Прим. № ____

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Навчальна практика»

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

КИЇВ – 2025

Робочу програму навчальної практики розглянуто та затверджено на засіданні кафедри ТЗК ЦКБ ННІ ІБ СК НА СБ України від «18» 12 2024 року, протокол № 16.

1. Опис навчальної дисципліни

Показник	Значення показника
Курс (и)	3
Семестр (и)	6
Обсяг *(кредити ЄКТС/години)*	3 / 90
Кількість змістових модулів	-
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	
семінарські заняття (СЗ)	
практичні заняття (ПЗ)	
лабораторні заняття (ЛЗ)	-
індивідуальні завдання (ІЗ)	
самостійна робота (СР)	90
форма підсумкового контролю *(семестр)*	диф. залік (6)

2. Мета та завдання навчальної дисципліни

2.1. Мета та основні завдання вивчення навчальної дисципліни

Мета: полягає у закріпленні теоретичних знань, формуванні практичних навичок, розвитку аналітичного мислення, засвоєнні командної роботи, ознайомлені з реальними системами та інструментами, що сприяє інтеграції теоретичних знань із практичними навичками, забезпечуючи підготовку у сфері кіберзахисту.

Завдання:

- відпрацювання тактик відбиття кібератак, а також симуляція кібератак з одночасним відпрацюванням методик кібернападів;
- формування навичок з практичної оцінки стану кібербезпеки, практичного застосування процесів та технологій тестування захищеності інформаційних систем в реальному середовищі.

2.2. Результати навчання

Обов'язкова навчальна дисципліна «Навчальна практика» 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/в.і.),* 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-06.	Використання знань з основних методів наукового пошуку; вміння узагальнювати отримані результати, обробки та аналізу інформації з різних джерел, оформлення та презентування результатів наукової діяльності, здатності

	використовувати статистичні методи в професійній діяльності.
ПРН-07.	Обґрунтовувати та визначати основні напрями створення та експлуатації системи та основних підсистем управління інформаційною безпекою та кібербезпекою, використовуючи інформаційні та комунікаційні технології для формування ефективної системи інформаційно-аналітичного забезпечення, підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.
ПРН-09.	Вміти здійснювати комплексний аналіз загроз національній безпеці, розробляти та реалізовувати ефективні стратегії їх нейтралізації, застосовуючи знання з основ теорії національної безпеки та синтезуючи різнопланову інформацію.
ПРН-20.	Визначати, розробляти та впроваджувати ефективні системи технічного захисту інформації на об'єктах інформаційної та кіберінфраструктури, застосовуючи сучасні технології та методи для забезпечення безпеки інформаційних ресурсів.
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.

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 VI						
Змістовий модуль 1.						
Тема 1. Основи кібербезпеки та розвідки	6					6
Тема 2. Організація роботи на кіберполігоні: правила, методи та техніка безпеки.	6					6
Тема 3. Захист інформаційних систем.	6					6
Тема 4. Огляд основних інструментів кіберполігону: сканери вразливостей, емулятори атак, моніторингові системи.	6					6
Тема 5. Аналіз відомих кібератак, виявлення типових схем і тактик зловмисників.	6					6
Тема 6. Розгляд різних типів кібератак (віруси, трояни, DDoS, фішинг тощо).	6					6
Тема 7. Ознайомлення з основними інструментами, що використовуються хакерами для проведення атак.	6					6
Тема 8. Конфігурування операційних систем для підвищення рівня безпеки.	6					6
Тема 9. Використання сучасного програмного забезпечення, систем моніторингу та аналізу безпеки.	8					8
Тема 10. Створення складних паролів, двофакторна аутентифікація. Усунення вразливостей операційних систем і програмного забезпечення.	6					6
Тема 11. Аналіз вразливостей мережевих протоколів (FTP, SSH, HTTP тощо).	6					6
Тема 12. Налаштування і використання фаєрволів для контролю мережевого трафіку.	8					8
Тема 13. Створення безпечних тунелів для передачі даних.	6					6
Тема 14. Аналіз мережевого трафіку на предмет ознак атак.	8					8
Підсумковий контроль *(диф. залік)*						
Всього годин за навчальну дисципліну	**90**					**90**

Організаційно-методичні вказівки до проведення навчальних занять та контрольних заходів:

Навчальна практика проводиться на базі центру кібербезпеки ННІ ІБ СК протягом двох тижнів з використанням віртуального середовища, яке імітує реальну ІТ-інфраструктуру компанії або організації - кіберполігону. На базі кіберполігону у студентів є можливість безпечно відпрацьовувати різноманітні сценарії кібератак, вивчати нові інструменти та вдосконалювати свої навички.

На початку практики завідувач кафедри ТЗК проводить інструктаж з техніки безпеки та пожежної безпеки щодо проходження студентами подальших навчальних занять.

За період навчальної практики студент повинен:

- ✓ отримати завдання для проходження навчальної практики;
- ✓ пройти інструктаж із техніки безпеки на базі практики;
- ✓ ознайомитися з теоретичним викладеним матеріалом;
- ✓ на базі викладеного матеріалу закріпити набуті знання у вигляді індивідуальних завдань (симуляцій, аналіз реальних інцидентів кібербезпеки);
- ✓ як підсумок виконати проєктну роботу у вигляді презентації;
- ✓ захистити проєкт.

4. Основні методи навчання

І. Методи організації та здійснення навчально-пізнавальної діяльності:

1. За джерелом інформації: словесні, наочні.

2. За логікою передачі і сприймання навчальної інформації: індуктивні, дедуктивні, аналітичні, синтетичні.

3. За ступенем самостійності мислення: репродуктивні, пошукові, дослідницькі.

4. За ступенем керування навчальною діяльністю: під керівництвом викладача; самостійна робота студентів: з книгою; виконання симуляцій; групова: аналіз реальних інцидентів кібербезпеки.

ІІ. Форми проведення занять:

Симуляції кібератак: відпрацювання сценаріїв атак та захисту.

Розв'язання кейсів: аналіз реальних інцидентів кібербезпеки.

Проєктна робота: розробка рішень для конкретних завдань кіберзахисту.

5. Оцінювання результатів навчання

Загальне методичне керівництво практикою здійснюється кафедрою ТЗК. Загальне керівництво виробничою практикою здійснює завідувач даної кафедри.

За підсумками навчальної практики студент надає на кафедру електронний варіант презентації за отриманим завданням та представляє проєктну роботу на засіданні кафедри ТЗК.

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	Кількість балів (максимальна)
Активність на заняттях	5
Якість виконання робіт	20
Результати симуляцій кібератак	20
Звіт про виконані завдання	15
Захист індивідуальних проєктів	40

Мінімальна кількість балів для допуску до підсумкового контролю - 60

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 практики

Основна література:

1. Марк Гудмен, Злочини майбутнього, Видавництво Фабула , 2019, 592с.
2. S. Caltagirone, A. Pendergast, and C. Betz, "Diamond Model of Intrusion Analysis", Center for Cyber Threat Intelligence and Threat Research, Hanover, MD, Technical Report ADA586960, 05 July 2013.
3. Dakshina Ranjan Kisku, Phalguni Gupta, Jamuna Kanta Sing Advances in Biometrics for Secure Human Authentication and Recognition Видавництво: CRC Press - дання: 2016, Сторінок: 352, ISBN: 9781138033771
4. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі [Текст]: Навчальний посібник / О.В.Курбан. – Київ: ВІКНУ, 2016. - 286 с
5. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою: Навч. посібник. Дніпро: Дніпроп. держ. Унт внутріш. справ, 2020. 144с.
6. Коробейнікова Т. І., Захарченко С. М. Технології захисту локальних мереж на основі обладнання CISCO Видавництво: Львівська політехніка Рік видання: 2021, С.: 232, ISBN: 978-966-941-583-7

Інформаційні ресурси:

1. 160 Cybersecurity Statistics 2023 : веб-сайт. URL: https://www.getastra.com/blog/security-audit/cyber-security-statistics/
2. Dev.ua : веб-сайт. URL: https://dev.ua/news/v-ukraini-zapustyly-kiberpolihon-dlia-praktychnoho-trenuvannia-spetsialistiv-vin-maie-150-stsenariiv-1686759364
3. Cranford J.J RED TEAM VS BLUE TEAM IN CYBERSECURITY : веб-сайт URL: https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/
4. Mitre.att&ck : веб-сайт. URL: https://attack.mitre.org/
5. OWASP : веб-сайт .URL: https://owasp.org/
6. Фішинг : веб-сайт URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/fishing/

7. What is a DDoS Attack? : веб-сайт URL: https://sucuri.net/guides/what-is-a-ddos-attack/
8. Cross Site Scripting (XSS) : веб-сайт URL: https://owasp.org/www-community/attacks/xss/
9. Підручник з SQL веб-сайт URL: https://www.w3schools.com/sql/default.asp
10. SSRF (SERVER-SIDE REQUEST FORGERY) : веб-айт URL: https://cqr.Company/web-vulnerabilities/ssrf/

Адреса розміщення робочої програми навчальної практики

_____

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

7. Дані про перегляд робочої програми навчальної практики

№ п/п	Дата, номер протоколу засідання кафедри (спільного засідання кафедр)	Рішення за результатами перегляду	Підпис керівника кафедри

29/3/1/4-133/6
23.01.25