НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Комп'ютерна та мережева криміналістика»

Освітня програма	Кіберзахист інформаційних ресурсів
Рівень вищої освіти	перший (бакалаврський)
Форма навчання	денна
Статус навчальної дисципліни	обов'язкова
Мова викладання	українська

КИЇВ – 2024

Робочу програму навчальної дисципліни розглянуто та затверджено на засіданні кафедри кібербезпеки ЦКБ ННІ ІБ СК НА СБ України від «02» 09 2024 року, протокол № 15.

1. Опис навчальної дисципліни

Показник	Значення показника
Курс	4
Семестр	8
Обсяг *(кредити ЄКТС/години)*	4 / 120
Кількість змістових модулів	2
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	30
семінарські заняття (СЗ)	
практичні заняття (ПЗ)	30
лабораторні заняття (ЛЗ)	-
самостійна робота (СР)	60
форма підсумкового контролю *(семестр)*	екзамен (8)

2. Мета та завдання навчальної дисципліни

2.1. Мета та основні завдання вивчення навчальної дисципліни

Мета: ознайомитися із засобами моніторингу та аналізу комп'ютерного мережевого трафіка для збору юридичних доказів і важливої інформації, яка може допомогти в процесі розслідування кіберінцидентів, навчитися використовувати інструменти для розслідування кібератак та надання практичних відомостей, які можна використовувати для прийняття коригувальних дій, розвинути навички у галузі інформаційної безпеки та кібербезпеки.

Завдання:

- вивчити ключові методи розслідування цифрових злочинів та порушень безпеки;
- вивчити процедури, що застосовуються при розслідуванні кіберзлочинів
- дослідити роботу інструментів для збирання цифрових доказів;
- оволодіти знаннями для аналізу цифрової інформації з метою відтворення хронології вчинення кіберінциденту;
- знати характеристику злочинності в мережі Інтернет;
- оволодіти програмами для розслідування кіберінцидентів;
- оволодіти способами реагування на кіберінциденти;
- вивчити інструменти для моніторингу та аналізу комп'ютерного мережевого трафіка для збору юридичних доказів;
- навчитися вивчати та досліджувати бази даних та пов'язані з ними метадані;
- вивчити методи відновлення та дослідження електронних листів;
- навчитися виявляти шкідливе програмне забезпечення;
- оволодіти знаннями щодо документування е-доказів.

2.2. Результати навчання

Обов'язкова навчальна дисципліна «Комп'ютерна та мережева криміналістика» спрямована на досягнення програмних результатів навчання, які в інтегрованому (синтезованому) вигляді визначені у профілі освітньо-професійної програми «Кіберзахист інформаційних ресурсів» *(від 11.09.2024 № 29/3/1/3-1277/ві),* а саме:

ПРН-03	Застосовувати результати алгоритмічного та абстрактного мислення, самостійного пошуку, аналізу та синтезу, методів теорії інформації, теорії систем та системного аналізу для ефективного вирішення завдань професійної діяльності, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.
ПРН-05	Адаптуватись до нових викликів та дій у певних ситуаціях, застосовувати знання державної та іноземних мов, інформаційно – комунікаційних технологій, комп'ютерної техніки для забезпечення професійної комунікації.
ПРН-13	Оцінювати стан безпеки особистості, суспільства та держави за окремими сферами забезпечення і видами діяльності на основі положень теорії безпеки окремих сфер забезпечення національної безпеки і видів діяльності.
ПРН-15	Аналізувати та упорядковувати основні властивості об'єктів безпеки окремих сфер забезпечення національної безпеки і видів діяльності та здійснювати класифікацію загроз об'єктам безпеки, класифікацію та ранжирування джерел загроз і уразливостей безпеки
ПРН-21	Вирішувати завдання захисту інформації, що обробляється на об'єктах інформаційної інфраструктури та кіберінфраструктури, з використанням методів, засобів і механізмів криптографічного захисту інформації, а також володіти методами сучасних систем цифрової криміналістики і застосовувати їх в дослідницькій та прикладній діяльності.
ПРН-22	Обґрунтовувати застосування методів та засобів захисту програмних засобів, оцінки забезпечення якості програмного забезпечення а також інформаційно-програмних ресурсів і процесів, що беруть участь в життєвому циклі застосунків
ПРН-24	Забезпечувати процеси захисту та функціонування інформаційно-комунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурнологічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
ПРН-25	Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів в сфері кібербезпеки

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 8						
Модуль 1. Форензика та її роль у розслідуванні кіберінцидентів						
Тема 1. Форензика як наука. Цифрові докази	**32**	**8**		**8**		**16**
Лекція 1. Форензика. Основні поняття та визначення		2				
Самостійна робота №1. Повторення матеріалів лекції №1						2
Лекція 2. Види форензики. Поняття цифрового сліду. Класифікація цифрових доказів		2				
Самостійна робота №2. Повторення матеріалів лекції №2						2
Лекція 3. Цифрові методи оперативної (попередньої) та експертної ідентифікації осіб. Пошук необхідних для розслідування інциденту цифрових даних		2				
Самостійна робота №3. Повторення матеріалів лекції №3						2
Практичне заняття 1. Open Source інструментарій для проведення цифрових розслідувань і збору даних				2		
Лекція 4. Вимоги до оформлення цифрових доказів для набуття ними статусу судового доказу.		2				
Практичне заняття 2. Робота з Digital Evidence & Forensics Toolkit				2		
Практичне заняття 3. Проведення заходів форензики – аналіз наслідків зламу ком'ютерних систем, визначення втрачених та скомпроментованих даних				2		
Практичне заняття 4. Інструменти для збирання цифрових доказів вчинення кіберзлочинів				2		
Самостійна робота №4. Оформлення протоколів для практичного заняття 1-4						10
Тема 2. Розслідування кіберзлочинів	**22**	**4**		**6**		**12**
Лекція 5. Відеофіксація гласних і негласних слідчих дій. Поліпшення якості відео, збільшення окремих ділянок зображення; визначення розмірів і швидкості руху об'єктів		2				
Практичне заняття 5. Вивчення Skadi як набіру утиліт з відкритим вихідним кодом для				2		

зберігання, оброблення та проведення розширеного аналізу криміналістичних артефактів і зображень						
Самостійна робота №5. Опрацювання матеріалів лекції 5						6
Лекція 6. Комп'ютерно-технічна експертиза під час розслідування кіберзлочинів, Встановлення схеми і хронології втручання, вилучення даних про способи атак		2				
Практичне заняття 6. Autopsy для цифрової криміналістики та графічний інтерфейс для аналізатора образів дисків і програм для цифрової криміналістики				2		
Практичне заняття 7. Веб-додаток для спільної роботи над складними і заплутаними розслідуваннями IRIS				2		
Самостійна робота №6. Опрацювання протоколів до практичного заняття №5-7						6
Тема 3. Цифрові експертизи	**16**	**4**		**4**		**8**
Лекція 7. Цифрова експертиза мобільних пристроїв та програмна комп'ютерна експертиза		2				
Практичне 8. Платформа Kuiper дя збору та аналізу доказів				2		
Лекція 8. Цифрова експертиза в інцидентах шахрайства		2				
Практичне заняття 9. Особливості роботи на платформі реагування на кіберінциденти безпеки TheHive				2		
Самостійна робота №7. Підготовка до модульної контрольної роботи №1						8
Модульна контрольна робота 1	**2**			**2**		
Всього годин за модуль 1	**72**	**16**		**20**		**36**
Модуль 2. Мережева криміналістика						
Тема 4. Основи мережевої криміналістики	**20**	**6**		**4**		**10**
Лекція 9. Шкідливе програмне забезпечення та методи його виявлення		2				
Практичне заняття 11. Інструменти моніторингу та виявлення шкідливого програмного забезпечення				2		
Лекція 10. Засоби моніторингу, реєстрації та аналізу мережевої активності		2				
Лекція 11. Методи та алгоритми розслідування та аналізу кіберінцидентів з використанням реал-тайм утиліт		2				

Практичне заняття 12. Робота з сніферами та програмним забезпеченням для аналізу мережевого трафіка SiLKTools				2		
Самостійна робота №8. Опрацювання матеріалів протоколів до практичного заняття №11-12						10
Тема 5. Робота з вилучення цифрових доказів	**28**	**8**		**4**		**14**
Лекція 12. Криміналістика баз даних. Робота з метаданими		2				
Лекція 13. Відновлення та дослідження електронних листів та контактів. Відновлення SIM-карт та телефонних контактів.		2				
Лекція 14. Фіксація слідів та збір доказів здійснення кібератак		2				
Практичне заняття 13. Програмне забезпечення для роботи з артефактами Інтернету та аналізу часових інтервалів				2		
Лекція 15. Розслідування кіберзлочинів		2				
Практичне заняття 14. Дослідження роботи інструментів та тестування на проникнення				2		
Самостійна робота №9. Підготовка до написання модульної контрольної роботи №2						12
Модульна контрольна робота 2	**2**			**2**		
Всього годин за модуль 2	**48**	**14**		**10**		**24**
Всього годин за 8 семестр	**120**	**30**		**30**		**60**
Підсумковий контроль за 8 семестр (*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 практичних 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 викладання навчальної дисципліни «Комп'ютерна та мережева криміналістика» використовуються такі методи навчання: індуктивний, дедуктивний, 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. Дослідницький 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.

Теоретична підготовка здобувачів вищої освіти забезпечується шляхом вивчення вимог керівних документів з питань національної та інформаційної безпеки, політико-правових аспектів формування інформаційного суспільства держави, науково-методичних засад державного управління національними інформаційними ресурсами як необхідної складової системи інформаційної безпеки.

Основними видами занять є лекції, практичні, семінарські та самостійні заняття.

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)	**0,8**
Підсумковий контроль (ПК)	**0,2**

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	Кількість балів (максимальна)
Робота на лекціях (ведення конспекту лекцій або інше)	5
Робота на практичних заняттях	50
Виконання завдань для самостійної роботи	5
Виконання модульної контрольної роботи	20
Екзамен	20

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

2. 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. Гаркуша А.М., Каланча І.Г. Виявлення та фіксація доказів, що мають електронну форму під час кримінального провадження: організаційні аспекти. *Наукові читання пам'яті Ганса Гросса:* збірник тез міжнародної науково-практичної конференції (м. Чернівці, 09 грудня 2021 р.). Чернівецький національний університет імені Юрія Федьковича. Чернівці: Технодрук, 2021. С. 72–76.

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

5. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури: підручник. Київ: КУБГ, 2019. 218 с.

6. Козюра В.Д., Хорошко В.О., Шелест М.Є., Ткач Ю.М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. 236с.

Допоміжна література:

1. Доказування у кримінальному провадженні: кол. авт. Київ: Національна академія прокуратури України, 2017. 346 с.

2. Електронні докази. Обшук / [О. І. Литвинчук, М. С. Сорока, І. В. Колесников та ін.]. Харків: Фактор, 2020. Ч. 1. 80 с.

3. Виходець Ю. О. До питання фіксування негласних слідчих (розшукових) дій, проведених з використанням комп'ютерних технологій. *Правова позиція*. 2022. № 2 (35). С. 108–111.

4. Ільїн К.І,. Стьопочкіна І.В. Безпека інформаційних систем: Лабораторний практикум: навч. посіб.. Київ : КПІ ім. Ігоря Сікорського, 2020. 60 с.

Інформаційні ресурси

1. Національна бібліотека ім. В.І.Вернадського / [Електронний ресурс]. – Режим доступу: http:www.nbuv.gov.ua/

2. Цифровий репозитарій ХНУГХ ім. А.Н.Бекетова / [Електронний ресурс]. – Режим доступу: http://eprints.kname.edu.ua/

3. Цифровий репозитарій Харківського національного університету ім. В.Н.Каразіна / [Електронний ресурс]. – Режим доступу: http://dspace.univer.kharkov.ua/handle/123456789/568

4.https://hackyourmom.com/kibervijna/kompyuterna-kryminalistyka-forenzyka-dobirka-korysnyh-posylan/

Адреса розміщення робочої програми навчальної дисципліни:

https://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.			

29/3/1/1-1537/бі
10.10.24