Прим. № 1

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Хмарні технології і захист веб-додатків»

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

КИЇВ – 2024

N 907 по пс 417

Робочу програму навчальної дисципліни розглянуто та схвалено на засіданні кафедри технічного захисту інформації від 18.09.2024 року, протокол № 12.

1. Опис навчальної дисципліни

Показник	Значення показника
Курс (и)	4
Семестр (и)	7
Обсяг *(кредити ЄКТС/години)*	4 / 120
Кількість змістових модулів	2
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	30
практичні заняття (ПЗ)	30
самостійна робота (СР)	60
форма підсумкового контролю *(семестр)*	Диф.залік (7)

Передумовами для вивчення та успішного засвоєння навчальної дисципліни «Хмарні технології і захист веб-додатків» є: «Інформаційні технології», «Програмні засоби захисту інформації», «Безпека смарт-технологій та Інтернет речей», «Безпека інформації в інформаційно-комунікаційних системах».

2. Мета та завдання навчальної дисципліни

2.1. Мета та основні завдання вивчення навчальної дисципліни

Мета:

вивчення теоретичних основ хмарних технологій, базових засад хмарних середовищ, їх внутрішньої структури, технологій безпечного функціонування Веб аплікацій і для набуття навиків безпечного їх використання.

Завдання:

формування професійної компетентності майбутніх фахівців в галузі безпеки Web-додатків та Web-сервісів, організації захисту інформаційних мережевих систем, систем ідентифікації, аутентифікації і авторизації користувачів та набуття навиків безпечної роботи в хмарі.

2.2. Результати навчання

Обов'язкова навчальна дисципліна «Хмарні технології і захист веб-додатків» спрямована на досягнення програмних результатів навчання, які в інтегрованому (синтезованому) вигляді визначені у профілі освітньо-професійної / освітньо-наукової програми «Кіберзахист інформаційних ресурсів» *(від 11.09.2024 № 29/3/1/3-1277 ві)*, а саме:

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-12. Планувати та організовувати особисту діяльність в умовах протиборства в інформаційній сфері та кіберпросторі для забезпечення інформаційної безпеки та кібербезпеки держави та організації.

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-17. Здійснювати заходи щодо запобігання розголошення секретної інформації, випадкам втрат матеріальних носіїв цієї інформації, заволодіння цією інформацією іноземними державами, іноземними юридичними особами, іноземцями, особами без громадянства та громадянами України, яким не надано допуск та доступ до неї.

ПРН-23. Захищати авторські права, комерційну таємницю, розробляти договори щодо розпорядження правами інтелектуальної власності в ІТ сфері.

ПРН-24. Забезпечувати процеси захисту та функціонування інформаційно-комунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

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 7						
Змістовий модуль 1. Захист Веб додатків						
Тема 1. Поняття атаки «людини посередині». Небезпека cookies через незахищені з'єднання.	**8**	**2**		**2**		**4**
Лекція 1. Поняття атаки «людини посередині». Небезпека cookies через незахищені з'єднання.		2				
Практичне заняття 1. Поняття атаки «людини посередині». Небезпека cookies через незахищені з'єднання.				2		
Самостійна робота 1. Поняття атаки «людини посередині». Небезпека cookies через незахищені з'єднання.						4
Тема 2. XSS та Cookie атаки з перехоплення інформації. Встановлення сигналів для використання практик ліквідації.	**8**	**2**		**2**		**4**
Лекція 2. XSS та Cookie атаки з перехоплення інформації. Встановлення сигналів для використання практик ліквідації.		2				
Практичне заняття 2. XSS та Cookie атаки з перехоплення інформації. Встановлення сигналів для використання практик ліквідації.				2		
Самостійна робота 2. XSS та Cookie атаки з перехоплення інформації. Встановлення сигналів для використання практик ліквідації.						4

Тема 3. Поняття безпечних cookies. Використання тимчасових cookies для подальшого зменшення ризиків.	**8**	**2**		**2**		**4**
Лекція 3. Поняття безпечних cookies. Використання тимчасових cookies для подальшого зменшення ризиків.		2				
Практичне заняття 3. Поняття безпечних cookies. Використання тимчасових cookies для подальшого зменшення ризиків.				2		
Самостійна робота 13. Поняття безпечних cookies. Використання тимчасових cookies для подальшого зменшення ризиків.						4
Тема 4. Розкриття інформації через robots.txt. Ризики в джерелах HTML. Ідентифікація ненадійних даних у параметрах запитів HTTP.	**8**	**2**		**2**		**4**
Лекція 4. Розкриття інформації через robots.txt. Ризики в джерелах HTML.		2				
Практичне заняття 4. . Ідентифікація ненадійних даних у параметрах запитів HTTP.				2		
Самостійна робота 4. Розкриття інформації через robots.txt. Ризики в джерелах HTML. Ідентифікація ненадійних даних у параметрах запитів HTTP.						4
Тема 5. Атаки масового призначення	**8**	**2**		**2**		**4**
Лекція 5. Атаки масового призначення		2				
Практичне заняття 5. Атаки масового призначення				2		
Самостійна робота 5. Атаки масового призначення						4
Тема 6. Складові SQLi атак. Тестування ризикованих рішень.	**8**	**2**		**2**		**4**
Лекція 6. Складові SQLi атак.		2				
Практичне заняття 6. Тестування ризикованих рішень..				2		
Самостійна робота 6. Складові SQLi атак. Тестування ризикованих рішень.						4
Тема 7. Поняття cross site атак. Встановлення атаки кликджекингу.	**8**	**2**		**2**		**4**
Лекція 7. Поняття cross site атак. Встановлення атаки кликджекингу.		2				
Практичне заняття 7. Поняття cross site атак. Встановлення атаки кликджекингу.				2		
Самостійна робота 7. Поняття cross site атак. Встановлення атаки кликджекингу.						4
Тема 8. Тестування ризиків у функції «запам'ятати мене». Тестування брутфорс автентифікації. Тестування незахищеної captcha	**8**	**2**		**2**		**4**
Лекція 8. Тестування ризиків у функції «запам'ятати мене».		2				

Практичне заняття 8. Тестування брутфорс автентифікації. **Модульний контроль №1**				2		
Самостійна робота 8. Тестування незахищеної captcha						4
Всього годин за змістовий модуль 1	**64**	**16**		**16**		**32**
Змістовий модуль 2. Хмарні технології						
Тема 9. Хмарні середовища: можливості, переваги та ризики. Стратегія розвитку хмари.	**8**	**2**		**2**		**4**
Лекція 9. Хмарні середовища: можливості, переваги та ризики.		2				
Практичне заняття 9. Стратегія розвитку хмари.				2		
Самостійна робота 9. Хмарні середовища: можливості, переваги та ризики. Стратегія розвитку хмари.						4
Тема 10. Програмне забезпечення як послуга.	**8**	**2**		**2**		**4**
Лекція 10. Програмне забезпечення як послуга.		2				
Практичне заняття 10. Програмне забезпечення як послуга.				2		
Самостійна робота 10. Програмне забезпечення як послуга.						4
Тема 11. Платформа Google AppEngine.	**8**	**2**		**2**		**4**
Лекція 11. Платформа Google AppEngine.		2				
Практичне заняття 11. Платформа Google AppEngine.				2		
Самостійна робота 11. Платформа Google AppEngine.						4
Тема 12. Платформа AWS.	**8**	**2**		**2**		**4**
Лекція 12. Платформа AWS.		2				
Практичне заняття 12. Платформа AWS.				2		
Самостійна робота 12. Платформа AWS.						4
Тема 13. Особливості розробки програмного забезпечення для хмарних інформаційних систем.	**8**	**2**		**2**		**4**
Лекція 13. Особливості розробки програмного забезпечення для хмарних інформаційних систем.		2				
Практичне заняття 13. Особливості розробки програмного забезпечення для хмарних інформаційних систем.				2		
Самостійна робота 13. Особливості розробки програмного забезпечення ля хмарних інформаційних систем.						4
Тема 14. Принципи управління хмарними інфраструктурами.	**8**	**2**		**2**		**4**
Лекція 14. Принципи управління хмарними інфраструктурами..		2				
Практичне заняття 14. Принципи управління хмарними інфраструктурами.				2		
Самостійна робота 14. Принципи управління хмарними інфраструктурами.						4

Тема 15. Мережеві аспекти хмарних технологій.	**6**	**2**		**2**		**4**
Лекція 15. Мережеві аспекти хмарних технологій.		2				
Самостійна робота 15. Мережеві аспекти хмарних технологій.						4
Всього годин за змістовий модуль 2	**54**	**14**		**12**		**28**
Підсумковий контроль (диференційований залік)	2					
Всього годин за навчальну дисципліну	**120**	**30**		**30**		**60**

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

1. Лекції проводять у лекційних залах, обладнаних засобами мультимедіа (мультимедійними проекторами, персональними комп'ютерами (ноутбуками), аудіосистемами).
2. Практичні заняття проводяться у комп'ютерних класах. Навчальна група поділяється на підгрупи, у кожній із яких не більше 15 курсантів. Кожен здобувач виконує завдання на індивідуальній робочій станції. Для проведення практичних занять залучається два викладача.
3. Для підготовки здобувуаучів до виконання модульних контрольних робіт та екзамену має бути 2-3 робочі дні, в яких не проводяться заняття з дисципліни «Хмарні технології і захист веб-додатків».

4. Основні методи навчання

Навчальна діяльність здійснюється шляхом лекційних, практичних занять, виконання модульних контрольних робіт, самостійної підготовки, консультацій, а також індивідуальних занять. При цьому використовуються мультимедійні технічні засоби та сучасні інформаційні технології, а також можливості глобальної мережі Інтернет.

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)	**0,4**
Підсумковий контроль (ПК)	**0,6**

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)	15
Робота на практичних заняттях	20
Виконання завдань для самостійної роботи	15
Виконання модульної контрольної роботи	50

Мінімальна кількість балів для допуску до підсумкового контролю 25.

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. Sathish Janani. Learn Arduino Products: All Arduino Boards, Tech Specs, Comparison, Software, Hardware, Code Functions. Amazon.com Services LLC, 2021
2. Олещенко Л.М. Програмування пристроїв Інтернету речей / Л.М. Олещенко, Я.В. Хіцко. – К.: КПІ ім. Ігоря Сікорського, 2019, – 47 с.
3. Наука про дані для Інтернету Речей та Інтернету Всього / За ред. І.С. СкаргаБандурової . – МОН України, Східноукраїнський університет ім. Володимира Даля, Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ». – 169с.
4. Cloud Computing: Concepts, Technology & Architecture (3rd Edition), by David Chappell.
5. Cloud Computing: Concepts, Technology & Architecture (4th Edition), by David Chappell.
6. Internet of Things: Principles and Paradigms (2nd Edition), by Mehdi Bennis, Walid Saad, and Mohamed-Slim Alouini.
7. Internet of Things: Concepts, Architecture and Applications, by Giuseppe Piro, Francesco De Rango, and Vincenzo Mancuso.

Допоміжна література:

1. Internet of Things (IoT). Available: http://www.cisco.com/c/en/us/solutions/internet-ofthings/overview.html
2. Internet of Things [Online]. Available: https://www.it.ua/ru/knowledge-base/technologyinnovation/internetveschej-internet-of-things-iot.
3. Internet of things news. Available: http://www.theinternetofthings.eu/
4. IoT Overview Handbook - http://postscapes.com/internet-of-things-handbook

Адреса розміщення робочої програми навчальної дисципліни

_____

(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.			
…			

29/3/1/4 - 1489/Вг
14. 10. 2024