 60 с.
6. Сенченко М. Мас-медіа, піар, як засоби маніпуляції/ М.І. Сенченко, О.М. Сенченко. – Київ: Ліра К, 2022. – 200 с.
7. Світова гібридна війна: український фронт: монографія / за заг. Ред. В.П. Горбуліна. – К.: НІСД, 2017. - 496 с.
8. Зелена книга протидії дезінформації / Упоряд. і заг. ред. С. Балан. – ГО «Інститут інформаційної безпеки». – К., 2022. – 178 с.

**Нормативно-правові акти:**

1. Конституція України (Відомості Верховної Ради України (ВВР), 1996, № 30).
2. Закон України "Про Службу безпеки України" від 25 березня 1992 року № 2229-XII.
3. Закон України "Про національну безпеку України" від 21.06.2018р. № 2469 – VIII.
4. Закон України "Про інформацію" від 02.10.1992 р. № 2457 – XII.
5. Закон України «Про доступ до публічної інформації» від 13 січня 2011 року № 2939-VI.
6. Закон України "Про державну таємницю" від 21.01.1994р. № 3855- XII.
7. Закон України «Про Національну програму інформатизації» від 1 грудня 2022 року № 2807-IX.
8. Закон України «Про медіа» від 13 грудня 2022 року № 2849-IX.
9. Закон України Про основні засади забезпечення кібербезпеки України від 5 жовтня 2017 року № 2163-VIII.
10. Закон України «Про Раду національної безпеки і оборони України» від 5 березня 1998 року № 183/98-ВР.
11. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23 лютого 2006 року № 3475-IV.
12. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III.
13. Указ Президента України №392/2020 Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України».
14. Указ Президента України №685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки".
15. Указ Президента України №56/2022 Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки».
16. Указ Президента України №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України".
17. Указ Президента України 242/2016 «Про Національний координаційний центр кібербезпеки».
18. Постанова Кабінету Міністрів України від 12 березня 2022 р. № 263

«Деякі питання забезпечення функціонування інформаційно- комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану».

**Інформаційні ресурси:**

1. Президент України – www.president.gov.ua
2. Кабінет Міністрів України – www.kmu.gov.ua
3. Верховна Рада України – www.rada.gov.ua

Адреса розміщення робочої програми навчальної дисципліни
платформа дистанційного навчання НА СБ України, moodle.nasbu.edu.ua

*(офіційний вебсайт НА СБУ / платформа дистанційного навчання / електронний ресурс навчально-наукового інституту, кафедри, бібліотеки тощо)*

## 7. Дані про перегляд робочої програми навчальної дисципліни[1]

| № п/п | Дата, номер протоколу засідання кафедри (спільного засідання кафедр) | Рішення за результатами перегляду | Підпис керівника кафедри |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

[1] Перегляд робочої програми навчальної дисципліни відбувається щорічно, з урахуванням результатів моніторингу та періодичного перегляду освітньої програми і, зокрема, отриманих від здобувачів вищої освіти та інших стейкхолдерів побажань та зауважень.