Прим. № ____

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	заочна
статус навчальної дисципліни	обов’язкова
мова викладання	українська

КИЇВ – 2025

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 Анастасія ВАВІЛЕНКОВА
«21» 07 2025 р.

1. Опис навчальної дисципліни

Показник	Значення показника
Курс	2
Семестр	3
Обсяг *(кредити ЄКТС/години)*	5 / 150
Кількість змістових модулів	1
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	8
семінарські заняття (СЗ)	8
практичні заняття (ПЗ)	-
лабораторні заняття (ЛЗ)	-
індивідуальні завдання (ІЗ)	-
самостійна робота (СР)	134
форма підсумкового контролю *(семестр)*	екзамен (3)

2. Мета та завдання навчальної дисципліни

2.1. Мета та основні завдання вивчення навчальної дисципліни

Мета: формування у здобувачів вищої освіти системи спеціальних знань щодо організації та супроводу процесів моніторингу й аудиту кібернетичної безпеки, 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:

– використовувати на практиці нормативні документи в галузі аудиту кібернетичної безпеки;

– проводити аудит і сертифікацію (атестацію) систем, підсистем інформаційної безпеки та систем управління інформаційною безпекою;

– визначати рівень якості та проведення контролю інфраструктури на основі критеріїв оцінки, технологій і методологій оцінювання стану КБ, ефективності функцій захисту інформації та рівня гарантій та їх коректності;

– проводити аналіз та володіти базовими технологіям визначення рівня ефективності систем і процесів інформаційної та кібернетичної безпеки підприємств та організацій;

– формувати звіти по результатам аналізу, процедурам проведеного аудиту і моніторингу, надавати рекомендації й пропозиції щодо протидії кіберінцидентам, підвищенню якості функціонування кібернетичної безпеки, а також інфраструктури організації в цілому.

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
1	*2*	*3*	*4*	*5*	*6*	*7*
Семестр 3						
Змістовий модуль 1. «Аудит інформаційної безпеки та кібербезпеки»						
Тема 1. Аудит інформаційної безпеки та кібербезпек	**150**	**8**	**8**			**134**
Лекція 1. Роль та задачі сучасної системи аудиту, контролю та моніторингу якості кібернетичної безпеки.		2				
Самостійна робота 1. Кращі світові практики, стандарти і вимоги до проведення процедур аудиту кібернетичної безпеки. Ринок послуг аудиту						22

кібербезпеки в світі.						
Самостійна робота 2. Сертифікація фахівців в галузі аудиту кібербезпеки. Аудит та моніторинг бізнес/операційних процесів підприємства.						22
Лекція 2. Методи та заходи планування процедур аудиту та моніторингу операційних процесів установи.		2				
Самостійна робота 3. Настанови щодо застосування стандартів ISO/IEC **з** безпеки та аудиту ІС і технологій: 17021, 17024, 15408, 15504						10
Семінарське заняття 1. Застосування вимог та положень стандартів ISO/IEC з безпеки та аудиту ІС і технологій: 17021, 17024, 15408, 15504			2			
Лекція 3. Критерії відповідності та довіри до інформаційних систем, показники та інструменти аудиту кібернетичної безпеки.		2				
Самостійна робота 4. Настанови щодо застосування вимог та положень стандартів CoBiT 5, ITAF						14
Семінарське заняття 2. Застосування вимог та положень стандартів CoBiT 5, ITAF			2			
Самостійна робота 5. Настанови щодо застосування вимог та положень стандартів ISO/IEC 27002:2024 27003:2015						14
Самостійна робота 6. Настанови щодо застосування вимог та положень стандартів ISO/IEC 27004:2018, 27006-2:2024						16
Семінарське заняття 3. Застосування вимог та положень стандартів ISO/IEC 27004:2018, 27006-2:2024			2			
Лекція 4.Організація та послідовність дій реалізації процесу та етапів аудиту кібернетичної безпеки		2				
Самостійна робота 7. Аналіз результатів аудиту та формування звітності функціонування системи кібербезпеки.						6
Самостійна робота 8. Настанови щодо застосування стандартів та кращих практик ITIL V3. IT Infrastructure Library, GTAG-8, CAATTs.						6
Семінарське заняття 4. Застосування вимог та положень стандартів та кращих практик ITIL V3. IT Infrastructure Library, GTAG-8, CAATTs.			2			
Самостійна робота 9. Настанови щодо застосування вимог та положень стандартів ISO/IEC 27006-2:2024 . Застосування вимог та положень стандартів ISO/IEC 27006-2:2024						6

Самостійна робота 10. Настанови щодо застосування вимог та положень ISO/IEC 27007:2022, 27008:2018						6
Самостійна робота 11. Застосування вимог та положень стандартів ISO/IEC 27007:2022, 27008:2018						6
Самостійна робота 12. Модульна контрольна робота						6
Всього годин за навчальну дисципліну	**150**	**8**	**8**			**134**
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 начальної 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	Max кількість балів
3 семестр	
Модуль №1 «Аудит інформаційної та кібербезпеки»	
Виконання та захист практичного заняття 1	15

Виконання та захист практичного заняття 2	15
Виконання та захист практичного заняття 3	15
Виконання та захист практичного заняття 4	15
Для допуску до виконання модульної контрольної роботи студент має набрати не менше набрати ***не менше 48 балів***	
Виконання модульної контрольної роботи №1	20
Усього за модулем	**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	*Відмінно – відмінне виконання лише з незначною кількістю помилок.* 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	*Дуже добре – вище середнього рівня, але з кількома помилками.* Здобувач вищої освіти вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв’язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна
C	75-83	*Добре – загалом правильна робота, але з певною кількістю помилок.* 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	*Задовільно – непогано, але зі значною кількістю недоліків.* 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	*Достатньо – 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	*Незадовільно – потрібна додаткова робота.* Здобувач вищої освіти володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу
F	1-34	*Незадовільно – 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. Богуш, В. Д. Бровко, В. П. Настрадін. - 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.			