МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЮРИДИЧНИЙ ФАКУЛЬТЕТ

ЗАТВЕРДЖУЮ
Декан юридичного факультету

Сергій БАНАХ _____
“30” 08 2024 р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи

Віктор ОСТРОВЕРХОВ _____
“30” 08 2024 р.

ЗАТВЕРДЖУЮ
Директор ННІНОТ
Святослав ПИТЕЛЬ _____
“30” 08 2024 р.

РОБОЧА ПРОГРАМА

з дисципліни

“СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ”

Ступінь вищої освіти – бакалавр
Галузь знань – 25 Воєнні науки, національна безпека, безпека державного кордону
Спеціальність — 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/ факультет	Курс	Семестр	Лекції	Практ.	ІРС	Тренінг	СРС	Разом	Екзамен
Денна	1	1	32	14	3	6	35	90	2
Заочна	1	1	8	4	-	-	78	90	2

30.08.2024 р.

Тернопіль: ЗУНУ, 2024

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.

Робочу програму склав доцент кафедри безпеки та правоохоронної діяльності, к.е.н. Андрій КОЛЕСНІКОВ

Робоча програма затверджена на засіданні кафедри безпеки та правоохоронної діяльності, протокол № 1 від 28.08.2024 р.

В.о. завідувача кафедри к.е.н. Юлія МУРАВСЬКА

Розглянуто та схвалено групою забезпечення спеціальності Національна безпека (за окремими сферами забезпечення і видами діяльності), протокол № 1 від 30.08.2024 р.

Керівник групи забезпечення спеціальності

д.ю.н., професор Василь ОМЕЛЬЧУК

Гарант ОП Василь ОМЕЛЬЧУК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
“Сучасні інформаційні технології”

1. Опис дисципліни
“ *Сучасні інформаційні технології* ”

Дисципліна “ Сучасні інформаційні технології ”	Галузь знань, спеціальність, ступінь вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 3	Галузь знань: 25 Воєнні науки, національна безпека, безпека державного кордону	Нормативна дисципліна циклу загальної підготовки, мова навчання українська
Кількість залікових модулів – 4	Спеціальність 256 Національна безпека (за окремими сферами забезпечення і видами діяльності)	Рік підготовки: *денна – 1* *заочна – 1* Семестр: *денна – 2* *заочна – 2*
Кількість змістовних модулів – 3	Ступінь вищої освіти – бакалавр	Лекції: *Денна – 32 год.* *Заочна – 8 год.* Практичні заняття: *Денна – 14 год.* *Заочна – 4 год.*
Загальна кількість годин – 90		Самостійна робота *Денна – 35 год.* *Заочна – 78 год.* Тренінг *Денна – 6 год.* ІРС – 3 год.
Тижневих годин: 6 год. з них аудиторних – 3 год.		Вид підсумкового контролю *– екзамен*

2. Мета й завдання дисципліни

“ Сучасні інформаційні технології ”

2.1. Мета вивчення дисципліни

Метою викладання навчальної дисципліни "Сучасні інформаційні технології" є формування у студентів спеціальності Національна безпека теоретичних знань і практичних навичок щодо сучасних інформаційних технологій та їх застосування у сфері національної безпеки, розуміння принципів роботи інформаційних систем, методів захисту інформації, а також розвиток здатності ефективно використовувати інформаційні ресурси та технології для забезпечення національної безпеки держави.

2.2. Завдання вивчення дисципліни

Основними завданнями вивчення дисципліни "Сучасні інформаційні технології" є формування у студентів спеціальності Національна безпека компетентностей щодо використання сучасних інформаційних технологій у сфері забезпечення національної безпеки.

Теоретична та практична підготовка фахівців з питань національної безпеки здійснюється згідно наступних питань:

- поняття про інформацію та інформаційні системи в контексті національної безпеки;
- зміст та стадії інформаційних процесів при аналізі загроз національній безпеці;
- основні засади формування інформаційних систем як джерел стратегічно важливої інформації;
- особливості застосування інформаційних систем в органах національної безпеки;
- інформаційні системи міжнародних організацій з питань безпеки;
- OSINT технології в системі національної безпеки;
- сучасні інтегровані інформаційні системи для моніторингу та аналізу загроз;
- технології інформаційних воєн та їх вплив на національну безпеку;
- роль аналізу соціальних інформаційних каналів в умовах військового конфлікту та гібридних загроз;
- штучний інтелект в системі превентивних заходів забезпечення національної безпеки;
- забезпечення конфіденційності та безпеки інформації в контексті державної таємниці;
- захист критичної інформаційної інфраструктури;
- розробка інформаційно-аналітичних матеріалів для прийняття рішень у сфері національної безпеки.

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

ЗК6. Здатність використовувати інформаційні та комунікаційні технології.

ЗК8. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

2.4. Передумови для вивчення дисципліни

Успішне засвоєння студентами матеріалу навчального курсу передбачає наявності базових знань з правознавства та інформатики.

2.5. 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.

3. Програма навчальної дисципліни
“ Сучасні інформаційні технології”

Змістовний модуль 1. Основи інформаційних технологій в системі національної безпеки

ТЕМА 1. ПОНЯТТЯ ПРО ІНФОРМАЦІЮ ТА ІНФОРМАЦІЙНІ СИСТЕМИ

Поняття інформації. Кількісні міри оцінки інформації. Види інформації та її властивості. Інформація та знання. Поняття про дані. Основні структури даних. Поняття інформаційної системи в контексті національної безпеки.

ТЕМА 2. ЗМІСТ ТА СТАДІЇ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ ПРИ РОЗСЛІДУВАННІ ЗЛОЧИНІВ

Суть і специфіка інформаційних процесів. Пошук і виявлення криміналістично значимої інформації. Сприйняття й фіксація криміналістично релевантної інформації. Обробка інформації. Використання інформації в системі національної безпеки.

ТЕМА 3. ОСНОВНІ ЗАСАДИ ФОРМУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ЯК ДЖЕРЕЛ КРИМІНАЛІСТИЧНО ЗНАЧУЩОЇ ІНФОРМАЦІЇ

Поняття та форми реєстрації облікової одиниці. Ідентифікація при побудові інформаційних систем. Геоінформаційні системи в забезпеченні національної безпеки.

ТЕМА 4. ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ В ОРГАНАХ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Характеристики основних інформаційно-аналітичних систем в діяльності органів національної безпеки. Особливості використання інформаційно-аналітичних систем окремими підрозділами. Єдина інформаційна система органів національної безпеки України.

Змістовний модуль 2. Спеціалізовані інформаційні технології в забезпеченні національної безпеки

ТЕМА 5. ІНФОРМАЦІЙНІ СИСТЕМИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ З ПИТАНЬ БЕЗПЕКИ

Сучасні інформаційні системи міжнародних організацій безпеки. Інформаційні системи Європолу та Інтерполу. Місія та завдання національних підрозділів взаємодії з міжнародними організаціями.

ТЕМА 6. OSINT ТЕХНОЛОГІЇ

Історія розвитку OSINT. Типи джерел OSINT. Основні інструменти та технології OSINT. Методологія проведення OSINT-розслідувань. Правові та етичні аспекти використання OSINT. OSINT у контексті національної безпеки.

ТЕМА 7. СУЧАСНІ ІНТЕГРОВАНІ ІНФОРМАЦІЙНІ СИСТЕМИ

Лекція-тренінг щодо формування навичок роботи з ліцензованим програмним забезпеченням для аналізу даних. Навички використання систем аналітики та візуалізації даних. Ознайомлення з передовими системами аналізу та обробки інформації.

ТЕМА 8. ТЕХНОЛОГІЇ ІНФОРМАЦІЙНИХ ВОЄН

Теоретичні основи інформаційних воєн. Типи інформаційних воєн. Технології та інструменти інформаційних воєн. Стратегії та тактики ведення інформаційних воєн. Захист від інформаційних атак в контексті національної безпеки.

Змістовний модуль 3. Інноваційні технології та інформаційна безпека в системі національної безпеки

ТЕМА 9. РОЛЬ АНАЛІЗУ СОЦІАЛЬНИХ ІНФОРМАЦІЙНИХ КАНАЛІВ В УМОВАХ ВІЙСЬКОВОГО КОНФЛІКТУ

Вплив соціальних медіа на інформаційний простір під час війни. Методи поширення дезінформації та пропаганди в соціальних мережах у воєнний час. Способи виявлення та протидії фейковим новинам і маніпулятивному контенту. Ознаки діяльності чат ботів.

ТЕМА 10. ШТУЧНИЙ ІНТЕЛЕКТ В ЗАПОБІГАННІ ТА РОЗСЛІДУВАННІ ЗЛОЧИНІВ

Основні напрямки використання штучного інтелекту. Роль штучного інтелекту в підвищенні ефективності системи національної безпеки. Способи використання штучного інтелекту при аналізі загроз. Обмеження та загрози щодо використання штучного інтелекту. Особливості законодавчого регулювання штучного інтелекту в Україні.

ТЕМА 11. ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ТА БЕЗПЕКИ ІНФОРМАЦІЇ

Класифікація технічних засобів зняття інформації. Ідентифікація, встановлення справжності. Методи паролювання. Криптографічні методи захисту. Політика безпеки під час роботи в мережі. Особливості захисту державної таємниці.

ТЕМА 12. ЗАХИСТ ІНФОРМАЦІЇ У МЕРЕЖНИХ СИСТЕМАХ

Основні поняття інформаційної безпеки. Типи загроз у мережних системах. Методи захисту мережних систем. Безпека критичної інфраструктури держави.

ТЕМА 13. РОЗРОБКА ІНФОРМАЦІЙНО-ДЕМОНСТРАЦІЙНИХ МАТЕРІАЛІВ

Тренінг з розробки інформаційно-аналітичних матеріалів для прийняття рішень у сфері національної безпеки.

4. Структура залікового кредиту дисципліни
“ Сучасні інформаційні технології”

денна форма навчання

	Кількість годин					
	Лекції	Практичні заняття	Самостійна робота	Індивідуальна робота	Тренінг	Контрольні заходи
Змістовий модуль 1. Основи інформаційних технологій в системі національної безпеки						
Тема 1. Поняття про інформацію та інформаційні системи	2	2	2	1	2	Опитування
Тема 2. Зміст та стадії інформаційних процесів при розслідуванні злочинів	2		2			Тести 15 хв
Тема 3. Основні засади формування інформаційних систем як джерел криміналістично значущої інформації	2	2	2			Опитування
Тема 4. Особливості застосування інформаційних систем в правоохоронних органах	2		2			Опитування, Модуль 1
Змістовний модуль 2. Спеціалізовані інформаційні технології в забезпеченні національної безпеки						
Тема 5. Інформаційні системи міжнародних організацій з протидії злочинності	2	1	3	1	2	Тренінг, завдання в Інтернеті
Тема 6. OSINT технології	4	2	3			Тренінг, завдання в Інтернеті
Тема 7. Сучасні інтегровані інформаційні системи	4	1	3			Тренінг, завдання
Тема 8. Технології інформаційних воєн	2	1	3			Опитування
Змістовний модуль 3. Інноваційні технології та інформаційна безпека в системі національної безпеки						
Тема 9. Роль аналізу соціальних інформаційних каналів в умовах військового конфлікту	4	1	3	1	2	Опитування
Тема 10. Штучний інтелект в запобіганні та розслідуванні злочинів	2	2	3			Опитування
Тема 11. Забезпечення конфіденційності та безпеки інформації	2		3			Опитування

Тема 12. Захист інформації у мережних системах	2	2	3			Опитування
Тема 13. Розробка інформаційно-демонстраційних матеріалів	2		3			Опитування Модуль 2 2 год
Разом	32	14	35	3		

заочна форма навчання

	Кількість годин			
	Лекції	Практичні заняття	Самостійна робота	Індивідуальна робота
Змістовий модуль 1. Основи інформаційних технологій в системі національної безпеки				
Тема 1. Поняття про інформацію та інформаційні системи	-	-	6	-
Тема 2. Зміст та стадії інформаційних процесів при розслідуванні злочинів	1	1	6	-
Тема 3. Основні засади формування інформаційних систем як джерел криміналістично значущої інформації	1	-	6	-
Тема 4. Особливості застосування інформаційних систем в правоохоронних органах	-	-	6	-
Змістовний модуль 2. Окремі особливості аналітичної діяльності				
Тема 5. Інформаційні системи міжнародних організацій з протидії злочинності	-	-	6	-
Тема 6. OSINT технології	1	1	6	-
Тема 7. Сучасні інтегровані інформаційні системи	1	1	6	-
Тема 8. Технології інформаційних воєн	1	-	6	-
Змістовний модуль 3. Інноваційні технології та інформаційна безпека в системі національної безпеки				
Тема 9. Роль аналізу соціальних інформаційних каналів в умовах військового конфлікту	1	-	6	-
Тема 10. Штучний інтелект в запобіганні та розслідуванні злочинів	1	-	6	
Тема 11. Забезпечення конфіденційності та безпеки інформації	1	1	6	
Тема 12. Захист інформації у мережних системах	-	-	6	
Тема 13. Розробка інформаційно-демонстраційних матеріалів	-	-	6	
Разом	8	4	78	-

5. Тематика практичних занять
“ Сучасні інформаційні технології”

Змістовний модуль 1. Основи інформаційних технологій в системі національної безпеки

ПРАКТИЧНЕ ЗАНЯТТЯ 1. ПОНЯТТЯ ПРО ІНФОРМАЦІЮ ТА ІНФОРМАЦІЙНІ СИСТЕМИ

Мета: засвоїти основні поняття інформації та інформаційних систем в контексті національної безпеки

1. Аналіз видів інформації та їх властивостей
2. Практичне застосування кількісних мір оцінки інформації
3. Робота з основними структурами даних
4. Огляд інформаційних систем, що використовуються в сфері національної безпеки

ЗМІСТ ТА СТАДІЇ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ ПРИ РОЗСЛІДУВАННІ ЗЛОЧИНІВ

Мета: вивчити особливості інформаційних процесів в контексті національної безпеки

1. Моделювання процесу пошуку і виявлення значимої інформації
2. Практика сприйняття й фіксації релевантної інформації
3. Методи обробки інформації в системі національної безпеки
4. Кейс-стаді: використання інформації при розслідуванні злочинів проти національної безпеки

ПРАКТИЧНЕ ЗАНЯТТЯ 2. ОСНОВНІ ЗАСАДИ ФОРМУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ЯК ДЖЕРЕЛ КРИМІНАЛІСТИЧНО ЗНАЧУЩОЇ ІНФОРМАЦІЇ

Мета: опанувати принципи формування інформаційних систем для потреб національної безпеки

1. Практика реєстрації облікових одиниць в інформаційних системах
2. Методи ідентифікації при побудові інформаційних систем
3. Робота з геоінформаційними системами в контексті національної безпеки

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ В ОРГАНАХ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Мета: вивчити специфіку використання інформаційних систем в органах національної безпеки

1. Аналіз основних інформаційно-аналітичних систем в діяльності органів національної безпеки
2. Практичне використання інформаційно-аналітичних систем
3. Робота з Єдиною інформаційною системою органів національної безпеки України

Змістовний модуль 2. Спеціалізовані інформаційні технології в забезпеченні національної безпеки

ПРАКТИЧНЕ ЗАНЯТТЯ 3. ІНФОРМАЦІЙНІ СИСТЕМИ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ З ПИТАНЬ БЕЗПЕКИ

Мета: ознайомитися з міжнародними інформаційними системами в сфері безпеки

1. Практична робота з інформаційними системами Європолу
2. Аналіз можливостей інформаційних систем Інтерполу
3. Моделювання взаємодії національних підрозділів з міжнародними організаціями

OSINT ТЕХНОЛОГІЇ

Мета: опанувати основні інструменти та методи OSINT

1. Практика роботи з різними джерелами OSINT
2. Проведення навчального OSINT-розслідування
3. Аналіз правових та етичних аспектів використання OSINT в національній безпеці

ПРАКТИЧНЕ ЗАНЯТТЯ 4. СУЧАСНІ ІНТЕГРОВАНІ ІНФОРМАЦІЙНІ СИСТЕМИ

Мета: набути практичних навичок роботи з сучасними інформаційними системами

1. Практична робота з ліцензованим програмним забезпеченням для аналізу даних
2. Тренінг з використання систем аналітики та візуалізації даних
3. Практичне ознайомлення з передовими системами аналізу та обробки інформації

ТЕХНОЛОГІЇ ІНФОРМАЦІЙНИХ ВОЄН

Мета: вивчити практичні аспекти інформаційних воєн та захисту від них

1. Аналіз кейсів інформаційних воєн
2. Практика виявлення та протидії інформаційним атакам
3. Розробка стратегій захисту від інформаційних загроз

Змістовний модуль 3. Інноваційні технології та інформаційна безпека в системі національної безпеки

ПРАКТИЧНЕ ЗАНЯТТЯ 5. РОЛЬ АНАЛІЗУ СОЦІАЛЬНИХ ІНФОРМАЦІЙНИХ КАНАЛІВ В УМОВАХ ВІЙСЬКОВОГО КОНФЛІКТУ

Мета: опанувати методи аналізу соціальних медіа в контексті національної безпеки

1. Практика виявлення дезінформації в соціальних мережах
2. Методи протидії фейковим новинам і маніпулятивному контенту
3. Аналіз діяльності чат ботів та методи їх виявлення

ШТУЧНИЙ ІНТЕЛЕКТ В ЗАПОБІГАННІ ТА РОЗСЛІДУВАННІ ЗЛОЧИНІВ

Мета: вивчити практичні аспекти використання ШІ в системі національної безпеки

1. Аналіз кейсів використання ШІ в системі національної безпеки

2. Практика роботи з системами ШІ для аналізу загроз
3. Обговорення етичних аспектів та обмежень використання ШІ

ПРАКТИЧНЕ ЗАНЯТТЯ 6. ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ТА БЕЗПЕКИ ІНФОРМАЦІЇ

Мета: опанувати практичні методи захисту інформації

1. Практика використання методів паролювання та криптографічного захисту
2. Розробка політики безпеки для роботи в мережі
3. Тренінг з захисту державної таємниці

ПРАКТИЧНЕ ЗАНЯТТЯ 7. ЗАХИСТ ІНФОРМАЦІЇ У МЕРЕЖНИХ СИСТЕМАХ

Мета: вивчити практичні аспекти захисту мережних систем

1. Аналіз типових загроз у мережних системах
2. Практика застосування методів захисту мережних систем
3. Розробка стратегій захисту критичної інфраструктури

РОЗРОБКА ІНФОРМАЦІЙНО-ДЕМОНСТРАЦІЙНИХ МАТЕРІАЛІВ

Мета: набути практичних навичок розробки аналітичних матеріалів

1. Тренінг з розробки інформаційно-аналітичних матеріалів
2. Практика створення презентацій для прийняття рішень у сфері національної безпеки
3. Аналіз та обговорення розроблених матеріалів

6. Самостійна робота

Метою виконання самостійної роботи є поглиблене вивчення сучасних інформаційних технологій та їх застосування в системі національної безпеки України.

Виконання самостійної роботи необхідно починати з вивчення відповідних розділів підручників, навчальних посібників, наукових джерел тощо, що наведені у переліку рекомендованої літератури, а також додаткової літератури і практичних матеріалів, які студент повинен знайти і опрацювати самостійно.

Тема: Аналіз інформаційних загроз національній безпеці України (за вибором студента).

Кожен студент повинен виконати 5 завдань.

Завдання:

1. Зберіть та проаналізуйте статистичні дані про обрану інформаційну загрозу національній безпеці за останні 5 років. Визначте тенденції та можливі причини змін.
2. Проведіть OSINT-дослідження (мінімум 10 джерел) щодо обраної загрози. Зверніть увагу на методи реалізації загрози, потенційні наслідки та існуючі методи протидії.
3. Вивчіть нормативно-правову базу та стратегічні документи України щодо протидії обраній інформаційній загрозі. Визначте ключові аспекти державної політики у цій сфері.

4. Проаналізуйте роль сучасних інформаційних технологій у виявленні, попередженні та протидії обраній загрозі. Наведіть приклади використання конкретних технологій та систем.

5. Підготуйте комплексний аналітичний звіт, який має містити аналіз зібраних даних, висновки та рекомендації щодо вдосконалення системи протидії обраній інформаційній загрозі національній безпеці України.

Очікувані результати:

- Поглиблене розуміння специфіки обраної інформаційної загрози та її впливу на національну безпеку України.
- Набуття практичних навичок збору, аналізу та візуалізації даних з використанням сучасних інформаційних технологій.
- Розвиток аналітичного мислення та вміння формулювати обґрунтовані висновки і рекомендації в сфері національної безпеки.
- Вдосконалення навичок підготовки аналітичних звітів з питань національної безпеки.

Самостійна робота оцінюється відповідно до наступних критеріїв:

1. Повнота та релевантність зібраної інформації (25 балів):
   - Збір статистичних даних (0-5 балів)
   - OSINT-дослідження (0-10 балів)
   - Аналіз нормативно-правової бази (0-5 балів)
   - Аналіз ролі інформаційних технологій (0-5 балів)
2. Якість аналізу даних та обґрунтованість висновків (30 балів):
   - Глибина аналізу статистичних даних (0-7 балів)
   - Якість OSINT-дослідження (0-8 балів)
   - Аналіз нормативно-правової бази та державної політики (0-7 балів)
   - Аналіз ролі інформаційних технологій у протидії загрозі (0-8 балів)
3. Структурованість та логічність викладу матеріалу в аналітичному звіті (20 балів):
   - Чіткість структури звіту (0-5 балів)
   - Логічність викладу (0-5 балів)
   - Послідовність аргументації (0-5 балів)
   - Якість висновків та рекомендацій (0-5 балів)
4. Дотримання вимог до оформлення роботи (15 балів):
   - Правильність оформлення посилань (0-5 балів)
   - Грамотність та стиль викладу (0-5 балів)
   - Відповідність форматуванню (0-5 балів)
5. Своєчасність виконання завдання (10 балів):
   - Вчасне подання роботи (10 балів)
   - Запізнення до 1 дня (-2 бали)
   - Запізнення до 3 днів (-5 балів)
   - Запізнення більше 3 днів (-10 балів)

7. Тренінг з дисципліни

Метою проведення тренінгу є формування та розвиток практичних навичок роботи з відкритими джерелами інформації та аналітичними методами в контексті національної безпеки.

Тренінг проводиться у формі індивідуального OSINT-дослідження та аналізу потенційної загрози національній безпеці України.

Завдання тренінгу:

1. Кожен студент отримує індивідуальне завдання - дослідити конкретну потенційну загрозу національній безпеці України (наприклад, діяльність певного підозрілого об'єкта, організації чи особи).
2. Використовуючи лише відкриті джерела інформації (пошукові системи, соціальні мережі, відкриті бази даних, новинні ресурси тощо), зібрати максимальну кількість доступної інформації про об'єкт дослідження.
3. Провести аналіз зібраних даних, виявити зв'язки, закономірності та потенційні ризики для національної безпеки.
4. Створити схему зв'язків об'єкта дослідження, використовуючи будь-які доступні інструменти (наприклад, MS PowerPoint, draw.io, або навіть намалювати від руки).
5. Підготувати аналітичну записку (до 5 сторінок) з оцінкою рівня загрози та рекомендаціями щодо подальших дій.

Тривалість тренінгу: 4 академічні години.

Система оцінювання тренінгу (максимум 100 балів):

1. Якість та повнота зібраної інформації (0-30 балів):
   - Різноманітність використаних джерел (0-10 балів)
   - Релевантність зібраної інформації (0-15 балів)
   - Дотримання етичних норм при зборі інформації (0-5 балів)
2. Аналіз даних (0-25 балів):
   - Глибина аналізу (0-10 балів)
   - Виявлення неочевидних зв'язків та закономірностей (0-10 балів)
   - Оцінка достовірності інформації (0-5 балів)
3. Схема зв'язків (0-15 балів):
   - Інформативність схеми (0-5 балів)
   - Логічність та зрозумілість (0-5 балів)
   - Відповідність схеми аналітичним висновкам (0-5 балів)
4. Аналітична записка (0-30 балів):
   - Структурованість та логічність викладу (0-10 балів)
   - Обґрунтованість висновків (0-10 балів)
   - Практичність та реалістичність рекомендацій (0-10 балів)

За результатами тренінгу проводиться загальне обговорення, де кожен студент коротко представляє свої результати, а викладач надає зворотній зв'язок та рекомендації щодо вдосконалення навичок OSINT-досліджень та аналітичної роботи в контексті національної безпеки.

8. Засоби оцінювання та методи демонстрування результатів навчання

В процесі вивчення дисципліни "***Сучасні інформаційні технології***" використовуються методи оцінювання навчальної роботи студента:

– поточне тестування та опитування;

– підсумкове оцінювання по кожному змістовному модулю;
– оцінювання виконання тренінгу;
– оцінювання виконання самостійної роботи.

9. Критерії, форми поточного та підсумкового контролю

В процесі вивчення дисципліни "***Сучасні інформаційні технології***" рівень підготовки студентів оцінюється шляхом здачі іспиту. Іспит виставляється відповідно до затвердженої шкали:

Модуль 1		Модуль 2	Модуль 3	Модуль 4
20%	20%	5%	15%	40%
Поточне оцінювання (визначається як середнє арифметичне за теми 1-13)	Модульний контроль (2 теоретичні питання по 30 балів та 20 тестів по 2 бали кожен)	Тренінг (відповідно до розписаних критеріїв)	Самостійна робота (відповідно до розписаних критеріїв)	Екзамен (2 теоретичні питання по 30 балів та 20 тестів по 2 бали кожен)

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)

10. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№ п/п	Найменування	Номер теми
1	Технічне забезпечення: мультимедійний проєктор, ноутбук, проєкційний екран	1-13
2	Базове програмне забезпечення: ОС Windows. Стандартне програмне забезпечення базових інформаційних технологій: MS Office (Word, Excel, PowerPoint, Microsoft Visio). Телекомунікаційне програмне забезпечення (Internet Explorer, Google Chrome,Viber тощо).	1-13
3	Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності).	1-13
4	Комунікаційне програмне забезпечення Zoom для проведення занять в режимі on-line (за необхідності).	1-13

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Бурячок В. Л., Гулак Г. М., Толубко В. Б. Інформаційна та кібербезпека: соціотехнічний аспект. Київ : ДУТ, 2020. 288 с.
2. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. Київ : Видавнича група BHV, 2019. 608 с.

3. Гуцалюк М. В. Кібербезпека України: аналіз сучасного стану. Інформація і право. 2018. № 1. С. 54-65.
4. Дубов Д. В. Стратегічні аспекти кібербезпеки України. Стратегічні пріоритети. 2021. № 1. С. 118-126.
5. Золотар О. О. Інформаційна безпека людини: теорія і практика. Київ : АртЕк, 2018. 446 с.
6. Карпенко О. В., Кудрявцев О. Ю. Інформаційно-аналітична діяльність в публічному управлінні. Харків : ХНУ імені В. Н. Каразіна, 2020. 196 с.
7. Корж І. Ф. Державна безпека: методологічні підходи до системи складових поняття. Правова інформатика. 2019. № 4. С. 72-78.
8. Ліпкан В. А. Національна безпека України. Київ : КНТ, 2018. 576 с.
9. Марущак А. І. Інформаційне право: регулювання інформаційної діяльності. Київ : Скіф, 2020. 344 с.
10. Нізовцев Ю. Ю. Щодо окремих аспектів розвитку системи забезпечення кібербезпеки України. Інформаційна безпека людини, суспільства, держави. 2019. № 2. С. 144-153.
11. Пилипчук В. Г., Дзьобань О. П. Інформаційне суспільство: філософсько-правовий вимір. Ужгород : ІВА, 2019. 282 с.
12. Почепцов Г. Г. Сучасні інформаційні війни. Київ : Києво-Могилянська академія, 2018. 504 с.
13. Сніцаренко П. М., Саричев Ю. О. Роль і місце інформаційного забезпечення в системі державного управління. Державне управління: теорія та практика. 2019. № 1. С. 46-56.
14. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України. Київ : УБС НБУ, 2019. 440 с.
15. Шевчук О. М. Національна система кібербезпеки: проблеми правового регулювання. Інформація і право. 2020. № 2. С. 86-98.
16. Arquilla J., Ronfeldt D. Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica : RAND Corporation, 2018. 380 p.
17. Choucri N. Cyberpolitics in International Relations. Cambridge : MIT Press, 2019. 312 p.
18. Deibert R. J. Black Code: Surveillance, Privacy, and the Dark Side of the Internet. Toronto : Signal, 2020. 312 p.
19. Geers K. Strategic Cyber Security. Tallinn : NATO Cooperative Cyber Defence Centre of Excellence, 2018. 169 p.
20. Klimburg A. The Darkening Web: The War for Cyberspace. New York : Penguin Press, 2019. 432 p.
21. Libicki M. C. Cyberdeterrence and Cyberwar. Santa Monica : RAND Corporation, 2018. 240 p.
22. Nye J. S. Cyber Power. Cambridge : Harvard Kennedy School, 2019. 24 p.
23. O'Neil C. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. New York : Crown, 2018. 272 p.
24. Singer P. W., Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford : Oxford University Press, 2020. 306 p.
25. Zittrain J. The Future of the Internet -- And How to Stop It. New Haven : Yale University Press, 2019. 352 p.