Прим. № ____

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

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Управління кіберінцидентами»

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

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.

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 *(кредити ЄКТС/години)*	6 / 180
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)	120
форма підсумкового контролю *(семестр)*	екзамен (3)

2. Мета та завдання навчальної дисципліни

2.1. Мета та основні завдання вивчення навчальної дисципліни

Мета: формування системи спеціальних знань щодо організації процесу управління кіберінцидентами, ознайомлення та реалізація всіх етапів процесу управління кіберінцидентами, зокрема виявлення подій, категоризації та аналізу, реагування на кіберінциденти та поліпшення можливостей систем після усунення кіберінцидентів, підготовка фахівців, здатних ефективно реагувати на загрози кібербезпеці, опанування сучасними методами управління процесами кіберзахисту в умовах динамічних кіберзагроз.

Завдання:

– засвоїти теорію, концепцію та методологію управління кіберінцидентами;

– оволодіти навичками використання інструментів та технік виявлення, аналізу та реагування на події інформаційної безпеки;

– знати основні типи кіберінцидентів та їх життєвий цикл;

– знати етапи управління кіберінцидентами;

– оволодіти навичками щодо складання плану реагування на кіберінциденти;

– навчитися відновлювати дані та сервіси після інциденту інформаційної безпеки;

– оволодіти знаннями щодо аналізу причин інциденту та вміти розробляти заходи для запобігання кіберінцидентам;

– вивчити структуру, функції та роль центрів операційної безпеки;

– вивчити методології реагування на інциденти інформаційної безпеки;

– ознайомитися з програмним забезпеченням для збору та аналізу цифрових доказів.

2.2. Результати навчання

Обов'язкова навчальна дисципліна «Управління кіберінцидентами» 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 3	Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог.
ПРН 7	Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.
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 контролюючими органами.
ПРН 19	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
ПРН 23	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
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.

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. «Основи управління кіберінцидентами»						
Тема 1. Основи управління кіберінцидентами	**92**	**16**	**16**			**60**
Лекція 1. Поняття кіберінциденту та події інформаційної безпеки. Найвідоміші кіберінциденти в Україні та світі		2				
Семінарське заняття 1. Аналіз кіберінцидентів у світовій практиці			2			

Лекція 2. Категоризація та життєвий цикл кіберінцидентів.		2				
Семінарське заняття 2. Дослідження ланцюжка виникнення кіберінцидентів			2			
Самостійна робота 1. Дослідження статистики кіберінцидентів в Україні						10
Лекція 3. Джерела даних, методи та засоби виявлення кіберінцидентів		2				
Семінарське заняття 3**.** Аналіз роботи онлайн-платформи Shodan для пошуку і аналізу об’єктів, ресурсів та пристроїв у мережі Інтернет			2			
Самостійна робота 2. Дослідження різниці між подією інфомраційної безпеки та кіберінцидентом						10
Лекція 4. Виявлення подій. Знайомство з платформою MISP		2				
Семінарське заняття 4. Дослідження роботи сканерів вразливостей			2			
Лекція 5. Класифікація вразливостей комп’ютерних мереж та систем		2				
Семінарське заняття 5. Застосування аналізаторів мережевого трафіка			2			
Лекція 6. Сортування та аналіз подій		2				
Семінарське заняття 6. Ідентифікація та аналіз кіберінцидентів: методи та інструменти			2			
Лекція 7. Реагування та відновлення після кіберінциденту		2				
Самостійна робота 3. Логування та моніторинг як ключові елементи виявлення інцидентів						10
Семінарське заняття 7. Стримування, викорінення та відновлення після інцидентів			2			
Лекція 8. Поліпшення можливостей в процесі управління подіями інформаційної безпеки. Ретроспектива		2				
Самостійна робота 4. Аналіз зловмисного програмного забезпечення						15
Самостійна робота 5. Реагування на інциденти, пов'язані з хмарними технологіями та мобільними пристроями.						15

Семінарське заняття 8. **Модульна контрольна робота 1**			**2**			
Всього годин за модуль 1	**92**	**16**	**16**			**60**
Змістовий модуль 2. «Реагування на кіберінциденти»						
Тема 2. Реагування на кіберінциденти	**88**	**14**	**14**			**60**
Лекція 1. Класифікація вразливостей інформаційних систем		2				
Семінарське заняття 1. Види вразливостей, основні характеристики, спрямованість, експлойти			2			
Лекція 2. Моніторинг подій інформаційної безпеки		2				
Семінарське заняття 2. Складання плану реагування на кіберінциденти			2			
Самостійна робота 1. Основні аспекти складання інструкцій щодо реагування на кіберінциденти						15
Лекція 3. Центри операційної безпеки, їх основні функції, структура та ролі. Команди реагування на кіберінциденти SERT/CSIRT, їх відмінності		2				
Семінарське заняття 3. Побудова проєкту центру операційної безпеки SOC.			2			
Лекція 4. Засоби реагування на кіберінциденти. Рішення для захисту кінцевих точок EDR/XDR, SIEM/SOAR/xSOAR		2				
Самостійна робота 2. Аналіз реальних кейсів щодо реагування на кіберінциденти						15
Семінарське заняття 4. Види тестування систем. Робота з системами IPS. Робота з системами IDS.			2			
Лекція 5. Аналіз інцидентів та цифрова криміналістика. Цифрові докази		2				
Самостійна робота 4. Задачі цифрової криміналістики						15
Семінарське заняття 5. Життєвий цикл цифрових доказів, криміналістичні копії, ланцюг зберігання			2			
Лекція 6. Організаційні та правові аспекти розслідування кіберінцидентів		2				
Семінарське заняття 6. Сценарії розслідування кіберінцидентів			2			
Лекція 7. Національне та міжнародне		2				

законодавство у сфері кібербезпеки. Звітування та комунікація						
Самостійна робота 5. Використання програм Autopsy, EnCase, FTK Imager						15
Семінарське заняття 7. **Модульна контрольна робота 2**			2			
Всього годин за модуль 2	**88**	**14**	**14**			**60**
Всього годин за навчальну дисципліну	**180**	**30**	**30**			**120**
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 «Управління кіберінцидентами» 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 практичних 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	Вид навчальної роботи	Max кількість балів
3 семестр			
Модуль №1 «Основи управління кіберінцидентами»		Модуль №2 «Реагування на кіберінциденти»	
Виконання та захист семінарське 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
Для допуску до виконання модульної контрольної роботи №1 студент має набрати не менше набрати ***не менше 15 балів***		*Для допуску до виконання модульної контрольної роботи №2 студент має набрати* ***не менше 15 балів***	
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	*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. Вавіленкова А.І. Теоретичні засади та практика управління кіберінцидентами / А. І. Вавіленкова: монографія. – К.: Нац. акад. СБУ, 2025. – 146 с.

2. 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.

3. Основи кіберпростору, кібербезпеки та кіберзахисту: Навч. посібник / В. М. Богуш, В. В. Богуш, В. Д. Бровко [та ін.]. - К. : Ліра-К, 2021. – 554с.

4. Вавіленкова А. І. Методи і моделі протидії кібератакам: навч. посіб. Київ: НА СБУ, 2023. - 136 с.

5. Міжнародне співробітництво у сфері запобігання та протидії транснаціональній злочинності [Текст] : монографія / І. М. Леган. – Чернігів : НУ «Чернігівська політехніка», 2021. – 328 с.

6. Кібербезпека «суспільства знань»: Монографія / О. Д. Довгань, А. В. Тарасюк, Т. Ю. Ткачук. - К.; Одеса : Фенікс, 2021. - 176с.

7. Когут Ю. Кібервійна та безпека об'єктів критичної інфраструктури: Консалтингова компанія Сідкон, 2021. – 332 с.

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. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.]; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ: Вид-во Нац. акад. внутр. справ, 2020. 104 с.

3. А.Ковбель Forensic IV: Злочин та покарання: книга 2. Київ: Кінцевий бенефіцеар, 2024. - 192 с.

Інформаційні ресурси:

1. CERT-UA - Урядова команда реагування на комп'ютерні надзвичайні події України. URL: https://cert.gov.ua

2. Державна служба спеціального зв'язку та захисту інформації. URL: https://cip.gov.ua/ua

3. Правила обміну інформацією про кіберінциденти. Рішенням Національного координаційного центру кібербезпеки при Раді національної безпеки та оборони України (Протокол №21 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 09.02.2023). URL: https://scpc.gov.ua/api/files/bc88a70b-4996-48b3-8491-44409c3aae23

4. ENISA Considerations on the Traffic Light Protocol. URL: https://www.enisa.europa.eu/topics/cyber-threats.

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.			