НАЦІОНАЛЬНЕ АГЕНТСТВО ІЗ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

ВІДОМОСТІ
про самооцінювання освітньої програми

Заклад вищої освіти	**Національна академія Служби безпеки України**
Освітня програма	**64490 Кіберзахист у сфері інформаційних технологій та кіберпросторі**
Рівень вищої освіти	**Магістр**
Спеціальність	**256 Національна безпека**

Відомості про самооцінювання є частиною акредитаційної справи, поданої до Національного агентства із забезпечення якості вищої освіти для акредитації зазначеної вище освітньої програми. Відповідальність за підготовку і зміст відомостей несе заклад вищої освіти, який подає програму на акредитацію.

Детальніше про мету і порядок проведення акредитації можна дізнатися на вебсайті Національного агентства – https://naqa.gov.ua/

Використані скорочення:

ID	ідентифікатор
ВСП	відокремлений структурний підрозділ
ЄДЕБО	Єдина державна електронна база з питань освіти
ЄКТС	Європейська кредитна трансферно-накопичувальна система
ЗВО	заклад вищої освіти
ОП	освітня програма

Загальні відомості

1. Інформація про ЗВО (ВСП ЗВО)

Реєстраційний номер ЗВО у ЄДЕБО	**1339**
Повна назва ЗВО	**Національна академія Служби безпеки України**
Ідентифікаційний код ЗВО	**20001823**
ПІБ керівника ЗВО	**Черняк Андрій Миколайович**
Посилання на офіційний веб-сайт ЗВО	**https://nasbu.edu.ua**

2. Посилання на інформацію про ЗВО (ВСП ЗВО) у Реєстрі суб'єктів освітньої діяльності ЄДЕБО

https://registry.edbo.gov.ua/university/1339

☒ЗВО є вищим військовим навчальним закладом (закладом вищої освіти із специфічними умовами навчання)

3. Загальна інформація про ОП, яка подається на акредитацію

ID освітньої програми в ЄДЕБО	**64490**
Назва ОП	**Кіберзахист у сфері інформаційних технологій та кіберпросторі**
Галузь знань	**25 Воєнні науки, національна безпека, безпека державного кордону**
Спеціальність	**256 Національна безпека**
Спеціалізація (за наявності)	*відсутня*
Рівень вищої освіти	**Магістр**
Тип освітньої програми	**Освітньо-професійна**
Вступ на освітню програму здійснюється на основі ступеня (рівня)	**Бакалавр, Магістр (ОКР «спеціаліст»)**
Структурний підрозділ (кафедра або інший підрозділ), відповідальний за реалізацію ОП	**Навчально-науковий інститут інформаційної безпеки та стратегічних комунікацій (ННІ ІБ СК)**
Інші навчальні структурні підрозділи (кафедра або інші підрозділи), залучені до реалізації ОП	**Кафедри: кібербезпеки, інформаційної безпеки держави, технічного захисту кіберпростору, безпеки інформаційно-комунікаційних систем, стратегічних комунікацій та прикладної лінгвістики, управління та інформаційно-аналітичного забезпечення оперативно-службової діяльності, філософії, ділової української мови, романо-германських мов, спеціальна кафедра СК-2**
Місце (адреса) провадження освітньої діяльності за ОП	**03066, м. Київ, вул. М. Максимовича, 22, 03118, м. Київ, проспект Валерія Лобановського, 98, 03186, м. Київ, вул. Авіаконструктора Антонова, 2/32, корпус № 92**
Освітня програма передбачає присвоєння професійної кваліфікації	*передбачає*
Професійна кваліфікація, яка присвоюється за ОП (за наявності)	**-**
Мова (мови) викладання	**Українська**
ID гаранта ОП у ЄДЕБО	**420869**
ПІБ гаранта ОП	**Вавіленкова Анастасія Ігорівна**
Посада гаранта ОП	**Завідувач кафедри**
Корпоративна електронна адреса гаранта ОП	**vai_nniibsk_na@ssu.gov.ua**
Контактний телефон гаранта ОП	**+38(066)-751-65-01**
Додатковий телефон гаранта ОП	**+38(067)-841-06-65**

Форми здобуття освіти на ОП	Термін навчання
очна денна	2 р. 0 міс.
заочна	2 р. 6 міс.

4. Загальні відомості про ОП, історію її розроблення та впровадження

Постановою Кабінету Міністрів України від 01.02.2017 р. № 53 до Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого постановою Кабінету Міністрів України від 29.04.2015 р. № 266, була введена нова спеціальність 256 Національна безпека (за окремими сферами забезпечення і видами діяльності), а державним органам, які забезпечують виконання завдань у сфері національної безпеки, надано право затверджувати в рамках нової спеціальності вид діяльності за погодженням із Міністерством освіти і науки України (далі – МОН України).
СБУ, за погодженням з МОН України, у рамках спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) було визначено відповідний вид діяльності (забезпечення державної безпеки в інформаційній сфері), за якою СБУ формує і розміщує державне замовлення на підготовку фахівців, наукових, науково-педагогічних кадрів, перепідготовку та підвищення кваліфікації кадрів (наказ ЦУ СБУ від 04.07.2017 № 410 «Про затвердження виду діяльності (спеціалізації) спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності)»). Цим же наказом провадження освітньої діяльності, пов'язаної з цільовою підготовкою фахівців, наукових, науково-педагогічних кадрів, перепідготовки і підвищення кваліфікації кадрів для потреб СБУ, інших суб'єктів національної безпеки України за спеціальністю (спеціалізацією) 256.04 Національна безпека (забезпечення державної безпеки в інформаційній сфері) покладено на Національну академію Служби безпеки України (далі – НА СБУ).
Стратегія національної безпеки України, затверджена Указом Президента України від 14.09.2020 року № 392/2020, серед поточних та прогнозованих загроз національній безпеці та національним інтересам визначає, зокрема, поширення міжнародної злочинності у кіберпросторі, використання проти України інформаційно-психологічних та кіберзасобів, а посилення спроможностей національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі є одним із пріоритетних напрямків забезпечення національної безпеки. Ефективне забезпечення виконання завдань із протидії кіберзагрозам потребувало формування відповідного кадрового потенціалу. З цією метою у 2021 році в НА СБУ була розроблена та затверджена рішенням Вченої ради від 24.06.2021 року, протокол № 8, освітньо-професійна програма «Кіберзахист у сфері інформаційних технологій та кіберпросторі» зі спеціалізації 256.04 Національна безпека (кіберзахист, забезпечення державної безпеки в інформаційній сфері) для другого (магістерського) рівня вищої освіти (розпорядження НА СБУ від 12.05.2021 № 13 «Про створення проєктних груп з розробки освітньо-професійних програм першого (бакалаврського) та другого (магістерського) рівня вищої освіти у межах спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) для підготовки студентів»), (далі – ОП). Керівник проєктної групи – Юдін О.К., доктор технічних наук, професор, гарант ОП (до 27.07.2022р.). До розроблення ОП були долучені провідні науково-педагогічні співробітники (працівники) НА СБУ (далі – НПП), співробітники практичних підрозділів СБУ.
ОП отримала схвальні відгуки зовнішніх стейкхолдерів (Національний координаційних центр кібербезпеки Ради національної безпеки і оборони України; Громадська організація «ІСАКА КИЇВ»).
При створенні ОП, як методичні вказівки, використовувалися Методичні рекомендації для розроблення профілів ступеневих програм, включаючи програмні компетентності та програмні результати навчання (Рашкевич Ю.М., 2016 р.), примірний зразок освітньо-професійної програми для першого (бакалаврського) та другого (магістерського) рівнів вищої освіти (рекомендаційний лист МОН від 28.04.2017 № 1/9-239).
Інформація про ОП була внесена до Правил прийому до Національної академії Служби безпеки України у 2021 році (від 30.12.2020 № 29/13971/ві) та у 2021/2022 навчальному році здійснено перший набір на навчання (станом на 01.10.2025 року на ОП загалом навчається 117 здобувачів вищої освіти, серед яких 50 очна (денна) форма навчання та 67 здобувачів вищої освіти заочна форма навчання).
Метою розроблення ОП на той час було формування та розвиток у здобувачів вищої освіти професійних компетентностей до розв'язування задач дослідницького та інноваційного характеру у галузі національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері) та організації і забезпечення кібербезпеки у сфері інформаційних технологій та кіберпросторі для підготовки висококваліфікованих професіоналів у галузі національної безпеки, здатних розв'язувати задачі дослідницького та/або інноваційного характеру, вирішувати практичні проблеми організаційно-технічного забезпечення інформаційної безпеки та кібербезпеки, захищеності інформаційного простору і кіберпростору держави в цілому або окремих суб'єктів інфраструктури від ризику стороннього інформаційного або кібернетичного впливу на основі застосування аналітичних процесів в управлінні інформаційною безпекою та кібербезпекою.
У 2022 році, у зв'язку з рухом кадрів, гарантом ОП визначена Вавіленкова А.І., професор кафедри кібербезпеки центру кібербезпеки ННІ ІБСК, доктор технічних наук, доцент (наказ НА СБУ від 28.07.2022 року № 126 «Про внесення змін до наказу Національної академії Служби безпеки України від 28.07.2021 № 196 «Про визначення гарантів освітніх програм»).
З урахуванням пропозицій здобувачів вищої освіти та потенційних стейкхолдерів проєктною групою та гарантом ОП у взаємодії з відповідними кафедрами здійснена робота з перегляду ОП з метою приведення її у відповідність до Стандарту вищої освіти зі спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) для другого (магістерського) рівня вищої освіти, затвердженого наказом МОН України від 23.12.2021 р. № 1423, та введеного в дію з 2022/2023 навчального року, (оновлена редакція ОП затверджена рішенням Вченої ради від 29.09.2022 року, протокол № 12).
У жовтні 2022 року ОП надано умовну (відкладену) акредитацію відповідно до Постанови Кабінету Міністрів України від 16.03.2022 р. № 295 «Про особливості акредитації освітніх програм, за якими здійснюють підготовку здобувачі вищої освіти, в умовах воєнного стану» (протокол засідання Національного агентства із забезпечення якості вищої освіти №19(24) від 25.10.2023 р.).

У зв'язку з рухом кадрів у червні 2023 року було оновлено склад проєктної групи (розпорядження НА СБУ від 08.06.2023 № 20 «Про створення проєктної групи освітньо-професійної програми «Кіберзахист у сфері інформаційних технологій та кіберпросторі» для другого (магістерського) рівня вищої освіти»). Керівник проєктної групи – Вавіленкова А.І., доктор технічних наук, професор, гарант ОП.
У зв'язку із реалізацією в освітній діяльності НА СБ України Автоматизованої системи управління навчальним закладом, що потребує зміни кредитів освітніх компонент (не менше трьох кредитів ЄКТС), співвіднесення розподілу аудиторного навантаження з графіком освітнього процесу в частині, що стосується кількості тижнів теоретичного навчання, дотримання єдиних підходів до визначення обсягу самостійної роботи в межах навчального плану підготовки магістрів, необхідністю підвищення технічної складової та врахування зауважень стейкхолдерів і здобувачів вищої освіти, а також введенням заочної форми навчання, проєктною групою та гарантом ОП у взаємодії з відповідними кафедрами здійснена робота з перегляду ОП (оновлена редакція ОП затверджена рішенням Вченої ради від 29.06.2023 року, протокол № 8).
Оновлена ОП отримала схвальні відгуки від зовнішніх стейкхолдерів та була успішно акредитована (сертифікат №8258 від 16.05.2024, строк дії 01.07.2029).
У зв'язку із проведенням постакредитаційного моніторингу та планового перегляду програми з метою усунення недоліків та врахування рекомендацій членів акредитаційної комісії та членів галузевої експертної ради Національного агенства із забезпечення якості вищої освіти освітньо-професійну програму оновлено рішенням Вченої ради Національної академії СБ України від 27 червня 2024 року, протокол № 11.
У зв'язку з отриманням ліцензії на провадження освітньої діяльності за освітніми програмами зі спеціальності 256 «Національна безпека» як регульованої (наказ МОН від 27.06.2024 №449-л), відповідно до стандарту вищої освіти України зі спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності), затвердженого наказом Міністерства освіти і науки України від 23.12.2021 року № 1423 «Про затвердження стандарту вищої освіти зі спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності для другого (магістерського) рівня вищої світи» та на основі проведення постакредитаційного моніторингу освітньо-професійної програми ID 53772 було розроблено ОП «Кіберзахист у сфері інформаційних технологій та кіберпросторі» (ID 64490), яка отримала схвальні рецензії (Національний координаційних центр кібербезпеки Ради національної безпеки і оборони України та Державна служба спеціального зв'язку та захисту інформації України) та була введена у дію з 2024/2025 навчального року.

5. Інформація про контингент здобувачів вищої освіти на ОП станом на 1 жовтня поточного навчального року у розрізі форм здобуття освіти та ліцензійний обсяг за ОП

Рік навчання	Навчальний рік, у якому відбувся набір здобувачів відповідного року навчання	Обсяг набору на ОП у відповідному навчальному році	Контингент студентів на відповідному році навчання станом на 1 жовтня поточного навчального року		У тому числі іноземців	
			ОД	*З*	*ОД*	*З*
1 курс	2025 - 2026	50	28	22	0	0
2 курс	2024 - 2025	50	24	21	0	0
3 курс	2023 - 2024	245		22		0

Умовні позначення: ОД – очна денна; ОВ – очна вечірня; З – заочна; Дс – дистанційна; М – мережева; Дл – дуальна.

6. Інформація про інші ОП ЗВО за відповідною спеціальністю

Рівень вищої освіти	Інформація про освітні програми
початковий рівень (короткий цикл)	*програми відсутні*
перший (бакалаврський) рівень	**53771 Контррозвідувальний захист кібербезпеки держави та об`єктів критичної інфраструктури** **64486 Організація захисту інформації з обмеженим доступом** **64489 Контррозвідувальний захист кібербезпеки держави та об`єктів критичної інфраструктури** **34732 Організація захисту інформації з обмеженим доступом** **51970 Контррозвідувальний захист кібербезпеки держави та об`єктів критичної інфраструктури** **51577 Кіберзахист інформаційних ресурсів** **50494 Організація захисту інформації з обмеженим доступом** **64488 Кіберзахист інформаційних ресурсів** **53773 Кіберзахист інформаційних ресурсів** **53774 Організація захисту інформації з обмеженим доступом**
другий (магістерський) рівень	**64492 Забезпечення державної безпеки в інформаційній сфері** **64490 Кіберзахист у сфері інформаційних технологій та кіберпросторі** **64491 Організація захисту інформації з обмеженим доступом** **53776 Забезпечення державної безпеки в інформаційній сфері** **53775 Організація захисту інформації з обмеженим доступом** **48021 Забезпечення державної безпеки в інформаційній сфері** **50493 Організація захисту інформації з обмеженим доступом**

	34733 Організація захисту інформації з обмеженим доступом **53772 Кіберзахист у сфері інформаційних технологій та кіберпросторі** **51578 Кіберзахист у сфері інформаційних технологій та кіберпросторі**
третій (освітньо-науковий/освітньо-творчий) рівень	*програми відсутні*

7. Інформація про площі приміщень ЗВО станом на момент подання відомостей про самооцінювання, кв. м.

	Загальна площа	Навчальна площа
Усі приміщення ЗВО	33639	8822
Власні приміщення ЗВО (на праві власності, господарського відання або оперативного управління)	33639	8822
Приміщення, які використовуються на іншому праві, аніж право власності, господарського відання або оперативного управління (оренда, безоплатне користування тощо)	0	0
Приміщення, здані в оренду	0	0

Примітка. Для ЗВО із ВСП інформація зазначається:
- щодо ОП, яка реалізується у базовому ЗВО – без урахування приміщень ВСП;
- щодо ОП, яка реалізується у ВСП – лише щодо приміщень даного ВСП.

8. Документи щодо ОП

Документ	Назва файла	Хеш файла
Освітня програма	*ОПП_2024_регульована_final_64490.pdf*	Hm/RK14YxfoRvdwSjlnaIRDicG693T7B/QWw5Z3vZLo=
Навчальний план за ОП	*Навчальний план_денна форма_2024_ID64490.pdf*	JXQZAcPBoWdxUp+d4szXj5EqmOGAWhUjBdfOmCm4zvo=
Навчальний план за ОП	*Навчальний план_заочна форма_2024_ID64490.pdf*	R95fybV3Mqi2ObD1RzH69XiByKBYkWY+KoU9/UpF1Qc=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензия_1_НКЦК_РНБО_регульована.pdf*	fiwbVH9/QD4mNc8vtAtInFfYoqUyO5xk4xoIzROLpjc=
Матеріали від ЗВО: пропозиції та рекомендації від роботодавців, таблиця відповідності публікацій наукових керівників напрямам (тематикам) досліджень аспірантів (для ОП третього рівня освіти)	*Рецензия_2_Держспецзв'язку_регульована.pdf*	JodR00aEm1tP2h3X1GLWoi0nsmoSeL13DGQ14Bb+n5I=

9. Інформація про наявність в акредитаційній справі інформації з обмеженим доступом
☒ Справа містить інформацію з обмеженим доступом

Зазначте, які частини відомостей про самооцінювання містять інформацію з обмеженим доступом, до якого виду інформації з обмеженим доступом вона належить та на якій підставі (із зазначенням відповідних норм законодавства та/або реквізитів рішення про обмеження доступу до інформації)

Частина відомостей про самооцінювання, яка містить інформацію з обмеженим доступом	Вид інформації з обмеженим доступом	Опис інформації, доступ до якої обмежений	Підстава для обмеження доступу до інформації
Додатки: Таблиця 2. Зведена інформація про викладачів освітньо-професійної програми «Кіберзахист у	службова	Відомості щодо проходження співробітниками СБ України служби (роботи, навчання) в СБ України	Перелік відомостей, що становлять службову інформацію у Службі безпеки України,

сфері інформаційних технологій та кіберпросторі» другого (магістерського) рівня вищої освіти.			затверджений наказом ЦУ СБУ від 21.08.2012 № 400 (р. 5.7, 5.8, 5.23, 11.1). Перелік відомостей, що містять службову інформацію в Міністерстві освіти і науки України, затверджений наказом МОН України від 02.01.2019 № 1 (п.2.3).

1. Проєктування освітньої програми

Чи освітня програма дає можливість досягти результатів навчання, визначених стандартом вищої освіти за відповідною спеціальністю та рівнем вищої освіти? Якщо стандарт вищої освіти за відповідною спеціальністю та рівнем вищої освіти відсутній, поясніть, яким чином визначені ОП програмні результати навчання відповідають вимогам Національної рамки кваліфікацій для відповідного кваліфікаційного рівня?

Відповідно до законів України «Про освіту», «Про вищу освіту» визначені ОП результати навчання відповідають дескрипторам сьомого рівня Національної рамки кваліфікацій, затвердженої постановою КМУ від 23.11.2011 р. № 1341 (в редакції постанови КМУ від 11.06.2025 р. № 686, https://zakon.rada.gov.ua/ laws/show/1341-2011-%D0%BF/paran12#n12).
Всі результати навчання, визначені Стандартом вищої освіти зі спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) для другого (магістерського) рівня вищої освіти, затвердженого наказом МОН України від 23.12.2021р. № 1423 (https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2021/12/24/256-Nats.bezpeka-mahistr.pdf), а саме ПРН-1, ПРН-2, ПРН-3, ПРН-4, ПРН-5, ПРН-6, ПРН-7, ПРН-8, ПРН-9, ПРН-10, ПРН-11, ПРН-12, ПРН-13, ПРН-14, ПРН-15, включені до програмних результатів навчання даної ОП (профілю п.7). Зазначені результати досягаються шляхом реалізації освітніх компонент відповідно до «Матриці забезпечення програмних результатів навчання відповідними компонентами освітньо-професійної програми», зокрема, ОК-1 «Методологія наукових досліджень та академічна доброчесність», ОК-2 «Риторика та стилістика наукових праць», ОК-3 «Теорія прийняття рішень», ОК-4 «Іноземна мова професійного спрямування», ОК-5 «Гендерна політика в системі національної безпеки та оборони України», ОК-6 «Теорія кіберпростору, кібербезпеки та кіберзахисту», ОК-7 «Інформаційне протиборство», ОК-8 «Прикладні системи штучного інтелекту в кіберпросторі», ОК-9 «Організаційно-правове забезпечення кіберзахисту», ОК-10 «Актуальні проблеми інформаційної безпеки», ОК-11 «Застосування методів і засобів OSINT у Web-середовищі», ОК-12 «Методи і моделі протидії кіберзагрозам», ОК-13 «Кіберзахист об'єктів критичної інфраструктури», ОК-14 «Управління кіберінцидентами», ОК-15 «Аудит інформаційної безпеки та кібербезпеки», ОК-16 «Безпека розподілених інформаційних ресурсів та хмарні технології», ОК-17 «Територіальна оборона, мобілізаційна підготовка та мобілізація», ОК-18 «Науково-дослідна практика» та ОК-19 «Кваліфікаційна (магістерська) робота»

Чи зміст освітньої програми враховує вимоги відповідних професійних стандартів (за наявності)?

Професійний стандарт відсутній.

Чи мета освітньої програми та програмні результати навчання визначаються з урахуванням потреб заінтересованих сторін (стейкголдерів)?
- здобувачі вищої освіти та випускники програми

Інтереси здобувачів вищої освіти були враховані під час формулювання цілей та програмних результатів навчання, визначених НА СБУ (ПРН 16 – ПРН 26) на основі взаємодії з практичними підрозділами СБУ з метою підготовки професіоналів з організації інформаційної безпеки, що відображено у ОП.
До проєктної групи ОП включено представників здобувачів вищої освіти та випускників даної ОП (розпорядження НА СБУ від 21.05.2025 № 53/дск).
На базі НА СБУ щорічно проводяться зустрічі з випускниками минулих років, а також зустрічі з представниками практичних підрозділів, круглі столи та конференції, де здобувачі вищої освіти беруть участь у обговореннях.
Структура ОП передбачає можливість для формування здобувачем індивідуальної освітньої траєкторії в обсязі 30 ЄКТС (25%), передбаченому законодавством (наказ №487 від 29.12.2023 р. про затвердження Положення про порядок реалізації права здобувачів вищої освіти на вільний вибір навчальних дисциплін в НА СБУ, https://nasbu.edu.ua/uploads/p_146_20054365.pdf). Пропозиції здобувачів вищої освіти та випускників щорічно враховуються під час коригування ОП за результатами опитувань, які проводить гарант ОП (https://nasbu.edu.ua/ua/253-kiberzahist-osvitno-profesiyni-programi-drugogomagisterskogo-rivnya-vischoi-osviti), функціонує скринька довіри. Здобувачі вищої освіти даної ОП представлені у складі Студентської ради, Вченої ради ННІ ІБ СК та Вченої ради НА СБУ, де на засіданнях можуть висловлювати пропозиції та зауваження до змісту ОП, зокрема ПРН, що формуються НА СБУ.

- роботодавці

Зворотній зв'язок із роботодавцями здійснюється шляхом залучення роботодавців до проєктної групи, шляхом отримання рецензій на проєкти ОП (під час оновлення ОП було враховано рецензії від ДІАЗ СБУ, НКЦК РНБО, Держспецзв'язку), безпосередньої взаємодії щодо погодження структур освітніх компонент (за ОП погоджено РПНД семи навчальних дисциплін з Департаментом інформаційно-аналітичного забезпечення СБ України), викладацької

діяльності (два освітніх компоненти на ОП), шляхом спілкування роботодавців зі здобувачами вищої освіти на робочих зустрічах (червень 2024 року, грудень 2024 року, червень 2025 року). Також зв'язок із роботодавцями здійснюється шляхом отримання відгуків від слухачів курсів підвищення кваліфікації, керівників науково-дослідної практики, організаторів CTF-змагань у сфері кібербезпеки, під час проведення спільних заходів (щорічних круглих столів «Актуальні питання застосування прикладних систем штучного інтелекту в кібербезпеці», «Основні аспекти форензики та їх значення для формування компетентностей фахівця з кібербезпеки», «Актуальні питання забезпечення кібербезпеки об'єктів критичної інфраструктури»), спільних публікацій наукових матеріалів, науково-практичних конференцій (щорічна Всеукраїнська науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави» https://nasbu.edu.ua/ua/news-1-8-769-konferenciya-z-informaciynoi-bezpeki), національних кластерів з кібербезпеки (https://nasbu.edu.ua/ua/news-1-8-608-nacionalniy-klaster-kiberbezpeki-v-akademii-sbu).

- академічна спільнота

Інтереси академічної спільноти враховуються під час формування мети ОП та ПРН шляхом удосконалення приведення її змісту у відповідність до сучасних потреб у сфері кібербезпеки, як частини національної безпеки, використання практичних матеріалів в навчально-методичному забезпеченні, підвищенні професійного рівня науково-педагогічних працівників за профілем викладання.
У рамках двосторонніх угод та меморандумів про співпрацю НА СБУ взаємодіє з провідними закладами вищої освіти і науковими установами України (https://nasbu.edu.ua/ua/news-1-8-692-pochatok-spivpraci-mizh-nacionalnoyu-akademieyu-sbu-ta-zahidnoukrainskim-nacionalnim-universitetom, https://nasbu.edu.ua/ua/news-1-8-615-nacionalna-akademiya-sbu-ta-crdf-global-v-ukraini-stali-partnerami, https://nasbu.edu.ua/ua/news-1-8-754-spivrobitniki-ta-kursanti-akademii-sbu-rozpochali-navchannya-na-treningu-vid-arma). Також викладачі НА СБУ комунікують з представниками інших академічних спільнот у складі робочих груп СБ України, гарант ОП Вавіленкова А.І. є головою робочої групи з розробки стандарту державної мови «Термінологія у сфері кібербезпеки», входить до складу НМК 6 Інформаційні технології, підкомісія F5 Кібербезпека та захист інформації (наказ МОН України від 23.05.2025 №750), робочих груп з розроблення професійних стандартів у сфері кібербезпеки з 2023 року по теперішній час (наказ Держспецзв'язку від 28.04.2025 №272) (засідання 15.05.2025), зокрема за професіями у сфері інформаційної безпеки та кібербезпеки, участі у наукових форумах і заходах.

- інші стейкхолдери

-

Чи мета освітньої програми відповідає місії та стратегії закладу вищої освіти?

Діяльність НА СБУ, відповідно до Статуту Національної академії Служби безпеки України (у редакції наказу ЦУ СБУ від 19.08.2024 № 413, https://nasbu.edu.ua/uploads/p_60_50137472.pdf) спрямована на створення умов, необхідних для здобуття вищої і післядипломної освіти, проведення наукової діяльності в інтересах зміцнення національної безпеки України та ефективного виконання завдань забезпечення державної безпеки. Статут визначає засади та пріоритети освітньої діяльності НА СБУ, зокрема домінування цінностей, зорієнтованих на професіоналізм, відданість справі, інноваційність, творчість та відповідальність учасників освітнього процесу.
Мета ОП, що полягає у формуванні та розвитку у здобувачів вищої освіти професійних компетентностей до розв'язування задач дослідницького та інноваційного характеру у галузі національної безпеки та організації і забезпеченні кібербезпеки у сфері інформаційних технологій та кіберпросторі, відповідає місії НА СБУ на період до 2030 року (схвалена рішенням Вченої ради НА СБУ від 27.11.2025, протокол №11), що визначає Академію хабом підготовки та розвитку фахівців і лідерів для СБ України, інших суб'єктів сектору безпеки і оборони України. Через впровадження трансформаційної освіти, дослідницької діяльності, інтеграцію передових міжнародних стандартів унікального українського досвіду НА СБ України забезпечує стратегічну здатність СБ України та сектору безпеки і оборони України будувати сильну систему національної безпеки.

Чи мета освітньої програми та програмні результати навчання визначаються з урахуванням тенденцій розвитку науки і спеціальності?

НА СБУ є провідним закладом вищої освіти, який має значний досвід підготовки фахівців у сфері національної безпеки. НА СБУ сформувала комплексну концепцію та створила власну школу підготовки фахівців із забезпечення державної безпеки за напрямками захисту інформаційного простору держави, забезпечення кібернетичної безпеки держави та кіберзахисту у сфері інформаційних технологій та кіберпросторі.
Під час формулювання мети та ПРН, визначених НА СБУ, розробниками ОП враховані тенденції розвитку спеціальності 256 Національна безпека, потреби СБУ, інших суб'єктів забезпечення національної безпеки України, які здійснюють виконання завдань із протидії загрозам національним інтересам і національній безпеці України у сфері інформаційних технологій та кіберпросторі. Джерелом інформації про такі тенденції найчастіше були відгуки представників професійної спільноти, органів (підрозділів) СБУ, інших суб'єктів національної безпеки України та опрацювання наукових досліджень за спеціальністю, які проводяться в НА СБУ.
Формування мети ОП дозволяє забезпечити практично спрямований зміст ОП та підготувати професіоналів, які володіють сучасним системним мисленням, теоретичними знаннями і практичними навичками, необхідними для розв'язання задач дослідницького та/або інноваційного характеру та практичних проблем забезпечення національної безпеки в інформаційній сфері, включаючи інформаційну безпеку, кібербезпеку, безпеку інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури (ПРН-1 – ПРН-26).

Чи мета освітньої програми та програмні результати навчання визначаються з урахуванням тенденцій розвитку ринку праці, галузевого та регіонального контексту?

Під час формулювання мети та програмних результатів навчання ОП галузевий контекст враховано шляхом залучення до проєктування ОП представників суб'єктів забезпечення національної безпеки України, зокрема, органів і підрозділів СБУ (Департамент інформаційно-аналітичного забезпечення СБ України, Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБ України, Національний координаційний центр Кібербезпеки при РНБО України, Держспецзв'язку).
Мета ОП та ПРН ОП формулювалися відповідно до тенденцій ринку праці (аналізу професійних стандартів, вимог роботодавців, потреб СБУ, дослідження трансформацій професій під впливом технологій), урахування галузевого контенту (стратегії кібербезпеки України, стратегії СБУ, міжнародних стандартів та рамки кваліфікацій, думки галузевих експертів), з урахуванням регіонального контексту (наявних та перспективних роботодавців, регіональних програм розвитку, потреб регіональних органів СБУ, безпекових потреб).

Чи мета освітньої програми та програмні результати навчання визначаються з урахуванням досвіду аналогічних вітчизняних освітніх програм?

Так, під час визначення мети та програмних результатів навчання ОП проєктною групою було розглянуто аналогічні вітчизняні програми, що готують магістрів за спеціальністю 256 Національна безпека, зокрема, Національного університету оборони України («Стратегічне керівництво у секторі безпеки і оборони»), КНУ ім. Т. Шевченка («Стратегічний менеджмент у сфері національної безпеки»), НУ «Острозька академія» («Національна безпека (за окремими сферами забезпечення і видами діяльності)»), Житомирської політехніки («Національна безпека»).
Фахівців у сфері інформаційної безпеки та кібербезпеки у київському регіоні готують: НТТУ «КПІ», НАУ, ДУІКТ, інші заклади вищої освіти. Однак, їх освітні програми зорієнтовані переважно на технічний захист інформації.
НА СБУ є провідним українським ЗВО, у якому сформувалася комплексна концепція та власна школа підготовки фахівців із кіберзахисту, у цих сферах. ОП є унікальною, забезпечує інтегровану підготовку професіоналів та реалізується виключно НА СБУ, виходячи з набутого досвіду підготовки кадрів для потреб суб'єктів національної безпеки України, зокрема, в інформаційній сфері.

Чи мета освітньої програми та програмні результати навчання визначаються з урахуванням досвіду аналогічних іноземних освітніх програм?

Так, під час визначення мети та програмних результатів навчання ОП проєктною групою було розглянуто аналогічні іноземні освітні програми, зокрема, об'єднуюча програма «International Master in Security, Intelligence and Strategic Studies (IMSISS)» - це спільна магістерська програма Erasmus Mundus (EMJMD), яку реалізують консорціум університетів у Європі, програму «Master of Arts in International Security Studies (MISS)», спільну з Університетом Бундесверу в Мюнхені, орієнтовану на військових практиків та держслужбовців, де вивчає протидію тероризму та кібербезпеку.
Зарубіжний досвід вивчався із нормативних актів європейських держав, міжнародних стандартів ISO під час стажувань і конференцій, міжнародних відряджень та тренінгів на різноманітних онлайн платформах, зокрема, NATO Deep Academy, присвячених питанням кібербезпеки для сфери національної безпеки в зарубіжних країнах й був використаний при формуванні цілей та програмних результатів навчання даної ОП.
З урахуванням зарубіжного та вітчизняного досвіду підготовки подібних фахівців, ОП максимально адаптована до потреб замовника і формує у здобувача вищої освіти здатність вирішувати інноваційні завдання у сфері інформаційної безпеки та кібербезпеки. Саме це робить ОП конкурентоздатною з-поміж інших вітчизняних та зарубіжних освітніх програм, а випускники ОП матимуть переваги щодо працевлаштування та подальшого кар'єрного зростання в органах суб'єктів національної безпеки України.

2. Структура та зміст освітньої програми

Яким є обсяг ОП (у кредитах ЄКТС)?

120

Яким є обсяг освітніх компонентів (у кредитах ЄКТС), спрямованих на формування компетентностей, визначених стандартом вищої освіти за відповідною спеціальністю та рівнем вищої освіти (за наявності)?

90

Який обсяг (у кредитах ЄКТС) відводиться на дисципліни за вибором здобувачів вищої освіти?

30

Продемонструйте, що зміст ОП відповідає предметній області заявленої для неї спеціальності (спеціальностям, якщо освітня програма є міждисциплінарною)?

Зміст ОП відповідає предметній області заявленої для неї спеціальності 256 Національна безпека (за окремими

сферами забезпечення і видами діяльності). Зміст ОП має чітку структуру за семестрами та роками навчання. Освітні компоненти, включені до ОП, підпорядковані логіці викладання з тими компонентами, що є передумовами для їх вивчення, становлять логічну взаємопов'язану систему та в сукупності дають можливість досягти сформульваної мети, а також запланованих та відображених в ОП програмних результатів навчання.
Об'єктом вивчення та діяльності ОП є національна безпека України в цілому та її сфери і види діяльності, реальні та потенційні загрози національній безпеці України; керівництво сектором безпеки і оборони України та його складовими; національні інтереси України у сфері кібербезпеки, заходи і засоби своєчасного виявлення, запобігання та нейтралізації загроз державній та кібербезпеці у сфері інформаційних технологій та кіберпросторі, що передбачає вивчення процесів, явищ, проблем забезпечення національної безпеки в інформаційній сфері та кіберпросторі.
Теоретичний зміст предметної області складають поняття, категорії, концепції, принципи, методи та засоби забезпечення національної безпеки в інформаційній сфері та кіберпросторі, через забезпечення програмних результатів навчання відповідними освітніми компонентами, зокрема, «Теорія кіберпростору, кібербезпеки та кіберзахисту», «Інформаційне протиборство», «Теорія прийняття рішень», «Організаційно-правове забезпечення кіберзахисту», «Актуальні проблеми інформаційної безпеки», «Аудит інформаційної безпеки та кібербезпеки».
ОП має прикладну орієнтацію щодо організації та застосування засобів кібербезпеки, як однієї з складових для здійснення кіберзахисту у сфері інформаційних технологій та кіберпросторі, орієнтується на сучасні наукові дослідження в галузі кібербезпеки, враховує специфіку роботи підприємств різних форм власності у цьому напрямі; базується на апробованих практичних результатах із врахуванням сучасного стану та перспектив розвитку сфери кіберзахисту, зокрема, такі освітні компоненти, як «Прикладні системи штучного інтелекту в кіберпросторі», «Застосування методів і засобів OSINT у Web-середовищі», «Методи і моделі протидії кіберзагрозам», «Кіберзахист об'єктів критичної інфраструктури», «Управління кіберінцидентами».

Яким чином здобувачам вищої освіти забезпечена можливість формування індивідуальної освітньої траєкторії?

Формування індивідуальної освітньої траєкторії здобувачів вищої освіти відбувається відповідно до Положення про організацію освітнього процесу в Національній академії Служби безпеки України (наказ НА СБУ від 31.08.2015 № 234, зі змінами від 23.02.2024р., https://nasbu.edu.ua/uploads/p_146_77039577.pdf) та Положення про порядок реалізації права здобувачів вищої освіти на вільний вибір навчальних дисциплін в Національній академії Служби безпеки України (наказ НА СБУ від 29.12.2023р. №487 https://nasbu.edu.ua/uploads/p_146_20054365.pdf).
ННІ ІБСК, відповідальний за реалізацію ОП, забезпечує вибір навчальних дисциплін у обсязі, визначеному ОП відповідно до Стандарту вищої освіти зі спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) для другого (магістерського) рівня вищої освіти, затвердженого наказом МОН України від 23.12.2021р. № 1423, що складає 25% (30 ЄКТС/ 900 годин). База вибіркових навчальних дисциплін щороку оновлюється та зберігається у загальноакадемічному каталозі вибіркових дисциплін, розміщеного в АСУ та на платформі Moodle НА СБУ. Здобувачі вищої освіти мають змогу формувати індивідуальну освітню траєкторію як через вибір навчальних дисциплін, обрання теми магістерського дослідження, місця проходження практики, так і через можливості внутрішньої та зовнішньої мобільності. За допомогою куратора навчальної групи здобувач вищої освіти формує власний індивідуальний навчальний план

Яким чином здобувачі вищої освіти можуть реалізувати своє право на вибір навчальних дисциплін?

Порядок вільного вибору здобувачем вищої освіти навчальних дисциплін регламентується п. 2.10. Положення про організацію освітнього процесу в Національній академії Служби безпеки України, затвердженого наказом НА СБУ від 31.08.2015 № 234, зі змінами від 23.02.2024р., №90, https://nasbu.edu.ua/uploads/p_146_77039577.pdf) та Положенням про порядок реалізації права здобувачів вищої освіти на вільний вибір навчальних дисциплін в Національній академії Служби безпеки України (наказ №487 від 29.12.2023р., №487 https://nasbu.edu.ua/uploads/p_146_20054365.pdf) .
Безпосередня організація та інформаційне забезпечення вільного вибору навчальних дисциплін у межах даної ОП покладається на ННІ ІБСК, який провадить відповідну освітню діяльність. Створений загальноакадемічний каталог навчальних дисциплін, що пропонуються на вибір здобувача вищої освіти, який щорічно оновлюється, доступний для ознайомлення на платформі дистанційного навчання Moodle та в АСУ. Важливо, що до цього реєстру входять як дисципліни, що планувалися лише як вибіркові, так і ті нормативні дисципліни усіх інших спеціальностей та рівнів, які можуть бути кадрово та організаційно забезпечені. Вільний вибір навчальних дисциплін здійснюється шляхом персонального голосування здобувача вищої освіти в Автоматизованій системі управління навчальним закладом, впровадженій в Національній академії Служби безпеки України (https://asu.nasbu.edu.ua/). Перелік та анотації навчальних дисциплін за вільним вибором затверджується кафедрами не пізніше вересня місяця поточного навчального року.
Вивчення навчальних дисциплін вільного вибору на даній ОП планується у обсязі, встановленому для її вибіркової складової (30 ЄКТС/25% від її загального обсягу). Навчальні дисципліни вільного вибору здобувачів освітнього ступеня магістра вводяться з другого семестру першого курсу. Термін вивчення навчальної дисципліни вільного вибору становить один семестр обсягом 3 кредити ЄКТС.
Вибір навчальних дисциплін здійснюється шляхом особистого голосування студентів в АСУ НА СБУ через відповідний модуль («Особисте» - «Запис на вибіркові навчальні дисципліни»). Персональний склад відповідних навчальних груп з вивчення навчальних дисциплін за вільним вибором затверджується наказом НА СБУ не пізніше грудня місяця (накази НА СБУ від 12.11.2024 № 506-509 про формування навчальних груп з вивчення навчальних дисциплін за вільним вибором в ННІ ІБ СК).
Навчальні дисципліни, обрані здобувачем вищої освіти, включаються до індивідуального навчального плану (навчальної картки) і є обов'язковими для оцінювання.

Опишіть, яким чином ОП та навчальний план передбачають практичну підготовку здобувачів вищої освіти, яка дозволяє здобути компетентності, необхідні для подальшої професійної діяльності

ОП та навчальним планом передбачена науково-дослідна практика здобувачів вищої освіти (9 ЄКТС / 6 тижнів), яка є обов'язковим компонентом ОП і має на меті набуття професійних навичок, компетенцій для подальшої професійної та наукової діяльності та регулюється положенням про практичну підготовку здобувачів вищої освіти, які навчаються за кошти фізичних та юридичних осіб в НА СБУ, затверджене наказом НА СБУ від 04.09.2025, https://nasbu.edu.ua/uploads/p_146_64101481.pdf.
Науково-дослідна практика на даній ОП передбачає ознайомлення здобувачів вищої освіти зі структурою, проблематикою та результатами діяльності підприємств (організацій, установ) та їх провідних спеціалістів; визначення стану розробки питань кібербезпеки у вітчизняній та іноземній літературі; оволодіння методикою обробки та аналізу експериментальних даних; отримання досвіду практичної роботи, а також опанування умінь викладу отриманих результатів у вигляді звітів, публікацій, доповідей.
У процесі науково-дослідної практики налагоджуються зв'язки з органами (підрозділами) суб'єктів національної безпеки України, державним та бізнес секторами кібербезпеки, ІТ-сектором України, відповідно до методичних рекомендацій призначаються керівники від бази практики, з якими й узгоджуються цілі та завдання практики для кожного здобувача вищої освіти.
Матеріали за результатами науково-дослідної практики, відгуки керівників практики на місцях, захист звітів з практики забезпечують зворотний зв'язок з роботодавцями з метою удосконалення ОП.

Продемонструйте, що ОП дозволяє забезпечити набуття здобувачами вищої освіти соціальних навичок (soft skills) упродовж періоду навчання

З урахуванням рекомендацій МОН України (лист від 11.03.2015 № 1/9-120 «Про організацію вивчення гуманітарних дисциплін») ОП передбачено вивчення гуманітарних навчальних дисциплін циклу загальної підготовки («Методологія наукових досліджень та академічна доброчесність», «Риторика та стилістика наукових праць», «Гендерна політика в системі національної безпеки та оборони України», які забезпечують формування загальних компетентностей, світоглядних і громадянських якостей, морально-етичних цінностей, загальнокультурної підготовки здобувачів вищої освіти.
Соціальні навички формуються також освітніми компонентами професійної підготовки («Інформаційне протиборство», «Актуальні проблеми інформаційної безпеки», «територіальна оборона, мобілізаційна підготовка та мобілізація»), а опосередковано – через освітні компоненти вільного вибору здобувачів вищої освіти («Лідерство та ефективні комунікації для фахівців сектора безпеки та оборони України», «Міжнародне гуманітарне право», «Основи саморозвитку та лідерства», «Психологічна безпека та стрес-менеджмент в професійній діяльності»).
Розвитку soft skills сприяє також використання різноманітних методів навчання, а саме: робота в групах, ділові ігри, міні-дослідження, ситуативні задачі та творчі завдання, участь у CTF-змаганнях. Позитивний вплив здійснює фізичне виховання та спортивні досягнення особового складу НА СБУ, волонтерська діяльність, зустрічі з творчими колективами, покази сучасного кіно (https://nasbu.edu.ua/ua/news/1/category/8).

Продемонструйте, що зміст освітньої програми має чітку структуру; освітні компоненти, включені до освітньої програми, становлять логічну взаємопов'язану систему та в сукупності дають можливість досягти заявленої мети та програмних результатів навчання. Продемонструйте, що зміст освітньої програми забезпечує формування загальнокультурних та громадянських компетентностей, досягнення програмних результатів навчання, що передбачають готовність здобувача самостійно здійснювати аналіз та визначати закономірності суспільних процесів

Зміст ОП має чітку структуру, що будується на основі її компонентів, що включають обов'язкові освітні компоненти циклу загальної підготовки (18 ЄКТС / 540 годин) та циклу професійної підготовки (72 ЄКТС / 2160 годин). Освітні компоненти ОП становлять логічну взаємопов'язану та послідовну систему та в сукупності дають можливість досягти заявленої мети та програмних результатів навчання, що відображено у п.2.2 ОП «Структурно-логічна схема освітньо-професійної програми».
До ОП включені обов'язкові ОК, які спрямовані на здобуття знань і практичних навичок для формування загальнокультурних та громадянських компетентностей (ОК-1, ОК-2, ОК-3, ОК-4, ОК-5), поглиблене вивчення іноземної мови (ОК-3), формування загальних і фахових компетентностей у сфері формування логічного мислення та аналітичного аналізу (ОК-2, ОК-7, ОК-10, ОК-17), аналізу властивостей об'єктів безпеки, класифікації загроз, джерел та вразливостей в сфері національної безпеки (ОК-8, ОК-9, ОК-11, ОК-12, ОК-13, ОК-14, ОК-15, ОК-16), розуміння та реалізації комплексних стратегій управління інформаційною та кібербезпекою на різних рівнях (ОК-9, ОК-11, ОК-12, ОК-13, ОК-14, ОК-15), залучення здобувачів вищої освіти до науково-дослідної роботи (ОК-1, ОК-2, ОК-18), посилену практичну підготовку (ОК-18, ОК-19) тощо. Перелік компонентів ОП також містить вибіркові дисципліни для поглиблення фахової підготовки. Такий підхід та логічна послідовність компонентів ОП дає змогу досягти заявленої мети та програмних результатів навчання.
Досягнення програмних результатів навчання, що передбачають готовність здобувача самостійно здійснювати аналіз та визначати закономірності суспільних процесів також відображені у п. 4.1. ОП «Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми»

Який підхід використовує ЗВО для співвіднесення обсягу окремих освітніх компонентів ОП (у кредитах ЄКТС) із фактичним навантаженням здобувачів вищої освіти (включно із самостійною роботою)?

Навчальний час здобувача вищої освіти за ОП визначається кількістю облікових одиниць часу, відведеного на її реалізацію (120 ЄКТС). Відповідно до Положення про організацію освітнього процесу в Національній академії Служби безпеки України (зі змінами від 23.02.2024р., №90, https://nasbu.edu.ua/uploads/p_146_77039577.pdf),

Правил внутрішнього розпорядку НА СБУ, Порядку організації самостійної роботи здобувачів вищої освіти Національної академії Служби безпеки України (наказ НА СБУ від 23.08.2017 № 273, https://nasbu.edu.ua/uploads/p_146_94018257.pdf) навчальний день здобувача освітнього ступеня магістра становить не більше 9 академічних годин, навчальний тиждень – не більше 50 академічних годин, аудиторне навантаження – не більше 30 годин на тиждень. Для даної ОП максимальне тижневе навантаження становить 1 кредит / 30 годин (денна), 3,13 кредити / 94 години (заочна) форма та мінімальне тижневе навантаження 0,63 кредити / 19 годин (денна) та 2,46 кредити / 74 години (заочна).
Час, відведений для самостійної роботи здобувача вищої освіти – від 1/3 до 2/3 загального обсягу часу, відведеного для вивчення конкретної навчальної дисципліни. Показник співвідношення між навчальними заняттями і годинами самостійної роботи здобувачів вищої освіти даної ОП становить обсяг навчальних занять 39,1 кредити / 1172 годин (денна), 13,2 кредити / 396 годин (заочна), а обсяг самостійної роботи відповідно 80,9 кредити / 2428 годин для денної форми та 106,8 кредити / 3204 годин для заочної форми.

Яким чином структура освітньої програми, освітні компоненти забезпечують практикоорієнтованість освітньої програми? Якщо за ОП здійснюється підготовка здобувачів вищої освіти за дуальною формою освіти, опишіть модель та форми її реалізації

Практикоорієнтованість ОП забезпечується через структуру, що включає практичні та семінарські заняття, вибіркові дисципліни та тісну взаємодію зі стейкхолдерами, а також включає обов'язковий освітній компонент ОК-18 «Науково-дослідна практика» (9 ЄКТС / 6 тижнів), яка має на меті набуття професійних навичок, компетенцій для подальшої професійної та наукової діяльності.
На даній ОП підготовка за дуальною формою здобуття вищої освіти не здійснюється.

Яким чином ОП забезпечує набуття здобувачами навичок і компетентностей направлених на досягнення глобальних цілей сталого розвитку до 2030 року, проголошених резолюцією Генеральної Асамблеї Організації Об'єднаних Націй від 25 вересня 2015 року № 70/1, визначених Указом Президента України від 30 вересня 2019 року № 722

- ціль 4 забезпечується шляхом провадження студентсько-центрованого, проблемно-орієнтованого навчання, самонавчання, навчання через практику з використанням ситуаційних завдань та сучасних програмних засобів, дотримання академічної доброчесності (Кодекс академічної доброчесності в НА СБУ, 06.12.2019р., https://nasbu.edu.ua/uploads/p_146_17253437.pdf) та справедливої якісної освіти (https://nasbu.edu.ua/ua/146-normativne-zabezpechennya-osvitnogo-procesu-osvitnya-diyalnist).
- ціль 5 досягається тим, що для вступників на ОП не передбачено вікових, соціальних і гендерних обмежень, реалізовано принцип рівних прав та можливостей за ознакою статті при формуванні постійного складу НА СБУ (жіночої-52%, чоловічої-48%), у ОП є обов'язковий освітній компонент «Гендерна політика в системі національної безпеки та оборони України», також в НА СБУ ведеться просвітницька робота з питань гендерної рівності (лекції (https://nasbu.edu.ua/ua/49-genderna-politika-osvitnya-diyalnist), викладачі беруть участь у тематичних тренінгах та зустрічах).
- ціль 9 досягається шляхом використання у навчальному процесі на ОП сучасного технічного обладнання, інноваційних технологій та сучасних методів навчання.
- ціль 16 реалізована на ОП шляхом виховання у здобувачів вищої освіти культурних навичок, патріотизму, розвитку професійної підготовки з урахуванням специфічних особливостей забезпечення державної безпеки у сфері інформаційних технологій та кіберпросторі.

3. Доступ до освітньої програми та визнання результатів навчання

Наведіть посилання на вебсторінку, яка містить інформацію про правила прийому на навчання та вимоги до вступників ОП

https://nasbu.edu.ua/ua/219-pravila-priyomu-do-nacionalnoi-akademii-sluzhbi-bezpeki-ukraini-u-2025-roci-informaciya-dlya-abiturientiv

Поясніть, як правила прийому на навчання та вимоги до вступників ураховують особливості ОП?

НА СБУ на підставі ліцензії МОН та в межах ліцензійного обсягу оголошує конкурсні пропозиції для прийому вступників на другий (магістерський) рівень вищої освіти за спеціальністю 256 Національна безпека, за кошти фізичних та/або юридичних осіб, які подали заяви на вступ до Академії у порядку та строки, що визначені Правилами прийому до НА СБУ (https://vstup.osvita.ua/doc/files/2024/receptionRule/1339_1.pdf).
Для здобуття ступеня магістра за спеціальністю 256 Національна безпека приймаються особи, які здобули ступінь бакалавра або магістра (спеціаліста). Прийом здійснюється на конкурсній основі, загальна кількість набраних балів включає результати єдиного вступного іспиту, бали за фаховий іспит (програма якого враховує особливості даної ОП (https://nasbu.edu.ua/uploads/p_152_53345441.pdf)), а також передбачає обов'язкову наявність мотиваційних листів (https://nasbu.edu.ua/ua/168-polozhennya-pro-motivaciyniy-list-informaciya-dlya-abiturientiv).
Вимоги до компетентності вступників з управління інформаційної безпеки визначено з урахуванням положень законодавства України у сфері захисту інформації. Навчальний матеріал, що виноситься на фахове вступне випробування, структурований за такими змістовними модулями: окремі тематичні положення нормативно-правового забезпечення у сфері інформаційної безпеки та кібербезпеки, основи інформаційних технологій, мови і

технології програмування, комп'ютерні системи та мережі, кіберзахист інформаційних ресурсів.

Яким документом ЗВО регулюється питання визнання результатів навчання та кваліфікацій, отриманих на інших освітніх програмах? Яким чином забезпечується доступність цієї процедури для учасників освітнього процесу?

Порядок прийому, переведення, відрахування і поновлення здобувачів вищої освіти в НА СБУ визначається актами законодавства України, нормативно-правовими актами МОН та СБУ.
Питання визнання результатів навчання, отриманих в інших закладах вищої освіти, регулюється Положенням про організацію освітнього процесу в НА СБУ (наказ від 31.08.2015 № 234, зі змінами від 23.02.2024р., https://nasbu.edu.ua/uploads/p_146_77039577.pdf).
На підставі заяви здобувача освіти та його академічної довідки укладається перелік навчальних дисциплін для зарахування та/або складання академічної різниці, що розглядається комісією з питань поновлення, переведення осіб, які навчаються у закладах вищої освіти, на навчання за кошти фізичних (юридичних) осіб до Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій (наказ про створення комісії від 06.08.2024 № 320). За наявності розбіжностей заявникові видається відомість ліквідування академічної різниці, де встановлено терміни ліквідації та перелік навчальних дисциплін, які потрібно скласти. Після успішного складання академічної різниці у встановлений термін заявник відповідним наказом поновлюється на навчання до НА СБУ за відповідною ОП. Результати фіксуються в індивідуальному навчальному плані здобувача вищої освіти.

Наведіть конкретні приклади та прийняті рішення щодо визнання результатів навчання та кваліфікацій, отриманих на інших освітніх програмах (зокрема під час академічної мобільності)

Випадків визнання результатів навчання та кваліфікацій, отриманих на інших освітніх програмах (зокрема, під час академічної мобільності) на даній ОП не було.

Яким документом ЗВО регулюється питання визнання результатів навчання, отриманих в неформальній та/або інформальній освіті? Яким чином забезпечується доступність цієї процедури для учасників освітнього процесу?

Усі питання освітнього процесу в НА СБУ регулюються Положенням про організацію освітнього процесу в Національній академії Служби безпеки України (наказ НА СБУ від 31.08.2015 № 234, зі змінами від 23.02.2024р., №90, https://nasbu.edu.ua/uploads/p_146_77039577.pdf) та Положенням про порядок визнання результатів навчання, отриманих у неформальній та/або інформальній освіті здобувачами вищої освіти Національної академії Служби безпеки України (наказ №489 від 29.12.2023, https://nasbu.edu.ua/uploads/p_146_61814152.pdf).
Для визнання (перерахування) результатів навчання, отриманих у неформальній освіті, здобувач подає заяву та завірені у встановленому порядку копії документів, що підтверджують участь здобувача в заході неформальної освіти (свідоцтва, сертифікати, дипломи тощо, які підтверджують ті компетентності, які здобувач отримав під час навчання).

Наведіть конкретні приклади та прийняті рішення щодо визнання результатів навчання отриманих у неформальній та/або інформальній освіті

На даній ОП випадків визнання результатів навчання отриманих у неформальній та/або інформальній освіті не було.

4. Навчання і викладання за освітньою програмою

Продемонструйте, що освітній процес на освітній програмі відповідає вимогам законодавства (наведіть посилання на відповідні документи). Яким чином методи, засоби та технології навчання і викладання на ОП сприяють досягненню мети та програмних результатів навчання?

Освітній процес на ОП відповідає вимогам ЗУ «Про освіту», «Про вищу освіту», «Про наукову і науково-технічну діяльність», «Про забезпечення функціонування української мови як державної» та регламентується Положенням про організацію освітнього процесу в Національній академії Служби безпеки України (наказ НА СБУ від 31.08.2015 № 234, зі змінами від 23.02.2024р., №90, https://nasbu.edu.ua/uploads/p_146_77039577.pdff). Освітній процес сприяє досягненню заявлених в ОП цілей, програмних результатів, відповідає вимогам студентоцентрованого підходу, принципам академічної свободи, створенню психологічно безпечного освітнього середовища.
Організація освітнього процесу за даною ОП безпосередньо покладена на структурний підрозділ НА СБУ – ННІ ІБСК (наказ НА СБУ від 20.08.2025р. №71), специфіка освітніх послуг якого полягає, насамперед, у формуванні у здобувачів вищої освіти компетентностей, що дозволяють ефективно виконувати завдання із забезпечення державної безпеки відповідно до компетенції суб'єктів національної безпеки України, зокрема у сфері інформаційної безпеки та кіберпросторі.
Досягнення програмних результатів навчання забезпечується через врахування індивідуальних особливостей здобувачів вищої освіти, їх інтересів, здібностей, ціннісних орієнтацій при організації та здійсненні їх навчально-пізнавальної діяльності, формування професійної компетентності освітніх компонентів.

Продемонструйте, яким чином методи, засоби та технології навчання і викладання відповідають вимогам студентоцентрованого підходу. Яким є рівень задоволеності здобувачів вищої освіти методами навчання і викладання відповідно до результатів опитувань?

Студентоцентрований підхід досягається через право обирати теми курсових робіт (ОК-13), індивідуальні завдання, право обирати теми кваліфікаційних (магістерських) робіт (ОК-19), обрання бази практичної підготовки, обрання дисциплін вільного вибору (30 ЄКТС / 900 год.) відповідно до власних інтересів (накази НА СБУ від 12.11.2024 №№ 506-509 про формування навчальних груп К-241м, К-241м/з з вивчення навчальних дисциплін за вільним вибором у 2024/2025 та 2025/2026 навчальних роках).
Рівень задоволеності здобувачів вищої освіти процесом навчання і викладання вивчається шляхом проведення опитувань, анкетувань, соціологічних досліджень, а також під час щорічних зустрічей керівництва НА СБУ зі здобувачами вищої освіти.
Опитування здобувачів у 2024 та 2025 році (https://nasbu.edu.ua/uploads/p_253_44446245.pdf, https://nasbu.edu.ua/uploads/p_253_58652340.pdf) показало, що здобувачі вищої освіти задоволені методами навчання і викладання на ОП (100% опитаних (з них 75% задоволені на 100%, 18,8% на 80-90% та 6,3% на 50-70%)). Переважна більшість ЗВО зазначають, що викладачі ефективно підбирають методи та прийоми навчання для досягнення мети заняття. Опитування здобувачів вищої освіти даної ОП засвідчило, що рівень задоволеності методами навчання і викладання складає: задоволені 98% респондентів, не задоволені – 2 %.

Продемонструйте, яким чином забезпечується відповідність методів, засобів та технологій навчання і викладання на ОП принципам академічної свободи

Методи навчання і викладання на ОП дозволяють реалізуватися принципам академічної свободи, оскільки передбачається їх максимальна варіативність, урахування свободи слова і творчості.
НПП і здобувачі вищої освіти мають право на академічну свободу, що регламентується Положенням про організацію освітнього процесу в Національній академії Служби безпеки України (наказ НА СБУ від 31.08.2015 № 234, зі змінами від 23.02.2024р., №90, https://nasbu.edu.ua/uploads/p_146_77039577.pdf).
Принцип академічної свободи реалізується НПП при укладанні робочих програм навчальних дисциплін і безпосередньо у викладацькій роботі: обираються методи та засоби навчання, які забезпечують високу якість освітнього процесу з урахуванням особливостей контингенту здобувачів вищої освіти, рівня їх підготовки, інтересів, психологічних особливостей, освітніх запитів тощо.
Досягненню програмних результатів навчання, визначених ОП, сприяє застосування НПП як традиційних, так і сучасних інтерактивних методів і прийомів навчання і виховання. Свобода навчання забезпечується застосуванням різноманітних форм дистанційного, змішаного навчання і самонавчання, що дозволяє поєднувати навчання з роботою. Здобувачі вищої освіти, які навчаються на ОП, підтвердили дотримання у НА СБУ достатньо високого рівня академічної свободи (93,8%).

Опишіть, яким чином і у які строки учасникам освітнього процесу надається інформація щодо цілей, змісту та очікуваних результатів навчання, порядку та критеріїв оцінювання у межах окремих освітніх компонентів

На основі затвердженої ОП та навчальних планів розробляються робочі програми навчальних дисциплін, які доводяться до відома здобувачів вищої освіти шляхом розміщення на сайті НА СБУ (https://nasbu.edu.ua/ua/253-kiberzahist-osvitno-profesiyni-programi-drugogo-magisterskogo-rivnya-vischoi-osviti), на платформі дистанційного навчання Moodle, що дає змогу ознайомитися з програмними результатами навчання, методами і критеріями оцінювання. Інформація щодо цілей, змісту та очікуваних результатів навчання, порядку та критеріїв оцінювання у межах окремих освітніх компонентів доводиться за такою схемою. На організаційних зборах здобувачів вищої освіти перед початком навчання надається загальна інформація про ОП, також ця інформація розміщується на інформаційних стендах, в електронній бібліотеці, в АСУ та на платформі Moodle СБУ.
Щодо окремих освітніх компонентів інформація надається на першому навчальному занятті або на настановній конференції з практики як в усному вигляді, так і з орієнтацією на інформаційні стенди, електронну бібліотеку, e-mail студентських груп.
З метою удосконалення освітньої діяльності, з урахуванням рекомендацій МОН України від 09.07.2018 № 1/9-434 щодо структури та змісту робочої програми навчальної дисципліни та досвіду провідних закладів вищої освіти України, в НА СБУ здійснені заходи (розпорядження від 12.04.2023 № 136) з впровадження в освітній процес нової форми робочої програми навчальної дисципліни.

Опишіть, яким чином відбувається поєднання навчання і досліджень під час реалізації ОП

У НА СБУ всіляко підтримується наукова творчість здобувачів освітнього ступеня магістра, створено необхідні умови для їх творчого розвитку і здійснення науково-дослідної роботи та регламентується Положенням про наукове товариство студентів (курсантів, слухачів), аспірантів, докторантів і молодих вчених Національної академії Служби безпеки України (наказ НА СБУ від 02.07.2025 № 55, https://nasbu.edu.ua/uploads/p_146_85665238.pdf), Положенням про організацію наукової діяльності в НА СБУ (наказ НА СБУ від 24.02.2024 № 80, https://nasbu.edu.ua/uploads/p_146_49012933.pdf).
Науково-дослідницький компонент даної ОП впроваджується шляхом залучення здобувачів освітнього ступеня магістра до самостійних наукових досліджень, участі у науково-практичних конференціях, круглих столах, семінарах тощо.
На кафедрі кібербезпеки центру кібербезпеки ННІ ІБ СК було створено науковий гурток «Кіберботи» (витяг з протоколу засідання кафедри №11 від 28.03.2023.). Здобувачі вищої освіти даної ОП відвідують гурток, активно беруть участь у наукових заходах, що проводяться НА СБ України, та круглих столах («Актуальні питання застосування прикладних систем штучного інтелекту в кібербезпеці» лютий 2024 року та 2025 року, «Основні

аспекти форензики та їх значення для формування компетентностей фахівця з кібербезпеки» квітень 2025 року, «Актуальні питання забезпечення кібербезпеки об'єктів критичної інфраструктури» жовтень 2024-2025 рр.).
Також здобувачі вищої освіти беруть участь у дослідницькій діяльності шляхом підготовки кваліфікаційних (магістерських) робіт, а під час проходження науково-дослідної практики та під час участі у науково-дослідних роботах, що функціонують в Центрі кібербезпеки НА СБУ. За результатами наукової діяльності здобувачів вищої освіти даної ОП у 2024-2025 році опубліковано 68 тез доповідей на різних міжнародних та всеукраїнських форумах, а також отримано близько 60 сертифікатів Міжмережевої академії Cisco, що функціонує в НА СБУ, 30 здобувачів вищої освіти груп К-241м та К-241м/з отримали сертифікат з курсу «ChatGPT для підвищення власної ефективності» в Дія. Освіта.
Одним із видів самостійної наукової творчості здобувача освітнього ступеня магістра є підготовка кваліфікаційної (магістерської) роботи, яка характеризує рівень його теоретичної підготовленості, оволодіння методикою наукового дослідження, здатність до систематизації та закріплення теоретичних і практичних знань, наукової інформації, аналізу актуальних проблем за відповідною спеціальністю, розроблення на цій підставі рекомендацій практичного характеру (наказ НА СБУ від 10.12.2025 № 131 «Про закріплення за здобувачами вищої освіти тем кваліфікаційних (магістерських) робіт та призначення наукових керівників»).

Продемонструйте, із посиланням на конкретні приклади, яким чином викладачі оновлюють зміст освітніх компонентів на основі наукових досягнень і сучасних практик у відповідній галузі

На кафедрах, які забезпечують навчання за ОП, провадиться системна робота щодо оновлення змісту освітніх компонентів на основі наукових досягнень і сучасних практик у галузі 25 «Воєнні науки, національна безпека, безпека державного кордону». Запрошуються кращі фахівці галузі для проведення тренінгів та семінарів, під час яких аналізуються робочі програми навчальних дисциплін та виробляються рекомендації щодо оновлення їх змісту: (https://nasbu.edu.ua/ua/news-1-8-608-nacionalniy-klaster-kiberbezpeki-v-akademii-sbu, https://nasbu.edu.ua/ua/news-1-8-845-vebinar-z-bezpeki-informacii-nato-v-akademii-sbu, https://nasbu.edu.ua/ua/news-1-8-776-yak-zminilis-strategichni-komunikacii-v-umovah-viyni-ekspertne-obgovorennya-na-iii-mizhnarodniy-naukovo-praktichniy-konferencii).
Забезпечено участь НПП, задіяного до реалізації ОП, у заходах із підвищення кваліфікації за напрямом забезпечення інформаційної та кібербезпеки. Отримані нові знання про розвиток та інновації галузевої науки, тенденції сучасних педагогічних технологій впроваджуються в освітній процес НА СБУ, обговорюються на науково-методичних (міжкафедральних) семінарах, використовуються при розробці та щорічному оновленні навчально-методичного забезпечення окремих освітніх компонентів. Відповідно до п. 3.4 Розпорядження НА СБУ № 19 від 25.04.2024 «Щодо упорядкування організації підвищення кваліфікації наукового та науково-педагогічного складу НА СБУ».
Зокрема, матеріали підвищення кваліфікації гаранта ОП «Європейські практики наукової досконалості в цифрову еру», що реалізується за підтримки програми ERASMUS + Європейської комісії, у рамках проєкту Кафедра Жана Моне «Зміцнення лідерства та спроможності ЄС у сфері науки та інновацій» (101175767—EU_STRENGHTS—ERASMUS-JMO-2024-HEI-TCH-RSCH) 2024-2027* "EU Practices of Excellent Research in a Digital Era", а також Міжнародне стажування на тему «Неформальна освіта у підготовці бакалаврів та магістрів в країнах Європейського Союзу та Україні» було імплементовано в методичні рекомендації до організації та проведення науково-дослідної практики за даною ОП. «Міжнародне стажування на тему «International experience of using artificial intelligence in the educational process (part I)»» гаранта ОП було імплементоване у тексти лекцій з ОК-8 «Прикладні системи штучного інтелекту».
За результатами наукових досліджень із проблем забезпечення національної безпеки, зокрема інформаційної та кібербезпеки, гарант ОП, НПП, задіяні до реалізації даної ОП, здійснюють підготовку наукових та навчально-методичних праць, спрямованих на інформаційне забезпечення освітніх компонентів ОП.
Результати наукових досліджень презентуються перед викладацьким складом та здобувачами

Опишіть, яким чином навчання, викладання та наукові дослідження пов'язані з інтернаціоналізацією діяльності за освітньою програмою та закладу вищої освіти

Принцип інтернаціоналізації у межах відомчої освіти здійснюється НА СБУ у порядку, визначеному законодавством України і нормативно-правовими актами СБУ, із дотриманням вимог нормативно-правових документів СБУ щодо нерозголошення інформації, що містить державну таємницю, та дотримання режиму секретності.
З метою наближення професійної підготовки кадрів для потреб суб'єктів національної безпеки України до євроатлантичних стандартів у сфері безпеки НПП мають змогу брати участь у міжнародних безпекових проєктах, проходити закордонні стажування в університетах, вивчати провідний досвід міжнародних структур (НАТО (навчання НПП за програмами NATO DEEP), ОБСЄ, іноземні партнерські спецслужби).
Навчання, викладання у межах ОП пов'язане із інтернаціоналізацією передусім завдяки можливості відвідувати лекції досвідчених закордонних фахівців, які приїжджають до НА СБУ у рамках співпраці. Так, у межах Річної національної програми під егідою Комісії України – «Україна-НАТО» за безпосереднього сприяння Центру міжнародного співробітництва СБУ впроваджено системне проведення інформаційних заходів про НАТО для здобувачів вищої освіти НА СБУ.

5. Контрольні заходи, оцінювання здобувачів вищої освіти та академічна доброчесність

Яким чином форми контрольних заходів та критерії оцінювання здобувачів вищої освіти дають можливість встановити досягнення здобувачем вищої освіти результатів навчання для окремого освітнього компонента та/або освітньої програми в цілому?

Контроль є складовою системи забезпечення якості НА СБУ та визначення рівня сформованості компетентностей ОП. На ефективність контролю впливає успішна реалізація його функцій: зворотного зв'язку, оціночної, навчальної, розвиваючої, яким притаманні такі якості як цілеспрямованість, репрезентативність, об'єктивність та систематичність.
У НА СБУ для оцінювання рівня навчальної діяльності здобувачів вищої освіти діє накопичувальна кредитно-модульна рейтингова система, що передбачає оцінювання студентів за усіма видами аудиторної та позааудиторної (самостійної, індивідуальної) навчальної діяльності, спрямована на опанування навчального матеріалу з освітньо-професійної програми: поточний контроль, модульний, підсумковий контроль, письмові та усні диференційовані заліки й екзамени, тестування, реферати, презентації, проходження науково-дослідної практики, написання курсових робіт, підготовка та захист кваліфікаційної (магістерської) роботи. Рівень досягнутих результатів навчання вимірюється у трьох системах оцінювання: 100-бальній, національній та за шкалою ЄКТС. Критерії та методи оцінювання розробляються кафедрами й визначаються в робочих програмах навчальних дисциплін.
На ОП передбачено поточний, модульний контроль, підсумковий контроль, атестацію у вигляді складання іспиту та публічного захисту кваліфікаційних (магістерських) робіт. Поточний контроль здійснюється за допомогою контрольних завдань та різних видів тестового контролю під час проведення практичних, семінарських занять, виконання здобувачами вищої освіти індивідуальних завдань. Модульний контроль проводиться у формі тестування або виконання письмових робіт у вигляді відповідей на запитання білетів до модульних контрольних робіт, підсумковий контроль проводиться у вигляді екзамену, диференційованого заліку, захисту курсової роботи з метою оцінки досягнутих результатів навчання (чи його окремих завершених етапів).

Яким чином забезпечуються чіткість та зрозумілість форм контрольних заходів та критеріїв оцінювання навчальних досягнень здобувачів вищої освіти?

Чіткість та зрозумілість форм контрольних заходів та критеріїв оцінювання навчальних досягнень здобувачів вищої освіти забезпечуються системною роботою кафедр щодо їх планування і формулювання (з метою надання методичної допомоги НПП розроблені Методичні рекомендації щодо оцінювання здобувачів освіти в Національній академії Служби безпеки України, наказ НА СБУ від 15.11.2015 № 339, https://nasbu.edu.ua/uploads/p_146_95053091.pdf); наскрізною роз'яснювальною (консультативною) роботою НПП, кураторів навчальних груп зі здобувачами вищої освіти; проведенням з НПП тренінгів із укладання екзаменаційних завдань, ділових ігор за процедурами екзаменів, апеляцій, перескладань тощо.
Види контрольних заходів, час, місце та інша інформація щодо їх проведення доводиться до відома здобувачів вищої освіти через розклад навчальних занять, який розміщений в Автоматизованій системі управління Національної академії Служби безпеки України (https://asu.nasbu.edu.ua/), а також під час проведення навчальних занять та консультацій.
Для подальшого поліпшення якості підготовки фахівців за ОП, передбачене удосконалення системи внутрішнього забезпечення якості вищої освіти в НА СБУ, зокрема, передбачено проведення ректорських контрольних робіт відповідно до Положення про ректорський контроль рівня знань курсантів, слухачів, студентів Національної академії Служби безпеки України (затверджено наказом НА СБУ від 17.04.2015 № 137, https://nasbu.edu.ua/uploads/p_146_23031572.pdf).

Яким чином і у які строки інформація про форми контрольних заходів та критерії оцінювання доводяться до здобувачів вищої освіти?

Інформація про форми контрольних заходів міститься у робочих програмах навчальних дисциплін, каталогах ОП, а також розміщується на платформі дистанційного навчання Moodle (https://moodle.nasbu.edu.ua/), доводиться до здобувачів вищої освіти на першому занятті з навчальної дисципліни, НПП інформує про форми контрольних заходів, детально роз'яснює усі вимогами і процедури оцінювання; куратор навчальної групи на початку навчального року доводить до здобувачів вищої освіти інформацію про контрольні заходи з кожної навчальної дисципліни.
Інформація про критерії оцінювання здобувачів вищої освіти міститься у Положенні про організацію освітнього процесу в Національній академії Служби безпеки України (наказ НА СБУ від 31.08.2015 № 234, зі змінами від 23.02.2024р. №90, https://nasbu.edu.ua/uploads/p_146_77039577.pdf), Положенні про екзаменаційну комісію Національної академії Служби безпеки України (наказ НА СБУ від 16.01.2016 № 20, https://nasbu.edu.ua/uploads/p_146_24968273.pdf), Положенні про кваліфікаційні роботи здобувачів вищої освіти в Національній академії Служби безпеки України (наказ НА СБУ від 01.11.2016 № 313, https://nasbu.edu.ua/uploads/p_146_13331643.pdf), Методичних рекомендаціях щодо оцінювання здобувачів освіти в Національній академії Служби безпеки України (наказ НА СБУ від 15.11.2015 № 339, https://nasbu.edu.ua/uploads/p_146_95053091.pdf), а також у програмах атестації (https://nasbu.edu.ua/uploads/p_253_41887029.pdf).

Яким чином форми атестації здобувачів вищої освіти відповідають вимогам стандарту вищої освіти (за наявності)? Продемонструйте, що результати навчання підтверджуються результатами єдиного державного кваліфікаційного іспиту за спеціальностями, за якими він запроваджений

Стандарт вищої освіти зі спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) для другого (магістерського) рівня вищої освіти (наказ МОН України від 23.12.2021 № 1423, https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2021/12/24/256-Nats.bezpeka-mahistr.pdf) передбачає дві форми атестації здобувачів: атестація здобувачів вищої освіти здійснюється у формі атестаційного іспиту та публічного захисту кваліфікаційної (магістерської) роботи, що відповідає п.3 «Форми атестації здобувачів вищої освіти» даної ОП, а також враховано у графіку освітнього процесу навчального плану денної та заочної форми навчання за даною ОП.

Яким документом ЗВО регулюється процедура проведення контрольних заходів? Яким чином забезпечується його доступність для учасників освітнього процесу?

Процедура проведення контрольних заходів регулюється у розділі V. Форми організації освітнього процесу, підрозділі 5.4. Контрольні заходи Положення про організацію освітнього процесу в Національній академії Служби безпеки України (наказ НА СБУ від 31.08.2015 № 234, зі змінами від 23.02.2024р., №90, https://nasbu.edu.ua/uploads/p_146_77039577.pdf), Положенням про екзаменаційну комісію Національної академії Служби безпеки України (наказ НА СБУ від 16.01.2016 № 20 (зі змінами), https://nasbu.edu.ua/uploads/p_146_24968273.pdf); Положенням про ректорський контроль рівня знань курсантів, слухачів, студентів Національної академії Служби безпеки України (наказ НА СБУ від 17.04.2015 № 137, https://nasbu.edu.ua/uploads/p_146_23031572.pdf).
Зазначені розпорядчі документи доступні усім учасникам освітнього процесу, вони розміщені у читальному залі та на інформаційному ресурсі бібліотеки НА СБУ, на сайті НА СБУ у розділі «Про Академію» - «Освітня діяльність» - «Організація освітнього процесу» та на платформі дистанційного навчання Moodle.

Яким чином процедури проведення контрольних заходів забезпечують об'єктивність екзаменаторів? Якими є процедури запобігання та врегулювання конфлікту інтересів? Наведіть приклади застосування відповідних процедур на ОП

Об'єктивність екзаменаторів забезпечується ознайомленням здобувачів вищої освіти з прикладами завдань поточного, модульного та підсумкового контролю, та критеріями оцінювання результатів на початку семестру, письмовою формою контролю, відкритістю інформації про умови, критерії оцінки, строки здачі контрольних заходів, єдині правила їх перездачі, можливістю оскарження результатів атестації.
Відповідно до Положення про організацію освітнього процесу в Національній академії Служби безпеки України (наказ НА СБУ від 31.08.2015 № 234, зі змінами від 23.02.2024р., №90, https://nasbu.edu.ua/uploads/p_146_77039577.pdf), об'єктивність НПП при проведенні контрольних заходів забезпечується через наступні процедури: повторне складання екзаменів допускається не більше двох разів з кожної навчальної дисципліни: перший – НПП, другий – комісії у складі не менше трьох НПП, яка створюється директором навчально-наукового інституту; проведення лише письмових екзаменів та їх вибіркова перевірка іншим екзаменатором.
Упродовж реалізації ОП, заявленої на акредитацію, випадки конфліктів інтересів щодо об'єктивності екзаменаторів зафіксовані не були.

Яким чином процедури ЗВО урегульовують порядок повторного проходження контрольних заходів? Наведіть приклади застосування відповідних правил на ОП

Порядок повторного проходження контрольних заходів врегульовано Положенням про організацію освітнього процесу в Національній академії Служби безпеки України (наказ НА СБУ від 31.08.2015 № 234, зі змінами від 23.02.2024р., №90, https://nasbu.edu.ua/uploads/p_146_77039577.pdf) і передбачає стандартні етапи: отримання відомості складання заліково-екзаменаційної сесії в індивідуальні терміни (у разі складання сесії у індивідуальному порядку), аркуш успішності (при перескладанні контрольного заходу), ознайомлення з графіком перескладань, перескладання.

Яким чином процедури ЗВО урегульовують порядок оскарження процедури та результатів проведення контрольних заходів? Наведіть приклади застосування відповідних правил на ОП

Відповідно до Положення про організацію освітнього процесу в Національній академії Служби безпеки України (наказ НА СБУ від 31.08.2015 № 234, зі змінами від 23.02.2024р., №90, https://nasbu.edu.ua/uploads/p_146_77039577.pdf), об'єктивність НПП при проведенні підсумкових контрольних заходів забезпечується через наступні процедури: повторне складання допускається не більше двох разів з відповідної навчальної дисципліни: один раз НПП, другий – комісії у складі не менше трьох НПП, яка створюється директором ННІ ІБСК; у разі проведення письмових екзаменів – вибіркова перевірка другим екзаменатором.
Порядок подання апеляцій та їх розгляд екзаменаційною комісією визначає Положення про екзаменаційну комісію Національної академії Служби безпеки України (наказ НА СБУ від 16.01.2016 № 20, https://nasbu.edu.ua/uploads/p_146_24968273.pdf).
Випадків оскарження процедури та результатів проведення контрольних заходів на даній ОП не було.
Також для вирішення спірних питань з оцінювання знань на вступних випробуваннях (співбесіда, вступні іспити, фахові та додаткові вступні випробування) в НА СБУ діє апеляційна комісія. Наказ про склад апеляційної комісії затверджується наказом НА СБУ; головою апеляційної комісії призначається перший проректор (з навчальної роботи) або проректор з наукової роботи; склад апеляційної комісії формується з числа провідних НПП, які не є членами екзаменаційних, предметних, фахових атестаційних комісій НА СБУ. До складу апеляційної комісії можуть включатися представники підрозділів, органів СБУ.

Які документи ЗВО містять політику, стандарти і процедури дотримання академічної доброчесності?

Політика та стандарти дотримання особовим складом НА СБУ академічної доброчесності визначаються Законом України «Про Службу безпеки України», Статутами Збройних Сил України, Положенням про проходження військової служби військовослужбовцями Служби безпеки України (Указ Президента України від 27.12.2007 № 1262/2007), Положенням про проходження військової служби (навчання) курсантами вищих військових навчальних закладів (військових навчальних підрозділів закладів вищої освіти) Служби безпеки України (Указ Президента

України від Указ Президента України від 09.10.2019 № 739/2019), Кодексом доброчесності співробітника Служби безпеки України, Кодексом академічної доброчесності в Національній академії Служби безпеки України (наказ НА СБУ від 06.12.2019 № 340, https://nasbu.edu.ua/uploads/p_146_17253437.pdf).
При цьому, просування цінностей етики, академічної доброчесності серед особового складу НА СБУ здійснюється шляхом планових виховних заходів зі здобувачами вищої освіти, у навчально-наукових колективах, та організацією дієвого контролю з боку керівництва НА СБУ.
В ОП є освітній компонент ОК-1 «Методологія наукових досліджень та академічна доброчесність», а НПП, задіяні на викладанні ОП, у 2023 році пройшли онлайн на платформі Prometheus курс «Академічна доброчесність: онлайн курс для викладачів», про що отримано відповідні сертифікати.

Які технологічні рішення використовуються на ОП як інструменти протидії порушенням академічної доброчесності? Вкажіть посилання на репозиторій ЗВО, що містить кваліфікаційні роботи здобувачів вищої освіти ОП

Для протидії порушенням академічної доброчесності в НА СБУ використовується програма "Strikeplagiarism.com" .
Використання інструментів протидії порушенням академічної доброчесності унормоване використанням:
– Договір про надання послуг між НА СБУ та ТОВ «Плагіат» (від 13.06.2025 № 146, https://nasbu.edu.ua/uploads/p_146_22378618.pdf);
– Інструкція користувача системи «Strikeplagiarism.com» (https://nasbu.edu.ua/uploads/p_146_45423540.pdf).

Яким чином ЗВО популяризує академічну доброчесність серед здобувачів вищої освіти ОП?

Яким чином ЗВО популяризує академічну доброчесність серед здобувачів вищої освіти ОП?
Популяризація академічної доброчесності серед здобувачів вищої освіти відбувається через проведення просвітницьких заходів (лекції, тренінги) щодо поширення та дотримання ідеї академічної доброчесності. Також академічна доброчесність як позитивна практика популяризується в НА СБУ шляхом розміщенням на стендах та електронних табло інформації про принципи та різновиди порушень академічної доброчесності, через постійну роз'яснювальну роботу НПП під час навчальних занять, при написанні конкурсних, кваліфікаційних робіт, статей, тез доповідей на конференції, через актив студентської ради, локальні інформаційні ресурси ННІ ІБСК (група «Старости»), під час бесід із здобувачами вищої освіти.
В ОП введено освітній компонент ОК-1 «Методологія наукових досліджень та академічна доброчесність»

Яким чином ЗВО реагує на порушення академічної доброчесності? Наведіть приклади відповідних ситуацій щодо здобувачів вищої освіти відповідної ОП

У НА СБУ випадки академічної недоброчесності регулюються Кодексом академічної доброчесності в Національній академії Служби безпеки України (наказ НА СБУ від 06.12.2019 № 340, https://nasbu.edu.ua/uploads/p_146_17253437.pdf). Факт встановлення низької оригінальності наукових праць є підставою відмови у наданні рекомендації для друку або відправлення таких матеріалів на доопрацювання; низький відсоток оригінальності кваліфікаційних робіт здобувачів є підставою для прийняття рішення про недопущення до захисту або відправлення матеріалів на доопрацювання.
Факти порушення академічної доброчесності на даній ОП відсутні.

6. Людські ресурси

Продемонструйте, що викладачі, залучені до реалізації освітньої програми, з огляду на їх кваліфікацію та/або професійний досвід спроможні забезпечити освітні компоненти, які вони реалізують у межах освітньої програми, з урахуванням вимог щодо викладачів, визначених законодавством

До реалізації ОП залучені найбільш кваліфіковані НПП, які мають значний досвід викладання, публікації у фахових виданнях та виданнях, що індексуються у міжнародних наукометричних базах тощо.
До освітнього процесу на ОП залучаються НПП з урахуванням їх кваліфікації, професійного досвіду та професійної активності за останні 5 років відповідно до п.38 Ліцензійних умов провадження освітньої діяльності. Реалізацію обов'язкових освітніх компонент ОП забезпечують 17 НПП, працюють на постійній основі — 14 НПП (82,35%), із них мають науковий ступінь та/або вчене звання — 17 НПП (100%), зокрема доктори наук та/або професори — 9 НПП (52,94%), кандидати наук та/або доценти — 8 НПП (47,06%), на умовах сумісництва задіяні 3 фахівці-практики; у загальній структурі викладацького складу ОП частка жінок складає 35%, чоловіків - 65%.

Продемонструйте, що процедури конкурсного відбору викладачів є прозорими, недискримінаційними, дають можливість забезпечити потрібний рівень їхнього професіоналізму для успішної реалізації освітньої програми та послідовно застосовуються

Необхідний рівень професіоналізму НПП під час конкурсного добору забезпечується наступним чином: результати професійної діяльності НПП за спеціальністю або навчальною дисципліною (відповідно до Ліцензійних умов провадження освітньої діяльності); проведення пробного відкритого заняття з метою визначення рівня готовності НПП проводити певні види занять відповідно до встановлених вимог; організація таких занять здійснюється на рівні кафедри, навчально-наукового інституту та безпосередньо НПП відповідно до Порядку організації

контрольних, взаємних відвідувань і відкритих навчальних занять (наказ НА СБУ від 29.12.2016 № 406, https://nasbu.edu.ua/uploads/p_146_80228813.pdf); у подальшому враховуються участь НПП у процесах забезпечення якості вищої освіти, результати опитування здобувачів вищої освіти, рейтингу НПП відповідно до Положення про визначення індивідуального рейтингу науково-педагогічного працівника Національної академії Служби безпеки України (№29/19-539 від 24.10.2011, https://nasbu.edu.ua/uploads/p_146_92157185.pdf) та Порядком проведення конкурсу на заміщення вакантних посад завідувача кафедри, професора, доцента, старшого викладача, викладача Національної академії Служби безпеки України (наказ НА СБУ від 25.07.2025р. №65, https://nasbu.edu.ua/uploads/p_146_77751234.pdf).

Опишіть, із посиланням на конкретні приклади, яким чином заклад вищої освіти залучає роботодавців, їх організації, професіоналів-практиків та експертів галузі до реалізації освітнього процесу

НА СБУ залучає до аудиторних занять на ОП професіоналів-практиків, експертів галузі, представників роботодавців, запрошуючи їх на майстер-класи, семінари, тренінги, лекційні, практичні та лабораторні заняття. З метою належної підтримки відносин у сфері наукової та освітньої діяльності, підтримання належного зв'язку з практичними підрозділами до реалізації ОП залучені представники практичних підрозділів, експерти галузі, зокрема:
- доктор технічних наук, професор, працівник Державного науково-дослідного інституту технологій кібербезпеки Держспецзв'язку України викладає ОК-15 «Аудит інформаційної безпеки та кібербезпеки»;
- доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора В. Бурячка Факультету інформаційних технологій Київського університету ім. Бориса Грінченка залучений до проведення занять з ОК-9 «Організаційно-правове забезпечення кіберзахисту», є керівником з написання кваліфікаційних (магістерських) робіт;
- гостьові лекції для здобувачів вищої освіти даної ОП проводять з вересня 2024 року представники НКЦК РНБО України;
- до навчального процесу групи К-241м залучався фахівець-експерт у сфері OSINT;
- аудиторні практичні заняття з профорієнтаційною ціллю проводили представники ДІАЗ та ДКІБ СБУ;
- 7 робочих програм за даною ОП погоджені з ДІАЗ СБУ.

Яким чином ЗВО сприяє професійному розвиткові викладачів ОП? Наведіть конкретні приклади такого сприяння

Сприяння професійному розвиткові НПП становить цілісну систему: із надання взаємної методичної допомоги на кафедрах, на рівні структурного підрозділу переходить в систему тренінгової роботи щодо закріплення наставника, курси молодих викладачів, стажування у практичних підрозділах СБУ (план План стажування на 2024/2025 н.р., №29/11-5952/ві від 11.07.2024, план підвищення кваліфікації у закладах вищої освіти України у 2024/2025 н.р., наказ НА СБУ № 249 від 24.07.2024), провідних закладах вищої освіти.
У НА СБУ нормативно удосконалено порядок планування та оформлення результатів стажування у практичних підрозділах, механізм їх імплементації у навчальний процес (розпорядження НА СБУ від 19.10.2023 №41 «Щодо упорядкування організації підвищення кваліфікації науково та науково-педагогічного складу НА СБУ»). За результатами підвищення кваліфікації (стажування) НПП звітують перед кафедральними колективами.
Для НПП НА СБУ існує можливість опублікування результатів наукових досліджень у відомчих фахових виданнях НА СБУ (Збірник наукових праць, Науковий вісник), науково-практичному журналі «Інформаційна безпека людини, держави, суспільства», вивчати досвід колег на відкритих та показових заняттях, брати участь у наукових форумах, заходах. Щомісяця досвідчені НПП проводять показові (відкриті) заняття, які можуть відвідати усі бажаючі НПП й удосконалити професійний досвід.

Наведіть конкретні приклади заохочення розвитку викладацької майстерності

Інформація щодо результатів професійного розвитку та досягнень НПП розглядається на засіданнях кафедр, вчених радах інститутів та НА СБ України, доводиться в академії на загальних зборах. НПП заохочуються у порядку, встановленому нормативно-правовими актами СБУ і розпорядчими документами НА СБУ (нагородження подякою, грамотою, розміщення фотографій НПП на Дошці пошани НА СБУ (Положення про Дошку пошани НА СБУ, наказ від 04.12.2018 № 321). Матеріальне заохочення НПП (преміювання, нагородження цінним подарунком тощо) здійснюється у порядку, встановленому нормативно-правовими актами СБУ.
Серед НПП, що забезпечують викладання на даній ОП є викладачі, відзначені подяками, грамотами ректора НА СБУ та Голови СБУ, а також отримували матеріальне заохочення у 2025 році.

7. Освітнє середовище та матеріальні ресурси

Продемонструйте, яким чином навчально-методичне забезпечення, фінансові та матеріально-технічні ресурси (програмне забезпечення, обладнання, бібліотека, інша інфраструктура тощо) ОП забезпечують досягнення визначених ОП мети та програмних результатів навчання

Навчально-методичне та інформаційне забезпечення за номенклатурою, якістю і кількістю забезпечує усі освітні компоненти, дає можливість досягати визначених ОП цілей і програмних результатів навчання. Рівень забезпечення освітнього процесу обладнанням, інструментарієм, методичною літературою, сучасною аудіо-

,відеотехнікою, комп'ютерами, мультимедійним обладнанням відповідає нормативним вимогам. Обладнання лекційних залів, аудиторій, навчальних класів, кабінетів періодично оновлюється і сприяє ефективному проведенню всіх видів навчальних занять за ОП. Функціонує 1 стадіон та 2 спортивні зали, 3 спортивні майданчики з тренажерним обладнанням та інші допоміжні навчально-тренувальні споруди. На базі ННІ ІБСК НА СБУ створено Центр кібербезпеки, який займається дослідженням і впровадженням сучасних підходів до формування академічних та професійних компетентностей фахівців.
НА СБУ розташована на 3 окремих об'єктах (м. Київ: вул. М. Максимовича, 22; проспект В. Лобановського, 98; вул. Авіаконструктора Антонова, 2/32) із загальною площею приміщень – 33639 м2. Санітарно-технічний стан будівель і споруд задовільний і відповідає вимогам щодо їх експлуатації, що підтверджується відповідними висновками контролюючих органів.
З метою підготовки і підвищення рівня знань здобувачів вищої освіти та отримання ними практичного досвіду в галузі інформаційної та кібербезпеки створено центр кібербезпеки ННІ ІБ СК НА СБУ. Бібліотечний фонд складає понад 100 тис. друкованих примірників та понад 30 найменувань наукових фахових та періодичних видань

Продемонструйте, яким чином заклад вищої освіти забезпечує доступ викладачів і здобувачів вищої освіти до відповідної інфраструктури та інформаційних ресурсів, потрібних для навчання, викладацької та/або наукової діяльності в межах освітньої програми, відповідно до законодавства

Освітнє середовище, створене в НА СБУ, дозволяє задовольнити потреби та інтереси здобувачів вищої освіти завдяки збалансованості матеріальних засобів (обладнання аудиторій, лабораторій, тренінгових центрів, виділення та оформлення простору для «student life», консультаційних центрів тощо), налагодженій взаємодії із студентськими колективами через інститути кураторства, проведення консультацій та опитувань, а також сприйняття здобувачів вищої освіти як рівноправних партнерів у побудові їх освітньої траєкторії, відповідності критеріям студентоцентрованого навчання.
Користування студентами, НПП матеріально-технічною базою, інфраструктурними, соціально-побутовими об'єктами, інформаційними ресурсами НА СБУ здійснюється на безоплатній основі. Доступ на об'єкти НА СБУ учасникам освітнього процесу надається з урахуванням відомчих вимог до забезпечення безпеки та охорони. Студенти мають доступ до спортивного та тренажерних залів у позанавчальний час. Доступ до навчально-методичного забезпечення освітніх компонент ОП здійснюється через платформу дистанційного навчання Moodle НА СБУ, що дозволяє забезпечити безперервність освітнього процесу в умовах дії правового режиму воєнного стану. У навчальних аудиторіях Інституту робоче місце викладача обладнане комп'ютером з проводовим Інтернетом, інтерактивною дошкою. Пошук та облік виданої літератури у загальній бібліотеці організовано за електронними каталогами. Для автоматизації всіх етапів навчального процесу в НА СБУ впроваджено Автоматизовану систему управління навчальним закладом.

Опишіть, яким чином освітнє середовище надає можливість задовольнити потреби та інтереси здобувачів вищої освіти, які навчаються за освітньою програмою, та є безпечним для їх життя, фізичного та ментального здоров'я

У НА СБУ є власна медична служба, персонал якої контролює стан здоров'я працівників і здобувачів вищої освіти, санітарно-гігієнічний стан об'єктів харчування та умови розміщення і проживання в гуртожитках.
З огляду на відомчу належність та з метою забезпечення безпеки здобувачів вищої освіти усі об'єкти НА СБУ перебувають під охороною, впроваджено пропускний режим. НА СБУ забезпечує безпечність освітнього середовища для життя та здоров'я здобувачів вищої освіти (включаючи психічне здоров'я) суворим дотриманням норм техніки безпеки, постійним інструктуванням НПП та здобувачів вищої освіти, проведенням різноманітних заходів, які стосуються надання першої домедичної допомоги, здорового способу життя тощо. Кожний курс має журнал з безпеки життєдіяльності, де фіксуються планові та позапланові інструктажі (рівень задоволеності здобувачів безпечністю освітнього середовища складає 100 %).
Безпечність освітнього середовища в умовах воєнного стану забезпечується відповідно до розпорядження НА СБУ щодо заходів безпеки під час отримання сигналу повітряної тривоги (№46 від 27.11.23), а також Розпорядження Міністерства оборони України про збереження життя особового складу під час надходження сигналу «Повітряна тривога («Ракетна небезпека»)» (№82/0 від 05.12.2023р.).
Щодо психічного здоров'я дбають згідно з Положенням про запобігання та протидію булінгу (цькуванню) та сексуальним домаганням у Національній академії Служби безпеки України (наказ №488 від 29.12.2023 р. https://nasbu.edu.ua/uploads/p_146_25808033.pdf).

Опишіть, яким чином заклад вищої освіти забезпечує освітню, організаційну, інформаційну, консультативну та соціальну підтримку, підтримку фізичного та ментального здоров'я здобувачів вищої освіти, які навчаються за освітньою програмою.

Механізми освітньої, організаційної, інформаційної, консультативної та соціальної підтримки здобувачів вищої освіти врегульовано законодавством України, відомчими нормативно-правовими актами СБУ, структурною побудовою та розпорядчими документами НА СБУ, плановими позиціями роботи ННІ ІБСК, кафедр, інших структурних підрозділів, що забезпечують навчально-виховний процес.
Інформаційна підтримка здійснюється через активну комунікацію, яка проводиться зі здобувачами вищої освіти: через Студентську раду, члени якої беруть участь у вдосконаленні ОП; представників студентського самоврядування, котрі є членами Вченої ради НА СБУ (2 особи), вченої ради ННІ ІБСК (2 особи); кураторів навчальних груп (комунікація здійснюється через локальні інформаційні ресурси навчально-наукового інституту, у месенджерах WhatsApp та Signal, соціальних мережах Facebook та Instagram, сторінку izi_sbu). Щоденно в ННІ ІБСК призначаються відповідальні із числа НПП, які ведуть різнобічну комунікацію зі здобувачами вищої освіти в гуртожитку – від освітніх консультацій до питань безпеки життєдіяльності. З метою інформаційної підтримки та

відкритості освітнього процесу впроваджено електронний журнал обліку роботи академічної групи (наказ НА СБ України від 26.11.2019 № 331, https://nasbu.edu.ua/uploads/p_146_24239846.pdf).

Яким чином ЗВО створює достатні умови для реалізації права на освіту особами з особливими освітніми потребами? Наведіть посилання на конкретні приклади створення таких умов на ОП (якщо такі були)

НА СБУ працює над створенням достатніх умов для реалізації права на освіту особами з особливими освітніми потребами таким чином, щоб вони мали можливість повноцінно соціалізуватися та результативно навчатися. В НА СБУ діє Порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення в Національній академії Служби безпеки України (наказ НА СБУ від 19.07.2024 №284, https://nasbu.edu.ua/uploads/p_146_22162071.pdf). Зокрема, у ННІ ІБСК на першому поверсі навчального корпусу та гуртожитку створено відповідний інклюзивний простір для осіб з особливими освітніми потребами. Для потреб тих, хто вже здобуває вищу освіту, та майбутніх (потенційних) здобувачів вищої освіти пристосовані їдальня, бібліотека, приміщення на території центру кібербезпеки тощо. Працює сектор організації та здійснення психологічної роботи, фахівець з виховної роботи.
Особи з особливими освітніми потребами на даній ОП відсутні.

Продемонструйте наявність унормованих антикорупційних політик, процедур реагування на випадки цькування, дискримінації, сексуального домагання, інших конфліктних ситуацій, які є доступними для всіх учасників освітнього процесу та яких послідовно дотримуються під час реалізації освітньої програми

Відповідно до Положення про організацію освітнього процесу в Національній академії Служби безпеки України (наказ НА СБУ від 31.08.2015 № 234, зі змінами від 23.02.2024р. №90, https://nasbu.edu.ua/uploads/p_146_77039577.pdf), а також Положення про запобігання та протидію булінгу (цькуванню) та сексуальним домаганням у Національній академії Служби безпеки України (наказ №488 від 29.12.2023 р, https://nasbu.edu.ua/uploads/p_146_25808033.pdf).
Відповідно до Положення про екзаменаційну комісію Національної академії Служби безпеки України (наказ НА СБУ від 16.01.2016 № 20) діє процедура запобігання та врегулювання конфлікту інтересів під час атестації здобувачів вищої освіти. Під час формування та перед підписанням наказу про створення екзаменаційних комісій усі НПП повинні письмово (рапорт/заява) повідомити про відсутність чи наявність конфлікту інтересів. Після цього здійснюється вивчення інформації і приймається рішення щодо включення того чи іншого НПП до складу екзаменаційної комісії, видається відповідний розпорядчий документ НА СБУ.
У НА СБУ визначено графік прийому учасників освітнього процесу керівництвом та функціонує скринька довіри. Для розгляду спірних питань залучаються найбільш досвідчені працівники НА СБУ. Інструментом для вирішення конфліктних ситуацій є методи реагування на конфліктні ситуації керівником структурного підрозділу: бесіда з конфліктуючими сторонами з метою визначення причин та сутності конфліктної ситуації; ініціювання створення тимчасової спеціальної комісії щодо врегулювання конфліктної ситуації; інформування органів внутрішніх справ у випадку спірної ситуації або у випадку трактування однієї з конфліктуючих сторін конфліктної ситуації як кримінальної; інформування учасників конфліктної ситуації про висновки тимчасової спеціальної комісії та запропоновані проєкти рішень; контроль за дотриманням запропонованих висновків та рішень тимчасової спеціальної комісії.
Під час реалізації ОП випадків подібних конфліктних ситуацій не було.

8. Внутрішнє забезпечення якості освітньої програми

Яким документом ЗВО регулюються процедури розроблення, затвердження, моніторингу та періодичного перегляду ОП? Наведіть посилання на цей документ, оприлюднений у відкритому доступі на своєму вебсайті

Положення про освітню програму Національної академії Служби безпеки України (наказ НА СБУ від 29.12.2023 №490, https://nasbu.edu.ua/uploads/p_146_48077580.pdf)

Яким чином та з якою періодичністю відбувається перегляд ОП? Які зміни були внесені до ОП за результатами останнього перегляду, чим вони були обґрунтовані?

Періодичний перегляд ОП здійснюється щорічно, відповідно до планових позицій НА СБУ.
Під час останнього перегляду ОП, що акредитується (рішення Вченої ради НА СБУ від 29.08.2024, протокол №13) у зв'язку з отриманням ліцензії на провадження освітньої діяльності за освітніми програмами зі спеціальності 256 «Національна безпека» як регульованої (наказ МОН від 27.06.2024 №449-л), відповідно до стандарту вищої освіти України зі спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності), затвердженого наказом Міністерства освіти і науки України від 23.12.2021 року № 1423 «Про затвердження стандарту вищої освіти зі спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності для другого (магістерського) рівня вищої світи» та на основі проведення постакредитаційного моніторингу освітньо-професійної програми ID 53772 «Кіберзахист у сфері інформаційних технологій та кіберпросторі». Було введено освітній компонент ОК-2 «Риторика та стилістика наукових праць» (3 кредити ЄКТС), сформована одна структурно-логічна схема освітньо-професійної програми (п.2 ОП) для денної та заочної

форми. Також змінено назву освітнього компонента «Актуальні питання національної безпеки України» на «Актуальні проблеми інформаційної безпеки», на урахування зауважень в рецензії від Держспецзв'язку курсову роботу перенесено до освітнього компонента «Кіберзахист об'єктів критичної інфраструктури» у другий семестр, а освітній компонент «Безпека розподілених інформаційних систем та хмарні технології» - у четвертий семестр. Під час останнього перегляду ОП (рішення Вченої ради НА СБУ від 26.06.2025, протокол № 6) було враховано рецензії стейкхолдерів, що надійшли як зауваження на проєкт ОП, зокрема, на рекомендацію ДІАЗ СБУ посилено технічну складову ОП і замість ОК «Теорія кіберпростору, кібербезпеки та кіберзахисту» введено «Системне адміністрування та організація безпеки ІТ-сервісів», замість «Актуальні проблеми інформаційної безпеки» введено «Системи управління базами даних», враховано рекомендацію Держспецзв'язку та зменшено кількість кредитів для ОК «Аудит інформаційної безпеки та кібербезпеки» (4 кредити ЄКТС), на рекомендацію ДІАЗ СБУ та НКЦК РНБО доповнено теми в освітніх компонентах «Управління кіберінцидентами», «Методи і моделі протидії кіберзагрозам» та «Кіберзахист об'єктів критичної інфраструктури».

Продемонструйте, із посиланням на конкретні приклади, як здобувачі вищої освіти залучені до процесу періодичного перегляду ОП та інших процедур забезпечення її якості, а їх пропозиції беруться до уваги під час перегляду ОП

Здобувачі вищої освіти залучені до процесу періодичного перегляду ОП та інших процедур забезпечення її якості через: участь в обговоренні ОП (здобувачі вищої освіти денної та заочної форми входять до складу проєктної групи ОП (розпорядження НА СБУ від 21.05.2025 № 53/дск); пропозиції, висловлені на Студентській раді, Вченій раді ННІ ІБ СК та Вченій раді НА СБУ; періодичні опитування щодо рівня задоволеності освітнім процесом за ОП. Зокрема, за результатами опитування щодо рівня задоволеності здобувачів вищої освіти, що проводилося у грудні 2024 року у групі К-231м та К-241м (https://nasbu.edu.ua/uploads/p_253_44446245.pdf), здійснено актуалізацію тем для ОК «Прикладні системи штучного інтелекту в кіберпросторі», «Кіберзахист об'єктів критичної інфраструктури», «Методи і моделі протидії кіберзагрозам» та «Управління кіберінцидентами», щоб покращити баланс між теоретичними матеріалами та практичними завданнями.

Яким чином студентське самоврядування бере участь у процедурах внутрішнього забезпечення якості ОП?

Діяльність органів самоврядування в НА СБУ, до яких залучені студенти ОП, регламентована Положенням про студентське самоврядування в ННІ ІБ СК НА СБУ (від 20.12.2023, протокол №3 https://nasbu.edu.ua/uploads/p_146_87799479.pdf). Студентське самоврядування бере участь у процедурах внутрішнього забезпечення якості ОП через: обговорення з представниками студентського самоврядування на вчених радах ННІ ІБ СК та НА СБУ питань забезпечення організації освітнього процесу за ОП; спонукання здобувачів вищої освіти до участі в анкетуванні та опитуваннях щодо якості викладання за ОП; сприяння публічності інформації про ОП через спілкування та обговорення у групі «Старости» та в кожній студентській групі в месенджерах; поширення інформації серед здобувачів вищої освіти про принципи академічної доброчесності. Також є щорічний моніторинг рівня задоволеності здобувачів вищої освіти (https://nasbu.edu.ua/uploads/p_253_58652340.pdf, https://nasbu.edu.ua/uploads/p_253_44446245.pdf). Такі заходи дають можливість вносити зміни в освітній процес за ОП. Регулярно керівництвом НА СБУ, ННІ ІБСК, гарантом ОП проводяться зустрічі з представниками здобувачів вищої освіти, в межах яких відбувається обговорення проблемних питань, пов'язаних з освітнім процесом. Для цього попередньо збираються запити, які аналізуються в процесі діалогу зустрічей. Внутрішня оцінка ефективності реалізації ОП здійснюється шляхом обговорення результатів підсумкового контролю на рівні Студентської ради та вченої ради ННІ ІБ СК.

Продемонструйте, із посиланням на конкретні приклади, як роботодавці безпосередньо або через свої об'єднання залучені до періодичного перегляду ОП та інших процедур забезпечення її якості

Роботодавці залучені до процесу періодичного перегляду ОП, оскільки входять до складу проєктної групи ОП (розпорядження НА СБУ від 21.05.2025 № 53/дск), безпосередньо викладають на ОП, а тому гарант ОП протягом року отримує відгуки про здобувачів вищої освіти, питання підготовки фахівців у сфері кіберзахисту та інформаційної безпеки, як майбутніх оперативних співробітників, так і цивільних фахівців, постійно обговорюються під час щорічної науково-практичної конференції «Актуальні проблеми управління інформаційною безпекою держави», яка проводиться на базі НА СБУ (https://nasbu.edu.ua/ua/news-1-8-769-konferenciya-z-informaciynoi-bezpeki), круглих столів, що проводяться кафедрою кібербезпеки ЦКБ ННІ ІБ СК, під час робочих зустрічей з потенційними роботодавцями, зокрема представниками Національного координаційного центру кібербезпеки при РНБО України, ДІАЗ СБУ, ДКІБ СБУ, Державної служби спеціального зв'язку та захисту інформації України.

Опишіть практику збирання, аналізу та врахування інформації щодо кар'єрного шляху та траєкторій працевлаштування випускників ОП (зазначте в разі проходження акредитації вперше)

Щороку (січень) відзначається «День Академії», а у жовтні місяці – «День інституту», це ті комунікаційні майданчики, де традиційно збираються випускники минулих років, відбувається обговорення питань працевлаштування та кар'єрного зростання випускників, здійснюється зворотний зв'язок щодо якості освітнього процесу, різних аспектів практичної цінності освітніх компонентів відповідних освітніх програм. Збирання та врахування інформації щодо кар'єрного шляху випускників НА СБУ здійснюється через систему щорічних опитувань (https://nasbu.edu.ua/uploads/p_253_65773684.pdf), на основі чого і відбувається коригування ОП «Кіберзахист у сфері інформаційних технологій та кіберпросторі» (перший випуск у лютому 2023 року). Зокрема, на основі опитування щодо того, знання з яких освітніх компонент випускники застосовують під час своєї роботи, в ОП для набору 2025 року було замінено освітній компонент «Територіальна оборона, мобілізаційна підготовка та

мобілізація» на «Кіберзахист інформаційних систем сектору безпеки та оборони держави».
У зв'язку з отриманням ліцензії на провадження освітньої діяльності за освітніми програмами зі спеціальності 256 «Національна безпека» як регульованої (наказ МОН від 27.06.2024 №449-л), відповідно до стандарту вищої освіти України зі спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності), дана ОП ID 64490 (затверджена рішенням Вченої ради НА СБУ від 29.08.2024, протокол №13) акредитується вперше.

Продемонструйте, що система забезпечення якості закладу вищої освіти забезпечує вчасне реагування на результати моніторингу освітньої програми та/або освітньої діяльності з реалізації освітньої програми, зокрема здійсненого через опитування заінтересованих сторін

В НА СБУ здійснюється щорічний моніторинг та періодичне оновлення освітніх програм підготовки здобувачів вищої освіти. До переліку основних пропозицій, що були сформульовані у ході здійснення процедур внутрішнього забезпечення якості ОП за час її реалізації доцільно віднести такі: оновлення організаційно-розпорядчих документів у частині організації освітнього процесу з урахуванням змін законодавства; активізація роботи у сфері впровадження дуальної та неформальної освіти, активізації академічної мобільності здобувачів вищої освіти та НПП; оновлення технічних засобів навчання та програмного забезпечення, необхідних для якісної підготовки фахівців у сфері кіберзахисту; здійснення благоустрою аудиторного фонду та соціальної інфраструктури ННІ ІБСК.
За результатами моніторингу освітньої діяльності з ОП було:
оновлено Статут Національної академії Служби безпеки України (у редакції наказу ЦУ СБУ від 19.08.2024 № 413, https://nasbu.edu.ua/uploads/p_60_50137472.pdf);
оновлено Положення про організацію освітнього процесу в Національній академії Служби безпеки України (наказ НА СБУ
від 31.08.2015 № 234, зі змінами від 23.02.2024р., №90, https://nasbu.edu.ua/uploads/p_146_77039577.pdf);
розроблено Положення про дистанційний курс у Національній академії Служби безпеки України (наказ НА СБУ від 21.04.2025 № 31, https://nasbu.edu.ua/uploads/p_146_83962763.pdf);
затверджено Порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення (наказ НА СБУ від 19.07.2024 № 284, https://nasbu.edu.ua/uploads/p_146_22162071.pdf);
забезпечено можливість оприлюднення на веб-сайті НА СБУ проєктів змін у освітню програму для можливості ознайомлення широкої аудиторії стейкхолдерів та описів навчальних дисциплін (https://nasbu.edu.ua/ua/253-kiberzahist-osvitno-profesiyni-programi-drugogo-magisterskogo-rivnya-vischoi-osviti).

Продемонструйте, що результати зовнішнього забезпечення якості вищої освіти беруться до уваги під час удосконалення ОП. Яким чином зауваження та рекомендації з останньої акредитації та акредитацій інших ОП були враховані під час удосконалення цієї ОП?

За результатами проведення постакредитаційного моніторингу ОП ID53772 «Кіберзахист у сфері інформаційних технологій та кіберпросторі», акредитована (сертифікат №8258 від 16.05.2024, строк дії 01.07.2029) було здійснено:
- критерій 1: було введено освітній компонент ОК-2 «Риторика та стилістика наукових праць» (3 кредити ЄКТС), розділ освітньо-професійної програми «4 – Придатність випускників до працевлаштування та подальшого навчання» відповідає Стандарту вищої освіти для другого (магістерського) рівня вищої освіти за спеціальністю 256 «Національна безпека за окремими сферами забезпечення і видами діяльності»;
- критерій 2: сформована одна структурно-логічна схема освітньо-професійної програми (п.2 ОП) для денної та заочної форми;
- критерій 3: на веб-сайті НА СБУ оприлюднено розмір плати за навчання для очної та заочної форми навчання (https://nasbu.edu.ua/ua/217-vartist-navchannya-dlya-studentiv-informaciya-dlya-abiturientiv);
- критерій 4: розробляються електронні відеокурси та інтерактивні завдання для стимулювання до вивчення освітніх компонент, а також застосовуються навчальні матеріали Міжмережевої академії Cisco;
- критерій 5: оновлено та переопрацьовано положення НА СБУ;
- критерій 6: продовжено організацію опитування здобувачів вищої освіти після закінчення кожного семестру, а також випускників ОП;
- критерій 7: у приміщеннях центру кібербезпеки, де відбувається ремонт, передбачена наявність пандусів для забезпечення реалізації права на освіту осіб з особливими освітніми потребами. Органи студентського самоврядування проінформовано щодо вчасного виявлення серед здобувачів вищої освіти осіб з особливими потребами;
- критерій 8: до органів студентського самоврядування включено представників ОП денної та заочної форми навчання;
- критерій 9: на веб-сайтів НА СБУ було розміщено проєкт оновленої ОП та оголошення про очікування зауважень та рекомендацій від широкої аудиторії стейкхолдерів (https://nasbu.edu.ua/uploads/p_79_56018453.pdf, https://nasbu.edu.ua/ua/news-1-8-609-ogoloshennya). Оновлені РПНД з освітніх компонент розміщені на сайті НА СБУ та на платформі дистанційного навчання Moodle.

Опишіть, яким чином учасники академічної спільноти залучені до процедур внутрішнього забезпечення якості ОП

До процедур внутрішнього забезпечення якості ОП залучений гарант ОП, члени проєктної груп, НПП, керівники ННІ та допоміжних структурних підрозділів, адміністрація, помічник ректора (із забезпечення якості вищої освіти), студентське самоврядування. Питання якості ОП обговорюються на засіданнях Вченої ради НА СБУ, вченої ради ННІ ІБ СК, щорічних Установчих зборах перед початком навчального року, міжкафедральних семінарах, засіданнях кафедр, службових нарадах гарантів ОП, кураторів навчальних груп, методичного складу ЦООД, ННІ ІБ СК. Гарант ОП, проєктна група здійснює моніторинг та періодичний перегляд ОП, забезпечують вчасне реагування на запити усіх категорій стейкхолдерів. Результати заліково-екзаменаційних сесій, атестації студентів ОП обговорюються на

рівні кафедр, ректорату, Вченої ради ННІ ІБ СК. З урахуванням цілей ОП здійснюється добір НПП для реалізації відповідних освітніх компонентів, при цьому враховується відповідність освітньої та/або професійної кваліфікації, рівень професійної активності. До процедур якості ОП залучена Наглядова рада НА СБУ.
Учасники академічної спільноти залучені до процедур забезпечення якості на всіх етапах реалізації ОП. Під час щорічних Установчих зборів наукового та науково-педагогічного складу з нагоди нового навчального року, на засіданнях кафедр, вчених рад навчально-наукових інститутів, Вченої ради НА СБУ, нарадах проєктних груп ОП, кураторів навчальних груп відбувається обговорення питань якості освітньої діяльності та освітнього процесу і процедур їх забезпечення.

Продемонструйте, що в академічній спільноті закладу вищої освіти формується культура якості освіти

Здійснення процесів і процедур внутрішнього забезпечення якості освіти в НА СБУ відбувається в зоні відповідальності структурних підрозділів (навчально-науковий інститут, кафедра, центр організації освітньої діяльності, відділ кадрового забезпечення, відділ роботи з особовим складом, загальна бібліотека, сектор спеціальних навчальних фондів, відділ інформаційного забезпечення) та колегіальних органів (вчена рада навчально-наукового інституту, Вчена рада НА СБУ). Діяльність усіх підрозділів НА СБУ, задіяних у процедурах внутрішнього забезпечення якості освіти, регулюється окремими нормативними актами – положеннями, наказами, розпорядженнями.
Концепція системи внутрішнього забезпечення якості вищої освіти в НА СБУ (https://nasbu.edu.ua/uploads/p_146_19371306.pdf) визначає засади впровадження та забезпечення процедур якості освіти. Робота із забезпечення якості освіти в НА СБУ здійснюється на інституційній основі шляхом функціонування Наглядової ради НА СБУ, яка систематично визначає проблемні питання та перспективи розвитку освітнього процесу в інтересах забезпечення національної безпеки України (https://nasbu.edu.ua/ua/news-1-8-625-aktualni-pitannya-ta-perspektivi-rozvitku-sistemi-zabezpechennya-yakosti-osviti-v-akademii-sbu-obgovorili-pid-chas-drugogo-zasidannya-naglyadovoi-radi-zakladu). Гарант ОП (наказ НА СБУ від 09.08.2022, № 1, https://nasbu.edu.ua/uploads/p_146_35683724.pdf) та група забезпечення освітніх програм спеціальності здійснюють моніторинг та періодичний перегляд ОП.

9. Прозорість і публічність

Якими документами ЗВО регулюються права та обов'язки усіх учасників освітнього процесу? Яким чином забезпечується їх доступність для учасників освітнього процесу?

Права та обов'язки усіх учасників освітнього процесу НА СБУ визначаються законодавством України, Положенням про проходження військової служби військовослужбовцями Служби безпеки України (Указ Президента України від 27.12.2007 № 1262/2007), нормативно-правовими актами СБУ, Статутом Національної академії Служби безпеки України (у редакції наказу ЦУ СБУ від 21.10.2016 № 560, https://nasbu.edu.ua/ua/60-statut-nacionalnoi-akademii-sbu-istoriya-akademii), Колективним договором між адміністрацією Національної академії Служби безпеки України і Первинною профспілковою організацією Національної академії СБ України (№ 111 від 28.07.2017), Положенням про організацію освітнього процесу в Національній академії Служби безпеки України (наказ НА СБУ від 31.08.2015 № 234, зі змінами від 23.02.2024р., №90, https://nasbu.edu.ua/uploads/p_146_77039577.pdf), Положенням про гаранта освітньої програми НА СБУ (наказ НА СБУ від 09.08.2022 №148, https://nasbu.edu.ua/uploads/p_146_35683724.pdf), Правилами поведінки здобувачів вищої освіти в Національній академії СБ України (https://nasbu.edu.ua/uploads/p_146_28524882.pdf), відповідними положеннями про структурні підрозділи, посадовими інструкціями співробітників (працівників) та контрактами.
В установленому законодавством порядку усім учасникам освітнього процесу забезпечена доступність до зазначених документів, зокрема через вебсайт СБУ та НА СБУ.

Наведіть посилання на вебсторінку, яка містить інформацію про оприлюднення ЗВО відповідного проєкту освітньої програми для отримання зауважень та пропозицій заінтересованих сторін (стейкголдерів).

Посилання на веб-сторінку, яка містить інформацію про оприлюднення на офіційному веб-сайті НА СБУ проєкту ОП з метою отримання зауважень: https://nasbu.edu.ua/ua/204-proekti-osvitno-profesiyni-programi, зокрема, сам проєкт ОП: https://nasbu.edu.ua/uploads/p_204_75156769.pdf
Також оголошення окремо розміщувалося на офіційному веб-сайті НА СБУ у розділі «Новини про Академію» для ОП, що оновлювалася на основі постакредитаційного моніторингу: https://nasbu.edu.ua/ua/news-1-8-609-ogoloshennya

Наведіть посилання на оприлюднену у відкритому доступі на своєму вебсайті інформацію про освітню програму (освітню програму у повному обсязі, навчальні плани, робочі програми навчальних дисциплін, можливості формування індивідуальної освітньої траєкторії здобувачів вищої освіти) в обсязі, достатньому для інформування відповідних заінтересованих сторін та суспільства

https://nasbu.edu.ua/ua/253-kiberzahist-osvitno-profesiyni-programi-drugogo-magisterskogo-rivnya-vischoi-osviti

11. Перспективи подальшого розвитку ОП

Якими загалом є сильні та слабкі сторони ОП?

Сильні сторони:
– ОП є єдиною і унікальною в Україні щодо підготовки магістра зі спеціальності 256 Національна безпека саме з акцентом на спеціалізацію у сфері інформаційних технологій та кіберпросторі;
– в умовах зростаючого попиту на фахівців, здатних протидіяти інформаційним загрозам у сучасному безпековому середовищі, випускники ОП матимуть переваги щодо працевлаштування та подальшого кар'єрного зростання в органах (підрозділах) суб'єктів національної безпеки, державному та бізнес секторах кібербезпеки, ІТ-секторі України;
– кадрове забезпечення ОП дозволяє забезпечити якісну підготовку здобувачів освітнього ступеня магістра; науково-педагогічні співробітники (працівники), задіяні до реалізації ОП, здійснюють наукові дослідження за спеціальністю 256 Національна безпека та/або є фахівцями-практиками в галузі інформаційної безпеки та кібербезпеки;
– матеріально-технічне забезпечення ОП, зокрема сучасні комп'ютерні класи зі спеціалізованим обладнанням на базі центру кібербезпеки, наукові лабораторії та програмне забезпечення Мережевої академії Cisco, забезпечують формування у здобувачів вищої освіти фахових компетентностей, навичок і вмінь у галузі інформаційної безпеки та кібербезпеки згідно системи міжнародних стандартів, кращих світових практик;
– налагоджена система проведення навчальних занять за дистанційною формою в умовах введення правового режиму воєнного стану;
– освітнє середовище НА СБУ, що сприяє розвитку і формуванню всебічно розвинутої особистості сучасного здобувача вищої освіти: громадянина, патріота, фахівця.

Слабкі сторони:
– складність реалізації програм академічної мобільності учасників освітнього процесу;
– потребують удосконалення процедури дуальної освіти.

Якими є перспективи розвитку ОП упродовж найближчих 3 років? Які конкретні заходи ЗВО планує здійснити задля реалізації цих перспектив?

НА СБУ є закладом вищої освіти, що здійснює підготовку фахівців для потреб суб'єктів національної безпеки, зокрема СБУ. Наразі СБУ перебуває у стадії реформування, потребуватиме змін і система підготовки кадрів для цієї сфери, що впливає на формування перспектив ОП, коригування її змісту, аби вона могла врахувати і забезпечувати кадрові потреби суб'єктів національної безпеки України.
Для даної ОП актуальною є потреба розглянути можливість проходження процедур визнання відповідності освітньо-професійної програми вимогам професійного стандарту, зокрема, «Фахівець з реагування на інциденти кібербезпеки». Щорічно коригувати перелік дисциплін вільного вибору для здобувачів вищої освіти на основі світових практик, міждисциплінарних підходів споріднених спеціальностей, імплементації зарубіжних методів та методик підвищення ефективності навчання.
Розвиток в Україні та за її межами інформаційного суспільства на фоні процесів глобалізації й загострення економічної конкуренції мають наслідком збільшення загроз інформаційній безпеці державних та недержавних інституцій. З огляду на це основними напрямами розвитку ОП будуть актуалізація переліку та змісту освітніх компонентів з урахуванням перманентних змін нормативно-правової бази у сфері забезпечення державної безпеки в інформаційній сфері, передового досвіду країн ЄС та НАТО, збільшення питомої ваги практичної підготовки в структурі ОП, активізація участі стейкхолдерів в освітньому процесі, що сприятиме покращанню якості професійної підготовки кіберфахівців.

Запевнення

Запевняємо, що уся інформація, наведена у відомостях та доданих до них матеріалах, є достовірною.

Гарантуємо, що ЗВО за запитом експертної групи надасть будь-які документи та додаткову інформацію, яка стосується освітньої програми та/або освітньої діяльності за цією освітньою програмою.

Надаємо згоду на опрацювання та оприлюднення цих відомостей про самооцінювання та усіх доданих до них матеріалів у повному обсязі у відкритому доступі.

Додатки:

Таблиця 1. Інформація про обов'язкові освітні компоненти ОП

Таблиця 2. Зведена інформація про викладачів ОП

Таблиця 3. Матриця відповідності програмних результатів навчання, освітніх компонентів, методів навчання та

оцінювання

***

Шляхом підписання цього документа запевняю, що я належним чином уповноважений на здійснення такої дії від імені закладу вищої освіти та за потреби надам документ, який посвідчує ці повноваження.

Документ підписаний кваліфікованим електронним підписом/кваліфікованою електронною печаткою.

Інформація про КЕП

ПІБ: Черняк Андрій Миколайович

Дата: 19.01.2026 р.

Таблиця 1. Інформація про освітні компоненти ОП

Назва освітнього компонента	**Вид освітнього компонента**	**Силабус або інші навчально-методичні матеріали**		**Якщо освітній компонент потребує спеціального матеріально-технічного та/або інформаційного забезпечення, наведіть відомості щодо нього***
		Назва файла	**Хеш файла**	
Методи і моделі протидії кіберзагрозам (денна форма)	навчальна дисципліна	*ОК_12_Методи і моделі протидії кіберзагрозам_2024_денна.pdf*	eoujf/REy3f6r6lzYocMLVS1VyLACCk1X9PmgbWOu/c=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний:* *- комплектами ПК;* *- інтерактивною дошкою Intboard UT-TBI82X;* *- проєктором BenQ MX808STX;* *- комутатором TP-Link TL SG 3428X;* *Спеціалізований комп'ютерний клас №124, 53,2 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook* *Спеціалізований комп'ютерний клас №125, 54,15 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook* *Спеціалізований комп'ютерний клас №126, 54,15 м2* *Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook* *Спеціалізований комп'ютерний*

				клас №127, 44,88 м2 *Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook* *Серверна:* *- сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.;* *- сервер Supermicro C813MLJ06N50026;* *- фаєрвол Cisco ASA 5506;* *- комутатор RV345P – 2 шт.;* *- комутатор Cisco Catalyst 1000 Series*
Методи і моделі протидії кіберзагрозам (заочна форма)	навчальна дисципліна	*ОК_12_Методи і моделі протидії кіберзагрозам_2024_заочна.pdf*	jq1dZnYfTk7AQoLQ12oxdhSmfBPiGInGfjKBsB/30pg=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний:* *- комплектами ПК;* *- інтерактивною дошкою Intboard UT-TBI82X;* *- проєктором BenQ MX808STX;* *- комутатором TP-Link TL SG 3428X;* *Спеціалізований комп'ютерний клас №124, 53,2 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook* *Спеціалізований комп'ютерний клас №125, 54,15 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook* *Спеціалізований комп'ютерний клас №126, 54,15 м2* *Комплект ПК – 15 шт., 2022 року*

				у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook Спеціалізований комп'ютерний клас №127, 44,88 м2 Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook Серверна: - сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.; - сервер Supermicro C813MLJ06N50026; - фаєрвол Cisco ASA 5506; - комутатор RV345P – 2 шт.; - комутатор Cisco Catalyst 1000 Series
Кіберзахист об'єктів критичної інфраструктури (денна форма)	навчальна дисципліна	*ОК_13_Кіберзахист об'єктів критичної інфраструктури_2024_денна.pdf*	4DQqS4oq2WeInWb1hL/KEVu1gKa2fBA2lvy68gsdEvA=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний: - комплектами ПК; - інтерактивною дошкою Intboard UT-TBI82X; - проєктором BenQ MX808STX; - комутатором TP-Link TL SG 3428X; Спеціалізований комп'ютерний клас №124, 53,2 м2 Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook Спеціалізований комп'ютерний клас №125, 54,15 м2 Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet*

				Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook Спеціалізований комп'ютерний клас №126, 54,15 м2 Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook Спеціалізований комп'ютерний клас №127, 44,88 м2 Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook Серверна: - сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.; - сервер Supermicro C813MLJ06N50026; - фаєрвол Cisco ASA 5506; - комутатор RV345P – 2 шт.; - комутатор Cisco Catalyst 1000 Series
Кіберзахист об'єктів критичної інфраструктури (заочна форма)	навчальна дисципліна	*ОК_13_Кіберзахист об'єктів критичної інфраструктури_2024_заочна.pdf*	5xiPyhglU96SKRBOjmhrt3AIES7dkdr//2YeY5IGWFo=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний: - комплектами ПК; - інтерактивною дошкою Intboard UT-TBI82X; - проєктором BenQ MX808STX; - комутатором TP-Link TL SG 3428X; Спеціалізований комп'ютерний клас №124, 53,2 м2 Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A,*

				Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook Спеціалізований комп'ютерний клас №125, 54,15 м2 Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook Спеціалізований комп'ютерний клас №126, 54,15 м2 Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook Спеціалізований комп'ютерний клас №127, 44,88 м2 Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook Серверна: - сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.; - сервер Supermicro C813MLJ06N50026; - фаєрвол Cisco ASA 5506; - комутатор RV345P – 2 шт.; - комутатор Cisco Catalyst 1000 Series
Кіберзахист об'єктів	курсова робота	*Методичні_рекоме*	JszOo6zCrwMsCkhw	*Спеціалізовані комп'ютерні класи*

критичної інфраструктури	(проект)	*нд_курсова_КЗОКІ_2024.pdf*	vGaWlm84vxBigoWHPSCiBaGuVdc=	*на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний:* *- комплектами ПК;* *- інтерактивною дошкою Intboard UT-TBI82X;* *- проєктором BenQ MX808STX;* *- комутатором TP-Link TL SG 3428X;* *Спеціалізований комп'ютерний клас №124, 53,2 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook* *Спеціалізований комп'ютерний клас №125, 54,15 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook* *Спеціалізований комп'ютерний клас №126, 54,15 м2* *Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook* *Спеціалізований комп'ютерний клас №127, 44,88 м2* *Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box,*

				дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook *Серверна:* *- сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.;* *- сервер Supermicro C813MLJ06N50026;* *- фаєрвол Cisco ASA 5506;* *- комутатор RV345P – 2 шт.;* *- комутатор Cisco Catalyst 1000 Series*
Управління кіберінцидентами (денна форма)	навчальна дисципліна	*ОК_14_Управління кіберінцидентами_2024_денна.pdf*	4mFqzZz5Ja1YycLWAg2eeltRmOT2Tiy6YnX/ygmhdhU=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний:* *- комплектами ПК;* *- інтерактивною дошкою Intboard UT-TBI82X;* *- проєктором BenQ MX808STX;* *- комутатором TP-Link TL SG 3428X;* *Спеціалізований комп'ютерний клас №124, 53,2 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook* *Спеціалізований комп'ютерний клас №125, 54,15 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook* *Спеціалізований комп'ютерний клас №126, 54,15 м2* *Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення*

				Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook *Спеціалізований комп'ютерний клас №127, 44,88 м2* *Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook* *Серверна:* *- сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.;* *- сервер Supermicro C813MLJ06N50026;* *- фаєрвол Cisco ASA 5506;* *- комутатор RV345P – 2 шт.;* *- комутатор Cisco Catalyst 1000 Series*
Управління кіберінцидентами (заочна форма)	навчальна дисципліна	*ОК_14_Управління кіберінцидентами_2024_заочна.pdf*	EI5UkA+NmMxxYPTdrS5jwpN64agCmlnOKdM3AnhFqz0=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний:* *- комплектами ПК;* *- інтерактивною дошкою Intboard UT-TBI82X;* *- проєктором BenQ MX808STX;* *- комутатором TP-Link TL SG 3428X;* *Спеціалізований комп'ютерний клас №124, 53,2 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook* *Спеціалізований комп'ютерний клас №125, 54,15 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook*

				Спеціалізований комп'ютерний клас №126, 54,15 м2 *Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook* *Спеціалізований комп'ютерний клас №127, 44,88 м2* *Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: віртуальні машини VM Ware, Virtual Box, дистрибутив Linux Kali, програмне забезпечення Мережевої академії Cisco, iMindMap, MindManager, IBM i2 Analyst's Notebook* *Серверна:* *- сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.;* *- сервер Supermicro C813MLJ06N50026;* *- фаєрвол Cisco ASA 5506;* *- комутатор RV345P – 2 шт.;* *- комутатор Cisco Catalyst 1000 Series*
Аудит інформаційної безпеки та кібербезпеки (денна форма)	навчальна дисципліна	*ОК_15_Аудит інформаційної безпеки та кібербезпеки_2024_денна.pdf*	XOTdAwWK2a5/mfP+8sh/CbngRlMTMJr98WM9UWfhB3A=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний:* *- комплектами ПК;* *- інтерактивною дошкою Intboard UT-TBI82X;* *- проєктором BenQ MX808STX;* *- комутатором TP-Link TL SG 3428X;* *Спеціалізований комп'ютерний клас №124, 53,2 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №125, 54,15 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+*

				монітор DELL23.8'+COBRA SK *Спеціалізований комп'ютерний клас №126, 54,15 м2* *Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №127, 44,88 м2* *Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Серверна:* *- сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.;* *- сервер Supermicro C813MLJ06N50026;* *- фаєрвол Cisco ASA 5506;* *- комутатор RV345P – 2 шт.;* *- комутатор Cisco Catalyst 1000 Series*
Аудит інформаційної безпеки та кібербезпеки (заочна форма)	навчальна дисципліна	*ОК_15_Аудит інформаційної безпеки та кібербезпеки_2024_ заочна.pdf*	ORqHzKSeA6dkTyrDxlVytADZQNbqDufWwFFSnU1fSNA=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний:* *- комплектами ПК;* *- інтерактивною дошкою Intboard UT-TBI82X;* *- проєктором BenQ MX808STX;* *- комутатором TP-Link TL SG 3428X;* *Спеціалізований комп'ютерний клас №124, 53,2 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №125, 54,15 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №126, 54,15 м2* *Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №127, 44,88 м2* *Комплект ПК – 12 шт., 2022 року*

				у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Серверна: - сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.; - сервер Supermicro C813MLJ06N50026; - фаєрвол Cisco ASA 5506; - комутатор RV345P – 2 шт.; - комутатор Cisco Catalyst 1000 Series
Безпека розподілених інформаційних ресурсів та хмарні технології (денна форма)	навчальна дисципліна	*ОК_16_Безпека розподілених інформаційних ресурсів та хмарні технології_2025_денна.pdf*	lOlQ5fmomSlN2gYEoOim2aDRsXnYRgmOezQXb1lh86k=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний: - комплектами ПК; - інтерактивною дошкою Intboard UT-TBI82X; - проєктором BenQ MX808STX; - комутатором TP-Link TL SG 3428X; Спеціалізований комп'ютерний клас №124, 53,2 м2 Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Спеціалізований комп'ютерний клас №125, 54,15 м2 Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Спеціалізований комп'ютерний клас №126, 54,15 м2 Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Спеціалізований комп'ютерний клас №127, 44,88 м2 Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Серверна: - сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.; - сервер Supermicro C813MLJ06N50026; - фаєрвол Cisco ASA 5506;*

				- комутатор RV345P – 2 шт.; *- комутатор Cisco Catalyst 1000 Series*
Безпека розподілених інформаційних ресурсів та хмарні технології (ззаочна форма)	навчальна дисципліна	*ОК_16_Безпека розподілених інформаційних ресурсів та хмарні технології_2025_заочна.pdf*	eb5Ojw+/Rp4WeaVXDYqJ6ZM44vnW9lzPryx2QI428KA=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний:* *- комплектами ПК;* *- інтерактивною дошкою Intboard UT-TBI82X;* *- проєктором BenQ MX808STX;* *- комутатором TP-Link TL SG 3428X;* *Спеціалізований комп'ютерний клас №124, 53,2 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №125, 54,15 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №126, 54,15 м2* *Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №127, 44,88 м2* *Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Серверна:* *- сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.;* *- сервер Supermicro C813MLJ06N50026;* *- фаєрвол Cisco ASA 5506;* *- комутатор RV345P – 2 шт.;* *- комутатор Cisco Catalyst 1000 Series*
Територіальна оборона, мобілізаційна підготовка та мобілізація (денна форма)	навчальна дисципліна	*ОК_17_Територіальнаоборона, мобілізаційна підготовка та мобілізація_2024_денна.pdf*	cP97s2vyWfN7tKZgltBIyoLHKvYmwAEYrn5IukimKuc=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний:* *- комплектами ПК;* *- інтерактивною дошкою Intboard UT-TBI82X;* *- проєктором BenQ MX808STX;* *- комутатором TP-Link TL SG 3428X;*

				Спеціалізований комп'ютерний клас №124, 53,2 м2 *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №125, 54,15 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №126, 54,15 м2* *Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №127, 44,88 м2* *Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Серверна:* *- сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.;* *- сервер Supermicro C813MLJ06N50026;* *- фаєрвол Cisco ASA 5506;* *- комутатор RV345P – 2 шт.;* *- комутатор Cisco Catalyst 1000 Series*
Територіальна оборона, мобілізаційна підготовка та мобілізація (заочна форма)	навчальна дисципліна	*ОК_17_Територіальнаоборона, мобілізаційна підготовка та мобілізація_2024_заочна.pdf*	OcZSeyKxQeFY5PopVhdM35ZWHP2bztDZJWyndVMZiRA=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний:* *- комплектами ПК;* *- інтерактивною дошкою Intboard UT-TBI82X;* *- проєктором BenQ MX808STX;* *- комутатором TP-Link TL SG 3428X;* *Спеціалізований комп'ютерний клас №124, 53,2 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №125, 54,15 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core*

				i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK *Спеціалізований комп'ютерний клас №126, 54,15 м2* *Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №127, 44,88 м2* *Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Серверна:* *- сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.;* *- сервер Supermicro C813MLJ06N50026;* *- фаєрвол Cisco ASA 5506;* *- комутатор RV345P – 2 шт.;* *- комутатор Cisco Catalyst 1000 Series*
Науково-дослідна практика (денна форма)	практика	*ОК_18_Науково-дослідна практика_2024_денна.pdf*	aWJCF420DVRZScx/7QeCdcN/n/ktJxFeiQD67I5Keog=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний:* *- комплектами ПК;* *- інтерактивною дошкою Intboard UT-TBI82X;* *- проєктором BenQ MX808STX;* *- комутатором TP-Link TL SG 3428X;* *Спеціалізований комп'ютерний клас №124, 53,2 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №125, 54,15 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №126, 54,15 м2* *Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4*

				16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK *Спеціалізований комп'ютерний клас №127, 44,88 м2* *Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Серверна:* *- сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.;* *- сервер Supermicro C813MLJ06N50026;* *- фаєрвол Cisco ASA 5506;* *- комутатор RV345P – 2 шт.;* *- комутатор Cisco Catalyst 1000 Series*
Науково-дослідна практика (заочна форма)	практика	*ОК_18_Науково-дослідна практика_2024_заочна.pdf*	+BhfHfnwtx1z3p3fO1Ofas8risxfq20j/yjybWmijiQ=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний:* *- комплектами ПК;* *- інтерактивною дошкою Intboard UT-TBI82X;* *- проєктором BenQ MX808STX;* *- комутатором TP-Link TL SG 3428X;* *Спеціалізований комп'ютерний клас №124, 53,2 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №125, 54,15 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №126, 54,15 м2* *Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №127, 44,88 м2* *Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Серверна:*

				- сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.; *- сервер Supermicro C813MLJ06N50026;* *- фаєрвол Cisco ASA 5506;* *- комутатор RV345P – 2 шт.;* *- комутатор Cisco Catalyst 1000 Series*
Кваліфікаційна (магістерська) робота	підсумкова атестація	*ОК_19_Методичні рекомендац_для_кваліфікац_магістер_роботи_2024.pdf*	wlkNY10RbUsiGFZjCcpaMbKznisV+CCyE/8d2iT9gU4=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний:* *- комплектами ПК;* *- інтерактивною дошкою Intboard UT-TBI82X;* *- проєктором BenQ MX808STX;* *- комутатором TP-Link TL SG 3428X;* *Спеціалізований комп'ютерний клас №124, 53,2 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №125, 54,15 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №126, 54,15 м2* *Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №127, 44,88 м2* *Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Серверна:* *- сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.;* *- сервер Supermicro C813MLJ06N50026;* *- фаєрвол Cisco ASA 5506;* *- комутатор RV345P – 2 шт.;* *- комутатор Cisco Catalyst 1000 Series*
Атестаційний іспит	підсумкова атестація	*ОК_19_Програма_іспит_2024.pdf*	Yh6ZjAhBONt4ZLRFLTCXaZQsIbPwcUhgAxGBYgZwZZI=	*Не потребує*
Застосування методів і	навчальна	*ОК_11_Застосуван*	/9Tn4nUtoT+uUDPg	*Освітній компонент*

засобів OSINT у Web-середовищі (заочна форма)	дисципліна	*ня методів і засобів OSINT у WEB-середовищі_2024_заочна.pdf*	hQC+DS0wrl0E1CnYHFTG371nXPQ=	*реалізується в онлайн-форматі та не потребує спеціального матеріально-технічного забезпечення. Усі заняття проводяться з використанням стандартних інструментів дистанційного навчання та відкритих OSINT-платформ, доступних через веб-браузер.*
Застосування методів і засобів OSINT у Web-середовищі (денна форма)	навчальна дисципліна	*ОК_11_Застосування методів і засобів OSINT у WEB-середовищі_2024_денна.pdf*	P3IAMi544WOyy4r1ZECsLHfUEmiMeeEUI69nh5VKqPw=	*Освітній компонент реалізується в онлайн-форматі та не потребує спеціального матеріально-технічного забезпечення. Усі заняття проводяться з використанням стандартних інструментів дистанційного навчання та відкритих OSINT-платформ, доступних через веб-браузер.*
Актуальні проблеми інформаційної безпеки (заочна форма)	навчальна дисципліна	*ОК_10_Актуальні проблеми інформаційної безпеки_заочна.pdf*	zr6YslOLMvGiVCFBZ9tNxRX0+tsi/SV+DeL1VTGChCU=	*Не потребує*
Актуальні проблеми інформаційної безпеки (денна форма)	навчальна дисципліна	*ОК_10_Актуальні проблеми інформаційної безпеки_денна.pdf*	linMIj1IpDCd2JKS5G0sOm5l+hvj7SNT2iVzQ0qV+eA=	*Не потребує*
Методологія наукових досліджень та академічна доброчесність (денна форма)	навчальна дисципліна	*ОК_1_Методологія наукових досліджень та академічна доброчесність_2024_денна.pdf*	TgHypALgtUU8SiSuaaQGOHJYsTgOzM+JmseQg6PzrO4=	*Не потребує*
Методологія наукових досліджень та академічна доброчесність (зочна форма)	навчальна дисципліна	*ОК_1_Методологія наукових досліджень та академічна доброчесність_2024_заочна.pdf*	ygzNsKkVlplPv5e3EoPsRyfoT/2e7fGSdVNhe6qIRA4=	*Не потребує*
Риторика та стилістика наукових праць (денна форма)	навчальна дисципліна	*ОК_2_Риторика та стилістика наукових праць_2024_денна.pdf*	QYKiPEKFE1x8pymkgY7Hg1xEs/UsjDrQEP2Zry0tnKY=	*Не потребує*
Риторика та стилістика наукових праць	навчальна дисципліна	*ОК_2_Риторика та стилістика наукових праць_2024_заочна.pdf*	yNDhuOal1nwOrsZ2Bvm/+CcfWpSPRPhUfcvzWnbyFiI=	*Не потребує*
Теорія прийняття рішень (денна форма)	навчальна дисципліна	*ОК_3_Теорія прийняття рішень_2024_денна.pdf*	QE6mKpIxz5AGrTk13jMC2raICY9ipfT75x7a7iXkmCg=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний:* *- комплектами ПК;* *- інтерактивною дошкою Intboard UT-TBI82X;* *- проєктором BenQ MX808STX;* *- комутатором TP-Link TL SG 3428X;* *Спеціалізований комп'ютерний клас №124, 53,2 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №125, 54,15 м2*

				Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Спеціалізований комп'ютерний клас №126, 54,15 м2 Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Спеціалізований комп'ютерний клас №127, 44,88 м2 Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Серверна: - сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.; - сервер Supermicro C813MLJ06N50026; - фаєрвол Cisco ASA 5506; - комутатор RV345P – 2 шт.; - комутатор Cisco Catalyst 1000 Series
Теорія прийняття рішень (заочна форма)	навчальна дисципліна	*ОК_3_Теорія прийняття рішень_2024_заочна.pdf*	etrvLBG1hcMxm03hG8TsLmRbbbvkl4qA4zaHUdn7mY8=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний: - комплектами ПК; - інтерактивною дошкою Intboard UT-TBI82X; - проєктором BenQ MX808STX; - комутатором TP-Link TL SG 3428X; Спеціалізований комп'ютерний клас №124, 53,2 м2 Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Спеціалізований комп'ютерний клас №125, 54,15 м2 Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Спеціалізований комп'ютерний клас №126, 54,15 м2 Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська*

				плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK *Спеціалізований комп'ютерний клас №127, 44,88 м2* *Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Серверна:* *- сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.;* *- сервер Supermicro C813MLJ06N50026;* *- фаєрвол Cisco ASA 5506;* *- комутатор RV345P – 2 шт.;* *- комутатор Cisco Catalyst 1000 Series*
Іноземна мова професійного спрямування (денна форма)	навчальна дисципліна	*ОК_4_Іноземна мова професійного спрямування_2024_денна.pdf*	lGQJXtqJNObwGHG62ubkRruwAm8zhyYw53WpS3J40qE=	*Не потребує*
Іноземна мова професійного спрямування (заочна форма)	навчальна дисципліна	*ОК_4_Іноземна мова професійного спрямування_2024_заочна.pdf*	Ys1Jwef5CGqvRtwZJQoPIZ8PZPIxXI58dFJKohhInt8=	*Не потребує*
Гендерна політика в системі національної безпеки та оборони України (денна форма)	навчальна дисципліна	*ОК_5_Гендерна політика в системі національної безпеки та оборони України_2024_денна.pdf*	C+ZjZyhTGIKEmFd1u9Q9XX9pmz1KnoRNAIHZQsnT5fA=	*Не потребує*
Теорія кіберпростору, кібербезпеки та кіберзахисту (денна форма)	навчальна дисципліна	*ОК_6_Теорія кіберпростору_кібербезпеки та кіберзахисту_2024_денна.pdf*	+Jv1J7Mj7OODcgepznbOxlR6tMcrmKspei4BdljDxBY=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний:* *- комплектами ПК;* *- інтерактивною дошкою Intboard UT-TBI82X;* *- проєктором BenQ MX808STX;* *- комутатором TP-Link TL SG 3428X;* *Спеціалізований комп'ютерний клас №124, 53,2 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №125, 54,15 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №126, 54,15 м2* *Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core*

				i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK *Спеціалізований комп'ютерний клас №127, 44,88 м2* *Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Серверна:* *- сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.;* *- сервер Supermicro C813MLJ06N50026;* *- фаєрвол Cisco ASA 5506;* *- комутатор RV345P – 2 шт.;* *- комутатор Cisco Catalyst 1000 Series*
Теорія кіберпростору, кібербезпеки та кіберзахисту (заочна форма)	навчальна дисципліна	*ОК_6_Теорія кіберпростору_кібербезпеки та кіберзахисту_2024_заочна.pdf*	oTVvGpVoZeJMx2dVqKEEt2OBIu+osVglxqzihbcK+fI=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний:* *- комплектами ПК;* *- інтерактивною дошкою Intboard UT-TBI82X;* *- проєктором BenQ MX808STX;* *- комутатором TP-Link TL SG 3428X;* *Спеціалізований комп'ютерний клас №124, 53,2 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №125, 54,15 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №126, 54,15 м2* *Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №127, 44,88 м2* *Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4*

				16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK *Серверна:* *- сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.;* *- сервер Supermicro C813MLJ06N50026;* *- фаєрвол Cisco ASA 5506;* *- комутатор RV345P – 2 шт.;* *- комутатор Cisco Catalyst 1000 Series*
Інформаційне протиборство (денна форма)	навчальна дисципліна	*ОК_7_Інформаційне протиборство_2024_денна.pdf*	yLVCaSoUAvyVxUm4klAACopGWvf7WdepCsu6jc8iZG8=	*Не потребує*
Інформаційне протиборство (заочна форма)	навчальна дисципліна	*ОК_7_Інформаційне протиборство_2024_заочна.pdf*	WCW+VLCh8K4bu6AXborsuEuuMhN3HkxwZ1103HOxqyo=	*Не потребує*
Прикладні системи штучного інтелекту в кіберпросторі (денна форма)	навчальна дисципліна	*ОК_8_Прикладні системи штучного інтелекту в кіберпросторі_2024_денна.pdf*	zd3iDAg4Y1fgJ+6/cD4PTrOQhsyuHG6JKIim1mEzHbw=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний:* *- комплектами ПК;* *- інтерактивною дошкою Intboard UT-TBI82X;* *- проєктором BenQ MX808STX;* *- комутатором TP-Link TL SG 3428X;* *Спеціалізований комп'ютерний клас №124, 53,2 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: ChatGPT, Gemini, Perplexity, NotebookLM* *Спеціалізований комп'ютерний клас №125, 54,15 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: ChatGPT, Gemini, Perplexity, NotebookLM* *Спеціалізований комп'ютерний клас №126, 54,15 м2* *Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Відкрите програмне забезпечення: ChatGPT, Gemini, Perplexity, NotebookLM* *Спеціалізований комп'ютерний клас №127, 44,88 м2* *Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core*

				i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Відкрите програмне забезпечення: ChatGPT, Gemini, Perplexity, NotebookLM Серверна: - сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.; - сервер Supermicro C813MLJ06N50026; - фаєрвол Cisco ASA 5506; - комутатор RV345P – 2 шт.; - комутатор Cisco Catalyst 1000 Series
Прикладні системи штучного інтелекту в кіберпросторі (заочна форма)	навчальна дисципліна	*ОК_8_Прикладні системи штучного інтелекту в кіберпросторі_2024_заочна.pdf*	HNvC+SvO2bcbVtprLCmNCPJhBifkthQTb/aeW4LOJMU=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний: - комплектами ПК; - інтерактивною дошкою Intboard UT-TBI82X; - проєктором BenQ MX808STX; - комутатором TP-Link TL SG 3428X; Спеціалізований комп'ютерний клас №124, 53,2 м2 Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Відкрите програмне забезпечення: ChatGPT, Gemini, Perplexity, NotebookLM Спеціалізований комп'ютерний клас №125, 54,15 м2 Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Відкрите програмне забезпечення: ChatGPT, Gemini, Perplexity, NotebookLM Спеціалізований комп'ютерний клас №126, 54,15 м2 Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Відкрите програмне забезпечення: ChatGPT, Gemini, Perplexity, NotebookLM Спеціалізований комп'ютерний клас №127, 44,88 м2 Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4*

				16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Відкрите програмне забезпечення: ChatGPT, Gemini, Perplexity, NotebookLM Серверна: - сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.; - сервер Supermicro C813MLJ06N50026; - фаєрвол Cisco ASA 5506; - комутатор RV345P – 2 шт.; - комутатор Cisco Catalyst 1000 Series
Організаційно-правове забезпечення кіберзахисту (денна форма)	навчальна дисципліна	*ОК_9_Організаційно-правове забезпечення кіберзахисту_2024_денна.pdf*	thC2UlIOLtKcmW35kQKXsYcnWQt/txapUdZUx7ELOHk=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний: - комплектами ПК; - інтерактивною дошкою Intboard UT-TBI82X; - проєктором BenQ MX808STX; - комутатором TP-Link TL SG 3428X; Спеціалізований комп'ютерний клас №124, 53,2 м2 Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Спеціалізований комп'ютерний клас №125, 54,15 м2 Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Спеціалізований комп'ютерний клас №126, 54,15 м2 Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Спеціалізований комп'ютерний клас №127, 44,88 м2 Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK Серверна: - сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.; - сервер Supermicro C813MLJ06N50026; - фаєрвол Cisco ASA 5506; - комутатор RV345P – 2 шт.; - комутатор Cisco Catalyst 1000 Series*

Організаційно-правове забезпечення кіберзахисту (заочна форма)	навчальна дисципліна	*ОК_9_Організаційно-правове забезпечення кіберзахисту_2024_заочна.pdf*	RAyRmz7xfbFXX3OwbXzgL9jCZuebljmlbsMb5Ck4t30=	*Спеціалізовані комп'ютерні класи на базі центру кібербезпеки НА СБУ, чотири спеціалізовані комп'ютерні класи, кожен з яких обладнаний:* *- комплектами ПК;* *- інтерактивною дошкою Intboard UT-TBI82X;* *- проєктором BenQ MX808STX;* *- комутатором TP-Link TL SG 3428X;* *Спеціалізований комп'ютерний клас №124, 53,2 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №125, 54,15 м2* *Комплект ПК – 16 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №126, 54,15 м2* *Комплект ПК – 15 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Спеціалізований комп'ютерний клас №127, 44,88 м2* *Комплект ПК – 12 шт., 2022 року у складі процесор Intel Core i710700K 3/8GHz (16MB Comet Lake, 95W,S1200), материнська плата ASUS PRIME H510M-A, Socket 1200, модуль пам'яті DDR4 16 GB/2666, Goodram x 2(32GB), жорсткий диск PC P300 1TB+ монітор DELL23.8'+COBRA SK* *Серверна:* *- сервер типу 5 Dell EMC PowerEdgeR750xs 210-AZYO WFBSU22-4310 – 2 шт.;* *- сервер Supermicro C813MLJ06N50026;* *- фаєрвол Cisco ASA 5506;* *- комутатор RV345P – 2 шт.;* *- комутатор Cisco Catalyst 1000 Series*
Гендерна політика в системі національної безпеки та оборони України (заочна форма)	навчальна дисципліна	*ОК_5_Гендерна політика в системі національної безпеки та оборони України_2024_заочна.pdf*	7NaxsfHPX74vHqNjcMpT3LdGGOcLg4JOm8fPdaOZpfE=	*Не потребує*

* наводяться відомості, як мінімум, щодо наявності відповідного матеріально-технічного забезпечення, його достатності для реалізації ОП; для обладнання/устаткування – також кількість, рік введення в експлуатацію, рік останнього ремонту; для програмного забезпечення – також кількість ліцензій та версія програмного забезпечення

Таблиця 2. Зведена інформація про відповідність НПП освітнім компонентам

Документ	Назва файла	Хеш файла
Документ	*Додаток 2_Зведена інформація про викладачів.pdf*	NgJdZ8a+VrGa32C8rOL9qtPyVn+EBCRE3udctZqwGQA=

Таблиця 3. Матриця відповідності програмних результатів навчання, освітніх компонентів, методів навчання та оцінювання

Програмні результати навчання ОП	ПРН відповідає результату навчання, визначеному стандартом вищої освіти (або охоплює його)	Обов'язкові освітні компоненти, що забезпечують ПРН	Методи навчання	Форми та методи оцінювання
ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.	☒	Організаційно-правове забезпечення кіберзахисту (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Застосування методів і засобів OSINT у Web-середовищі (денна форма)	Під час викладання навчальної дисципліни використовуються словесні, наочні, практичні та самостійні методи, що забезпечують формування результатів навчання. Лекційні заняття застосовуються для систематизованого викладу навчального матеріалу, введення термінології та розкриття теоретичних положень дисципліни. Практичні заняття спрямовані на формування практичних умінь шляхом виконання індивідуальних завдань, аналізу ситуаційних кейсів, опрацювання методів і засобів OSINT та моделювання оперативної обстановки. Самостійна робота здобувачів включає опрацювання літератури, виконання завдань аналітичного характеру, засвоєння інструментів OSINT та розвиток навичок критичного аналізу. У процесі навчання застосовуються дидактичні прийоми, орієнтовані на формування аналітичних здібностей, уміння працювати з неповними або суперечливими даними та здатності приймати	Для перевірки рівня засвоєння здобувачами вищої освіти знань, умінь та навичок з навчальної дисципліни проводиться оцінювання продовж навчання у вигляді поточного, модульного та підсумкового контролю. Для оцінки використовуються різні види робіт: - поточний контроль засвоєння матеріалу здійснюється шляхом перевірки практичних робіт; - модульний контроль проводиться в формі виконання завдання; - підсумковий контроль забезпечується проведенням диференційованого заліку в формі тесту.

			обґрунтовані рішення. Використовуються сучасні програмні засоби та WEB-ресурси, необхідні для виконання завдань дисципліни.	
		Методи і моделі протидії кіберзагрозам (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії, зокрема: - під час проведення лекцій використовується пояснювально-ілюстративний (інформаційно-рецептивний) метод, коли викладач подає готові знання (лекції, демонстрації, мультимедійні презентації, схеми, графіки), а здобувачі вищої освіти їх сприймають, осмислюють і запам'ятовують, це забезпечує швидку передачу великого обсягу інформації, систематизує матеріал	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Управління кіберінцидентами (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії, зокрема: - під час проведення лекцій використовується пояснювально-ілюстративний (інформаційно-рецептивний) метод, коли викладач подає готові знання (лекції, демонстрації, мультимедійні презентації, схеми, графіки), а здобувачі вищої освіти їх сприймають, осмислюють і запам'ятовують, це забезпечує швидку передачу великого обсягу інформації, систематизує матеріал	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Аудит інформаційної безпеки та кібербезпеки (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Безпека розподілених інформаційних	Під час викладання навчальної дисципліни	Поточний контроль Модульна контрольна

		ресурсів та хмарні технології (денна форма)	використовуються такі методи навчання як індуктивний, дедуктивний, продуктивний, дослідницький та метод стимулювання. Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить здобувачів вищої освіти до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. Продуктивний метод пов'язаний з опануванням нових знань у процесі творчої роботи. Дослідницький метод застосовується для засвоєння досвіду творчої діяльності, глибоких знань. Методи стимулювання спеціально спрямовані на формування позитивних мотивів навчання, стимулюють пізнавальну активність, водночас сприяють збагаченню здобувачів вищої освіти новою інформацією. Методи активізації навчального процесу: - мозкові атаки – метод розв'язання невідкладних завдань, сутність якого полягає в тому, щоб висловити якомога більшу кількість ідей за дуже обмежений проміжок часу, обговорити і здійснити їх селекцію; - кейс-метод – розгляд, аналіз конкретних ситуацій, який дає змогу наблизити процес навчання до реальної практичної діяльності; - презентації – виступи перед аудиторією, що використовуються для представлення певних досягнень, результатів роботи групи, звіту про виконання індивідуальних завдань тощо	робота Рейтингова система Екзамен
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
		Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки	Публічний захист

			завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	
		Прикладні системи штучного інтелекту в кіберпросторі (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії, зокрема: - під час проведення лекцій використовується пояснювально-ілюстративний (інформаційно-рецептивний) метод, коли викладач подає готові знання (лекції, демонстрації, мультимедійні презентації, схеми, графіки), а здобувачі вищої освіти їх сприймають, осмислюють і запам'ятовують, це забезпечує швидку передачу великого обсягу інформації, систематизує матеріал	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Кіберзахист об’єктів критичної інфраструктури (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії, зокрема: - під час проведення лекцій використовується пояснювально-ілюстративний (інформаційно-рецептивний) метод, коли викладач подає готові знання (лекції, демонстрації, мультимедійні презентації, схеми, графіки), а здобувачі вищої освіти їх сприймають, осмислюють і запам'ятовують, це забезпечує швидку передачу великого обсягу інформації, систематизує матеріал	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен), курсова робота

		Теорія кіберпростору, кібербезпеки та кіберзахисту (денна форма)	Під час викладання навчальної дисципліни використовуються такі методи навчання: індуктивний, дедуктивний, продуктивний, дослідницький та метод стимулювання. Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить слухачів до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. Продуктивний метод пов'язаний з опануванням нових знань у процесі творчої роботи. Дослідницький метод застосовується для засвоєння досвіду творчої діяльності, глибоких знань. Методи стимулювання спеціально спрямовані на формування позитивних мотивів навчання, стимулюють пізнавальну активність, водночас сприяють збагаченню слухачів новою інформацією. Теоретична підготовка слухачів забезпечується шляхом вивчення вимог керівних документів з питань національної, інформаційної безпеки та кібербезпеки, політико-правових аспектів формування інформаційного суспільства держави, науково-методичних засад державного управління національними інформаційними ресурсами як необхідної складової системи інформаційної безпеки (кібербезпеки). Навчальна діяльність здійснюється шляхом лекційних, семінарських занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій та використанням глобальної мережі.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Методологія наукових досліджень та академічна доброчесність (денна форма)	- використання сучасних наукових технологій навчання (мультимедійні засоби). 1. - діалектичний метод; 2. - емпіричні методи; - теоретичні (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод).	Поточний контроль Модульна контрольна робота Рейтингова система Диференційований залік

			3. - специфічні педагогічні методи та прийоми: ● методи організації навчальної діяльності (словесні, наочні, практичні); ● методи стимулювання і мотивації здобувачів освітнього рівня магістр; ● методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; ● індивідуальний підхід. ● самостійна робота здобувачів освіти.	
		Риторика та стилістика наукових праць (денна форма)	Словесні (лекція, пояснення, розповідь, бесіда), наочні (спостереження, ілюстрація, демонстрація) Словесні (лекція, пояснення, розповідь, бесіда), наочні (спостереження, ілюстрація, демонстрація), практичні (вправи, тестування) інформаційно-рецептивний метод, репродуктивний метод, індуктивний та дедуктивний методи; дискусії; під керівництвом викладача, самостійна робота Інформаційно-рецептивний метод, репродуктивний метод, дискусії, проблемний метод, частково-пошуковий (евристичний) метод, пошуковий (дослідний) метод	Усне опитування, виконання здобувачем освіти вправ на семінарському занятті. Авторський твір до художньо-публіцистичного альманаху «З Батьківщиною в серці» (за бажанням здобувача) Усне опитування, виконання здобувачем освіти вправ на семінарському занятті, завдань для самостійної роботи, модульної контрольної роботи; відповідь здобувача освіти на диференційованому заліку Виконання здобувачем освіти завдань для самостійної роботи, зокрема підготовка та виголошення фахової наукової промови. Участь у мовно-літературних конкурсах та авторський твір до художньо-публіцистичного альманаху «З Батьківщиною в серці» (за бажанням здобувача)
		Теорія прийняття рішень (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на практичних та семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (диференційований залік).
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	☐	Інформаційне протиборство (денна форма)	І. Методи організації та здійснення навчально-пізнавальної діяльності: - методи надання і сприйняття навчальної інформації словесні: лекція (традиційна, проблемна) із застосуванням комп'ютерних інформаційних технологій, семінари, пояснення, розповідь, бесіда; наочні: спостереження, ілюстрація, демонстрація; практичні: міні-дослідження, завдання); - методи передачі і сприйняття навчальної	1. Форми оцінювання поточної роботи: - презентації виконання індивідуальних і групових завдань; - участь у формуванні і підтриманні дискусії; - модерування дискусії на семінарських заняттях; - виконання завдань на практичних заняттях; - виконання індивідуальних додаткових завдань (за власним бажанням). 2. Контрольні заходи: - вирішення тестових завдань; - підготовка рефератів; - виконання модульної

контролюючими органами.			інформації: індуктивні, дедуктивні, аналітичні, синтетичні; - методи розвитку самостійності мислення: репродуктивні, пошукові, дослідницькі; - методи керування навчальною діяльністю: під керівництвом викладача; самостійна робота студентів: з книгою; виконання індивідуальних навчальних проектів. 2. Конкретні методи навчання за ОК та їх зв'язок із забезпеченням результатів навчання: - моделювання проблемних ситуацій професійної сфери різного характеру, що потребують наукового вирішення – реалізується шляхом поєднання методів моделювання, прогнозування та професійної аналітики у вирішенні невизначених задач професійної сфери. 3. Методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності: навчальні дискусії; створення ситуації пізнавальної новизни; створення ситуацій зацікавленості (метод цікавих аналогій тощо).	контрольної роботи; - екзамен.
		Актуальні проблеми інформаційної безпеки (денна форма)	1. Загальні методи організації і здійснення навчально-пізнавальної діяльності: - методи надання і сприйняття навчальної інформації: словесні (лекція, дискусія); наочні (ілюстрація, демонстрація, візуалізація); практичні (міні-дослідження, задачі); - методи логіки сприйняття навчальної інформації: індуктивний; дедуктивний; аналітичний, моделювання, тощо; - методи формування знань: репродуктивний; проблемно-пошуковий; - організаційні методи: навчальна робота під керівництвом викладача; самостійна творчо-пошукова робота з джерельною базою. 2. Конкретні методи навчання за ОК та їх зв'язок із забезпеченням результатів навчання: - міні-досліджень – полягає у стимулювання інтересу до дослідницької діяльності та реалізується шляхом постановки завдань на заняттях і самостійної підготовки через необхідність проведення власного аналізу відповідних джерел інформації в умовах невизначеності та формування варіантів	1. Форми оцінювання поточної роботи: - презентації виконання індивідуальних і групових завдань - участь у формуванні і підтриманні дискусії - моделювання дискусії на семінарських заняттях - виконання завдань на практичних заняттях - виконання індивідуальних додаткових завдань (за власним бажанням) 2. Контрольні заходи: - виконання модульної контрольної роботи - диференційований залік.

			рішень, пояснень, аргументації, узагальнень тощо за законами професійного мислення ; - моделювання проблемних ситуацій професійної сфери різного характеру, що потребують наукового вирішення – реалізується шляхом поєднання методів моделювання, прогнозування та професійної аналітики у вирішенні невизначених задач професійної сфери. Розвиток Soft Skills: - колективна робота малими групами та лідерство – реалізується шляхом групового формування завдань з розподілом ролей і елементами самоорганізації при виконанні і представленні результатів; - створення ситуацій зайнятості і пізнавальної новизни – реалізується шляхом формування атмосфери індивідуального залучення до спроб професійного вирішення актуальних і проблемних задач, формування перспективного та проблемного бачення; - заохочення до самонавчання і дослідницької творчості – реалізується шляхом демонстрації переваг творчого вирішення складних професійних задач, формування професійних пізнавальних і дослідницьких потреб.	
		Методи і моделі протидії кіберзагрозам (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Case-based learning (CBL), коли здобувачі вищої освіти аналізують реальні або симульовані кейси: • витік персональних даних; • зараження мережі шкідливим ПЗ; • вилучення цифрових носіїв у кіберзлочинця; • аналіз цифрових доказів у кримінальних провадженнях. 2) Incident Response Simulations - повноцінне моделювання кіберінциденту з ролями: аналітик безпеки, форензик, архітектор, аудитор, мисливець за загрозами. 3) Практичні роботи з використанням реальних цифрових артефактів: • Аналіз RAM (Volatility, Rekall). • Аналіз диск-іміджів (Autopsy, FTK Imager). • Робота з логами мережевих пристроїв. • Відновлення видалених	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).

			файлів. • Reverse engineering шкідливого ПЗ. 4) CTF-формат (Capture The Flag) з використанням Forensics-категорії: PCAP, диск-іміджі, стеганографія, криптоаналіз, лог-аналіз, тобто використання командних змагань з аналізу цифрових доказів, квести та сценарії для здобуття прапору за правильно виконане завдання на зразок, знайти артефакт; відновити послідовність подій; побудувати лінію часу атаки; підготувати доказову базу.	
		Управління кіберінцидентами (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Навчання на основі реальних кейсів (Case-Based Learning) - метод дозволяє зрозуміти логіку розвитку інцидентів, механізми прийняття рішень та вибір стратегії реагування – здобувачі вищої освіти аналізують реальні або модифіковані інциденти: DDoS на державну установу; компрометація AD; фішингові атаки зі зливом даних; інсайдерська загроза; рансомвер у критичній інфраструктурі; атаки на хмарні сервіси. 2) Tabletop Exercises (TTX) – настільні навчальні сценарії, коли студенти покроково розглядають сценарій кібератаки, реагують на оновлення, обставини та приймають рішення. 3) CTF з акцентом на Incident Response, коли пропонуються ігрові завдання: аналіз PCAP; пошук IoC; аналіз пам'яті; розбір логів (SIEM); побудова таймлайна атаки; визначення TTP за MITRE ATT&CK 4) Об'єднане навчання (Blended Learning) з використанням хмарних платформ та міжмережевої академії Cisco. - під час написання та захисту курсової роботи Collaborative Learning — командне розслідування інциденту 5) Метод критичного аналізу (Critical Thinking Drills), коли здобувачі вищої освіти отримують суперечливі артефакти, неповну інформацію.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Теорія прийняття рішень (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь),	Поточний контроль (усне опитування на практичних та семінарських заняттях; виконання тестових завдань;

			наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (диференційований залік).
		Теорія кіберпростору, кібербезпеки та кіберзахисту (денна форма)	Під час викладання навчальної дисципліни використовуються такі методи навчання: індуктивний, дедуктивний, продуктивний, дослідницький та метод стимулювання. Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить слухачів до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. Продуктивний метод пов'язаний з опануванням нових знань у процесі творчої роботи. Дослідницький метод застосовується для засвоєння досвіду творчої діяльності, глибоких знань. Методи стимулювання спеціально спрямовані на формування позитивних мотивів навчання, стимулюють пізнавальну активність, водночас сприяють збагаченню слухачів новою інформацією. Теоретична підготовка слухачів забезпечується шляхом вивчення вимог керівних документів з питань національної, інформаційної безпеки та кібербезпеки, політико-правових аспектів формування інформаційного суспільства держави, науково-методичних засад державного управління національними інформаційними ресурсами як необхідної складової системи інформаційної безпеки (кібербезпеки). Навчальна діяльність здійснюється шляхом лекційних, семінарських занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій та використанням глобальної мережі.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
ПРН 19. Аналізувати та	☐	Прикладні системи штучного інтелекту в	під час проведення практичних занять	Поточний контроль (усне опитування на практичних

оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.		кіберпросторі (денна форма)	використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Метод критичного аналізу (Critical Thinking Drills), коли здобувачі вищої освіти отримують суперечливі артефакти, неповну інформацію. 2) Project-Based Learning (PBL) — навчання через реальні AI-проєкти – створення здобувачами вищої освіти AI-моделей класифікації наративів; систем виявлення ботів; моделей для аналізу емоцій та семантики тексту; генеративних моделей deepfake-відео; AI-агентів для прогнозування ефективності ІО. 3) Data-Driven Learning із застосуванням OSINT, під час чого здобувачі вищої освіти працюють з відкритими даними соцмереж; Graph API; OSINT-інструментами; ML-моделями для аналізу поширення інформації.	заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Застосування методів і засобів OSINT у Web-середовищі (денна форма)	Під час викладання навчальної дисципліни використовуються словесні, наочні, практичні та самостійні методи, що забезпечують формування результатів навчання . Практичні заняття спрямовані на формування практичних умінь шляхом виконання індивідуальних завдань, аналізу ситуаційних кейсів, опрацювання методів і засобів OSINT та моделювання оперативної обстановки . У процесі навчання застосовуються дидактичні прийоми, орієнтовані на формування аналітичних здібностей, уміння працювати з неповними або суперечливими даними та здатності приймати обґрунтовані рішення. Використовуються сучасні програмні засоби та WEB-ресурси, необхідні для виконання завдань дисципліни.	Для перевірки рівня засвоєння здобувачами вищої освіти знань, умінь та навичок з навчальної дисципліни проводиться оцінювання продовж навчання у вигляді поточного, модульного та підсумкового контролю. Для оцінки використовуються різні види робіт: - поточний контроль засвоєння матеріалу здійснюється шляхом перевірки практичних робіт; - модульний контроль проводиться в формі виконання завдання; - підсумковий контроль забезпечується проведенням диференційованого заліку в формі тесту.
		Управління кіберінцидентами (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Навчання на основі реальних кейсів (Case-Based Learning) - метод дозволяє зрозуміти логіку розвитку інцидентів, механізми прийняття рішень та вибір стратегії реагування – здобувачі вищої освіти аналізують реальні або модифіковані інциденти: DDoS на державну установу; компрометація AD;	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).

			фішингові атаки зі зливом даних; інсайдерська загроза; рансомвер у критичній інфраструктурі; атаки на хмарні сервіси. 2) Tabletop Exercises (TTX) – настільні навчальні сценарії, коли студенти покроково розглядають сценарій кібератаки, реагують на оновлення, обставини та приймають рішення. 3) CTF з акцентом на Incident Response, коли пропонуються ігрові завдання: аналіз PCAP; пошук IoC; аналіз пам'яті; розбір логів (SIEM); побудова таймлайна атаки; визначення TTP за MITRE ATT&CK 4) Об'єднане навчання (Blended Learning) з використанням хмарних платформ та міжмережевої академії Cisco. - під час написання та захисту курсової роботи Collaborative Learning — командне розслідування інциденту 5) Метод критичного аналізу (Critical Thinking Drills), коли здобувачі вищої освіти отримують суперечливі артефакти, неповну інформацію.	
		Аудит інформаційної безпеки та кібербезпеки (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
		Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за	Публічний захист

			ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	
		Методи і моделі протидії кіберзагрозам (денна форма)	- під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Case-based learning (CBL), коли здобувачі вищої освіти аналізують реальні або симульовані кейси: • витік персональних даних; • зараження мережі шкідливим ПЗ; • вилучення цифрових носіїв у кіберзлочинця; • аналіз цифрових доказів у кримінальних провадженнях. 2) Incident Response Simulations - повноцінне моделювання кіберінциденту з ролями: аналітик безпеки, форензик, архітектор, аудитор, мисливець за загрозами. 3) Практичні роботи з використанням реальних цифрових артефактів: • Аналіз RAM (Volatility, Rekall). • Аналіз диск-іміджів (Autopsy, FTK Imager). • Робота з логами мережевих пристроїв. • Відновлення видалених файлів. • Reverse engineering шкідливого ПЗ. 4) CTF-формат (Capture The Flag) з використанням Forensics-категорії: PCAP, диск-іміджі, стеганографія, криптоаналіз, лог-аналіз, тобто використання командних змагань з аналізу цифрових доказів, квести та сценарії для здобуття прапору за правильно виконане завдання на зразок, знайти артефакт; відновити послідовність подій; побудувати лінію часу атаки; підготувати доказову базу.	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Кіберзахист об’єктів критичної інфраструктури (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Case-based learning (CBL), коли здобувачі вищої освіти аналізують реальні або симульовані кейси: • витік персональних даних; • зараження мережі шкідливим ПЗ;	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль

			• вилучення цифрових носіїв у кіберзлочинця; • аналіз цифрових доказів у кримінальних провадженнях. 2) Incident Response Simulations - повноцінне моделювання кіберінциденту з ролями: аналітик безпеки, форензик, архітектор, аудитор, мисливець за загрозами. 3) Практичні роботи з використанням реальних цифрових артефактів: • Аналіз RAM (Volatility, Rekall). • Аналіз диск-іміджів (Autopsy, FTK Imager). • Робота з логами мережевих пристроїв. • Відновлення видалених файлів. • Reverse engineering шкідливого ПЗ. 4) CTF-формат (Capture The Flag) з використанням Forensics-категорії: PCAP, диск-іміджі, стеганографія, криптоаналіз, лог-аналіз, тобто використання командних змагань з аналізу цифрових доказів, квести та сценарії для здобуття прапору за правильно виконане завдання на зразок, знайти артефакт; відновити послідовність подій; побудувати лінію часу атаки; підготувати доказову базу.	(екзамен), курсова робота
ПРН 17. Створювати та документально оформлювати організаційно-технічні та організаційно-правові моделі кіберзахисту, а також моделі захисту конфіденційності, організовувати та розробляти системи кіберзахисту у сфері інформаційних технологій та кіберпростору, здійснювати моніторинг та аудит інформаційної безпеки та кібербезпеки на підприємствах, установах та організаціях різних форм власності.	☐	Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	Публічний захист
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації	Диференційований залік

			теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	
		Методологія наукових досліджень та академічна доброчесність (денна форма)	- використання сучасних наукових технологій навчання (мультимедійні засоби). 1. - діалектичний метод; 2. - емпіричні методи; - теоретичні (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод). 3. - специфічні педагогічні методи та прийоми: ● методи організації навчальної діяльності (словесні, наочні, практичні); ● методи стимулювання і мотивації здобувачів освітнього рівня магістр; ● методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; ● індивідуальний підхід. ● самостійна робота здобувачів освіти.	Поточний контроль Модульна контрольна робота Рейтингова система Диференційований залік
		Теорія кіберпростору, кібербезпеки та кіберзахисту (денна форма)	Під час викладання навчальної дисципліни використовуються такі методи навчання: індуктивний, дедуктивний, продуктивний, дослідницький та метод стимулювання. Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить слухачів до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. Продуктивний метод пов'язаний з опануванням нових знань у процесі творчої роботи. Дослідницький метод застосовується для засвоєння досвіду творчої діяльності, глибоких знань. Методи стимулювання спеціально спрямовані на формування позитивних мотивів навчання, стимулюють пізнавальну активність, водночас сприяють збагаченню слухачів новою інформацією. Теоретична підготовка слухачів забезпечується шляхом вивчення вимог керівних документів з питань національної, інформаційної безпеки та кібербезпеки, політико-правових аспектів	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).

			формування інформаційного суспільства держави, науково-методичних засад державного управління національними інформаційними ресурсами як необхідної складової системи інформаційної безпеки (кібербезпеки). Навчальна діяльність здійснюється шляхом лекційних, семінарських занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій та використанням глобальної мережі.	
		Організаційно-правове забезпечення кіберзахисту (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
ПРН 18. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	☐	Безпека розподілених інформаційних ресурсів та хмарні технології (денна форма)	Під час викладання навчальної дисципліни використовуються такі методи навчання як індуктивний, дедуктивний, продуктивний, дослідницький та метод стимулювання. Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить здобувачів вищої освіти до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. Продуктивний метод пов'язаний з опануванням нових знань у процесі творчої роботи. Дослідницький метод застосовується для засвоєння досвіду творчої діяльності, глибоких знань. Методи стимулювання спеціально спрямовані на формування позитивних мотивів навчання, стимулюють пізнавальну активність, водночас сприяють збагаченню здобувачів вищої освіти новою інформацією. Методи активізації навчального процесу: - мозкові атаки – метод розв'язання невідкладних завдань, сутність якого полягає в тому, щоб висловити якомога більшу кількість ідей за дуже	Поточний контроль Модульна контрольна робота Рейтингова система Екзамен

			обмежений проміжок часу, обговорити і здійснити їх селекцію; - кейс-метод – розгляд, аналіз конкретних ситуацій, який дає змогу наблизити процес навчання до реальної практичної діяльності; - презентації – виступи перед аудиторією, що використовуються для представлення певних досягнень, результатів роботи групи, звіту про виконання індивідуальних завдань тощо	
		Територіальна оборона, мобілізаційна підготовка та мобілізація (денна форма)	Методи навчання: словесні методи (пояснення, інструктаж, розповідь, бесіда, навчальна дискусія), наочні методи (ілюстрування, демонстрування), практичні методи (вправи, практичні роботи), методи наукового пізнання (індукції і дедукції, аналізу, синтезу, порівняння, узагальнення, конкретизації, виділення головного)	Передбачені наступні методи оцінювання: поточні опитування під час проведення семінарських занять; визначення рівня засвоєння отриманих матеріалів та здатності їх застосовувати під час проведення практичних занять, підсумкове оцінювання під час проведення екзамену в усній формі.
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
		Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	Публічний захист
		Застосування методів і засобів OSINT у Web-середовищі (денна форма)	Під час викладання навчальної дисципліни використовуються словесні, наочні, практичні та самостійні методи, що	Для перевірки рівня засвоєння здобувачами вищої освіти знань, умінь та навичок з навчальної дисципліни проводиться

			забезпечують формування результатів навчання . Лекційні заняття застосовуються для систематизованого викладу навчального матеріалу, введення термінології та розкриття теоретичних положень дисципліни. Наочні методи передбачають використання ілюстративних матеріалів і мультимедійних засобів з метою підвищення ефективності сприйняття інформації та демонстрації окремих процесів, пов'язаних із застосуванням OSINT . Самостійна робота здобувачів включає опрацювання літератури, виконання завдань аналітичного характеру, засвоєння інструментів OSINT та розвиток навичок критичного аналізу . У процесі навчання застосовуються дидактичні прийоми, орієнтовані на формування аналітичних здібностей, уміння працювати з неповними або суперечливими даними та здатності приймати обґрунтовані рішення. Використовуються сучасні програмні засоби та WEB-ресурси, необхідні для виконання завдань дисципліни.	оцінювання продовж навчання у вигляді поточного, модульного та підсумкового контролю. Для оцінки використовуються різні види робіт: - поточний контроль засвоєння матеріалу здійснюється шляхом перевірки практичних робіт; - модульний контроль проводиться в формі виконання завдання; - підсумковий контроль забезпечується проведенням диференційованого заліку в формі тесту.
		Теорія прийняття рішень (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на практичних та семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (диференційований залік).
ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.	☒	Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до	Публічний захист

			самостійної професійної діяльності.	
		Організаційно-правове забезпечення кіберзахисту (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Аудит інформаційної безпеки та кібербезпеки (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
		Гендерна політика в системі національної безпеки та оборони України (денна форма)	I. Методи організації та здійснення навчально-пізнавальної діяльності: За джерелом інформації: словесні, наочні, практичні. Словесні методи навчання: лекція, пояснення, розповідь, бесіда, інструктаж. Наочні методи навчання: спостереження, ілюстрація, демонстрація. Практичні методи навчання: практичні заняття, вирішення ситуаційних задач. 2. За логікою передачі і сприймання навчальної інформації: індуктивний метод, дедуктивний метод. Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить здобувачів освіти до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. 3. Методи навчання залежно від типу пізнавальної	Оцінювання навчальних досягнень здобувачів вищої освіти здійснюється на основі поточного, модульного та підсумкового контролю. Поточний контроль проводиться з метою перевірки рівня засвоєння теоретичного матеріалу та сформованості практичних навичок у процесі аудиторної та самостійної роботи. Форми поточного контролю: - усне опитування на семінарських заняттях; - виконання тестових завдань; - аналіз і вирішення практичних (ситуаційних) завдань (кейсів); - участь у дискусіях та круглих столах; Модульний контроль проводиться після завершення кожного змістового модуля з метою узагальнення знань. Формою модульного контролю є модульна контрольна робота, що містить тестові та відкриті питання; Підсумкове оцінювання

			діяльності: інформаційно-рецептивний метод, репродуктивний метод, проблемний метод, частково-пошуковий (евристичний) метод, пошуковий (дослідний) метод. 4. Методи навчання за ступенем керування навчальною діяльністю: під керівництвом викладача, самостійна робота. 5. Методи стимулювання інтересу до навчання і мотивації навчально-пізнавальної діяльності: ділові та рольові ігри, дискусії і диспути. Методи стимулювання обов'язку і відповідальності. Мотиваційна сторона процесу навчання містить три групи мотивів: зовнішній (заохочення та засудження), змагальні (успіх порівняно з кимось або із самим собою), внутрішні (розкриваються як підґрунтя для плідної діяльності).	(диференційований залік) проводиться відповідно до навчального плану і спрямований на перевірку рівня засвоєння здобувачами програмних результатів навчання. Диференційований залік проводиться в усній формі, який включає теоретичні питання та практичні кейси. Оцінювання самостійної роботи Самостійна робота оцінюється за результатами підготовлених рефератів, підготовлених аналітичних записок та презентацій, участі в онлайн-дискусіях, підготовки доповідей або інформаційних повідомлень. Для оцінювання рівня навчальної діяльності здобувачів освіти здійснюється одночасно застосовуються три системи оцінювання: - за національною (4-бальною) шкалою; - 100-бальною шкалою; - шкалою ЄКТС
		Інформаційне протиборство (денна форма)	I. Методи організації та здійснення навчально-пізнавальної діяльності: - методи надання і сприйняття навчальної інформації словесні: лекція (традиційна, проблемна) із застосуванням комп'ютерних інформаційних технологій, семінари, пояснення, розповідь, бесіда; наочні: спостереження, ілюстрація, демонстрація; практичні: міні-дослідження, завдання); - методи передачі і сприйняття навчальної інформації: індуктивні, дедуктивні, аналітичні, синтетичні; - методи розвитку самостійності мислення: репродуктивні, пошукові, дослідницькі; - методи керування навчальною діяльністю: під керівництвом викладача; самостійна робота студентів: з книгою; виконання індивідуальних навчальних проектів. 2. Конкретні методи навчання за ОК та їх зв'язок із забезпеченням результатів навчання: - здійснення досліджень, що реалізується шляхом постановки завдань на заняттях з наступною самостійною підготовкою з проведенням аналізу джерел інформації в умовах невизначеності та формування варіантів рішень, пояснень, аргументації, узагальнень	1. Форми оцінювання поточної роботи: - презентації виконання індивідуальних і групових завдань; - участь у формуванні і підтриманні дискусії; - модерування дискусії на семінарських заняттях; - виконання завдань на практичних заняттях; - виконання індивідуальних додаткових завдань (за власним бажанням). 2. Контрольні заходи: - вирішення тестових завдань; - підготовка рефератів; - виконання модульної контрольної роботи; - екзамен.

			тощо за законами професійного мислення . 3. Методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності: навчальні дискусії; створення ситуації пізнавальної новизни; створення ситуацій зацікавленості (метод цікавих аналогій тощо).	
		Прикладні системи штучного інтелекту в кіберпросторі (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Метод критичного аналізу (Critical Thinking Drills), коли здобувачі вищої освіти отримують суперечливі артефакти, неповну інформацію. 2) Project-Based Learning (PBL) — навчання через реальні AI-проєкти – створення здобувачами вищої освіти AI-моделей класифікації наративів; систем виявлення ботів; моделей для аналізу емоцій та семантики тексту; генеративних моделей deepfake-відео; AI-агентів для прогнозування ефективності ІО. 3) Data-Driven Learning із застосуванням OSINT, під час чого здобувачі вищої освіти працюють з відкритими даними соцмереж; Graph API; OSINT-інструментами; ML-моделями для аналізу поширення інформації.	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Теорія прийняття рішень (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на практичних та семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (диференційований залік).
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.	☐	Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу,	Публічний захист

			аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	
		Інформаційне протиборство (денна форма)	I. Методи організації та здійснення навчально-пізнавальної діяльності: - методи надання і сприйняття навчальної інформації словесні: лекція (традиційна, проблемна) із застосуванням комп'ютерних інформаційних технологій, семінари, пояснення, розповідь, бесіда; наочні: спостереження, ілюстрація, демонстрація; практичні: міні-дослідження, завдання); - методи передачі і сприйняття навчальної інформації: індуктивні, дедуктивні, аналітичні, синтетичні; - методи розвитку самостійності мислення: репродуктивні, пошукові, дослідницькі; - методи керування навчальною діяльністю: під керівництвом викладача; самостійна робота студентів: з книгою; виконання індивідуальних навчальних проектів. 2. Конкретні методи навчання за ОК та їх зв'язок із забезпеченням результатів навчання: - навчально-наукової дискусії та розвитку презентаційних навичок (створення презентації, інфографіки) зі зверненням до науково-доктринальних ідей, концепцій, кращого міжнародного досвіду для обґрунтування власної професійної позиції та висновків ; - моделювання проблемних ситуацій професійної сфери різного характеру, що потребують наукового вирішення – реалізується шляхом поєднання методів моделювання, прогнозування та професійної аналітики у вирішенні невизначених задач професійної сфери ; - інтерактивні методи – аналіз цілей та інструментарію, що використовуються в професійній діяльності на основі наданих матеріалів, повідомлень в медіа, відеосюжетів тощо . 3. Методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності: навчальні дискусії; створення ситуації пізнавальної новизни;	1. Форми оцінювання поточної роботи: - презентації виконання індивідуальних і групових завдань; - участь у формуванні і підтриманні дискусії; - модерування дискусії на семінарських заняттях; - виконання завдань на практичних заняттях; - виконання індивідуальних додаткових завдань (за власним бажанням). 2. Контрольні заходи: - вирішення тестових завдань; - підготовка рефератів; - виконання модульної контрольної роботи; - екзамен.

			створення ситуацій зацікавленості (метод цікавих аналогій тощо).	
		Прикладні системи штучного інтелекту в кіберпросторі (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Метод критичного аналізу (Critical Thinking Drills), коли здобувачі вищої освіти отримують суперечливі артефакти, неповну інформацію. 2) Project-Based Learning (PBL) — навчання через реальні AI-проєкти – створення здобувачами вищої освіти AI-моделей класифікації наративів; систем виявлення ботів; моделей для аналізу емоцій та семантики тексту; генеративних моделей deepfake-відео; AI-агентів для прогнозування ефективності ІО. 3) Data-Driven Learning із застосуванням OSINT, під час чого здобувачі вищої освіти працюють з відкритими даними соцмереж; Graph API; OSINT-інструментами; ML-моделями для аналізу поширення інформації.	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Організаційно-правове забезпечення кіберзахисту (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Актуальні проблеми інформаційної безпеки (денна форма)	1. Загальні методи організації і здійснення навчально-пізнавальної діяльності: - методи надання і сприйняття навчальної інформації: словесні (лекція, дискусія); наочні (ілюстрація, демонстрація, візуалізація); практичні (міні-дослідження, задачі); - методи логіки сприйняття навчальної інформації: індуктивний; дедуктивний; аналітичний, моделювання, тощо; - методи формування знань: репродуктивний; проблемно-пошуковий; - організаційні методи: навчальна робота під керівництвом викладача; самостійна творчо-пошукова робота з джерельною базою. 2. Конкретні методи навчання за ОК та їх зв'язок із забезпеченням результатів навчання:	1. Форми оцінювання поточної роботи: - презентації виконання індивідуальних і групових завдань - участь у формуванні і підтриманні дискусії - моделювання дискусії на семінарських заняттях - виконання завдань на практичних заняттях - виконання індивідуальних додаткових завдань (за власним бажанням) 2. Контрольні заходи: - виконання модульної контрольної роботи - диференційований залік.

			- створення навчально-наукової дискусії – реалізується шляхом формування професійних потреб постійного звернення до науково-доктринальних ідей і концепцій для обґрунтування власної професійної позиції, висновку; - моделювання проблемних ситуацій професійної сфери різного характеру, що потребують наукового вирішення – реалізується шляхом поєднання методів моделювання, прогнозування та професійної аналітики у вирішенні невизначених задач професійної сфери ; - кейс-метод – вирішення комплексних завдань на основі наданих, комплектів матеріалів (зокрема рішень ЄСПЛ), повідомлень в медіа, відеосюжетів тощо . Розвиток Soft Skills: - колективна робота малими групами та лідерство – реалізується шляхом групового формування завдань з розподілом ролей і елементами самоорганізації при виконанні і представленні результатів; - створення ситуацій зайнятості і пізнавальної новизни – реалізується шляхом формування атмосфери індивідуального залучення до спроб професійного вирішення актуальних і проблемних задач, формування перспективного та проблемного бачення; - заохочення до самонавчання і дослідницької творчості – реалізується шляхом демонстрації переваг творчого вирішення складних професійних задач, формування професійних пізнавальних і дослідницьких потреб.	
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
ПРН 3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави	☒	Інформаційне протиборство (денна форма)	І. Методи організації та здійснення навчально-пізнавальної діяльності: - методи надання і сприйняття навчальної	1. Форми оцінювання поточної роботи: - презентації виконання індивідуальних і групових завдань; - участь у формуванні і

(кіберзахист, забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог.			інформації словесні: лекція (традиційна, проблемна) із застосуванням комп'ютерних інформаційних технологій, семінари, пояснення, розповідь, бесіда; наочні: спостереження, ілюстрація, демонстрація; практичні: міні-дослідження, завдання); - методи передачі і сприйняття навчальної інформації: індуктивні, дедуктивні, аналітичні, синтетичні; - методи розвитку самостійності мислення: репродуктивні, пошукові, дослідницькі; - методи керування навчальною діяльністю: під керівництвом викладача; самостійна робота студентів: з книгою; виконання індивідуальних навчальних проектів. 2. Конкретні методи навчання за ОК та їх зв'язок із забезпеченням результатів навчання: - здійснення досліджень, що реалізується шляхом постановки завдань на заняттях з наступною самостійною підготовкою з проведенням аналізу джерел інформації в умовах невизначеності та формування варіантів рішень, пояснень, аргументації, узагальнень тощо за законами професійного мислення ; - моделювання проблемних ситуацій професійної сфери різного характеру, що потребують наукового вирішення – реалізується шляхом поєднання методів моделювання, прогнозування та професійної аналітики у вирішенні невизначених задач професійної сфери ; - інтерактивні методи – аналіз цілей та інструментарію, що використовуються в професійній діяльності на основі наданих матеріалів, повідомлень в медіа, відеосюжетів тощо ; 3. Методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності: навчальні дискусії; створення ситуації пізнавальної новизни; створення ситуацій зацікавленості (метод цікавих аналогій тощо).	підтриманні дискусії; - модерування дискусії на семінарських заняттях; - виконання завдань на практичних заняттях; - виконання індивідуальних додаткових завдань (за власним бажанням). 2. Контрольні заходи: - вирішення тестових завдань; - підготовка рефератів; - виконання модульної контрольної роботи; - екзамен.
		Теорія прийняття рішень (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів	Поточний контроль (усне опитування на практичних та семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у

			навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (диференційований залік).
		Актуальні проблеми інформаційної безпеки (денна форма)	1. Загальні методи організації і здійснення навчально-пізнавальної діяльності: - методи надання і сприйняття навчальної інформації: словесні (лекція, дискусія); наочні (ілюстрація, демонстрація, візуалізація); практичні (міні-дослідження, задачі); - методи логіки сприйняття навчальної інформації: індуктивний; дедуктивний; аналітичний, моделювання, тощо; - методи формування знань: репродуктивний; проблемно-пошуковий; - організаційні методи: навчальна робота під керівництвом викладача; самостійна творчо-пошукова робота з джерельною базою. 2. Конкретні методи навчання за ОК та їх зв'язок із забезпеченням результатів навчання: - моделювання проблемних ситуацій професійної сфери різного характеру, що потребують наукового вирішення – реалізується шляхом поєднання методів моделювання, прогнозування та професійної аналітики у вирішенні невизначених задач професійної сфери ; - кейс-метод – вирішення комплексних завдань на основі наданих, комплектів матеріалів (зокрема рішень ЄСПЛ), повідомлень в медіа, відеосюжетів тощо ; Розвиток Soft Skills: - колективна робота малими групами та лідерство – реалізується шляхом групового формування завдань з розподілом ролей і елементами самоорганізації при виконанні і представленні результатів; - створення ситуацій зайнятості і пізнавальної новизни – реалізується шляхом формування атмосфери індивідуального залучення до спроб професійного вирішення актуальних і проблемних задач, формування перспективного та проблемного бачення; - заохочення до самонавчання і дослідницької творчості – реалізується шляхом демонстрації переваг творчого вирішення складних професійних задач, формування	1. Форми оцінювання поточної роботи: - презентації виконання індивідуальних і групових завдань - участь у формуванні і підтриманні дискусії - моделювання дискусії на семінарських заняттях - виконання завдань на практичних заняттях - виконання індивідуальних додаткових завдань (за власним бажанням) 2. Контрольні заходи: - виконання модульної контрольної роботи - диференційований залік.

			професійних пізнавальних і дослідницьких потреб.	
		Застосування методів і засобів OSINT у Web-середовищі (денна форма)	Під час викладання навчальної дисципліни використовуються словесні, наочні, практичні та самостійні методи, що забезпечують формування результатів навчання : Практичні заняття спрямовані на формування практичних умінь шляхом виконання індивідуальних завдань, аналізу ситуаційних кейсів, опрацювання методів і засобів OSINT та моделювання оперативної обстановки . У процесі навчання застосовуються дидактичні прийоми, орієнтовані на формування аналітичних здібностей, уміння працювати з неповними або суперечливими даними та здатності приймати обґрунтовані рішення. Використовуються сучасні програмні засоби та WEB-ресурси, необхідні для виконання завдань дисципліни.	Для перевірки рівня засвоєння здобувачами вищої освіти знань, умінь та навичок з навчальної дисципліни проводиться оцінювання продовж навчання у вигляді поточного, модульного та підсумкового контролю. Для оцінки використовуються різні види робіт: - поточний контроль засвоєння матеріалу здійснюється шляхом перевірки практичних робіт; - модульний контроль проводиться в формі виконання завдання; - підсумковий контроль забезпечується проведенням диференційованого заліку в формі тесту.
		Методи і моделі протидії кіберзагрозам (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Case-based learning (CBL), коли здобувачі вищої освіти аналізують реальні або симульовані кейси: • витік персональних даних; • зараження мережі шкідливим ПЗ; • вилучення цифрових носіїв у кіберзлочинця; • аналіз цифрових доказів у кримінальних провадженнях. 2) Incident Response Simulations - повноцінне моделювання кіберінциденту з ролями: аналітик безпеки, форензик, архітектор, аудитор, мисливець за загрозами. 3) Практичні роботи з використанням реальних цифрових артефактів: • Аналіз RAM (Volatility, Rekall). • Аналіз диск-іміджів (Autopsy, FTK Imager). • Робота з логами мережевих пристроїв. • Відновлення видалених файлів. • Reverse engineering шкідливого ПЗ. 4) CTF-формат (Capture The Flag) з використанням Forensics-категорії: PCAP, диск-іміджі, стеганографія, криптоаналіз, лог-аналіз, тобто використання командних змагань з аналізу цифрових доказів,	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).

			квести та сценарії для здобуття прапору за правильно виконане завдання на зразок, знайти артефакт; відновити послідовність подій; побудувати лінію часу атаки; підготувати доказову базу.	
		Управління кіберінцидентами (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Навчання на основі реальних кейсів (Case-Based Learning) - метод дозволяє зрозуміти логіку розвитку інцидентів, механізми прийняття рішень та вибір стратегії реагування – здобувачі вищої освіти аналізують реальні або модифіковані інциденти: DDoS на державну установу; компрометація AD; фішингові атаки зі зливом даних; інсайдерська загроза; рансомвер у критичній інфраструктурі; атаки на хмарні сервіси. 2) Tabletop Exercises (TTX) – настільні навчальні сценарії, коли студенти покроково розглядають сценарій кібератаки, реагують на оновлення, обставини та приймають рішення. 3) CTF з акцентом на Incident Response, коли пропонуються ігрові завдання: аналіз PCAP; пошук IoC; аналіз пам'яті; розбір логів (SIEM); побудова таймлайна атаки; визначення TTP за MITRE ATT&CK 4) Об'єднане навчання (Blended Learning) з використанням хмарних платформ та міжмережевої академії Cisco. - під час написання та захисту курсової роботи Collaborative Learning — командне розслідування інциденту 5) Метод критичного аналізу (Critical Thinking Drills), коли здобувачі вищої освіти отримують суперечливі артефакти, неповну інформацію.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Територіальна оборона, мобілізаційна підготовка та мобілізація (денна форма)	Методи навчання: словесні методи (пояснення, інструктаж, розповідь, бесіда, навчальна дискусія), наочні методи (ілюстрування, демонстрування), практичні методи (вправи, практичні роботи), методи наукового пізнання (індукції і дедукції, аналізу, синтезу, порівняння, узагальнення, конкретизації, виділення головного)	Передбачені наступні методи оцінювання: поточні опитування під час проведення семінарських занять; визначення рівня засвоєння отриманих матеріалів та здатності їх застосовувати під час проведення практичних занять, підсумкове оцінювання під час проведення екзамену в усній формі.

		Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	Публічний захист
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
ПРН 4. Організовувати роботу колективу, забезпечувати професійний розвиток його членів та досягнення поставлених цілей.	☒	Аудит інформаційної безпеки та кібербезпеки (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Гендерна політика в системі національної безпеки та оборони України (денна форма)	І. Методи організації та здійснення навчально-пізнавальної діяльності: За джерелом інформації: словесні, наочні, практичні. Словесні методи навчання: лекція, пояснення, розповідь, бесіда, інструктаж. Наочні методи навчання: спостереження, ілюстрація, демонстрація. Практичні методи навчання: практичні заняття, вирішення ситуаційних задач. 2. За логікою передачі і сприймання навчальної інформації: індуктивний метод, дедуктивний метод. Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить здобувачів освіти до узагальнень, визначення	Оцінювання навчальних досягнень здобувачів вищої освіти здійснюється на основі поточного, модульного та підсумкового контролю. Поточний контроль проводиться з метою перевірки рівня засвоєння теоретичного матеріалу та сформованості практичних навичок у процесі аудиторної та самостійної роботи. Форми поточного контролю: - усне опитування на семінарських заняттях; - виконання тестових завдань; - аналіз і вирішення практичних (ситуаційних) завдань (кейсів); - участь у дискусіях та круглих столах; Модульний контроль

			понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. 3. Методи навчання залежно від типу пізнавальної діяльності: інформаційно-рецептивний метод, репродуктивний метод, проблемний метод, частково-пошуковий (евристичний) метод, пошуковий (дослідний) метод. 4. Методи навчання за ступенем керування навчальною діяльністю: під керівництвом викладача, самостійна робота. 5. Методи стимулювання інтересу до навчання і мотивації навчально-пізнавальної діяльності: ділові та рольові ігри, дискусії і диспути. Методи стимулювання обов'язку і відповідальності. Мотиваційна сторона процесу навчання містить три групи мотивів: зовнішній (заохочення та засудження), змагальні (успіх порівняно з кимось або із самим собою), внутрішні (розкриваються як підґрунтя для плідної діяльності).	проводиться після завершення кожного змістового модуля з метою узагальнення знань. Формою модульного контролю є модульна контрольна робота, що містить тестові та відкриті питання; Підсумкове оцінювання (диференційований залік) проводиться відповідно до навчального плану і спрямований на перевірку рівня засвоєння здобувачами програмних результатів навчання. Диференційований залік проводиться в усній формі, який включає теоретичні питання та практичні кейси. Оцінювання самостійної роботи Самостійна робота оцінюється за результатами підготовлених рефератів, підготовлених аналітичних записок та презентацій, участі в онлайн-дискусіях, підготовки доповідей або інформаційних повідомлень. Для оцінювання рівня навчальної діяльності здобувачів освіти здійснюється одночасно застосовуються три системи оцінювання: - за національною (4-бальною) шкалою; - 100-бальною шкалою; - шкалою ЄКТС
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
		Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти	Публічний захист

			підтвердять готовність до самостійної професійної діяльності.	
		Теорія прийняття рішень (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії	Поточний контроль (усне опитування на практичних та семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (диференційований залік).
ПРН 13. Організовувати та здійснювати керівництво територіальною обороною, мобілізаційною підготовкою та мобілізацією у межах професійної компетентності.	☒	Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	Публічний захист
		Інформаційне протиборство (денна форма)	I. Методи організації та здійснення навчально-пізнавальної діяльності: - методи надання і сприйняття навчальної інформації словесні: лекція (традиційна, проблемна) із застосуванням комп'ютерних інформаційних технологій, семінари, пояснення, розповідь, бесіда; наочні: спостереження, ілюстрація, демонстрація; практичні: міні-дослідження, завдання); - методи передачі і сприйняття навчальної інформації: індуктивні, дедуктивні, аналітичні, синтетичні; - методи розвитку самостійності мислення: репродуктивні, пошукові, дослідницькі; - методи керування навчальною діяльністю: під керівництвом викладача; самостійна робота студентів: з книгою; виконання індивідуальних навчальних проектів. 2. Методи стимулювання	1. Форми оцінювання поточної роботи: - презентації виконання індивідуальних і групових завдань; - участь у формуванні і підтриманні дискусії; - модерування дискусії на семінарських заняттях; - виконання завдань на практичних заняттях; - виконання індивідуальних додаткових завдань (за власним бажанням). 2. Контрольні заходи: - вирішення тестових завдань; - підготовка рефератів; - виконання модульної контрольної роботи; - екзамен.

			інтересу до навчання і мотивації до навчально-пізнавальної діяльності: навчальні дискусії; створення ситуації пізнавальної новизни; створення ситуацій зацікавленості (метод цікавих аналогій тощо).	
		Територіальна оборона, мобілізаційна підготовка та мобілізація (денна форма)	Методи навчання: словесні методи (пояснення, інструктаж, розповідь, бесіда, навчальна дискусія), наочні методи (ілюстрування, демонстрування), практичні методи (вправи, практичні роботи), методи наукового пізнання (індукції і дедукції, аналізу, синтезу, порівняння, узагальнення, конкретизації, виділення головного)	Передбачені наступні методи оцінювання: поточні опитування під час проведення семінарських занять; визначення рівня засвоєння отриманих матеріалів та здатності їх застосовувати під час проведення практичних занять, підсумкове оцінювання під час проведення екзамену в усній формі.
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
ПРН 5. Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів.	☒	Методологія наукових досліджень та академічна доброчесність (денна форма)	- використання сучасних наукових технологій навчання (мультимедійні засоби). 1. - діалектичний метод; 2. - емпіричні методи; - теоретичні (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод). 3. - специфічні педагогічні методи та прийоми: ● методи організації навчальної діяльності (словесні, наочні, практичні); ● методи стимулювання і мотивації здобувачів освітнього рівня магістр; ● методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; ● індивідуальний підхід. ● самостійна робота здобувачів освіти.	Поточний контроль Модульна контрольна робота Рейтингова система Диференційований залік
		Іноземна мова професійного спрямування (денна форма)	Традиційні методи навчання: ● словесні методи: розповідь (монологічний), бесіда (діалогічний), синтезуючі або закріплюючі і контрольно-коректуючи; ● наочні методи (демонстрація); ● практичні методи: виконання усних і письмових вправ;	Результати навчання здобувача вищої освіти з навчальної дисципліни оцінюються за 100-бальною шкалою як сума балів поточного та підсумкового контролю. Поточний контроль передбачає перевірку набутих знань і навичок з різних видів мовленнєвої діяльності (читання,

			● робота з різними джерелами інформації (підручник, статті, словники); ● відео метод (наочне сприйняття інформації). ● індуктивний метод; ● дедуктивний метод; ● репродуктивний метод (відтворення готових зразків); ● частково-пошуковий (евристичний) метод; ● самостійна робота здобувачів; ● спеціальні методи – використання ситуативних та рольових ігор за темами модулів. Інноваційні методи навчання інтерактивна діяльність (парна, групова і робота в команді) з використанням сучасних методів організації роботи на занятті. мультимедійний супровід практичних занять.	аудіювання, говоріння, письмо), під час аудиторних занять, а також перевірку завдань для самостійної роботи і творчих завдань/проектів. Оцінювання здобувача вищої освіти під час поточного контролю здійснюється відповідно до норм кредитно-модульної системи, а також згідно з критеріями оцінювання різних видів навчальної діяльності.
		Інформаційне протиборство (денна форма)	I. Методи організації та здійснення навчально-пізнавальної діяльності: - методи надання і сприйняття навчальної інформації словесні: лекція (традиційна, проблемна) із застосуванням комп'ютерних інформаційних технологій, семінари, пояснення, розповідь, бесіда; наочні: спостереження, ілюстрація, демонстрація; практичні: міні-дослідження, завдання); - методи передачі і сприйняття навчальної інформації: індуктивні, дедуктивні, аналітичні, синтетичні; - методи розвитку самостійності мислення: репродуктивні, пошукові, дослідницькі; - методи керування навчальною діяльністю: під керівництвом викладача; самостійна робота студентів: з книгою; виконання індивідуальних навчальних проектів. 2. Конкретні методи навчання за ОК та їх зв'язок із забезпеченням результатів навчання: - здійснення досліджень, що реалізується шляхом постановки завдань на заняттях з наступною самостійною підготовкою з проведенням аналізу джерел інформації в умовах невизначеності та формування варіантів рішень, пояснень, аргументації, узагальнень тощо за законами професійного мислення ; - навчально-наукової дискусії та розвитку	1. Форми оцінювання поточної роботи: - презентації виконання індивідуальних і групових завдань; - участь у формуванні і підтриманні дискусії; - модерування дискусії на семінарських заняттях; - виконання завдань на практичних заняттях; - виконання індивідуальних додаткових завдань (за власним бажанням). 2. Контрольні заходи: - вирішення тестових завдань; - підготовка рефератів; - виконання модульної контрольної роботи; - екзамен.

			презентаційних навичок (створення презентації, інфографіки) зі зверненням до науково-доктринальних ідей, концепцій, кращого міжнародного досвіду для обґрунтування власної професійної позиції та висновків ; 3. Методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності: навчальні дискусії; створення ситуації пізнавальної новизни; створення ситуацій зацікавленості (метод цікавих аналогій тощо).	
		Організаційно-правове забезпечення кіберзахисту (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Актуальні проблеми інформаційної безпеки (денна форма)	1. Загальні методи організації і здійснення навчально-пізнавальної діяльності: - методи надання і сприйняття навчальної інформації: словесні (лекція, дискусія); наочні (ілюстрація, демонстрація, візуалізація); практичні (міні-дослідження, задачі); - методи логіки сприйняття навчальної інформації: індуктивний; дедуктивний; аналітичний, моделювання, тощо; - методи формування знань: репродуктивний; проблемно-пошуковий; - організаційні методи: навчальна робота під керівництвом викладача; самостійна творчо-пошукова робота з джерельною базою. 2. Конкретні методи навчання за ОК та їх зв'язок із забезпеченням результатів навчання: - міні-досліджень – полягає у стимулювання інтересу до дослідницької діяльності та реалізується шляхом постановки завдань на заняттях і самостійної підготовки через необхідність проведення власного аналізу відповідних джерел інформації в умовах невизначеності та формування варіантів рішень, пояснень, аргументації, узагальнень тощо за законами професійного мислення ; - створення навчально-наукової дискусії –	1. Форми оцінювання поточної роботи: - презентації виконання індивідуальних і групових завдань - участь у формуванні і підтриманні дискусії - моделювання дискусії на семінарських заняттях - виконання завдань на практичних заняттях - виконання індивідуальних додаткових завдань (за власним бажанням) 2. Контрольні заходи: - виконання модульної контрольної роботи - диференційований залік.

			реалізується шляхом формування професійних потреб постійного звернення до науково-доктринальних ідей і концепцій для обґрунтування власної професійної позиції, висновку ; - створення презентації, інфографіки – реалізується постійно присутній елемент/вимога при виконанні індивідуальних і колективних завдань з результатом, який передбачає демонстрацію/представлення для колег; Розвиток Soft Skills: - колективна робота малими групами та лідерство – реалізується шляхом групового формування завдань з розподілом ролей і елементами самоорганізації при виконанні і представленні результатів; - створення ситуацій зайнятості і пізнавальної новизни – реалізується шляхом формування атмосфери індивідуального залучення до спроб професійного вирішення актуальних і проблемних задач, формування перспективного та проблемного бачення; - заохочення до самонавчання і дослідницької творчості – реалізується шляхом демонстрації переваг творчого вирішення складних професійних задач, формування професійних пізнавальних і дослідницьких потреб.	
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
		Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності;	Публічний захист

			самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	
ПРН 8. Забезпечувати дотримання принципу гендерної рівності під час здійснення професійної діяльності.	☒	Гендерна політика в системі національної безпеки та оборони України (денна форма)	І. Методи організації та здійснення навчально-пізнавальної діяльності: За джерелом інформації: словесні, наочні, практичні. Словесні методи навчання: лекція, пояснення, розповідь, бесіда, інструктаж. Наочні методи навчання: спостереження, ілюстрація, демонстрація. Практичні методи навчання: практичні заняття, вирішення ситуаційних задач. 2. За логікою передачі і сприймання навчальної інформації: індуктивний метод, дедуктивний метод. Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить здобувачів освіти до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. 3. Методи навчання залежно від типу пізнавальної діяльності: інформаційно-рецептивний метод, репродуктивний метод, проблемний метод, частково-пошуковий (евристичний) метод, пошуковий (дослідний) метод. 4. Методи навчання за ступенем керування навчальною діяльністю: під керівництвом викладача, самостійна робота. 5. Методи стимулювання інтересу до навчання і мотивації навчально-пізнавальної діяльності: ділові та рольові ігри, дискусії і диспути. Методи стимулювання обов'язку і відповідальності. Мотиваційна сторона процесу навчання містить три групи мотивів: зовнішній (заохочення та засудження), змагальні (успіх порівняно з кимось або із самим собою), внутрішні (розкриваються як підґрунтя для плідної діяльності).	Оцінювання навчальних досягнень здобувачів вищої освіти здійснюється на основі поточного, модульного та підсумкового контролю. Поточний контроль проводиться з метою перевірки рівня засвоєння теоретичного матеріалу та сформованості практичних навичок у процесі аудиторної та самостійної роботи. Форми поточного контролю: - усне опитування на семінарських заняттях; - виконання тестових завдань; - аналіз і вирішення практичних (ситуаційних) завдань (кейсів); - участь у дискусіях та круглих столах; Модульний контроль проводиться після завершення кожного змістового модуля з метою узагальнення знань. Формою модульного контролю є модульна контрольна робота, що містить тестові та відкриті питання; Підсумкове оцінювання (диференційований залік) проводиться відповідно до навчального плану і спрямований на перевірку рівня засвоєння здобувачами програмних результатів навчання. Диференційований залік проводиться в усній формі, який включає теоретичні питання та практичні кейси. Оцінювання самостійної роботи Самостійна робота оцінюється за результатами підготовлених рефератів, підготовлених аналітичних записок та презентацій, участі в онлайн-дискусіях, підготовки доповідей або інформаційних повідомлень. Для оцінювання рівня навчальної діяльності здобувачів освіти здійснюється одночасно застосовуються три системи оцінювання: - за національною (4-бальною) шкалою; - 100-бальною шкалою; - шкалою ЄКТС
		Інформаційне	І. Методи організації та	1. Форми оцінювання

		протиборство (денна форма)	здійснення навчально-пізнавальної діяльності: - методи надання і сприйняття навчальної інформації словесні: лекція (традиційна, проблемна) із застосуванням комп'ютерних інформаційних технологій, семінари, пояснення, розповідь, бесіда; наочні: спостереження, ілюстрація, демонстрація; практичні: міні-дослідження, завдання); - методи передачі і сприйняття навчальної інформації: індуктивні, дедуктивні, аналітичні, синтетичні; - методи розвитку самостійності мислення: репродуктивні, пошукові, дослідницькі; - методи керування навчальною діяльністю: під керівництвом викладача; самостійна робота студентів: з книгою; виконання індивідуальних навчальних проектів. 2. Конкретні методи навчання за ОК та їх зв'язок із забезпеченням результатів навчання: - навчально-наукової дискусії та розвитку презентаційних навичок (створення презентації, інфографіки) зі зверненням до науково-доктринальних ідей, концепцій, кращого міжнародного досвіду для обґрунтування власної професійної позиції та висновків. 3. Методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності: навчальні дискусії; створення ситуації пізнавальної новизни; створення ситуацій зацікавленості (метод цікавих аналогій тощо).	поточної роботи: - презентації виконання індивідуальних і групових завдань; - участь у формуванні і підтриманні дискусії; - модерування дискусії на семінарських заняттях; - виконання завдань на практичних заняттях; - виконання індивідуальних додаткових завдань (за власним бажанням). 2. Контрольні заходи: - вирішення тестових завдань; - підготовка рефератів; - виконання модульної контрольної роботи; - екзамен.
ПРН 25. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.	☐	Організаційно-правове забезпечення кіберзахисту (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Аудит інформаційної безпеки та кібербезпеки (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна

			формування пізнавального інтересу як навчальні дискусії.	робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
		Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	Публічний захист
		Теорія кіберпростору, кібербезпеки та кіберзахисту (денна форма)	Під час викладання навчальної дисципліни використовуються такі методи навчання: індуктивний, дедуктивний, продуктивний, дослідницький та метод стимулювання. Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить слухачів до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. Продуктивний метод пов'язаний з опануванням нових знань у процесі творчої роботи. Дослідницький метод застосовується для засвоєння досвіду творчої діяльності, глибоких знань. Методи стимулювання спеціально спрямовані на формування позитивних	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).

			мотивів навчання, стимулюють пізнавальну активність, водночас сприяють збагаченню слухачів новою інформацією. Теоретична підготовка слухачів забезпечується шляхом вивчення вимог керівних документів з питань національної, інформаційної безпеки та кібербезпеки, політико-правових аспектів формування інформаційного суспільства держави, науково-методичних засад державного управління національними інформаційними ресурсами як необхідної складової системи інформаційної безпеки (кібербезпеки). Навчальна діяльність здійснюється шляхом лекційних, семінарських занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій та використанням глобальної мережі.	
ПРН 9. Синтезувати спектр заходів та підходів, що можуть використовуватись для вирішення проблем, пов'язаних з викликами глобальній, європейській та регіональній безпеці.	☒	Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
		Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	Публічний захист
		Безпека розподілених інформаційних ресурсів та хмарні технології (денна форма)	Під час викладання навчальної дисципліни використовуються такі методи навчання як індуктивний, дедуктивний,	Поточний контроль Модульна контрольна робота Рейтингова система Екзамен

			продуктивний, дослідницький та метод стимулювання. Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить здобувачів вищої освіти до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. Продуктивний метод пов'язаний з опануванням нових знань у процесі творчої роботи. Дослідницький метод застосовується для засвоєння досвіду творчої діяльності, глибоких знань. Методи стимулювання спеціально спрямовані на формування позитивних мотивів навчання, стимулюють пізнавальну активність, водночас сприяють збагаченню здобувачів вищої освіти новою інформацією. Методи активізації навчального процесу: - мозкові атаки – метод розв'язання невідкладних завдань, сутність якого полягає в тому, щоб висловити якомога більшу кількість ідей за дуже обмежений проміжок часу, обговорити і здійснити їх селекцію; - кейс-метод – розгляд, аналіз конкретних ситуацій, який дає змогу наблизити процес навчання до реальної практичної діяльності; - презентації – виступи перед аудиторією, що використовуються для представлення певних досягнень, результатів роботи групи, звіту про виконання індивідуальних завдань тощо	
		Організаційно-правове забезпечення кіберзахисту (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави	☒	Теорія кіберпростору, кібербезпеки та кіберзахисту (денна форма)	Під час викладання навчальної дисципліни використовуються такі методи навчання: індуктивний, дедуктивний, продуктивний, дослідницький та метод	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях,

(за сферами забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері).			стимулювання. Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить слухачів до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. Продуктивний метод пов'язаний з опануванням нових знань у процесі творчої роботи. Дослідницький метод застосовується для засвоєння досвіду творчої діяльності, глибоких знань. Методи стимулювання спеціально спрямовані на формування позитивних мотивів навчання, стимулюють пізнавальну активність, водночас сприяють збагаченню слухачів новою інформацією. Теоретична підготовка слухачів забезпечується шляхом вивчення вимог керівних документів з питань національної, інформаційної безпеки та кібербезпеки, політико-правових аспектів формування інформаційного суспільства держави, науково-методичних засад державного управління національними інформаційними ресурсами як необхідної складової системи інформаційної безпеки (кібербезпеки). Навчальна діяльність здійснюється шляхом лекційних, семінарських занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій та використанням глобальної мережі.	модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Прикладні системи штучного інтелекту в кіберпросторі (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Метод критичного аналізу (Critical Thinking Drills), коли здобувачі вищої освіти отримують суперечливі артефакти, неповну інформацію. 2) Project-Based Learning (PBL) — навчання через реальні AI-проєкти – створення здобувачами вищої освіти AI-моделей класифікації наративів; систем виявлення ботів; моделей для аналізу емоцій та семантики тексту;	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).

			генеративних моделей deepfake-відео; AI-агентів для прогнозування ефективності ІО. 3) Data-Driven Learning із застосуванням OSINT, під час чого здобувачі вищої освіти працюють з відкритими даними соцмереж; Graph API; OSINT-інструментами; ML-моделями для аналізу поширення інформації.	
		Організаційно-правове забезпечення кіберзахисту (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Територіальна оборона, мобілізаційна підготовка та мобілізація (денна форма)	Методи навчання: словесні методи (пояснення, інструктаж, розповідь, бесіда, навчальна дискусія), наочні методи (ілюстрування, демонстрування), практичні методи (вправи, практичні роботи), методи наукового пізнання (індукції і дедукції, аналізу, синтезу, порівняння, узагальнення, конкретизації, виділення головного)	Передбачені наступні методи оцінювання: поточні опитування під час проведення семінарських занять; визначення рівня засвоєння отриманих матеріалів та здатності їх застосовувати під час проведення практичних занять, підсумкове оцінювання під час проведення екзамену в усній формі.
		Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	Публічний захист
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які	Диференційований залік

			сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	
ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.	☒	Теорія прийняття рішень (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на практичних та семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (диференційований залік).
		Теорія кіберпростору, кібербезпеки та кіберзахисту (денна форма)	Під час викладання навчальної дисципліни використовуються такі методи навчання: індуктивний, дедуктивний, продуктивний, дослідницький та метод стимулювання. Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить слухачів до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. Продуктивний метод пов'язаний з опануванням нових знань у процесі творчої роботи. Дослідницький метод застосовується для засвоєння досвіду творчої діяльності, глибоких знань. Методи стимулювання спеціально спрямовані на формування позитивних мотивів навчання, стимулюють пізнавальну активність, водночас сприяють збагаченню слухачів новою інформацією. Теоретична підготовка слухачів забезпечується шляхом вивчення вимог керівних документів з питань національної, інформаційної безпеки та кібербезпеки, політико-правових аспектів формування інформаційного суспільства держави, науково-методичних засад державного управління національними інформаційними ресурсами як необхідної складової системи інформаційної безпеки (кібербезпеки). Навчальна діяльність здійснюється шляхом лекційних, семінарських	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).

			занять та самостійної підготовки з використанням технічних засобів та інформаційних технологій та використанням глобальної мережі.	
		Організаційно-правове забезпечення кіберзахисту (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Актуальні проблеми інформаційної безпеки (денна форма)	1. Загальні методи організації і здійснення навчально-пізнавальної діяльності: - методи надання і сприйняття навчальної інформації: словесні (лекція, дискусія); наочні (ілюстрація, демонстрація, візуалізація); практичні (міні-дослідження, задачі); - методи логіки сприйняття навчальної інформації: індуктивний; дедуктивний; аналітичний, моделювання, тощо; - методи формування знань: репродуктивний; проблемно-пошуковий; - організаційні методи: навчальна робота під керівництвом викладача; самостійна творчо-пошукова робота з джерельною базою. 2. Конкретні методи навчання за ОК та їх зв'язок із забезпеченням результатів навчання: - міні-досліджень – полягає у стимулювання інтересу до дослідницької діяльності та реалізується шляхом постановки завдань на заняттях і самостійної підготовки через необхідність проведення власного аналізу відповідних джерел інформації в умовах невизначеності та формування варіантів рішень, пояснень, аргументації, узагальнень тощо за законами професійного мислення ; - створення навчально-наукової дискусії – реалізується шляхом формування професійних потреб постійного звернення до науково-доктринальних ідей і концепцій для обґрунтування власної професійної позиції, висновку ; - моделювання проблемних ситуацій професійної сфери різного характеру, що потребують наукового вирішення – реалізується	1. Форми оцінювання поточної роботи: - презентації виконання індивідуальних і групових завдань - участь у формуванні і підтриманні дискусії - моделювання дискусії на семінарських заняттях - виконання завдань на практичних заняттях - виконання індивідуальних додаткових завдань (за власним бажанням) 2. Контрольні заходи: - виконання модульної контрольної роботи - диференційований залік.

			шляхом поєднання методів моделювання, прогнозування та професійної аналітики у вирішенні невизначених задач професійної сфери ; - кейс-метод – вирішення комплексних завдань на основі наданих, комплектів матеріалів (зокрема рішень ЄСПЛ), повідомлень в медіа, відеосюжетів тощо ; Розвиток Soft Skills: - колективна робота малими групами та лідерство – реалізується шляхом групового формування завдань з розподілом ролей і елементами самоорганізації при виконанні і представленні результатів; - створення ситуацій зайнятості і пізнавальної новизни – реалізується шляхом формування атмосфери індивідуального залучення до спроб професійного вирішення актуальних і проблемних задач, формування перспективного та проблемного бачення; - заохочення до самонавчання і дослідницької творчості – реалізується шляхом демонстрації переваг творчого вирішення складних професійних задач, формування професійних пізнавальних і дослідницьких потреб.	
		Застосування методів і засобів OSINT у Web-середовищі (денна форма)	Під час викладання навчальної дисципліни використовуються словесні, наочні, практичні та самостійні методи, що забезпечують формування результатів навчання. Лекційні заняття застосовуються для систематизованого викладу навчального матеріалу, введення термінології та розкриття теоретичних положень дисципліни. Наочні методи передбачають використання ілюстративних матеріалів і мультимедійних засобів з метою підвищення ефективності сприйняття інформації та демонстрації окремих процесів, пов'язаних із застосуванням OSINT . У процесі навчання застосовуються дидактичні прийоми, орієнтовані на формування аналітичних здібностей, уміння працювати з неповними або суперечливими даними та здатності приймати обґрунтовані рішення. Використовуються сучасні програмні засоби та WEB-ресурси, необхідні для виконання завдань	Для перевірки рівня засвоєння здобувачами вищої освіти знань, умінь та навичок з навчальної дисципліни проводиться оцінювання продовж навчання у вигляді поточного, модульного та підсумкового контролю. Для оцінки використовуються різні види робіт: - поточний контроль засвоєння матеріалу здійснюється шляхом перевірки практичних робіт; - модульний контроль проводиться в формі виконання завдання; - підсумковий контроль забезпечується проведенням диференційованого заліку в формі тесту.

			дисципліни.	
		Методи і моделі протидії кіберзагрозам (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Case-based learning (CBL), коли здобувачі вищої освіти аналізують реальні або симульовані кейси: • витік персональних даних; • зараження мережі шкідливим ПЗ; • вилучення цифрових носіїв у кіберзлочинця; • аналіз цифрових доказів у кримінальних провадженнях. 2) Incident Response Simulations - повноцінне моделювання кіберінциденту з ролями: аналітик безпеки, форензик, архітектор, аудитор, мисливець за загрозами. 3) Практичні роботи з використанням реальних цифрових артефактів: • Аналіз RAM (Volatility, Rekall). • Аналіз диск-іміджів (Autopsy, FTK Imager). • Робота з логами мережевих пристроїв. • Відновлення видалених файлів. • Reverse engineering шкідливого ПЗ. 4) CTF-формат (Capture The Flag) з використанням Forensics-категорії: PCAP, диск-іміджі, стеганографія, криптоаналіз, лог-аналіз, тобто використання командних змагань з аналізу цифрових доказів, квести та сценарії для здобуття прапору за правильно виконане завдання на зразок, знайти артефакт; відновити послідовність подій; побудувати лінію часу атаки; підготувати доказову базу.	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Кіберзахист об’єктів критичної інфраструктури (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Case-based learning (CBL), коли здобувачі вищої освіти аналізують реальні або симульовані кейси: • витік персональних даних; • зараження мережі шкідливим ПЗ; • вилучення цифрових носіїв у кіберзлочинця; • аналіз цифрових доказів у кримінальних провадженнях. 2) Incident Response Simulations - повноцінне моделювання кіберінциденту з ролями: аналітик безпеки, форензик, архітектор, аудитор, мисливець за загрозами.	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен), курсова робота

			3) Практичні роботи з використанням реальних цифрових артефактів: • Аналіз RAM (Volatility, Rekall). • Аналіз диск-іміджів (Autopsy, FTK Imager). • Робота з логами мережевих пристроїв. • Відновлення видалених файлів. • Reverse engineering шкідливого ПЗ. 4) CTF-формат (Capture The Flag) з використанням Forensics-категорії: PCAP, диск-іміджі, стеганографія, криптоаналіз, лог-аналіз, тобто використання командних змагань з аналізу цифрових доказів, квести та сценарії для здобуття прапору за правильно виконане завдання на зразок, знайти артефакт; відновити послідовність подій; побудувати лінію часу атаки; підготувати доказову базу.	
		Управління кіберінцидентами (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Навчання на основі реальних кейсів (Case-Based Learning) - метод дозволяє зрозуміти логіку розвитку інцидентів, механізми прийняття рішень та вибір стратегії реагування – здобувачі вищої освіти аналізують реальні або модифіковані інциденти: DDoS на державну установу; компрометація AD; фішингові атаки зі зливом даних; інсайдерська загроза; рансомвер у критичній інфраструктурі; атаки на хмарні сервіси. 2) Tabletop Exercises (TTX) – настільні навчальні сценарії, коли студенти покроково розглядають сценарій кібератаки, реагують на оновлення, обставини та приймають рішення. 3) CTF з акцентом на Incident Response, коли пропонуються ігрові завдання: аналіз PCAP; пошук IoC; аналіз пам'яті; розбір логів (SIEM); побудова таймлайна атаки; визначення TTP за MITRE ATT&CK 4) Об'єднане навчання (Blended Learning) з використанням хмарних платформ та міжмережевої академії Cisco. - під час написання та захисту курсової роботи Collaborative Learning — командне розслідування інциденту 5) Метод критичного аналізу (Critical Thinking Drills),	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).

			коли здобувачі вищої освіти отримують суперечливі артефакти, неповну інформацію.	
		Аудит інформаційної безпеки та кібербезпеки (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Безпека розподілених інформаційних ресурсів та хмарні технології (денна форма)	Під час викладання навчальної дисципліни використовуються такі методи навчання як індуктивний, дедуктивний, продуктивний, дослідницький та метод стимулювання. Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить здобувачів вищої освіти до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. Продуктивний метод пов'язаний з опануванням нових знань у процесі творчої роботи. Дослідницький метод застосовується для засвоєння досвіду творчої діяльності, глибоких знань. Методи стимулювання спеціально спрямовані на формування позитивних мотивів навчання, стимулюють пізнавальну активність, водночас сприяють збагаченню здобувачів вищої освіти новою інформацією. Методи активізації навчального процесу: - мозкові атаки – метод розв'язання невідкладних завдань, сутність якого полягає в тому, щоб висловити якомога більшу кількість ідей за дуже обмежений проміжок часу, обговорити і здійснити їх селекцію; - кейс-метод – розгляд, аналіз конкретних ситуацій, який дає змогу наблизити процес навчання до реальної практичної діяльності; - презентації – виступи перед аудиторією, що використовуються для представлення певних досягнень, результатів роботи групи, звіту про виконання індивідуальних	Поточний контроль Модульна контрольна робота Рейтингова система Екзамен

			завдань тощо	
		Методологія наукових досліджень та академічна доброчесність (денна форма)	- використання сучасних наукових технологій навчання (мультимедійні засоби). 1. - діалектичний метод; 2. - емпіричні методи; - теоретичні (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод). 3. - специфічні педагогічні методи та прийоми: ● методи організації навчальної діяльності (словесні, наочні, практичні); ● методи стимулювання і мотивації здобувачів освітнього рівня магістр; ● методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; ● індивідуальний підхід. ● самостійна робота здобувачів освіти.	Поточний контроль Модульна контрольна робота Рейтингова система Диференційований залік
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
		Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	Публічний захист
ПРН 6. Вільно спілкуватися державною та іноземною мовами усно і письмово для обговорення професійної	☒	Іноземна мова професійного спрямування (денна форма)	Традиційні методи навчання: ● словесні методи: розповідь (монологічний), бесіда (діалогічний), синтезуючі або закріплюючі і контрольно-коректуючи;	Результати навчання здобувача вищої освіти з навчальної дисципліни оцінюються за 100-бальною шкалою як сума балів поточного та підсумкового контролю.

діяльності, результатів досліджень та інновацій, пошуку та аналізу відповідної інформації.			● наочні методи (демонстрація); ● практичні методи: виконання усних і письмових вправ; ● робота з різними джерелами інформації (підручник, статті, словники); ● відео метод (наочне сприйняття інформації). ● індуктивний метод; ● дедуктивний метод; ● репродуктивний метод (відтворення готових зразків); ● частково-пошуковий (евристичний) метод; ● самостійна робота здобувачів; ● спеціальні методи – використання ситуативних та рольових ігор за темами модулів. Інноваційні методи навчання - інтерактивна діяльність (парна, групова і робота в команді) з використанням сучасних методів організації роботи на занятті. - мультимедійний супровід практичних занять.	Поточний контроль передбачає перевірку набутих знань і навичок з різних видів мовленнєвої діяльності (читання, аудіювання, говоріння, письмо), під час аудиторних занять, а також перевірку завдань для самостійної роботи і творчих завдань/проектів. Оцінювання здобувача вищої освіти під час поточного контролю здійснюється відповідно до норм кредитно-модульної системи, а також згідно з критеріями оцінювання різних видів навчальної діяльності.
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
		Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	Публічний захист
		Риторика та стилістика наукових праць (денна форма)	Словесні (лекція, пояснення, розповідь, бесіда), наочні (спостереження, ілюстрація,	Усне опитування, виконання здобувачем освіти вправ на семінарському занятті. Авторський твір до

			демонстрація) Словесні (лекція, пояснення, розповідь, бесіда), наочні (спостереження, ілюстрація, демонстрація), практичні (вправи, тестування) інформаційно-рецептивний метод, репродуктивний метод, індуктивний та дедуктивний методи; дискусії; під керівництвом викладача, самостійна робота Інформаційно-рецептивний метод, репродуктивний метод, дискусії, проблемний метод, частково-пошуковий (евристичний) метод, пошуковий (дослідний) метод	художньо-публіцистичного альманаху «З Батьківщиною в серці» (за бажанням здобувача) Усне опитування, виконання здобувачем освіти вправ на семінарському занятті, завдань для самостійної роботи, модульної контрольної роботи; відповідь здобувача освіти на диференційованому заліку Виконання здобувачем освіти завдань для самостійної роботи, зокрема підготовка та виголошення фахової наукової промови. Участь у мовно-літературних конкурсах та авторський твір до художньо-публіцистичного альманаху «З Батьківщиною в серці» (за бажанням здобувача)
ПРН 12. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки і є основою для прийняття ефективних рішень, проведення досліджень та критичного осмислення проблем у галузі національної безпеки.	☒	Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	Публічний захист
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
		Прикладні системи штучного інтелекту в кіберпросторі (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Метод критичного аналізу (Critical Thinking Drills), коли здобувачі вищої освіти отримують суперечливі артефакти, неповну інформацію. 2) Project-Based Learning (PBL) — навчання через реальні AI-проєкти –	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).

			створення здобувачами вищої освіти AI-моделей класифікації наративів; систем виявлення ботів; моделей для аналізу емоцій та семантики тексту; генеративних моделей deepfake-відео; AI-агентів для прогнозування ефективності ІО. 3) Data-Driven Learning із застосуванням OSINT, під час чого здобувачі вищої освіти працюють з відкритими даними соцмереж; Graph API; OSINT-інструментами; ML-моделями для аналізу поширення інформації.	
		Кіберзахист об'єктів критичної інфраструктури (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Case-based learning (CBL), коли здобувачі вищої освіти аналізують реальні або симульовані кейси: • витік персональних даних; • зараження мережі шкідливим ПЗ; • вилучення цифрових носіїв у кіберзлочинця; • аналіз цифрових доказів у кримінальних провадженнях. 2) Incident Response Simulations - повноцінне моделювання кіберінциденту з ролями: аналітик безпеки, форензик, архітектор, аудитор, мисливець за загрозами. 3) Практичні роботи з використанням реальних цифрових артефактів: • Аналіз RAM (Volatility, Rekall). • Аналіз диск-іміджів (Autopsy, FTK Imager). • Робота з логами мережевих пристроїв. • Відновлення видалених файлів. • Reverse engineering шкідливого ПЗ. 4) CTF-формат (Capture The Flag) з використанням Forensics-категорії: PCAP, диск-іміджі, стеганографія, криптоаналіз, лог-аналіз, тобто використання командних змагань з аналізу цифрових доказів, квести та сценарії для здобуття прапору за правильно виконане завдання на зразок, знайти артефакт; відновити послідовність подій; побудувати лінію часу атаки; підготувати доказову базу.	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен), курсова робота
ПРН 22. Оцінювати ризики для інформаційної безпеки та/або кібербезпеки	☐	Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний	Публічний захист

організації			метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
		Методи і моделі протидії кіберзагрозам (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Case-based learning (CBL), коли здобувачі вищої освіти аналізують реальні або симульовані кейси: • витік персональних даних; • зараження мережі шкідливим ПЗ; • вилучення цифрових носіїв у кіберзлочинця; • аналіз цифрових доказів у кримінальних провадженнях. 2) Incident Response Simulations - повноцінне моделювання кіберінциденту з ролями: аналітик безпеки, форензик, архітектор, аудитор, мисливець за загрозами. 3) Практичні роботи з використанням реальних цифрових артефактів: • Аналіз RAM (Volatility, Rekall). • Аналіз диск-іміджів (Autopsy, FTK Imager). • Робота з логами мережевих пристроїв. • Відновлення видалених файлів. • Reverse engineering шкідливого ПЗ. 4) CTF-формат (Capture The Flag) з використанням Forensics-категорії: PCAP, диск-іміджі, стеганографія, криптоаналіз, лог-аналіз, тобто використання командних змагань з	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).

			аналізу цифрових доказів, квести та сценарії для здобуття прапору за правильно виконане завдання на зразок, знайти артефакт; відновити послідовність подій; побудувати лінію часу атаки; підготувати доказову базу.	
		Кіберзахист об'єктів критичної інфраструктури (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Case-based learning (CBL), коли здобувачі вищої освіти аналізують реальні або симульовані кейси: • витік персональних даних; • зараження мережі шкідливим ПЗ; • вилучення цифрових носіїв у кіберзлочинця; • аналіз цифрових доказів у кримінальних провадженнях. 2) Incident Response Simulations - повноцінне моделювання кіберінциденту з ролями: аналітик безпеки, форензик, архітектор, аудитор, мисливець за загрозами. 3) Практичні роботи з використанням реальних цифрових артефактів: • Аналіз RAM (Volatility, Rekall). • Аналіз диск-іміджів (Autopsy, FTK Imager). • Робота з логами мережевих пристроїв. • Відновлення видалених файлів. • Reverse engineering шкідливого ПЗ. 4) CTF-формат (Capture The Flag) з використанням Forensics-категорії: PCAP, диск-іміджі, стеганографія, криптоаналіз, лог-аналіз, тобто використання командних змагань з аналізу цифрових доказів, квести та сценарії для здобуття прапору за правильно виконане завдання на зразок, знайти артефакт; відновити послідовність подій; побудувати лінію часу атаки; підготувати доказову базу.	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен), курсова робота
ПРН 23. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної	☐	Управління кіберінцидентами (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Навчання на основі реальних кейсів (Case-Based Learning) - метод дозволяє зрозуміти логіку розвитку інцидентів, механізми прийняття рішень та вибір стратегії реагування – здобувачі вищої освіти аналізують реальні або модифіковані інциденти:	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).

безпеки та/або кібербезпеки організації.			DDoS на державну установу; компрометація AD; фішингові атаки зі зливом даних; інсайдерська загроза; рансомвер у критичній інфраструктурі; атаки на хмарні сервіси. 2) Tabletop Exercises (TTX) – настільні навчальні сценарії, коли студенти покроково розглядають сценарій кібератаки, реагують на оновлення, обставини та приймають рішення. 3) CTF з акцентом на Incident Response, коли пропонуються ігрові завдання: аналіз PCAP; пошук IoC; аналіз пам'яті; розбір логів (SIEM); побудова таймлайна атаки; визначення TTP за MITRE ATT&CK 4) Об'єднане навчання (Blended Learning) з використанням хмарних платформ та міжмережевої академії Cisco. - під час написання та захисту курсової роботи Collaborative Learning — командне розслідування інциденту 5) Метод критичного аналізу (Critical Thinking Drills), коли здобувачі вищої освіти отримують суперечливі артефакти, неповну інформацію.	
		Безпека розподілених інформаційних ресурсів та хмарні технології (денна форма)	Під час викладання навчальної дисципліни використовуються такі методи навчання як індуктивний, дедуктивний, продуктивний, дослідницький та метод стимулювання. Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить здобувачів вищої освіти до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. Продуктивний метод пов'язаний з опануванням нових знань у процесі творчої роботи. Дослідницький метод застосовується для засвоєння досвіду творчої діяльності, глибоких знань. Методи стимулювання спеціально спрямовані на формування позитивних мотивів навчання, стимулюють пізнавальну активність, водночас сприяють збагаченню здобувачів вищої освіти новою інформацією. Методи активізації	Поточний контроль Модульна контрольна робота Рейтингова система Екзамен

			навчального процесу: - мозкові атаки – метод розв'язання невідкладних завдань, сутність якого полягає в тому, щоб висловити якомога більшу кількість ідей за дуже обмежений проміжок часу, обговорити і здійснити їх селекцію; - кейс-метод – розгляд, аналіз конкретних ситуацій, який дає змогу наблизити процес навчання до реальної практичної діяльності; - презентації – виступи перед аудиторією, що використовуються для представлення певних досягнень, результатів роботи групи, звіту про виконання індивідуальних завдань тощо	
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
		Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	Публічний захист
		Методи і моделі протидії кіберзагрозам (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Case-based learning (CBL), коли здобувачі вищої освіти аналізують реальні або симульовані кейси: • витік персональних даних; • зараження мережі шкідливим ПЗ; • вилучення цифрових носіїв у кіберзлочинця;	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).

			• аналіз цифрових доказів у кримінальних провадженнях. 2) Incident Response Simulations - повноцінне моделювання кіберінциденту з ролями: аналітик безпеки, форензик, архітектор, аудитор, мисливець за загрозами. 3) Практичні роботи з використанням реальних цифрових артефактів: • Аналіз RAM (Volatility, Rekall). • Аналіз диск-іміджів (Autopsy, FTK Imager). • Робота з логами мережевих пристроїв. • Відновлення видалених файлів. • Reverse engineering шкідливого ПЗ. 4) CTF-формат (Capture The Flag) з використанням Forensics-категорії: PCAP, диск-іміджі, стеганографія, криптоаналіз, лог-аналіз, тобто використання командних змагань з аналізу цифрових доказів, квести та сценарії для здобуття прапору за правильно виконане завдання на зразок, знайти артефакт; відновити послідовність подій; побудувати лінію часу атаки; підготувати доказову базу.	
		Актуальні проблеми інформаційної безпеки (денна форма)	1. Загальні методи організації і здійснення навчально-пізнавальної діяльності: - методи надання і сприйняття навчальної інформації: словесні (лекція, дискусія); наочні (ілюстрація, демонстрація, візуалізація); практичні (міні-дослідження, задачі); - методи логіки сприйняття навчальної інформації: індуктивний; дедуктивний; аналітичний, моделювання, тощо; - методи формування знань: репродуктивний; проблемно-пошуковий; - організаційні методи: навчальна робота під керівництвом викладача; самостійна творчо-пошукова робота з джерельною базою. 2. Конкретні методи навчання за ОК та їх зв'язок із забезпеченням результатів навчання: - міні-досліджень – полягає у стимулювання інтересу до дослідницької діяльності та реалізується шляхом постановки завдань на заняттях і самостійної підготовки через необхідність проведення власного аналізу відповідних джерел інформації в умовах невизначеності та	1. Форми оцінювання поточної роботи: - презентації виконання індивідуальних і групових завдань - участь у формуванні і підтриманні дискусії - моделювання дискусії на семінарських заняттях - виконання завдань на практичних заняттях - виконання індивідуальних додаткових завдань (за власним бажанням) 2. Контрольні заходи: - виконання модульної контрольної роботи - диференційований залік.

			формування варіантів рішень, пояснень, аргументації, узагальнень тощо за законами професійного мислення ; - кейс-метод – вирішення комплексних завдань на основі наданих, комплектів матеріалів (зокрема рішень ЄСПЛ), повідомлень в медіа, відеосюжетів тощо . Розвиток Soft Skills: - колективна робота малими групами та лідерство – реалізується шляхом групового формування завдань з розподілом ролей і елементами самоорганізації при виконанні і представленні результатів; - створення ситуацій зайнятості і пізнавальної новизни – реалізується шляхом формування атмосфери індивідуального залучення до спроб професійного вирішення актуальних і проблемних задач, формування перспективного та проблемного бачення; - заохочення до самонавчання і дослідницької творчості – реалізується шляхом демонстрації переваг творчого вирішення складних професійних задач, формування професійних пізнавальних і дослідницьких потреб.	
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.	☐	Інформаційне протиборство (денна форма)	I. Методи організації та здійснення навчально-пізнавальної діяльності: - методи надання і сприйняття навчальної інформації словесні: лекція (традиційна, проблемна) із застосуванням комп'ютерних інформаційних технологій, семінари, пояснення, розповідь, бесіда; наочні: спостереження, ілюстрація, демонстрація; практичні: міні-дослідження, завдання); - методи передачі і сприйняття навчальної інформації: індуктивні, дедуктивні, аналітичні, синтетичні; - методи розвитку самостійності мислення: репродуктивні, пошукові, дослідницькі; - методи керування навчальною діяльністю: під керівництвом викладача; самостійна робота студентів: з книгою; виконання індивідуальних навчальних проектів. 2. Конкретні методи навчання за ОК та їх зв'язок із забезпеченням результатів навчання: - здійснення досліджень, що	1. Форми оцінювання поточної роботи: - презентації виконання індивідуальних і групових завдань; - участь у формуванні і підтриманні дискусії; - модерування дискусії на семінарських заняттях; - виконання завдань на практичних заняттях; - виконання індивідуальних додаткових завдань (за власним бажанням). 2. Контрольні заходи: - вирішення тестових завдань; - підготовка рефератів; - виконання модульної контрольної роботи; - екзамен.

			реалізується шляхом постановки завдань на заняттях з наступною самостійною підготовкою з проведенням аналізу джерел інформації в умовах невизначеності та формування варіантів рішень, пояснень, аргументації, узагальнень тощо за законами професійного мислення ; - інтерактивні методи – аналіз цілей та інструментарію, що використовуються в професійній діяльності на основі наданих матеріалів, повідомлень в медіа, відеосюжетів тощо . 3. Методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності: навчальні дискусії; створення ситуації пізнавальної новизни; створення ситуацій зацікавленості (метод цікавих аналогій тощо).	
		Безпека розподілених інформаційних ресурсів та хмарні технології (денна форма)	Під час викладання навчальної дисципліни використовуються такі методи навчання як індуктивний, дедуктивний, продуктивний, дослідницький та метод стимулювання. Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить здобувачів вищої освіти до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. Продуктивний метод пов'язаний з опануванням нових знань у процесі творчої роботи. Дослідницький метод застосовується для засвоєння досвіду творчої діяльності, глибоких знань. Методи стимулювання спеціально спрямовані на формування позитивних мотивів навчання, стимулюють пізнавальну активність, водночас сприяють збагаченню здобувачів вищої освіти новою інформацією. Методи активізації навчального процесу: - мозкові атаки – метод розв'язання невідкладних завдань, сутність якого полягає в тому, щоб висловити якомога більшу кількість ідей за дуже обмежений проміжок часу, обговорити і здійснити їх селекцію; - кейс-метод – розгляд,	Поточний контроль Модульна контрольна робота Рейтингова система Екзамен

			аналіз конкретних ситуацій, який дає змогу наблизити процес навчання до реальної практичної діяльності; - презентації – виступи перед аудиторією, що використовуються для представлення певних досягнень, результатів роботи групи, звіту про виконання індивідуальних завдань тощо	
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
		Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	Публічний захист
ПРН 14. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються.	☒	Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
		Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод	Публічний захист

			аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	
		Територіальна оборона, мобілізаційна підготовка та мобілізація (денна форма)	Методи навчання: словесні методи (пояснення, інструктаж, розповідь, бесіда, навчальна дискусія), наочні методи (ілюстрування, демонстрування), практичні методи (вправи, практичні роботи), методи наукового пізнання (індукції і дедукції, аналізу, синтезу, порівняння, узагальнення, конкретизації, виділення головного)	Передбачені наступні методи оцінювання: поточні опитування під час проведення семінарських занять; визначення рівня засвоєння отриманих матеріалів та здатності їх застосовувати під час проведення практичних занять, підсумкове оцінювання під час проведення екзамену в усній формі.
		Актуальні проблеми інформаційної безпеки (денна форма)	1. Загальні методи організації і здійснення навчально-пізнавальної діяльності: - методи надання і сприйняття навчальної інформації: словесні (лекція, дискусія); наочні (ілюстрація, демонстрація, візуалізація); практичні (міні-дослідження, задачі); - методи логіки сприйняття навчальної інформації: індуктивний; дедуктивний; аналітичний, моделювання, тощо; - методи формування знань: репродуктивний; проблемно-пошуковий; - організаційні методи: навчальна робота під керівництвом викладача; самостійна творчо-пошукова робота з джерельною базою. 2. Конкретні методи навчання за ОК та їх зв'язок із забезпеченням результатів навчання: - створення презентації, інфографіки – реалізується постійно присутній елемент/вимога при виконанні індивідуальних і колективних завдань з результатом, який передбачає демонстрацію/представлення для колег . Розвиток Soft Skills: - колективна робота малими групами та лідерство – реалізується шляхом групового формування завдань з розподілом ролей і елементами самоорганізації при виконанні і представленні результатів;	1. Форми оцінювання поточної роботи: - презентації виконання індивідуальних і групових завдань - участь у формуванні і підтриманні дискусії - моделювання дискусії на семінарських заняттях - виконання завдань на практичних заняттях - виконання індивідуальних додаткових завдань (за власним бажанням) 2. Контрольні заходи: - виконання модульної контрольної роботи - диференційований залік.

			- створення ситуацій зайнятості і пізнавальної новизни – реалізується шляхом формування атмосфери індивідуального залучення до спроб професійного вирішення актуальних і проблемних задач, формування перспективного та проблемного бачення; - заохочення до самонавчання і дослідницької творчості – реалізується шляхом демонстрації переваг творчого вирішення складних професійних задач, формування професійних пізнавальних і дослідницьких потреб.	
		Іноземна мова професійного спрямування (денна форма)	Традиційні методи навчання: ● словесні методи: розповідь (монологічний), бесіда (діалогічний), синтезуючі або закріплюючі і контрольно-коректуючи; ● наочні методи (демонстрація); ● практичні методи: виконання усних і письмових вправ; ● робота з різними джерелами інформації (підручник, статті, словники); ● відео метод (наочне сприйняття інформації). ● індуктивний метод; ● дедуктивний метод; ● репродуктивний метод (відтворення готових зразків); ● частково-пошуковий (евристичний) метод; ● самостійна робота здобувачів; ● спеціальні методи – використання ситуативних та рольових ігор за темами модулів. Інноваційні методи навчання - інтерактивна діяльність (парна, групова і робота в команді) з використанням сучасних методів організації роботи на занятті. - мультимедійний супровід практичних занять.	Результати навчання здобувача вищої освіти з навчальної дисципліни оцінюються за 100-бальною шкалою як сума балів поточного та підсумкового контролю. Поточний контроль передбачає перевірку набутих знань і навичок з різних видів мовленнєвої діяльності (читання, аудіювання, говоріння, письмо), під час аудиторних занять, а також перевірку завдань для самостійної роботи і творчих завдань/проектів. Оцінювання здобувача вищої освіти під час поточного контролю здійснюється відповідно до норм кредитно-модульної системи, а також згідно з критеріями оцінювання різних видів навчальної діяльності.
		Риторика та стилістика наукових праць (денна форма)	Словесні (лекція, пояснення, розповідь, бесіда), наочні (спостереження, ілюстрація, демонстрація) Словесні (лекція, пояснення, розповідь, бесіда), наочні (спостереження, ілюстрація, демонстрація), практичні (вправи, тестування) інформаційно-рецептивний метод, репродуктивний метод, індуктивний та дедуктивний методи; дискусії; під керівництвом викладача, самостійна робота	Усне опитування, виконання здобувачем освіти вправ на семінарському занятті. Авторський твір до художньо-публіцистичного альманаху «З Батьківщиною в серці» (за бажанням здобувача) Усне опитування, виконання здобувачем освіти вправ на семінарському занятті, завдань для самостійної роботи, модульної контрольної роботи; відповідь здобувача освіти на диференційованому заліку Виконання здобувачем

			Інформаційно-рецептивний метод, репродуктивний метод, дискусії, проблемний метод, частково-пошуковий (евристичний) метод, пошуковий (дослідний) метод	освіти завдань для самостійної роботи, зокрема підготовка та виголошення фахової наукової промови. Участь у мовно-літературних конкурсах та авторський твір до художньо-публіцистичного альманаху «З Батьківщиною в серці» (за бажанням здобувача)
		Методологія наукових досліджень та академічна доброчесність (денна форма)	- використання сучасних наукових технологій навчання (мультимедійні засоби). 1. - діалектичний метод; 2. - емпіричні методи; - теоретичні (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод). 3. - специфічні педагогічні методи та прийоми: ● методи організації навчальної діяльності (словесні, наочні, практичні); ● методи стимулювання і мотивації здобувачів освітнього рівня магістр; ● методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; ● індивідуальний підхід. ● самостійна робота здобувачів освіти.	Поточний контроль Модульна контрольна робота Рейтингова система Диференційований залік
ПРН 26. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.	☐	Прикладні системи штучного інтелекту в кіберпросторі (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Метод критичного аналізу (Critical Thinking Drills), коли здобувачі вищої освіти отримують суперечливі артефакти, неповну інформацію. 2) Project-Based Learning (PBL) — навчання через реальні AI-проєкти – створення здобувачами вищої освіти AI-моделей класифікації наративів; систем виявлення ботів; моделей для аналізу емоцій та семантики тексту; генеративних моделей deepfake-відео; AI-агентів для прогнозування ефективності ІО. 3) Data-Driven Learning із застосуванням OSINT, під час чого здобувачі вищої освіти працюють з відкритими даними соцмереж; Graph API; OSINT-інструментами; ML-моделями для аналізу поширення інформації.	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Організаційно-правове забезпечення кіберзахисту (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних

			ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	(ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Методи і моделі протидії кіберзагрозам (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Case-based learning (CBL), коли здобувачі вищої освіти аналізують реальні або симульовані кейси: • витік персональних даних; • зараження мережі шкідливим ПЗ; • вилучення цифрових носіїв у кіберзлочинця; • аналіз цифрових доказів у кримінальних провадженнях. 2) Incident Response Simulations - повноцінне моделювання кіберінциденту з ролями: аналітик безпеки, форензик, архітектор, аудитор, мисливець за загрозами. 3) Практичні роботи з використанням реальних цифрових артефактів: • Аналіз RAM (Volatility, Rekall). • Аналіз диск-іміджів (Autopsy, FTK Imager). • Робота з логами мережевих пристроїв. • Відновлення видалених файлів. • Reverse engineering шкідливого ПЗ. 4) CTF-формат (Capture The Flag) з використанням Forensics-категорії: PCAP, диск-іміджі, стеганографія, криптоаналіз, лог-аналіз, тобто використання командних змагань з аналізу цифрових доказів, квести та сценарії для здобуття прапору за правильно виконане завдання на зразок, знайти артефакт; відновити послідовність подій; побудувати лінію часу атаки; підготувати доказову базу.	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Кіберзахист об’єктів критичної інфраструктури (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Case-based learning (CBL), коли здобувачі вищої освіти аналізують реальні або симульовані кейси: • витік персональних даних; • зараження мережі шкідливим ПЗ; • вилучення цифрових носіїв у кіберзлочинця; • аналіз цифрових доказів у кримінальних провадженнях.	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен), курсова робота

			2) Incident Response Simulations - повноцінне моделювання кіберінциденту з ролями: аналітик безпеки, форензик, архітектор, аудитор, мисливець за загрозами. 3) Практичні роботи з використанням реальних цифрових артефактів: • Аналіз RAM (Volatility, Rekall). • Аналіз диск-іміджів (Autopsy, FTK Imager). • Робота з логами мережевих пристроїв. • Відновлення видалених файлів. • Reverse engineering шкідливого ПЗ. 4) CTF-формат (Capture The Flag) з використанням Forensics-категорії: PCAP, диск-іміджі, стеганографія, криптоаналіз, лог-аналіз, тобто використання командних змагань з аналізу цифрових доказів, квести та сценарії для здобуття прапору за правильно виконане завдання на зразок, знайти артефакт; відновити послідовність подій; побудувати лінію часу атаки; підготувати доказову базу.	
		Управління кіберінцидентами (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Навчання на основі реальних кейсів (Case-Based Learning) - метод дозволяє зрозуміти логіку розвитку інцидентів, механізми прийняття рішень та вибір стратегії реагування – здобувачі вищої освіти аналізують реальні або модифіковані інциденти: DDoS на державну установу; компрометація AD; фішингові атаки зі зливом даних; інсайдерська загроза; рансомвер у критичній інфраструктурі; атаки на хмарні сервіси. 2) Tabletop Exercises (TTX) – настільні навчальні сценарії, коли студенти покроково розглядають сценарій кібератаки, реагують на оновлення, обставини та приймають рішення. 3) CTF з акцентом на Incident Response, коли пропонуються ігрові завдання: аналіз PCAP; пошук IoC; аналіз пам'яті; розбір логів (SIEM); побудова таймлайна атаки; визначення TTP за MITRE ATT&CK 4) Об'єднане навчання (Blended Learning) з використанням хмарних платформ та міжмережевої академії Cisco.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).

			- під час написання та захисту курсової роботи Collaborative Learning — командне розслідування інциденту 5) Метод критичного аналізу (Critical Thinking Drills), коли здобувачі вищої освіти отримують суперечливі артефакти, неповну інформацію.	
ПРН 21. Досліджувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури	☐	Аудит інформаційної безпеки та кібербезпеки (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Безпека розподілених інформаційних ресурсів та хмарні технології (денна форма)	Під час викладання навчальної дисципліни використовуються такі методи навчання як індуктивний, дедуктивний, продуктивний, дослідницький та метод стимулювання. Індуктивний метод полягає в тому, що викладач спершу викладає факти, проводить досліди, поступово підводить здобувачів вищої освіти до узагальнень, визначення понять. Дедуктивний метод полягає в тому, що викладач повідомляє загальне положення, закон, а потім роблячи висновки поступово підводить до конкретних висновків, ставить конкретні завдання. Продуктивний метод пов'язаний з опануванням нових знань у процесі творчої роботи. Дослідницький метод застосовується для засвоєння досвіду творчої діяльності, глибоких знань. Методи стимулювання спеціально спрямовані на формування позитивних мотивів навчання, стимулюють пізнавальну активність, водночас сприяють збагаченню здобувачів вищої освіти новою інформацією. Методи активізації навчального процесу: - мозкові атаки – метод розв'язання невідкладних завдань, сутність якого полягає в тому, щоб висловити якомога більшу кількість ідей за дуже обмежений проміжок часу, обговорити і здійснити їх селекцію; - кейс-метод – розгляд, аналіз конкретних ситуацій, який дає змогу наблизити процес навчання до реальної практичної діяльності;	Поточний контроль Модульна контрольна робота Рейтингова система Екзамен

			- презентації – виступи перед аудиторією, що використовуються для представлення певних досягнень, результатів роботи групи, звіту про виконання індивідуальних завдань тощо	
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
		Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	Публічний захист
		Застосування методів і засобів OSINT у Web-середовищі (денна форма)	Під час викладання навчальної дисципліни використовуються словесні, наочні, практичні та самостійні методи, що забезпечують формування результатів навчання . Практичні заняття спрямовані на формування практичних умінь шляхом виконання індивідуальних завдань, аналізу ситуаційних кейсів, опрацювання методів і засобів OSINT та моделювання оперативної обстановки . Самостійна робота здобувачів включає опрацювання літератури, виконання завдань аналітичного характеру, засвоєння інструментів OSINT та розвиток навичок критичного аналізу . У процесі навчання застосовуються дидактичні прийоми, орієнтовані на формування аналітичних здібностей, уміння	Для перевірки рівня засвоєння здобувачами вищої освіти знань, умінь та навичок з навчальної дисципліни проводиться оцінювання продовж навчання у вигляді поточного, модульного та підсумкового контролю. Для оцінки використовуються різні види робіт: - поточний контроль засвоєння матеріалу здійснюється шляхом перевірки практичних робіт; - модульний контроль проводиться в формі виконання завдання; - підсумковий контроль забезпечується проведенням диференційованого заліку в формі тесту.

			працювати з неповними або суперечливими даними та здатності приймати обґрунтовані рішення. Використовуються сучасні програмні засоби та WEB-ресурси, необхідні для виконання завдань дисципліни.	
ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності.	☒	Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	Публічний захист
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік
		Аудит інформаційної безпеки та кібербезпеки (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Актуальні проблеми інформаційної безпеки (денна форма)	1. Загальні методи організації і здійснення навчально-пізнавальної діяльності: - методи надання і сприйняття навчальної інформації: словесні (лекція, дискусія); наочні (ілюстрація, демонстрація, візуалізація); практичні (міні-дослідження, задачі); - методи логіки сприйняття навчальної інформації: індуктивний; дедуктивний;	1. Форми оцінювання поточної роботи: - презентації виконання індивідуальних і групових завдань - участь у формуванні і підтриманні дискусії - моделювання дискусії на семінарських заняттях - виконання завдань на практичних заняттях - виконання індивідуальних додаткових завдань (за власним бажанням)

			аналітичний, моделювання, тощо; - методи формування знань: репродуктивний; проблемно-пошуковий; - організаційні методи: навчальна робота під керівництвом викладача; самостійна творчо-пошукова робота з джерельною базою. 2. Конкретні методи навчання за ОК та їх зв'язок із забезпеченням результатів навчання: - створення навчально-наукової дискусії – реалізується шляхом формування професійних потреб постійного звернення до науково-доктринальних ідей і концепцій для обґрунтування власної професійної позиції, висновку ; - кейс-метод – вирішення комплексних завдань на основі наданих, комплектів матеріалів (зокрема рішень ЄСПЛ), повідомлень в медіа, відеосюжетів тощо ; Розвиток Soft Skills: - колективна робота малими групами та лідерство – реалізується шляхом групового формування завдань з розподілом ролей і елементами самоорганізації при виконанні і представленні результатів; - створення ситуацій зайнятості і пізнавальної новизни – реалізується шляхом формування атмосфери індивідуального залучення до спроб професійного вирішення актуальних і проблемних задач, формування перспективного та проблемного бачення; - заохочення до самонавчання і дослідницької творчості – реалізується шляхом демонстрації переваг творчого вирішення складних професійних задач, формування професійних пізнавальних і дослідницьких потреб.	2. Контрольні заходи: - виконання модульної контрольної роботи - диференційований залік.
		Кіберзахист об’єктів критичної інфраструктури (денна форма)	під час проведення практичних занять використовуються освітні методи, засновані на реальних кейсах, а саме: 1) Case-based learning (CBL), коли здобувачі вищої освіти аналізують реальні або симульовані кейси: • витік персональних даних; • зараження мережі шкідливим ПЗ; • вилучення цифрових носіїв у кіберзлочинця; • аналіз цифрових доказів у кримінальних провадженнях. 2) Incident Response	Поточний контроль (усне опитування на практичних заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен), курсова робота

			Simulations - повноцінне моделювання кіберінциденту з ролями: аналітик безпеки, форензик, архітектор, аудитор, мисливець за загрозами. 3) Практичні роботи з використанням реальних цифрових артефактів: • Аналіз RAM (Volatility, Rekall). • Аналіз диск-іміджів (Autopsy, FTK Imager). • Робота з логами мережевих пристроїв. • Відновлення видалених файлів. • Reverse engineering шкідливого ПЗ. 4) CTF-формат (Capture The Flag) з використанням Forensics-категорії: PCAP, диск-іміджі, стеганографія, криптоаналіз, лог-аналіз, тобто використання командних змагань з аналізу цифрових доказів, квести та сценарії для здобуття прапору за правильно виконане завдання на зразок, знайти артефакт; відновити послідовність подій; побудувати лінію часу атаки; підготувати доказову базу.	
		Інформаційне протиборство (денна форма)	1. Методи організації та здійснення навчально-пізнавальної діяльності: - методи надання і сприйняття навчальної інформації словесні: лекція (традиційна, проблемна) із застосуванням комп'ютерних інформаційних технологій, семінари, пояснення, розповідь, бесіда; наочні: спостереження, ілюстрація, демонстрація; практичні: міні-дослідження, завдання); - методи передачі і сприйняття навчальної інформації: індуктивні, дедуктивні, аналітичні, синтетичні; - методи розвитку самостійності мислення: репродуктивні, пошукові, дослідницькі; - методи керування навчальною діяльністю: під керівництвом викладача; самостійна робота студентів: з книгою; виконання індивідуальних навчальних проектів. 2. Конкретні методи навчання за ОК та їх зв'язок із забезпеченням результатів навчання: - навчально-наукової дискусії та розвитку презентаційних навичок (створення презентації, інфографіки) зі зверненням до науково-доктринальних ідей, концепцій, кращого міжнародного досвіду для	1. Форми оцінювання поточної роботи: - презентації виконання індивідуальних і групових завдань; - участь у формуванні і підтриманні дискусії; - модерування дискусії на семінарських заняттях; - виконання завдань на практичних заняттях; - виконання індивідуальних додаткових завдань (за власним бажанням). 2. Контрольні заходи: - вирішення тестових завдань; - підготовка рефератів; - виконання модульної контрольної роботи; - екзамен.

			обґрунтування власної професійної позиції та висновків ; - інтерактивні методи – аналіз цілей та інструментарію, що використовуються в професійній діяльності на основі наданих матеріалів, повідомлень в медіа, відеосюжетів тощо ; 3. Методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності: навчальні дискусії; створення ситуації пізнавальної новизни; створення ситуацій зацікавленості (метод цікавих аналогій тощо).	
		Організаційно-правове забезпечення кіберзахисту (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності.	☒	Кваліфікаційна (магістерська) робота	В ході проведення наукових досліджень будуть застосовуватись наступні методи: метод постановки завдання; діалектичний метод; емпіричний метод; теоретичний (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод); методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; самостійна робота зі здобувачами вищої освіти; методи формування пізнавального інтересу, аналізу підсумків роботи, конкретизації. У разі позитивного захисту, здобувачі вищої освіти підтвердять готовність до самостійної професійної діяльності.	Публічний захист
		Методологія наукових досліджень та академічна доброчесність (денна форма)	- використання сучасних наукових технологій навчання (мультимедійні засоби). 1. - діалектичний метод; 2. - емпіричні методи; - теоретичні (аналіз та синтез, індукція і дедукція, сходження від абстрактного до конкретного, ідеалізація, формалізація, метод аналогії, історичний метод). 3. - специфічні педагогічні методи та прийоми: ● методи організації навчальної діяльності (словесні, наочні,	Поточний контроль Модульна контрольна робота Рейтингова система Диференційований залік

			практичні); ● методи стимулювання і мотивації здобувачів освітнього рівня магістр; ● методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності; ● індивідуальний підхід. ● самостійна робота здобувачів освіти.	
		Теорія прийняття рішень (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на практичних та семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (диференційований залік).
		Інформаційне протиборство (денна форма)	І. Методи організації та здійснення навчально-пізнавальної діяльності: - методи надання і сприйняття навчальної інформації словесні: лекція (традиційна, проблемна) із застосуванням комп'ютерних інформаційних технологій, семінари, пояснення, розповідь, бесіда; наочні: спостереження, ілюстрація, демонстрація; практичні: міні-дослідження, завдання); - методи передачі і сприйняття навчальної інформації: індуктивні, дедуктивні, аналітичні, синтетичні; - методи розвитку самостійності мислення: репродуктивні, пошукові, дослідницькі; - методи керування навчальною діяльністю: під керівництвом викладача; самостійна робота студентів: з книгою; виконання індивідуальних навчальних проектів. 2. Конкретні методи навчання за ОК та їх зв'язок із забезпеченням результатів навчання: - здійснення досліджень, що реалізується шляхом постановки завдань на заняттях з наступною самостійною підготовкою з проведенням аналізу джерел інформації в умовах невизначеності та формування варіантів рішень, пояснень, аргументації, узагальнень тощо за законами професійного мислення ; - навчально-наукової дискусії та розвитку презентаційних навичок (створення презентації,	1. Форми оцінювання поточної роботи: - презентації виконання індивідуальних і групових завдань; - участь у формуванні і підтриманні дискусії; - модерування дискусії на семінарських заняттях; - виконання завдань на практичних заняттях; - виконання індивідуальних додаткових завдань (за власним бажанням). 2. Контрольні заходи: - вирішення тестових завдань; - підготовка рефератів; - виконання модульної контрольної роботи; - екзамен.

			інфографіки) зі зверненням до науково-доктринальних ідей, концепцій, кращого міжнародного досвіду для обґрунтування власної професійної позиції та висновків ; 3. Методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності: навчальні дискусії; створення ситуації пізнавальної новизни; створення ситуацій зацікавленості (метод цікавих аналогій тощо).	
		Організаційно-правове забезпечення кіберзахисту (денна форма)	Під час викладання передбачено застосування словесних (лекція, пояснення, розповідь), наочних (мультимедійні ілюстрація, демонстрація) та практичних методів навчання. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії.	Поточний контроль (усне опитування на семінарських заняттях; виконання тестових завдань; аналіз і вирішення практичних (ситуаційних) завдань (кейсів); участь у дискусіях, модульний контроль (модульна контрольна робота, що містить тестові та відкриті питання), підсумковий контроль (екзамен).
		Науково-дослідна практика (денна форма)	Методами навчання є різні види науково-дослідних робіт, методи організації та здійснення навчально-пізнавальної діяльності та методи стимулювання інтересу до навчання і мотивації до навчально-пізнавальної діяльності, які сприяють систематизації теоретичного матеріалу та вдосконаленню практичних вмінь та навичок.	Диференційований залік