Силабус курсу

Сучасні інформаційні технології

Ступінь вищої освіти – бакалавр

Галузь знань К Безпека та оборона
Спеціальність К3 Національна безпека
Освітньо-професійна програма «Національна безпека (за окремими сферами забезпечення і видами діяльності)»

Рік навчання: І

Кількість кредитів: 5 Мова викладання: українська

Керівник курсу

д.ю.н., доцент **Колесніков Андрій Павлович**

Контактна інформація a.kolesnikov@wunu.edu.ua

Опис 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.

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.

Структура курсу

Години (лек. / прак.)	Тема	Результати навчання	Завдання
2/2	Тема 1. Поняття про інформацію та інформаційні системи	Розуміти сутність інформації та її роль у національній безпеці. Вміти застосовувати кількісні міри оцінки інформації. Розрізняти види інформації та їх властивості. Аналізувати структури даних в контексті інформаційних систем. Усвідомлювати значення інформаційних систем для національної безпеки.	Опитування

2/2	Тема 2. Зміст та стадії інформаційних процесів при розслідуванні злочинів	Розуміти специфіку інформаційних процесів у сфері національної безпеки. Вміти виявляти та фіксувати криміналістично значиму інформацію. Застосовувати методи обробки інформації в контексті національної безпеки. Аналізувати ефективність використання інформації в розслідуваннях.	Тести 15 хв
2/2	Тема 3. Основні засади формування інформаційних систем як джерел криміналістично значущої інформації	Розуміти принципи реєстрації та ідентифікації в інформаційних системах. Вміти працювати з геоінформаційними системами. Аналізувати структуру та функціонування інформаційних систем у сфері національної безпеки	Опитування
2/2	Тема 4. Особливості застосування інформаційних систем в правоохоронних органах	Знати основні інформаційно-аналітичні системи в правоохоронній діяльності. Вміти використовувати інформаційно-аналітичні системи для вирішення завдань національної безпеки. Розуміти принципи роботи Єдиної інформаційної системи МВС України.	Опитування, Модуль 1
2/4	Тема 5. Інформаційні системи міжнародних організацій з протидії злочинності	Знати структуру та функції інформаційних систем Європолу та Інтерполу. Вміти використовувати міжнародні інформаційні системи для вирішення завдань національної безпеки. Розуміти роль Укрполу в міжнародній співпраці з питань безпеки	Тренінг, завдання в Інтернеті
4/4	Тема 6. OSINT технології	Розуміти принципи та методологію OSINT. Вміти використовувати різні джерела OSINT. Застосовувати OSINT-інструменти для збору та аналізу інформації. Оцінювати правові та етичні аспекти використання OSINT.	Тренінг, завдання в Інтернеті
4/4	Тема 7. Сучасні інтегровані інформаційні системи	Знати принципи роботи сучасних інтегрованих інформаційних систем. Вміти використовувати аналітичні інструменти для обробки даних. Застосовувати методи візуалізації даних для представлення результатів аналізу.	Тренінг, завдання
2/4	Тема 8. Технології інформаційних воєн	Розуміти сутність та види інформаційних воєн. Вміти виявляти ознаки інформаційних атак. Застосовувати стратегії захисту від інформаційних загроз. Аналізувати вплив інформаційних воєн на національну безпеку	Опитування
4/4	Тема 9. Роль аналізу соціальних інформаційних каналів в умовах військового конфлікту	Розуміти вплив соціальних медіа на інформаційний простір під час конфлікту. Вміти виявляти дезінформацію та пропаганду в соціальних мережах. Застосовувати методи протидії маніпулятивному контенту. Аналізувати діяльність ботів у соціальних мережах.	Опитування
2/4	Тема 10. Штучний інтелект в запобіганні та	Розуміти потенціал використання ШІ в сфері національної безпеки. Знати способи застосування ШІ при розслідуванні злочинів. Аналізувати обмеження та	Опитування

	розслідуванні злочинів	ризики використання ШІ. Розуміти правові аспекти застосування ШІ в Україні.	
2/4	Тема 11. Забезпечення конфіденційності та безпеки інформації	Знати методи захисту інформації, включаючи криптографічні. Вміти застосовувати принципи безпечної роботи в мережі. Розуміти особливості захисту державної таємниці. Аналізувати ризики та вразливості інформаційних систем.	Опитування
2/4	Тема 12. Захист інформації у мережних системах	Розуміти основні поняття інформаційної безпеки мережних систем. Вміти виявляти та аналізувати загрози у мережних системах. Застосовувати методи захисту мережних систем. Оцінювати безпеку критичної інфраструктури.	Опитування
2/4	Тема 13. Розробка інформаційно-демонстраційних матеріалів	Вміти створювати ефективні презентації з питань національної безпеки. Застосовувати методи візуалізації даних для представлення аналітичної інформації. Розробляти інформаційно-аналітичні матеріали для прийняття рішень у сфері національної безпеки.	Опитування Модуль 2 2 год

Літературні джерела

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.

Політика оцінювання

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	Модуль 5
10%	10%	10%	10%	5%	15%	40%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 2	Тренінг	Самостійна робота	Екзамен
визначається як середнє арифметичне за теми 1-8	2 теоретичні питання по 30 балів та 20 тестів по 2 бали кожен	визначається як середнє арифметичне за теми 9-13	2 теоретичні питання по 30 балів та 20 тестівпо 2 бали кожен	відповідно до розписаних критеріїв	відповідно до розписаних критеріїв	2 теоретичні питанняпо 30 балів та 20 тестів по 2 бали кожен

1. ПОТОЧНЕ ОПИТУВАННЯ МОДУЛІВ 1 І 3 (по 10% кожен)

Критерії оцінювання поточного опитування:

90-100 балів – у повному обсязі володіє навчальним матеріалом з сучасних інформаційних технологій у сфері національної безпеки, вільно та аргументовано викладає особливості роботи з інформаційними системами та OSINT-технологіями, глибоко розуміє питання інформаційної безпеки та захисту критичної інфраструктури, демонструє практичні навички роботи з міжнародними інформаційними системами та аналізу інформаційних загроз.

75-89 балів – достатньо повно володіє теоретичним матеріалом з інформаційних технологій у національній безпеці, але при викладанні окремих питань щодо роботи з інтегрованими системами або технологій інформаційних воєн не вистачає достатньої глибини аргументації, допускаються несуттєві неточності в розумінні специфіки застосування ШІ в системі національної безпеки.

65-74 бали - в цілому володіє навчальним матеріалом та викладає основний зміст тем про інформаційні технології, але без глибокого аналізу практичних аспектів їх застосування в органах національної безпеки, допускаючи суттєві неточності в розумінні принципів криптографічного захисту та мережної безпеки.

60-64 бали - не в повному обсязі володіє матеріалом з основ інформаційних технологій, фрагментарно викладає особливості роботи з різними інформаційними системами, недостатньо розкриває зміст питань щодо забезпечення конфіденційності та захисту державної таємниці.

1-59 балів - не володіє навчальним матеріалом з основних концепцій сучасних інформаційних технологій у національній безпеці, не може пояснити принципи роботи з інформаційними системами безпеки, не розуміє специфіки інформаційних загроз та методів протидії їм.

2. МОДУЛЬНІ КОНТРОЛІ 1-2 (по 10% кожен)

Структура модульного контролю:

- **2 теоретичні питання** (по 30 балів кожне = 60 балів)
- **20 тестів** (по 2 бали = 40 балів)

Критерії оцінювання теоретичного питання (30 балів):

25-30 балів - демонструє комплексне розуміння сучасних інформаційних технологій у системі національної безпеки, вільно оперує знаннями про інформаційні процеси при розслідуванні злочинів, аналізує особливості роботи з міжнародними інформаційними системами, розуміє специфіку OSINT-технологій та методи протидії інформаційним загрозам, наводить конкретні приклади з практики забезпечення національної безпеки.

15-24 балів - володіє основним теоретичним матеріалом про інформаційні технології у національній безпеці, але не завжди може встановити зв'язки між різними інформаційними системами та процесами, недостатньо аналізує практичні аспекти застосування технологій в органах безпеки, може мати прогалини в знаннях щодо особливостей міжнародного співробітництва.

5-14 балів - поверхнево викладає матеріал про окремі інформаційні технології, плутає різні системи та методології, не може пояснити принципи криптографічного захисту, має слабке розуміння ролі ШІ в системі національної безпеки, не розуміє специфіки інформаційних воєн.

1-4 балів - не володіє матеріалом про інформаційні технології у національній безпеці, не може назвати основні інформаційні системи органів безпеки, не розуміє їх призначення та принципи функціонування в контексті забезпечення національної безпеки.

Критерії оцінювання тестів (40 балів):

2 бали - правильна відповідь на тест **0 балів** - неправильна відповідь

3. ТРЕНІНГ (5%)

Тренінг: OSINT-дослідження потенційної загрози національній безпеці

90-100 балів - демонструє високопрофесійні навички OSINT-дослідження, ефективно використовує різноманітні відкриті джерела інформації, проводить глибокий аналіз зібраних даних з виявленням неочевидних зв'язків, створює інформативну та логічну схему зв'язків, підготовлює структуровану аналітичну записку з обґрунтованими висновками та практичними рекомендаціями.

75-89 балів - ефективно проводить OSINT-дослідження з використанням релевантних джерел, демонструє хороші аналітичні навички, створює якісну схему зв'язків, підготовлює добру аналітичну записку з незначними недоліками в структурі або обґрунтуванні висновків.

65-74 бали - базово використовує OSINT-методології, аналіз даних поверхневий, схема зв'язків стандартна без креативних елементів, аналітична записка має прийнятну якість, але відсутні глибокі аналітичні висновки.

60-64 бали - слабко використовує можливості відкритих джерел, аналіз зібраних даних неглибокий, схема зв'язків примітивна, аналітична записка низької якості з нереалістичними рекомендаціями.

1-59 балів - не вміє ефективно працювати з відкритими джерелами інформації, не може провести аналіз зібраних даних, не здатен створити логічну схему зв'язків, не може підготувати якісну аналітичну записку.

4. САМОСТІЙНА РОБОТА (15%)

Завдання: Аналіз інформаційних загроз національній безпеці України

90-100 балів - створює високоякісне комплексне дослідження обраної інформаційної загрози, ефективно збирає та аналізує статистичні дані, проводить професійне OSINT-дослідження з використанням різноманітних джерел, всебічно аналізує нормативно-правову базу, демонструє глибоке розуміння ролі інформаційних технологій у протидії загрозам, підготовлює структурований аналітичний звіт з обґрунтованими висновками та практичними рекомендаціями.

75-89 балів - підготовлює якісне дослідження з належним рівнем аналізу, використовує релевантні джерела та методи збору інформації, демонструє хороші аналітичні навички, може мати незначні недоліки в окремих компонентах дослідження або оформленні звіту.

60-74 балів - створює базове дослідження з поверхневим аналізом, обмежено використовує статистичні дані та OSINT-методи, аналіз нормативної бази недостатній, є суттєві недоліки в структурі звіту та обґрунтуванні висновків.

1-59 балів - не може створити якісне дослідження інформаційних загроз, неефективно використовує доступні джерела та методи, слабкі аналітичні навички, звіт не відповідає академічним стандартам, відсутні обґрунтовані висновки та рекомендації.

5. ЕКЗАМЕН (40%)

Структура екзаменаційного білета:

- **2 теоретичні питання** (по 30 балів = 60 балів)
- **20 тестів** (по 2 бали = 40 балів)

Критерії оцінювання теоретичного питання (30 балів):

25-30 балів - демонструє системні знання з усіх аспектів сучасних інформаційних технологій у національній безпеці, самостійно та правильно аналізує комплексні питання інформаційної безпеки держави, розуміє принципи роботи з криміналістично значущою інформацією, аналізує сучасні тенденції розвитку кіберзагроз, пропонує обґрунтовані рішення з урахуванням міжнародного досвіду.

15-24 балів - володіє основним матеріалом, але недостатньо глибоко аналізує практичні аспекти застосування інформаційних технологій у сфері безпеки, може мати прогалини в знаннях окремих систем або принципів їх функціонування, не завжди може встановити зв'язки між різними аспектами національної безпеки.

5-14 балів - поверхнево володіє матеріалом, плутає різні інформаційні системи та технології, не може пояснити принципи забезпечення інформаційної безпеки, має слабке розуміння ролі сучасних технологій у системі національної безпеки, не розуміє специфіки міжнародного співробітництва в цій сфері.

1-4 балів - не володіє базовими знаннями з дисципліни, не може назвати основні інформаційні системи національної безпеки, не розуміє принципів роботи з інформаційними загрозами та методів захисту критичної інфраструктури.

Критерії оцінювання тестів (40 балів):

2 бали - правильна відповідь на тест **0 балів** - неправильна відповідь

Шкала оцінювання студентів:

ECTS	Бали	Зміст
A	90-100	відмінно
B	85-89	добре
C	75-84	добре
D	65-74	задовільно
E	60-64	достатньо
FX	35-59	незадовільно з можливістю повторного складання
F	1-34	незадовільно з обов’язковим повторним курсом