Прим. № ____

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

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Методи і моделі протидії кіберзагрозам»

освітня програма	Кіберзахист у сфері інформаційних технологій та кіберпросторі (ID 64490)
рівень вищої освіти	другий (магістерський)
форма навчання	денна
статус навчальної дисципліни	обов’язкова
мова викладання	українська

КИЇВ – 2024

Робочу програму навчальної дисципліни розглянуто та схвалено на засіданні кафедри кібербезпеки від «02» 09 2024 року, протокол №15

Робочу програму навчальної дисципліни погоджено з гарантом освітньої програми

Завідувач кафедри кібербезпеки
ЦКБ ННІ ІБ СК НА СБ України
д.т.н., професор
«02» 09 2024 р.

Анастасія ВАВІЛЕНКОВА

1. Опис навчальної дисципліни

Показник	Значення показника
Курс	1
Семестр	2
Обсяг *(кредити ЄКТС/години)*	5 / 150
Кількість змістових модулів	2
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	18
семінарські заняття (СЗ)	-
практичні заняття (ПЗ)	38
лабораторні заняття (ЛЗ)	-
самостійна робота (СР)	94
форма підсумкового контролю *(семестр)*	екзамен (2)

2. Мета та завдання навчальної дисципліни

2.1. Мета та основні завдання вивчення навчальної дисципліни

Мета: підготовка професіоналів з організації інформаційної безпеки з урахуванням специфічних особливостей забезпечення державної безпеки шляхом організації кіберзахисту у сфері інформаційних технологій та кіберпросторі, які володіють методами протидії кіберзагрозам, стратегіями та моделями здійснення кібератак, методами виявлення уразливості систем та їх усунення, вміють застосовувати та розробляти моделі протидії кіберзагрозам, володіють методами боротьби з DDoS-атаками на підставі отриманих теоретичних та практичних знань.

Завдання:

- систематизація та розширення знань про методи соціальної інженерії, види шкідливого програмного забезпечення та кібератак;
- оволодіння стратегіями та моделями здійснення кібератак;
- засвоєння методів боротьби з DDos-атаками;
- вивчення методів маскування та шифрування даних для забезпечення захисту інформації;
- оволодіння сучасними технологіями організації захисту кінцевих точок;
- засвоєння навиків роботи з налаштуванням та використанням програмних сервісів організації захисту даних;
- засвоєння навиків роботи з інструментами моделювання кіберзахисту.

2.2. Результати навчання

Обов’язкова навчальна дисципліна «Методи і моделі протидії кіберзагрозам» спрямована на досягнення програмних результатів навчання, які в інтегрованому (синтезованому) вигляді визначені у профілі освітньо-професійної програми «Кіберзахист у сфері інформаційних технологій та кіберпросторі» *(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 22	Оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації
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 2						
Змістовий модуль 1. «Кіберзагрози. Основні аспекти виявлення та аналізу кіберзагроз»						
Тема 1. Кіберзагрози. Основні аспекти виявлення та аналізу кіберзагроз	**74**	**8**		**24**		**42**
Лекція 1. Поняття та класифікація кіберзагроз. Моделі порушників та їх характеристики		2				
Практичне заняття 1. Аналіз прикладів реальних кіберзагроз та атак. Класифікація кіберзагроз				2		
Самостійна робота 1. Вивчення термінології, ознайомлення з кубом кібербезпеки						8
Лекція 2. Методи виявлення та аналізу кіберзагроз		2				
Практичне заняття 2. Практика роботи з логами для виявлення ознак загроз				2		

Самостійна робота 2. Інструменти пошуку вразливостей для виявлення кіберзагроз						8
Практичне заняття 3. Класифікація кіберзагроз. Налаштування мережевого моніторингу				2		
Самостійна робота 3. Створення додаткових правил для роботи захисника Windows						8
Практичне заняття 4. Використання утиліти Wireshark для аналізу трафіку та виявлення кіберзагроз				2		
Лекція 3. Структура та основні функції систем виявлення вторгнень		2				
Практичне заняття 5. Використання IDS/IPS для виявлення атак				2		
Практичне заняття 6. Дослідження роботи SIEM-систем та їх ролі у протидії кіберзагрозам				2		
Практичне заняття 7. Практика роботи з SIEM-системою				2		
Самостійна робота 4. Структура SIEM-систем						8
Лекція 4. Методи кореляції та аналізу подій		2				
Практичне заняття 8. Застосування методів кореляції та аналізу подій				2		
Практичне заняття 9. Побудова сценаріїв реагування на кіберзагрози				2		
Практичне заняття 10. Криптографічні методи протидії кіберзагрозам.				2		
Практичне заняття 11. Шифрування з симетричним та асиметричним ключем				2		
Самостійна робота 5. Дослідження особливостей виявлення атак, організованих за моделлю Man in the Middle						10
Практичне заняття 12. Модульна контрольна робота 1				**2**		
Всього годин за перший модуль	**74**	**8**		**24**		**42**
Змістовний модуль №2. «Засоби протидії кіберзагрозам»						
Тема 2. Засоби протидії кіберзагрозам	**76**	**10**		**14**		**52**
Лекція 1. Методи захисту критичної інформаційної інфраструктури. Приховування даних. Маскування даних. Стеганографія.		2				
Практичне заняття 1. Аналіз матриці ATT&CK від MITRE для вивчення тенденцій в розвитку кібератак та уточнення тактики противника.				2		
Самостійна робота 1. Вивчення методів						8

стеганографії						
Лекція 2. Методи протидії шкідливому програмному забезпеченню		2				
Практичне заняття 2. Аналіз шкідливого програмного забезпечення у тестовому середовищі				2		
Самостійна робота 2. Класифікація шкідливого програмного забезпечення						8
Лекція 3. Моделі захисту від атак соціальної інженерії.		2				
Практичне заняття 3. Виявлення ознак фішингу та соціальної інженерії				2		
Лекція 4. DLP-системи та методи запобігання витоку даних		2				
Практичне заняття 4. Практика роботи з DLP-системами				2		
Практичне заняття 5. Організація захисту кінцевих точок, основні методи. Модель «нульової довіри» Zero Trust.				2		
Практичне заняття 6. Аналіз параметрів атак, пошук точок входу та уразливостей.				2		
Самостійна робота 3. Проходження курсу Cisco «Безпека кінцевих пристроїв»						20
Самостійна робота 4. Дослідження роботи програмних засобів захисту даних						8
Лекція 5. Моделі кіберзахисту державного рівня. Організаційно-технічна модель кіберзахисту		2				
Самостійна робота 5. Інструменти та практики протидії кіберзагрозам						8
Практичне заняття №7. Модульна контрольна робота 2				**2**		
Всього годин за другий модуль	**76**	**10**		**14**		**52**
Підсумковий контроль (*екзамен***)**						
Всього годин за дисципліну	**150**	**18**		**38**		**94**

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;

– виконання індивідуальних завдань (написання курсової роботи);

– аналітичний розгляд наукової публікації тощо.

Під час вивчення начальної дисципліни «Методи і моделі протидії кіберзагрозам» 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)	**0,8**
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	Max кількість балів	Вид навчальної роботи	Max кількість балів
2 семестр			
Модуль №1 «**Кіберзагрози. Основні аспекти виявлення та аналізу кіберзагроз**»		Модуль №2 «**Засоби протидії кіберзагрозам**»	
Виконання та захист практичного заняття 1-2	5	Виконання та захист семінарського заняття 1	5
Виконання та захист практичного заняття 3-4	5	Виконання та захист семінарського заняття 2-4	10
Виконання та захист практичного заняття 5-6	5	Виконання та захист семінарського заняття 5	5
Виконання та захист практичного заняття 7-8	5	Виконання та захист семінарського заняття 6	5
Виконання та захист практичного заняття 9-11	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. Методи і моделі протидії кібератакам : навч. посіб. / А. І. Вавіленкова. – Київ : Нац. акад. СБУ, 2023. – 144 с.

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

3. Методи та засоби технічного захисту інформації: Опорний конспект лекцій [Електронний ресурс]: навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: В.М. Луценко, Д.О. Прогонов. – Електронні текстові дані (1 файл: 1,80 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 289 с.

4. Організаційно-правові основи забезпечення кібербезпеки: підруч./ М.М.Присяжнюк, А.І. Марущак, Д.С. Мельник, В.В. Остроухов, М.В. Гуцалюк, О.П. Ткаченко; за заг. Ред. М.М. Присяжнюка. Київ: Видавництво Ліра-К, 2023. 320 с.

5. 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.

6. Комаров М. Ю. Методи та засоби захисту інформації від кібервпливів в комп’ютерних системах та мережах критичної інфраструктури – Дисертація на здобуття наукової ступені кандидат технічних наук , Київ -2021 р. – 171 с.

7. Харченко В.С., Яковлев С.В., Горбачик О.С. та ін. Забезпечення функціональної безпеки критичних інформаційно–керуючих систем :

монографія/ за ред. В.С.Харченка, С.В.Яковлева. Харків: Константа, 2019. – 272 с.

8. Безпека інформаційних систем: Лабораторний практикум [Електронний ресурс] : навч. посіб. для студ. спеціальностей 126 «Інформаційні системи та технології» / КПІ ім. Ігоря Сікорського; уклад.: К. І. Ільїн, І. В. Стьопочкіна. – Електронні текстові дані (1 файл: 2,1 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 60 с.

Допоміжна література:

9. Богуш, В. М. Кіберпростір: основи кібербезпеки та кіберзахисту : Навч. посібник: Ч.3 : Основи кіберзахисту / В. М. Богуш, В. Д. Бровко, В. П. Настрадін. - Київ : Нац. акад. СБУ, 2020. – 272с.

10. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах : навч. посіб. – Кропивницький: Видавець Лисенко В. Ф., 2020. – 295 с.

11. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.

12. Костюченко А.О., Горошко Ю.В. Віртуалізація операційних систем: навчально-методичний посібник. Ч.: ФОП Баликіна С.М., 2021. 56 с

13. Жилін А.В. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О.А. Успенський; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

Інформаційні ресурси

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

2. Інформаційно-комунікаційні технології. Веб - сайт ООН [Електронний ресурс]. – Режим доступу: http://www.un.org/ru/development/ict/index.shtml

3. Правове забезпечення кіберзахисту в Україні / [Електронний ресурс]. – Режим доступу: https://coordynata.com.ua/pravove-zabezpecenna-kiberzahistu-v-ukraini

4. Поняття та зміст кіберзагроз на сучасному етапі [Електронний ресурс]. – Режим доступу: https://goal-int.org/ponyattya-ta-zmist-kiberzagroz-na-suchasnomu-etapi.

5. Як зменшити ризики кіберзагроз, спрямованих проти інформаційної безпеки компаній [Електронний ресурс]. – Режим доступу: https://vkp.ua/publication/yak_zmenshiti_riziki_kiberzagroz_spryamovanikh_proti_informatsiynoi_bezpeki_kompaniy

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.