

**НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
ТА СТРАТЕГІЧНИХ КОМУНІКАЦІЙ
ЦЕНТР КІБЕРБЕЗПЕКИ
КАФЕДРА КІБЕРБЕЗПЕКИ**

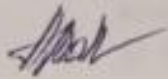
РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Аудит інформаційної безпеки та кібербезпеки»

освітня програма	Кіберзахист у сфері інформаційних технологій та кіберпросторі
рівень вищої освіти	другий (магістерський)
форма здобуття вищої освіти	очна (денна)
статус навчальної дисципліни	обов'язкова
мова викладання	українська

Робочу програму навчальної дисципліни розглянуто та затверджено на засіданні кафедри кібербезпеки ЦКБ ННІ ІБ СК НА СБ України від «21» липня 2025 року, протокол № 7.

Робочу програму навчальної дисципліни погоджено з гарантом освітньої програми

Завідувач кафедри кібербезпеки ЦКБ ННІ ІБ СК
Національної академії СБ України
доктор технічних наук, професор
«21» 07 2025 р.  Анастасія ВАВЛЕНКОВА

Робочу програму навчальної дисципліни погоджено з Управлінням інформаційних технологій та цифрових даних Департаменту інформаційно-аналітичного забезпечення Служби безпеки України

1. Опис навчальної дисципліни

Показник	Значення показника
Курс	2
Семестр	3
Обсяг (<i>кредити ЄКТС/години</i>)	5 / 150
Кількість змістових модулів	2
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	30
семінарські заняття (СЗ)	30
практичні заняття (ПЗ)	-
лабораторні заняття (ЛЗ)	-
індивідуальні завдання (ІЗ)	-
самостійна робота (СР)	90
форма підсумкового контролю (<i>семестр</i>)	екзамен (3)

2. Мета та завдання навчальної дисципліни

2.1. Мета та основні завдання вивчення навчальної дисципліни

Мета: формування у здобувачів вищої освіти теоретичних знань та практичних навичок, необхідних для проведення комплексного аудиту систем інформаційної безпеки та кібербезпеки на підприємствах та в організаціях, організації та супроводу процесів моніторингу й аудиту інформаційної безпеки та кібербезпеки, відповідності до критеріїв і показників якості безпеки, організації системи мінімізації ризиків, методів та засобів одержання об'єктивних оцінок про поточний стан інформаційної системи та інформаційної інфраструктури компанії.

Завдання:

- опанувати основні поняття, принципи, стандарти та методології аудиту інформаційної безпеки та кібербезпеки;
- набути навички планування, організації, проведення та документування етапів аудиту інформаційної безпеки та кібербезпеки;
- навчитися аналізувати результати й надавати рекомендації щодо усунення виявлених недоліків під час аудиту;
- вивчити сучасні програмні та апаратні засоби, що використовуються для проведення аудиту;
- набути навички комплексно оцінювати ризики, пов'язані з інформаційною безпекою, а розробляти ефективні стратегії захисту
- використовувати на практиці нормативні документи в галузі аудиту інформаційної безпеки та кібербезпеки;
- проводити аудит і сертифікацію (атестацію) систем, підсистем інформаційної безпеки та систем управління інформаційною безпекою.

2.2. Результати навчання

Обов'язкова навчальна дисципліна «Аудит інформаційної безпеки та кібербезпеки» спрямована на досягнення програмних результатів навчання, які в інтегрованому (синтезованому) вигляді визначені у профілі освітньо-професійної програми «Кіберзахист у сфері інформаційних технологій та кіберпростору» (від 11.09.2024 № 29/3/1/1-1276/ві), а саме:

ПРН 1	Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки.
ПРН 2	Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності.
ПРН 4	Організовувати роботу колективу, забезпечувати професійний розвиток його членів та досягнення поставлених цілей.
ПРН 7	Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.
ПРН 15	Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.
ПРН 19	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
ПРН 21	Досліджувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури
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.

3. Програма та структура навчальної дисципліни

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	ЛЗ	СР
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>
Семестр 3						
Змістовий модуль 1. «Основи аудиту інформаційної безпеки та кібербезпеки»						
Тема 1. Поняття, методи та процеси аудиту інформаційної безпеки та кібербезпеки.	80	18	14			48
Лекція 1. Вступ до аудиту інформаційної безпеки та кібербезпеки: поняття, цілі, види		2				
Семінарське заняття 1. Аналіз нормативно-			2			

правових актів, якими визначено проведення незалежного аудиту інформаційної безпеки та кібербезпеки на об'єктах критичної інфраструктури						
Лекція 2. Кращі світові практики, стандарти і вимоги до проведення процедур аудиту інформаційної безпеки та кібербезпеки.		2				
Семінарське заняття 2. Робота з міжнародними та національними стандартами у сфері аудиту інформаційної безпеки (ISO 27001, NIST, ДСТУ)			2			
Самостійна робота 1. Ринок послуг аудиту інформаційної безпеки та кібербезпеки в світі						10
Лекція 3. Ризик-орієнтований підхід в аудиті інформаційної безпеки та кібербезпеки.		2				
Семінарське заняття 3. Ідентифікація та оцінка ризиків інформаційної безпеки та кібербезпеки			2			
Самостійна робота 2. Сертифікація фахівців в галузі аудиту інформаційної безпеки та кібербезпеки						10
Лекція 4. Аналіз політики інформаційної безпеки за стандартом ISO/IEC 27001, 27002, 27004		2				
Семінарське заняття 4. Застосування вимог та положень стандартів ISO/IEC 27002:2024 для аналізу політики інформаційної безпеки			2			
Лекція 5. Правові аспекти аудиту інформаційної безпеки та кібербезпеки		2				
Семінарське заняття 5. Застосування вимог та положень стандартів ISO/IEC 27004:2018, ISO/IEC 27006-2:2024 для аналізу політики інформаційної безпеки			2			
Лекція 6. Методологія та етапи проведення аудиту інформаційної безпеки та кібербезпеки		2				
Семінарське заняття 6. Дослідження етапів проведення аудиту фізичної безпеки офісу.			2			
Лекція 7. Методи та заходи планування процедур моніторингу операційних процесів установи.		2				
Самостійна робота 3. Наставови щодо						10

застосування стандартів ISO/IEC з безпеки та аудиту інформаційних систем і технологій: 17021, 17024, 15408, 15504						
Семінарське заняття 7. Дослідження процесу аудиту політик та процедур інформаційної безпеки			2			
Лекція 8. Аудит фізичної безпеки інформаційних систем, аудит управління доступом та аудит захисту від шкідливого програмного забезпечення.		2				
Лекція 9. Аудит безпеки систем промислової автоматизації (SCADA)		2				
Самостійна робота 4. Настанови щодо застосування вимог та положень стандартів CoViT 5, ITAF						9
Самостійна робота 5. Налаштування та аудит прав доступу користувачів у доменній мережі						9
Семінарське заняття 8. Модульна контрольна робота 1	2		2			
Всього годин за модуль 1	82	18	16			48
Змістовий модуль 2. «Організація проведення аудиту інформаційної безпеки та кібербезпеки»						
Тема 2. Організація проведення аудиту інформаційної безпеки та кібербезпеки	66	12	12			42
Лекція 1. Організація процесу аудиту інформаційної безпеки та кібербезпеки. Ініціювання процедури аудиту		2				
Семінарське заняття 1. Розробка плану аудиту інформаційної безпеки для малої організації.			2			
Лекція 2. Послідовність дій та етапів аудиту інформаційної безпеки та кібербезпеки. Збір інформації для проведення аудиту та аналіз даних під час аудиту		2				
Семінарське заняття 2. Робота з інструментами аналізу даних під час аудиту інформаційної безпеки та кібербезпеки			2			
Лекція 3. Аналіз результатів аудиту та системи кібербезпеки.		2				
Семінарське заняття 3. Напрацювання рекомендацій за результатами аналізу стану організації інформаційної безпеки та			2			

кібербезпеки підприємства						
Лекція 4. Формування звітності на основі проведення аудиту інформаційної безпеки та кібербезпеки: документування результатів аудиту та підготовка аудиторського звіту		2				
Самостійна робота 1. Настанови щодо застосування стандартів та кращих практик ITIL V3. IT Infrastructure Library, GTAG-8, SAATTs.						14
Семінарське заняття 4. Написання аудиторського звіту щодо інформаційної безпеки та кібербезпеки підприємства з рекомендаціями для керівництва			2			
Самостійна робота 2. Настанови щодо застосування вимог та положень стандартів ISO/IEC 27006-2:2024						14
Лекція 5. Концепція впровадження системи аудиту інформаційної безпеки в Україні (“Дорожня карта”)		2				
Самостійна робота 3. Аналіз аудиторських звітів						14
Семінарське заняття 5. Проведення імітаційного аудиту інформаційної безпеки та кібербезпеки комп’ютерного класу			2			
Семінарське заняття 6. Написання звіту щодо проведення аудиту інформаційної безпеки та кібербезпеки комп’ютерного класу			2			
Лекція 6. Етапи реалізації Дорожньої карти створення системи контролю та аудиту інформаційної безпеки та кібербезпеки в Україні		2				
Семінарське заняття 7. Модульна контрольна робота 2	2		2			
Всього годин за модуль 2	68	12	14			42
Всього годин за навчальну дисципліну	150	30	30			90
Підсумковий контроль (екзамен)						

Організаційно-методичні вказівки до проведення навчальних занять та контрольних заходів: *при проведенні в режимі офлайн планувати проведення практичних занять в центрі кібербезпеки.*

4. Основні методи навчання

Під час викладання навчальної дисципліни передбачено застосування наступних форм.

Лекція – логічно вивершений, науково обґрунтований та систематизований виклад певного наукового або науково-педагогічного питання, ілюстрований засобами наочності та демонстрацією результатів досліджень.

Лекція є одним із основних видів і, водночас, методів проведення навчальних занять, призначених для засвоєння теоретичного матеріалу. Вона закладає основи наукових знань, визначаючи напрям, основний зміст та характер усіх видів навчальних занять, а також, головним чином, самостійної роботи здобувачів вищої освіти.

Практичне заняття – форма навчального заняття, на якому у здобувача вищої освіти під керівництвом викладача формуються вміння та навички практичного застосування теоретичних положень навчальної дисципліни шляхом виконання здобувачем вищої освіти відповідно сформульованих завдань.

Практичні заняття проводяться в аудиторії, оснащеною комп'ютерною технікою та технічними засобами навчання.

Практичне заняття включає в себе: проведення викладачем контролю знань, вмінь та навичок здобувачів вищої освіти, постановку загальної проблеми (завдання) та її обговорення за участю здобувачів вищої освіти, розв'язування завдань та їх обговорення, виконання контрольних завдань, їх перевірку та оцінювання викладачем.

Консультація – форма навчального заняття, на якому здобувач вищої освіти отримує від викладача відповіді на конкретні запитання або пояснення окремих теоретичних положень та їх використання на практиці.

Самостійна робота забезпечується навчально-методичними засобами, передбаченими для вивчення навчальної дисципліни: підручниками, навчально-методичними посібниками, конспектами лекцій, практикумами, електронно-обчислювальною технікою тощо.

Самостійна робота над засвоєнням навчального матеріалу може виконуватися в бібліотеці, комп'ютерному класі.

Форми самостійної роботи здобувачів вищої освіти:

- опрацювання теоретичних основ прослуханого лекційного матеріалу;
- вивчення окремих тем або питань, передбачених для самостійного опрацювання;
- виконання різних за формою і змістом завдань;
- підготовка до семінарських занять;
- підготовка до поточного, модульного та підсумкового контролю знань;
- пошук та огляд літературних джерел за проблематикою навчальної дисципліни;
- аналітичний розгляд наукової публікації тощо.

Під час вивчення початкової дисципліни «Аудит інформаційної безпеки та кібербезпеки» використовуються такі методи навчання:

– під час проведення лекційних занять – лекція-діалог, бесіда, а також наочних методів навчання, зокрема використання мультимедійних презентацій. Передбачено застосування таких методів формування пізнавального інтересу як навчальні дискусії;

– під час проведення семінарських занять – використання роздаткового матеріалу, нормативно-правові акти.

5. Оцінювання результатів навчання

5.1 Результати навчання здобувача вищої освіти з навчальної дисципліни оцінюються за 100-бальною шкалою як сума балів поточного та підсумкового контролю із застосуванням наступних вагових коефіцієнтів, загальна сума яких дорівнює 1:

Вид контролю	Ваговий коефіцієнт
Поточний контроль (К)	0,6
Підсумковий контроль (ПК)	0,4

Підсумкова семестрова оцінка (ПСО) обчислюється за формулою: ПСО=К+ПК

5.2. Складниками для обчислення балу поточного контролю здобувача вищої освіти є:

Види навчальної діяльності	Мак кількість балів	Вид навчальної роботи	Мак кількість балів
3 семестр			
Модуль №1 «Основи аудиту кібербезпеки»		Модуль №2 «Організація проведення аудиту кібербезпеки»	
Виконання та захист семінарського заняття 1	5	Виконання та захист семінарського заняття 1-2	5
Виконання та захист семінарського заняття 2	5	Виконання та захист семінарського заняття 3	5
Виконання та захист семінарського заняття 3-4	5	Виконання та захист семінарського заняття 4	5
Виконання та захист семінарського заняття 5-6	5	Виконання та захист семінарського заняття 5	5
Виконання та захист семінарського заняття 7	5	Виконання та захист семінарського заняття 6	5

<i>Для допуску до виконання модульної контрольної роботи №1 студент має набрати не менше 15 балів</i>		<i>Для допуску до виконання модульної контрольної роботи №2 студент має набрати не менше 15 балів</i>	
Виконання модульної контрольної роботи №1	15	Виконання модульної контрольної роботи №2	15
Усього за модулем №1	40	Усього за модулем №2	40
Усього за модулями №1, №2			80
Екзамен			20
Усього за дисципліною			100

Мінімальна кількість балів для допуску до підсумкового контролю 48 балів.

5.3. Шкала оцінювання здобувача вищої освіти

Оцінка за шкалою ЄКТС	Оцінка за 100-бальною шкалою	Значення оцінки
A	90-100	<i>Відмінно – відмінне виконання лише з незначною кількістю помилок.</i> Здобувач вищої освіти виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування і нахили.
B	84-89	<i>Дуже добре – вище середнього рівня, але з кількома помилками.</i> Здобувач вищої освіти вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв'язує справи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна
C	75-83	<i>Добре – загалом правильна робота, але з певною кількістю помилок.</i> Здобувач вищої освіти вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, серед яких є суттєві, добирати аргументи для підтвердження думок.
D	65-74	<i>Задовільно – непогано, але зі значною кількістю недоліків.</i> Здобувач вищої освіти відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння

		основних положень; з допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих.
E	60-64	<i>Достатньо</i> – виконання задовольняє мінімальні вимоги. Здобувач вищої освіти володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні.
FX	35-59	<i>Незадовільно</i> – потрібна додаткова робота. Здобувач вищої освіти володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу
F	1-34	<i>Незадовільно</i> – потрібна значна додаткова робота. Здобувач вищої освіти володіє матеріалом на рівні елементарного розпізнання і відтворення окремих фактів, елементів, об'єктів.

6. Ресурсне забезпечення навчальної дисципліни

Рекомендовані джерела інформації

Основна література:

1. Кіберпростір: основи кібербезпеки та кіберзахисту : Навч. посібник: У 3 ч. Ч.3 : Основи кіберзахисту / В. М. Богущ, В. Д. Бровко, В. П. Настратін. - Київ : Нац. акад. СБУ, 2020. - 272с.
2. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : Монографія / О. Левченко. - Житомир : Євро-Волинь, 2021. - 172с.
3. Кібервійна та безпека об'єктів критичної інфраструктури : Практ. посібник / Ю. І. Когут. - Київ : Консалтингова компанія "СІДКОН", 2021. - 332с.
4. Когут Ю. Кібервійна та безпека об'єктів критичної інфраструктури: Консалтингова компанія Сідкон, 2021. – 332 с.
5. Організаційно-правові основи забезпечення кібербезпеки : Підручник / М. В. Гуцалюк, А. І. Марущак, Д. С. Мельник [та ін.]; За заг. ред. Присяжнюка М.М. - Київ : Наук.-вид. відділ НА СБ України, 2023. - 320с.

Допоміжна література:

1. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с. : іл
2. Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів – Київ: ДУТ ННІЗІ, 2020. – 167 с.

Базові Стандарти.

1. ДСТУ ISO\IEC 9000 \ 9001: 2015. Системи менеджменту якості.

2. ДСТУ ISO\IEC 17021. Оцінка відповідності. Вимоги до органів, що здійснюють аудит і сертифікацію систем менеджменту.

3. ДСТУ ISO\IEC 17024. Оцінка відповідності. Загальні вимоги до органів по атестації персоналу. Схема сертифікації персоналу.

4. ДСТУ ISO\IEC 27001.

5. ДСТУ ISO / IEC 27002. Кодекс поведінки для перевірок інформаційної безпеки.

6. ДСТУ ISO / IEC 27003. Керівництво з впровадження СУІБ.

7. ДСТУ ISO / IEC 27004. Управління інформаційною безпекою - вимірювання;

8. ДСТУ ISO / IEC 27005. Управління ризиками інформаційної безпеки;

9. ДСТУ ISO / IEC 27006. Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою .

10. ДСТУ ISO / IEC 27007. Інструкції з перевірки СУІБ;

11. ДСТУ ISO / IEC TR 27008. Рекомендації для аудиторів перевірок інформаційної безпеки.

12. ДСТУ ISO/IEC 15408-1:2017 Інформаційні технології. Методи захисту. Критерії оцінки ч.1-5. Вступ та загальна модель (ISO/IEC 15408-1:2009, IDT).

13. ISO/IEC 15504 Information technology.Process assessment \ Інформаційні технології. Оцінка процесів ч.1-10.

14. COBIT 5 \ SACA. Control Objectives for Information and Related Technology \ Контрольні об'єкти інформаційних та суміжних технологій).

15. ITAF \ Information Technology Assurance Framework ISACA. Основні положення професійної практики аудиту та підтвердження довіри до ІС. Стандарт ITAF.

16. ITIL \ IT Infrastructure Library. Бібліотека інфраструктури інформаційних технологій.

17. Prince2 v.3. Проекти в контрольованому середовищі.

Інформаційні ресурси:

1. <http://uk.wikipedia.org> – Вікіпедія – Вільна енциклопедія

2. <https://www.mathcad.com/en/education>

3. www.zakon.rada.gov.ua

4. <http://cert.gov.ua/>

Адреса розміщення робочої програми навчальної дисципліни:

<https://moodle.academy.ssu.gov.ua>

(офіційний вебсайт НА СБУ / платформа дистанційного навчання / електронний ресурс навчально-наукового інституту, кафедри, бібліотеки тощо)

7. Дані про перегляд робочої програми навчальної дисципліни

№ п/п	Дата, номер протоколу засідання кафедри (спільного засідання кафедр)	Рішення за результатами перегляду	Підпис керівника кафедри
1.			
2.			
3.			
4.			
5.			