



Силабус курсу

Інформаційна безпека

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)

Дні занять:

Консультації:

Рік навчання: 2, Семестр: 3,4

Кількість кредитів: 5 Мова викладання: українська

Керівник курсу

Гордієнко Сергій Георгійович, д.ю.н., проф., проф. каф. безпеки та правоохоронної діяльності; Кравчук Віталій Леонтійович, викл. каф. безпеки та правоохоронної діяльності

Контактна інформація

vitaxa1981@i.ua, +380501010442

Опис 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.

Структура курсу

Години (лек. / сем.)	Тема	Результати навчання	Завдання
4/2	1. Теоретичні основи інформаційної безпеки держави	Визначення поняття контррозвідального режиму в Україні	Питання для обговорення
4/2	2. Загрози та виклики інформаційній безпеці	Засвоїти та закріпити теоретичні знання щодо питання історико-правової характеристики контррозвідального режиму в Україні	Питання для дискусії
4/2	3. Державна політика у сфері інформаційної безпеки України	Засвоїти та закріпити теоретичні знання щодо етапів, умов формування контррозвідального режиму в Україні та його забезпечення	Питання для обговорення
4/2	4. Загрози безпеці держави в інформаційній сфері	Дослідити нормативно-правове регулювання формування контррозвідального режиму	Питання для обговорення
4/2	5. Загрози суспільству та людині в інформаційній сфері	Ознайомитися з функціями Служби безпеки України із забезпечення контррозвідального режиму	Питання для дискусії
4/2	6. Кібербезпека держави	Глибше засвоїти та закріпити теоретичні знання про контррозвідальний режим та заходи адміністративного примусу	Питання для дискусії
4/1	7. Забезпечення інформаційної безпеки України	Навчитися здійснювати облік та реєстрацію фізичних осіб в Україні в контексті контррозвідальної діяльності	Питання для дискусії
4/1	8. Забезпечення інформаційної безпеки у зарубіжних країнах	Вивчення особливостей прикордонного та митного режимів в Україні	Питання для обговорення

Літературні джерела

- 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.
- Гордієнко С. Г. Основи агентурно-оперативної діяльності спецслужб України: навч. посіб. Київ: Юрінком Інтер, 2025. 776 с.
- Гордієнко С. Г., Доронін І. М. Інформаційно-правові аспекти захисту критичної інфраструктури України. *Інформація і право*. 2024. № 3(50). С. 115-123.
- 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-psychologichni-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://nbuviar.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., Браїловський 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.nauka.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 ефективність 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-gewahrleistung-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>.

Політика оцінювання

- **Політика щодо дедлайнів та перескладання:** Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-20 балів). Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).
- **Політика щодо академічної доброчесності:** Усі письмові роботи перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%. Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних пристроїв). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування (наприклад, програма Kahoot).
- **Політика щодо відвідування:** Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.

Оцінювання

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

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10%	10%	10%	10%	5%	15%	40%
<i>Поточне оцінювання</i>	<i>Модульний контроль №1</i>	<i>Поточне оцінювання</i>	<i>Модульний контроль №2</i>	<i>Тренінг</i>	<i>Самостійна робота</i>	<i>Екзамен</i>
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 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