МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЮРИДИЧНИЙ ФАКУЛЬТЕТ

ЗАТВЕРДЖУЮ
Т.в.о. декана юридичного факультету
Валентина СЛОМА
«29» серпня 2025 р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
Віктор ОСТРОВЕРХОВ
«29» серпня 2025 р.

ЗАТВЕРДЖУЮ
Директор Навчально-наукового
інституту новітніх освітніх технологій
Святослав ПИТЕЛЬ
«29» серпня 2025 р.

РОБОЧА ПРОГРАМА
з дисципліни
«ІНФОРМАЦІЙНА БЕЗПЕКА»

ступінь вищої освіти – бакалавр
галузь знань – 25 Воєнні науки, національна безпека, безпека державного кордону
спеціальності 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)»
освітньо-професійна програма – Національна безпека (за окремими сферами забезпечення і видами діяльності)

Кафедра безпеки та правоохоронної діяльності

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. (год.)	ІРС (год)	Тренінг (год.)	СРС (год.)	Разом (год.)	Екзамен (сем.)
Денна	2	3	32	14	3	6	65	120	3
заочна	2	3,4	8	4	-	-	108	120	4

Тернопіль – ЗУНУ
2025

Робоча програма складена на основі освітньо-професійної програми підготовки бакалавра галузі знань 25 Воєнні науки, національна безпека, безпека державного кордону спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) затвердженої Вченою радою ЗУНУ, протокол №11 від 26.06.2024 р.

Робоча програма розроблена Сергієм ГОРДІЄНКО – д.ю.н., доцент кафедри безпеки та правоохоронної діяльності, Віталієм КРАВЧУКОМ – викладач кафедри безпеки та правоохоронної діяльності

Робоча програма затверджена на засіданні кафедри безпеки та правоохоронної діяльності, протокол № 2, від 26.08.2025 р.

В.о. завідувача кафедри ___
к.е.н., доцент _____ Юлія МУРАВСЬКА

Гарант ОП
д.ю.н., професор Василь ОМЕЛЬЧУК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Інформаційна безпека»

1. ОПИС ДИСЦИПЛІНИ

Дисципліна «Інформаційна безпека ” «	Галузь знань, спеціальність, СВО	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 4	25 Воєнні науки, національна безпека, безпека державного кордону	**Статус дисципліни** Нормативна дисципліна циклу професійної підготовки **Мова навчання** українська
Кількість залікових модулів – 5	256 Національна безпека (за окремими сферами забезпечення і видами діяльності»)	Рік підготовки : *денна – 2* Семестр: *денна – 3* *заочна 3,4*
Кількість змістових модулів – 2	Ступінь вищої освіти – бакалавр	Лекції: *Денна – 32 год.* *Заочна – 8 год.* Практичні заняття: *Денна – 14 год.* Заочна – 4 год.
Загальна кількість годин – 120		Самостійна робота: *Денна – 71 год.* *(в т.ч. тренінг – 6 год.)* Індивідуальна робота : *Денна – 3 год.*
Тижневих годин: 8 год., з них аудиторних – 3 год.		Вид підсумкового контролю – екзамен

2. МЕТА Й ЗАВДАННЯ ДИСЦИПЛІНИ

«Інформаційна безпека»

2.1. Мета вивчення дисципліни

Основною метою навчальної дисципліни «Інформаційна безпека» є: ознайомлення студентів з особливостями та проблемами забезпечення інформаційної безпеки держави, у тому числі, в розрізі її складників; набуття навик щодо здійснення комплексного аналізу об'єкта безпеки з можливістю ідентифікувати чинники, індикатори, національні інтереси безпеки, загрози безпеці, а також задля здійснення оцінки рівня та визначення стану будь-якого виду безпеки; набуття знань задля систематизації необхідних заходів зміцнення будь-якого виду безпеки.

Мета проведення лекцій полягає у:

- викладенні студентам у відповідності з програмою та робочим планом основних засад інформаційної безпеки держави;
- сформувати у студентів цілісну систему теоретичних знань з дисципліни "Інформаційна безпека".

Мета проведення практичних занять:

- глибше засвоїти та закріпити теоретичні знання, одержані на лекціях;
- засвоїти методику оцінки рівня та визначення стану інформаційної безпеки.

2.2. Завдання вивчення дисципліни

Студенти повинні набути теоретичних і практичних знань щодо особливостей забезпечення інформаційної безпеки держави, у тому числі, в розрізі її складників, навчитися виявляти виклики, ризики безпеки та ідентифікувати загрози, з метою виокремлення конкретних заходів щодо їх мінімізації, локалізації чи ліквідації задля підвищення рівня безпеки.

Завдання проведення лекцій полягає у тому, щоб ознайомити студентів із концептуальними, методологічними засадами та практикою забезпечення інформаційної безпеки держави (її структурних складових).

Завдання проведення практичних занять полягає у тому, щоб виробити у студентів практичні навички аналітичного мислення в процесі оцінки рівня небезпеки, можливих загроз і шляхів їх нейтралізації.

2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни

Кожен студент повинен отримати певний набір компетентностей, формування яких здійснюється через результати навчання. Результати навчання повинні формулюватися таким чином, щоб досягати однієї чи декількох перерахованих нижче компетентностей:

ЗК2. Застосовувати знання у практичних ситуаціях.

ЗК11. Здатність виявляти, ставити та вирішувати проблеми.

СК7. Здатність використання отриманих знань із загальновійськової підготовки. Використання фізично-бойової підготовки, при необхідності, у службовій діяльності.

2.4. Результати навчання

РН6. Вміти орієнтуватися в джерелах інформації з сучасних проблем національної безпеки України та зарубіжних країн й орієнтуватися у військовій тематиці.

РН11. Демонструвати навички професійного використання інформації щодо аналізу діяльності конкретних безпекових інститутів.

Пререквізити:

Вступ до спеціальності

Національна безпека України

Постреквізити:

Інформаційно-аналітична діяльність спецслужб

Курсова робота

OSINT-технології у системі національної безпеки

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗМІСТОВИЙ МОДУЛЬ 1. ІНФОРМАЦІЙНА БЕЗПЕКА: ТЕОРЕТИЧНИЙ ЕКСКУРС

ТЕМА 1. ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Сутність інформаційної безпеки держави. Мета інформаційної безпеки. Основні поняття інформаційної безпеки України. Інформаційний вплив та його різновиди. Об’єкти інформаційного впливу. Глобальні загрози інформаційній безпеці України. Характеристика системи управління інформаційною безпекою України.

ТЕМА 2. ЗАГРОЗИ ТА ВИКЛИКИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Глобальні виклики та загрози. Національні виклики та загрози.

ТЕМА 3. ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Загальна характеристика інтересів держави у сфері інформаційної безпеки. Характеристика інформаційної політики держави. Стратегія формування та розвитку єдиного інформаційного простору України.

ЗМІСТОВИЙ МОДУЛЬ 2. ХАРАКТЕРИСТИКА ОКРЕМИХ ВИДІВ ЗАГРОЗ ТА НАПРЯМКИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

ТЕМА 4. ЗАГРОЗИ БЕЗПЕЦІ ДЕРЖАВИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Сутність і зміст загроз безпеці держави в інформаційній сфері. види загроз безпеці держави в інформаційній сфері та їх характеристика. Інформаційні війни як джерело загроз безпеці держави в інформаційній сфері. Спеціальні інформаційні операції в міжнародній політиці України. Інформаційна зброя як засіб ведення інформаційної війни.

ТЕМА 5. ЗАГРОЗИ СУСПІЛЬСТВУ ТА ЛЮДИНІ В ІНФОРМАЦІЙНІЙ СФЕРІ

Маніпулювання свідомістю людини: поняття та інструментарій дослідження. Способи та технології маніпулювання свідомістю людини. Технології масового маніпулятивного впливу. Чинники, що впливають на напрями реалізації сугестивних технологій маніпулятивного впливу. Головні принципи здійснення маніпулятивних технологій в засобах масової інформації. Інформаційно-психологічна безпека особи.

ТЕМА 6. КІБЕРБЕЗПЕКА ДЕРЖАВИ

Сутність кібербезпеки. Кібербезпека у системі інформаційної безпеки України: ознаки. Різниця між поняттями "інформаційна безпека" та "кібер безпека". Інтернет як платформа для маніпулятивного впливу. Комп'ютерна злочинність та кібертероризм як загрози інформаційній безпеці. Можливі заходи зміцнення кібербезпеки України. Кібербезпека та кіберзагрози. Кібербезпека в умовах розгортання четвертої промислової революції (industry 4.0): виклики та можливості для України.

ТЕМА 7. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Стан інформаційної безпеки держави. Виявлення та нейтралізація загроз інформаційній безпеці України. Потенційні загрози інформаційній безпеці України. Міжнародний досвід правового забезпечення інформаційної безпеки держави. Структура загальнодержавної системи забезпечення інформаційної безпеки України, завдання та функції її суб'єктів. Стратегічні цілі, напрями реалізації та очікувані результати Стратегії інформаційної безпеки України. Можливості підвищення ступеня інформаційної безпеки. Діяльність спеціальних служб України у сфері забезпечення інформаційної безпеки держави.

ТЕМА 8. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ЗАРУБІЖНИХ КРАЇНАХ

Стратегія інформаційної безпеки США. Особливості правління національною безпекою в Китаї. Політика інформаційної безпеки Німеччини. Політика інформаційної безпеки Франції. Державна стратегія інформаційної безпеки Японії. Особливості забезпечення інформаційної безпеки в країнах ЄС.

4. СТРУКТУРА ЗАЛІКОВОГО КРЕДИТУ

денна форма навчання

№	Теми	Лекції	Практичні заняття	СРС	Тренінг	Індивідуальна робота	Контрольні заходи
	ЗМІСТОВИЙ МОДУЛЬ 1. ІНФОРМАЦІЙНА БЕЗПЕКА : ТЕОРЕТИЧНИЙ ЕКСКУРС						
1	Теоретичні основи інформаційної безпеки держави	4	2	10	4	1	Питання для обговорення
2	Загрози та виклики інформаційній безпеці	4	2	10			Питання для дискусії
3	Державна політика у сфері інформаційної безпеки України.	4	2	10			Питання для обговорення
	ЗМІСТОВИЙ МОДУЛЬ 2. ХАРАКТЕРИСТИКА ОКРЕМИХ ВИДІВ ЗАГРОЗ ТА НАПРЯМКИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ						
4	Загрози безпеці держави в інформаційній сфері	4	2	10	2	2	Питання для обговорення
5	Загрози суспільству та людині в інформаційній сфері	4	2	10			Питання для дискусії
6	Кібербезпека держави	4	2	5			Питання для дискусії
7	Забезпечення інформаційної безпеки України	4	1	5			Питання для дискусії
8	Забезпечення інформаційної безпеки у зарубіжних країнах	4	1	5			Питання для обговорення
	ВСЬОГО	**32**	**14**	**65**	**6**	**3**	

заочна форма навчання

№	Теми	Лекції	Практичні заняття	СРС	
	ЗМІСТОВИЙ МОДУЛЬ 1. ІНФОРМАЦІЙНА БЕЗПЕКА : ТЕОРЕТИЧНИЙ ЕКСКУРС				
1	Теоретичні основи інформаційної безпеки держави	1	2	10	
2	Загрози та виклики інформаційній безпеці	1		10	
3	Державна політика у сфері інформаційної безпеки України.	1		10	
	ЗМІСТОВИЙ МОДУЛЬ 2. ХАРАКТЕРИСТИКА ОКРЕМИХ ВИДІВ ЗАГРОЗ ТА НАПРЯМКИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ				
4	Загрози безпеці держави в інформаційній сфері	1	1	16	
5	Загрози суспільству та людині в інформаційній сфері	1		18	
6	Кібербезпека держави	1		10	
7	Забезпечення інформаційної безпеки України	1	1	18	
8	Забезпечення інформаційної безпеки у зарубіжних країнах	1		16	
	ВСЬОГО	**8**	**4**	**108**	

5. ТЕМАТИКА ПРАКТИЧНИХ ЗАНЯТЬ

ЗМІСТОВИЙ МОДУЛЬ 1. ІНФОРМАЦІЙНА БЕЗПЕКА: ТЕОРЕТИЧНИЙ ЕКСКУРС

ТЕМА 1. ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Мета: опанувати теоретичний базис інформаційної безпеки держави, основну термінологію з безпекознавства.

Питання для обговорення:

1. Сутність інформаційної безпеки держави.
2. Мета інформаційної безпеки.
3. Основні поняття інформаційної безпеки України.
4. Інформаційний вплив та його різновиди.
5. Об’єкти інформаційного впливу.
6. Глобальні загрози інформаційній безпеці України.
7. Характеристика системи управління інформаційною безпекою України.

Питання для перевірки знань:

1. Обґрунтувати сутність поняття «Інформаційна безпека».
2. Назвати чинники, що впливають на рівень забезпечення інформаційної безпеки держави.
3. Охарактеризувати зовнішні та внутрішні загрози національній безпеці України.
4. Обґрунтувати різницю між такими поняттями: «чинник», «небезпека», «ризик», «загроза».
5. Ідентифікувати інформаційні виклики національній безпеці України.
6. Конкретизувати об’єкти та суб’єкти інформаційної безпеки України.
7. Що таке національні інтереси?
8. Конкретизувати національні інтереси України.
9. Здійснити характеристику структурних складових інформаційної безпеки держави.
10. Охарактеризувати органи, що здійснюють управління інформаційною безпекою України.

ТЕМА 2. ЗАГРОЗИ ТА ВИКЛИКИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Мета: з’ясувати загрози для системи інформаційної безпеки

Питання для обговорення:

1. Глобальні виклики та загрози.
2. Національні виклики та загрози.

ТЕМА 3. ДЕРЖАВНА ПОЛІТИКА У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Мета: з’ясувати сутність та особливості забезпечення державної політики щодо інформаційної безпеки

Питання для обговорення:

1. Загальна характеристика інтересів держави у сфері інформаційної безпеки.
2. Характеристика інформаційної політики держави.
3. Стратегія формування та розвитку єдиного інформаційного простору України.

Питання для перевірки знань:

1. Обґрунтувати сутність інтересів держави у сфері інформаційної безпеки.
2. Визначити загрози державній безпеці України в умовах війни.
3. Конкретизувати чинники та індикатори інформаційної політики держави.

ЗМІСТОВИЙ МОДУЛЬ 2. ХАРАКТЕРИСТИКА ОКРЕМИХ ВИДІВ ЗАГРОЗ ТА НАПРЯМКИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

ТЕМА 4. ЗАГРОЗИ БЕЗПЕЦІ ДЕРЖАВИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Мета: з’ясувати сутність загроз безпеці держави в інформаційній сфері.

Питання для обговорення:

1. Сутність і зміст загроз безпеці держави в інформаційній сфері.
2. Види загроз безпеці держави в інформаційній сфері та їх характеристика.
3. Інформаційні війни як джерело загроз безпеці держави в інформаційній сфері.
4. Спеціальні інформаційні операції в міжнародній політиці України.
5. Інформаційна зброя як засіб ведення інформаційної війни.

Питання для перевірки знань:

1. Обґрунтувати сутність поняття “інформаційна безпека”.
2. Систематизувати зовнішні та внутрішні загрози інформаційній безпеці України.
3. Охарактеризувати індикатори інформаційної безпеки.
4. Ідентифікувати національні економічні інтереси України в контексті використання методів інформаційної війни.
5. Обґрунтувати інституційні засади забезпечення інформаційних операцій в міжнародній політиці України.
6. Що варто розуміти під системою забезпечення інформаційної безпеки?
7. Охарактеризувати позитивні та негативні тенденції використання інформаційної зброї в Україні.
8. Які заходи необхідно реалізувати для зміцнення інформаційної безпеки України?

ТЕМА 5. ЗАГРОЗИ СУСПІЛЬСТВУ ТА ЛЮДИНІ В ІНФОРМАЦІЙНІЙ СФЕРІ

Мета: опанувати основи протидії маніпулюванню свідомістю людей, визначити загрози, основні напрями здійснення маніпулятивних технологій в засобах масової інформації.

Питання для обговорення:

1. Маніпулювання свідомістю людини: поняття та інструментарій дослідження.
2. Способи та технології маніпулювання свідомістю людини.
3. Технології масового маніпулятивного впливу.
4. Чинники, що впливають на напрями реалізації сугестивних технологій маніпулятивного впливу.
5. Головні принципи здійснення маніпулятивних технологій в засобах масової інформації.
6. Інформаційно-психологічна безпека особи.

Питання для перевірки знань:

1. Обґрунтувати сутність категоріального поняття «маніпулювання свідомістю людини «.
2. Назвати чинники, що впливають на рівень маніпулювання свідомістю людини.
3. Що Ви розумієте під поняттям «технологій маніпулятивного впливу»?
4. Що Ви розумієте під поняттям: «Інформаційно-психологічна безпека особи».
5. Конкретизувати інструментарій дослідження технології маніпулювання свідомістю людини.
6. Визначити екологічні закони та головні принципи Інформаційно-психологічної безпеки особи.
7. Конкретизувати загрози екологічній безпеці на національному та світовому

ТЕМА 6. КІБЕРБЕЗПЕКА ДЕРЖАВИ

Мета: опанувати сутність та особливості забезпечення кібербезпеки держави, з’ясувати виклики та загрози бкіберезпеці України**,** напрями її зміцнення.

Питання для обговорення:

1. Сутність кібербезпеки.
2. Кібербезпека у системі інформаційної безпеки України: ознаки.
3. Різниця між поняттями «інформаційна безпека» та «кібербезпека».
4. Інтернет як платформа для маніпулятивного впливу.
5. Комп’ютерна злочинність та кібертероризм як загрози інформаційній безпеці.
6. Можливі заходи зміцнення кібербезпеки України.
7. Кібербезпека та кіберзагрози.
8. Кібербезпека в умовах розгортання четвертої промислової революції (industry 4.0): виклики та можливості для України.

Питання для перевірки знань:

1. В чому полягає сутність кубербезпеки?

2. Чи існує різниця між поняттями «інформаційна безпека» та «кібер безпека»?

3. Охарактеризувати виклики кібер безпеці України**.**

4. Визначити гібридні загрози кібер безпеці України.

5. Охарактеризувати нормативно-правове забезпечення кібер безпеки.

6. Конкретизувати інституційно-правове забезпечення кібер безпеки.

7. Що Ви розумієте під поняттям: «кіберзагроза»?

8. Які існують стратегії кібер безпеки?

9. Охарактеризуйте проблеми досягнення миру в Україні в умовах розгортання четвертої промислової революції (industry 4.0).

10. Узагальнити можливі заходи зміцнення кібер безпеки України.

ТЕМА 7. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Мета: визначити та засвоїти особливості забезпечення інформаційної безпеки, з'ясувати загрози інформаційній безпеці України та можливі заходи щодо їх нейтралізації.

Питання для обговорення:

1. Стан інформаційної безпеки держави.
2. Виявлення та нейтралізація загроз інформаційній безпеці України.
3. Потенційні загрози інформаційній безпеці України.
4. Міжнародний досвід правового забезпечення інформаційної безпеки держави.
5. Структура загальнодержавної системи забезпечення інформаційної безпеки України, завдання та функції її суб'єктів.
6. Стратегічні цілі, напрями реалізації та очікувані результати Стратегії інформаційної безпеки України.
7. Можливості підвищення ступеня інформаційної безпеки.
8. Діяльність спеціальних служб України у сфері забезпечення інформаційної безпеки держави.

Питання для перевірки знань:

1. Інтерпретувати зміст категоріального поняття «інформаційна безпека».

2. Здійснити характеристику категорійно-понятійного апарату інформаційної безпеки**.**

3. Охарактеризувати правове забезпечення системи інформаційної безпеки держави.

4. Визначити методи забезпечення інформаційної безпеки.

5. Конкретизувати внутрішні та зовнішні загрози інформаційній безпеці України.

6. Які Ви вбачаєте потенційні загрози інформаційній безпеці України?

7. Обґрунтувати особливості **в**иявлення та нейтралізації загроз інформаційній безпеці України.

8. Визначити можливості підвищення ступеня інформаційної безпеки.

ТЕМА 8. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ЗАРУБІЖНИХ КРАЇНАХ

Мета: з’ясувати особливості забезпечення інформаційної безпеки у зарубіжних країнах та можливості застосування розглянутого іноземного досвіду у вітчизняній практиці з метою зміцнення інформаційної безпеки України.

Питання для обговорення:

1. Стратегія інформаційної безпеки США.
2. Управління національною безпекою в Китаї.
3. Політика інформаційної безпеки Німеччини.
4. Політика інформаційної безпеки Франції.
5. Державна стратегія інформаційної безпеки Японії.
6. Особливості забезпечення інформаційної безпеки в країнах ЄС.

Питання для перевірки знань:

1. Охарактеризувати стратегію інформаційної безпеки США.
2. Відобразити особливості управління національною безпекою в Китаї.
3. Конкретизувати політику інформаційної безпеки Німеччини.
4. Відобразити політику інформаційної безпеки Франції.
5. Охарактеризувати державну стратегію інформаційної безпеки Японії.
6. Перелічити основні загрози національній безпеці зарубіжних країн (тих, що Вами досліджувалися).
7. Узагальнити заходи щодо підвищення рівня національної безпеки.
8. Виходячи із зарубіжної практики забезпечення національної безпеки, конкретизувати окремі напрями зміцнення інформаційної безпеки України.
9. З’ясувати особливості забезпечення інформаційної безпеки в країнах ЄС.
10. Окреслити стратегічні дії уряду задля зміцнення інформаційної безпеки України.

6. САМОСТІЙНА РОБОТА

Для успішного вивчення і засвоєння дисципліни «Інформаційна безпека» студенти повинні володіти значним обсягом інформації, частину якої вони отримують і опрацьовують шляхом самостійної роботи. Самостійна робота полягає в опрацюванні положень чинного господарського законодавства та навчальної і наукової фахової літератури. Самостійна робота є обов'язковим модулем освітньої компоненти «Господарське право та процес» та передбачає виконання:

- блоку 1 – завдань по кожній із тем дисципліни за вибором студента;
- блоку 2 – у формі реферату, есе чи аналітичної доповіді.

Блок 1 самостійної роботи:

№ теми	Тематика
Тема 1	Розробити структурно-логічну схему контррозвідувального режиму в Україні
Тема 2	Розробити структурно-логічну схему історико-правової характеристики контррозвідувального режиму в Україні
Тема 3	Розробити структурно-логічну схему етапів, умов формування контррозвідувального режиму в Україні та його забезпечення
Тема 4	Охарактеризувати нормативно-правове регулювання формування контррозвідувального режиму
Тема 5	Розробити структурно-логічну схему функцій Служби безпеки України із забезпечення контррозвідувального режиму
Тема 6	Розробити структурно-логічну схему заходів адміністративного примусу
Тема 7	Розробити структурно-логічну схему обліку та реєстрації фізичних осіб в Україні в контексті контррозвідувальної діяльності
Тема 8	Визначити особливостей прикордонного та митного режимів в Україні
	Разом

Оцінка за блок 1 самостійної роботи визначається як середнє арифметичне оцінок, отриманих за виконання завдань по темах 1–8.

Блок 2 самостійної роботи – написання реферату, есе чи аналітичної доповіді за темами:

1. Еволюція загроз інформаційній безпеці у XXI столітті
2. Використання біометричних технологій для забезпечення інформаційної безпеки
3. Критичні вразливості національних інформаційних систем
4. Розвідка з відкритих джерел (OSINT) у забезпеченні інформаційної безпеки
5. Протидія інформаційним впливам іноземних спецслужб
6. Механізми формування позитивного іміджу держави в інформаційному просторі
7. Інформаційна безпека виборчих процесів
8. Електронні підписи та їх роль у захисті державної інформації
9. Соціальна інженерія як загроза для інформаційної безпеки
10. Використання блокчейн-технологій для захисту державних даних
11. Міжнародні стандарти у сфері інформаційної безпеки
12. Питання етичної хакерської діяльності для потреб держави
13. Захист об'єктів критичної інфраструктури від інформаційних атак
14. Державна політика щодо протидії фейковим новинам
15. Програми кібергігієни для державних службовців
16. Інформаційна безпека у сфері оборони та безпеки
17. Моніторинг та аудит інформаційної безпеки державних органів
18. Інформаційне протиборство в умовах воєнного конфлікту
19. Захист інтелектуальної власності в умовах цифровізації
20. Моделювання загроз у системах державного управління
21. Розробка національних протоколів реагування на кіберінциденти
22. Забезпечення безпеки комунікацій урядових структур
23. Штучний інтелект як інструмент кібератак проти держави
24. Роль міжнародних організацій у зміцненні інформаційної безпеки України
25. Протидія технологічному шпигунству в державному секторі
26. Створення та розвиток національних CERT/CSIRT команд
27. Тренування та навчання персоналу з питань інформаційної безпеки
28. Етичні аспекти використання інформаційних технологій органами влади
29. Перспективи розвитку законодавства України у сфері кібербезпеки
30. Культура інформаційної безпеки як фактор стійкості держави

Виконанню самостійної роботи має передувати ґрунтовне опрацювання рекомендованих джерел, періодичних видань (газет, журналів), наукових статей, законодавчих та підзаконних актів, джерел-Інтернет.

Робота повинна мати творчий, аналітичний, критичний і самостійний характер з тим, щоб забезпечити всебічно і добре обґрунтовані висновки.

Структура роботи:

Титульна сторінка, що містить назву навчального закладу, кафедри, дисципліни, тему реферату, ПІБ студента, групу, рік виконання.

Зміст, що містить перелік складових частин наскрізного проєкту із зазначенням сторінок.

Вступ – коротке введення в тему дослідження (1-2 сторінки).

Основна частина, що поділяється на розділи з теоретичним аналізом (12-15 сторінок).

Висновки – узагальнення результатів дослідження та пропозиції (1-2 сторінки).

Список літератури – перелік використаних джерел оформлюється відповідно до ДСТУ 8302:2015.

Додатки – за необхідності включаються графіки, таблиці, діаграми, які не увійшли до основного тексту.

Цитування та посилання: використання посилань на літературні джерела є обов'язковим. Посилання подаються у квадратних дужках із зазначенням номера джерела та сторінки (наприклад, [5, с. 123]).

Використання неавторських текстів без належного цитування не допускається.

Критерії оцінювання самостійної роботи:

90–100 балів – зміст виконаного здобувачем завдання для самостійної роботи повністю відповідає встановленим вимогам, містить елементи самостійного дослідження, а під час презентації результатів виконаного завдання здобувач демонструє знання і розуміння теми, викладає матеріал у логічній послідовності, показує уміння аналізувати і узагальнювати теоретичний і практичний матеріал та високий рівень підготовки презентації.

75–89 балів – зміст виконаного здобувачем завдання для самостійної роботи в основному відповідає встановленим вимогам, можуть бути несуттєві неточності, здобувач презентує матеріал у логічній послідовності, робить певні узагальнення і висновки, але на додаткові контрольні запитання відсутня повна відповідь, не наводить практичних прикладів у контексті тематичного теоретичного матеріалу або допускається незначних помилок у формулюванні понять, розрахунках при розв'язанні практичних завдань, презентація роботи при цьому має незначні недоліки як за змістом, так і за оформленням.

60–74 бали – у виконаному здобувачем завданні для самостійної роботи на недостатньому рівні висвітлено проблему, яка досліджувалася, логічного не завершені аналіз і оцінка стану об'єкту дослідження; наведені авторські пропозиції і рекомендації є загальними (без урахування особливостей об'єкту дослідження) і недостатньо обґрунтованими; здобувач припускається значних помилок у розрахунках при розв'язанні практичних завдань роботи; матеріал презентує фрагментарно, без логічної послідовності, відповіді на запитання нечіткі, презентація роботи при цьому має значні недоліки як за змістом, так і за оформленням.

1–59 балів – зміст виконаного здобувачем завдання для самостійної роботи не розкрито, оформлення і презентація роботи не відповідає встановленим вимогам, відповіді на запитання відсутні, неточні або неповні, не наведені шляхи вирішення проблеми або вони не обґрунтовані та випадкові.

7. ОРГАНІЗАЦІЯ І ПРОВЕДЕННЯ ТРЕНІНГУ

Тренінг «Методи виявлення та нейтралізації інформаційних атак»

Тренінг з дисципліни «Інформаційна безпека» проводиться у навчальному процесі підготовки бакалаврів права з метою вироблення практичних навичок роботи у команді, розвитку здатності прогнозувати поведінку інших учасників та освоєння методів групової комунікації у вирішенні завдань із захисту прав та свобод людини.

Порядок проведення тренінгу

Вступна частина проводиться з метою ознайомлення студентів з темою тренінгового заняття.

Організаційна частина полягає у створенні робочого настрою у колективі студентів, визначенні правил проведення тренінгового заняття. Можлива наявність роздаткового матеріалу у вигляді таблиць, бланків документів.

Практична частина реалізовується шляхом виконання завдань у групах студентів з певних проблемних питань теми тренінгового заняття.

Підведення підсумків. Обговорюється результати виконаних завдань у групах. Обмін думками з питань, які виносились на тренінгові заняття.

Завдання для тренінгу:

1) Розкрити значення ланцюга поширення інформації.

2) Проаналізувати методи виявлення та нейтралізації інформаційних атак.

3) Сформувати у здобувачів практичних навичок розпізнавання інформаційних атак.

Кожне завдання тренінгу оцінюється окремо за 100 бальною шкалою.

Критерії оцінювання тренінгу:

90–100 балів – здобувач у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час відповідей, ґрунтовно аналізує аналітичні матеріали, глибоко та всебічно розкриває зміст завдань тренінгу.

75–89 балів – достатньо повно володіє навчальним матеріалом, але на додаткові контрольні запитання відсутня повна відповідь, при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки, поверхнево аналізує аналітичні матеріали.

60–74 бали – в цілому володіє навчальним матеріалом та викладає його основний зміст, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності, відповіді на запитання нечіткі, допускає помилки та поверхнево аналізує аналітичні матеріали.

1–59 балів – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст завдань тренінгу, допускаючи при цьому суттєві неточності, не аналізує аналітичні матеріали.

8. ЗАСОБИ ОЦІНЮВАННЯ ТА МЕТОДИ ДЕМОНСТРУВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

У процесі вивчення дисципліни «Інформаційна безпека» використовуються такі засоби оцінювання та методи демонстрування результатів навчання:

– поточне опитування, тестування;
– презентації результатів виконаних завдань;
– оцінювання результатів модульного контролю;
– оцінювання результатів самостійної роботи студентів;
– наукова дискусія;
– інші види індивідуальних і групових завдань;
– екзамен.

9. ПОЛІТИКА ОЦІНЮВАННЯ

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань студентами і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу студент може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими студентами, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. Відвідування занять є обов'язковим, пропуски практичних занять відпрацьовуються. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

10. КРИТЕРІЇ, ФОРМИ ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ

Підсумковий бал (за 100-бальною шкалою) з дисципліни «Інформаційна безпека» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Модуль 1		**Модуль 2**		**Модуль 3**	**Модуль 4**	**Модуль 5**
10%	10%	10%	10%	5%	15%	40%
Поточне оцінювання	*Модульний контроль №1*	*Поточне оцінювання*	*Модульний контроль №2*	*Тренінг*	*Самостійна робота*	*Екзамен*

Оцінка за поточне опитування визначається як середнє арифметичне з оцінок, отриманих під час практичних занять	Підсумкова письмова робота	Оцінка за поточне опитування визначається як середнє арифметичне з оцінок, отриманих під час практичних занять	Підсумкова письмова робота	Оцінка за тренінг визначається як середнє арифметичне з оцінок, отриманих під час виконання завдань тренінгу	Оцінка за самостійну роботу визначається як середнє арифметичне оцінок, отриманих за виконання завдань самостійної роботи блоку 1 і 2	Тестові завдання Задачі Теоретичне питання

Шкала оцінювання:

За шкалою університету	За національною шкалою	За шкалою ECTS
90-100	відмінно	A (відмінно)
85-89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)

11. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Вид методичного забезпечення	Номер теми
Мультимедійний проектор EpsonEB-S05	1-8
Прикладне програмне забезпечення загального призначення (засоби Microsoft Office)	1-8

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Гордієнко С. Г., Доронін І. М. Правові проблеми використання технологій штучного інтелекту у контексті забезпечення національної безпеки України. *Інформація і право*. 2024. № 2(49). С. 128-137.
2. Гордієнко С. Г. Основи агентурно-оперативної діяльності спецслужб України: навч. посіб. Київ: Юрінком Інтер, 2025. 776 с.
3. Гордієнко С. Г., Доронін І. М. Інформаційно-правові аспекти захисту критичної інфраструктури України. *Інформація і право*. 2024. № 3(50). С. 115-123.
4. Гордієнко С. Інформаційна війна, інформаційно-психологічні операції, пропаганда, чи дезінформування на війні?. Юридичний вісник України / Національна безпека № 16-17 (1500-1501) 16-30 квітня 2024 року. С. 30-32. URL: https://lexinform.com.ua/dumka-eksperta/informatsijna-vijna-informatsijno-psyhologichni-operatsiyi-propaganda-chy-dezinformuvannya-na-vijni/.
5. Гордієнко С. Г. Трансформація поняття «державна безпека». *Юридична Україна*. 2020, № 8.-78. С. 12-23.
6. Стратегія інформаційної безпеки: Указ Президента України від 28.12.21 р. № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069.
7. Довгань О. Д., Ткачук Т. Ю. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право*. 2018. № 1(24). С. 89-103.
8. Ткачук Т. Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: монографія. Київ: ТОВ «Видавничий дім «АртЕк»», 2018. 411 с.
9. Золотар О. О. Правові основи інформаційної безпеки людини: автореф. дис. …д-ра юрид. наук: спеціальність 12.00.07. Харків. 2018. 37 с.
10. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: автореф. дис. …канд. юрид. наук: спеціальність 12.00.07. Львів. 2019. 23 с.
11. Солодка О. М. Пріоритети удосконалення інформаційної безпеки України. *Інформація і право*. 2015. № 3(15). С. 36-42.
12. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів. Резонанс. 2017. № 18. С. 3-14. URL: http://nbuviap.gov.ua/images/ rezonans/ 2017/rez18.pdf.
13. Гордієнко С. Доктринальні положення інформаційної безпеки України в умовах сучасності. Юридичний вісник. 2019. № 3. URL: https://lexinform.com.ua/dumka-eksperta/doktryn alni-polozhennya-informatsijnoyi-bezpeky-ukrayiny-v-umovah-suchasnosti.
14. Самохвалов Ю. Я., Браіловський М. М. Оцінка інформаційної безпеки організації за критерієм впевненості. *Захист інформації.* 2019. Т. 21. № 1. С. 13-24.
15. Турчак А. В. Основні засади державної політики забезпечення інформаційної безпеки в Україні. Інвестиції: практика та досвід. 2019. № 11. С. 123-127.
16. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий журнал*. 2020. № 2. С. 200-203.
17. Колесніков А. Особливості захисту інформації в діяльності органів здійснення правосуддя. *Економіка. Фінанси. Право*. 2024. № 5. С. 8-12
18. Kolesnikov A. Artificial intelligence in crime prevention and investigation. *Наукові записки. Серія: право*. 2023. Випуск 15. С. 292-295.

19. Колесніков А., Карапетян О. Штучний інтелект: переваги та загрози використання. *Ефективна економіка*. 2023. № 8. URL: https://www. nayka. com.ua/index.php/ee/article/view/1991/.
20. Муравська Ю., Метельський І., Романів Р. Перспективи використання технологій штучного інтелекту у юриспруденції та правоохоронній діяльності. *Актуальні проблеми правознавства*. 2024. Випуск. 2. С. 90-98.
21. Муравська Ю., Сліпченко Т. Правове регулювання штучного інтелекту в Україні та світі. *Актуальні проблеми правознавства.* 2024. Випуск 1. С.188-196.
22. Вівчар О. І., Муравська Ю. Є., Гевко В. Л. Практичні контексти національної безпеки на умовах партнерства: позитивні екстерналії та ефективість забезпечення. *Вісник Хмельницького національного університету*. Серія: економічні науки.2022. № 1 С. 7-11.

Додаткові джерела

1. Muravska Yuliia. Theoretical and conceptual approaches to defining the concept and forms of economic intelligence.in the Ukrainian scientific practice. Osteuropa-Recht. 2022. Vol. 4. P. 476-485.
https://www.nomos-elibrary.de/10.5771/0030-6444-2022-4-421/die-gewaehrleistung-der-informationssicherheit-in-der-ukraine-verwaltungs-und-strafrechtliche-massnahmen-jahrgang-68-2022-heft-4?page=1.
2. Kovalchuk O., Banakh S., Kolesnikov A., Masonkova M., Chopyk P., Basistyi P. Association Rules Mining in Crime Data Analysis. *14th International Conference on Advanced Computer Information Technologies (ACIT)*, Ceske Budejovice, Czech Republic, 2024, pp. 144-149.
3. Government Documents on National Security Policy: U.S. Policy Documents. 2021 URL:https://guides.lib.purdue.edu/c.php?g=352327&p=2375334
4. Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law. By Radim Polčák and Dan Jerker B. Svantesson. Northampton, MA: Edward Elgar, 2017. Pp. xvii, 268. ISBN: 978-1-78643-921-5.
5. Nato Strategic Communications Handbook (Draft For Use). URL: https:// www.lymec.eu/wp-content/uploads/2017/09/TT-140221-NATO-STRATEGICCOMMUNICATIONS-HANDBOOK-DRAFT-FOR-USE-2015-BI.pdf.