НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра Комп'ютерних систем, мереж та кібербезпеки

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г. Глазунова
"__" _____ 2023 р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем, мереж та кібербезпеки
Протокол №10 від "17" травня 2023 р.
Завідувач кафедри
(доц. Касаткін Д.Ю.)

РОЗГЛЯНУТО
Гарант ОП
«Кібербезпека»

_____
Гарант ОП
_____ (проф. Лахно В.А.)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Проведення розслідувань інцидентів інформаційної безпеки

спеціальність 125
освітня програма КБ
Факультет (ННІ) ІТ
Розробники: Професор каф. КСМ та КІБ, д.т.н., професор Лахно В.А.
(посада, науковий ступінь, вчене звання)

Київ – 2023 р.

1. Опис навчальної дисципліни
Проведення розслідувань інцидентів інформаційної безпеки
(назва)

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	*Бакалавр*	
Спеціальність	*125 – КБ*	
Освітня програма	*Кібербезпека*	
Характеристика навчальної дисципліни		
Вид	Вибіркова	
Загальна кількість годин	150	
Кількість кредитів ECTS	5	
Кількість змістових модулів	1	
Курсовий проект (робота) (за наявності)		
Форма контролю	*Екзамен*	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки (курс)	4	
Семестр	8	
Лекційні заняття	24 год.	
Практичні, семінарські заняття		
Лабораторні заняття	24 год.	
Самостійна робота	102 год.	
Індивідуальні завдання		
Кількість тижневих аудиторних годин для денної форми навчання	4 год.	

2. Мета, завдання та компетентності навчальної дисципліни

Місце і роль дисципліни в системі підготовки фахівців відповідно до навчального плану. Дана навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області кібербезпеки.

Завдання: теоретична та практична підготовка здобувачів до проведення розслідувань інцидентів інформаційної безпеки в різних установах та на підприємствах, зокрема АПК.

У результаті вивчення навчальної дисципліни студент повинен

знати: норми законодавчої та нормативно-правової бази України та вимоги відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;

вміти: впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур

захисту; впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної, і/або кібербезпеки.

Набуття компетентностей:

загальні компетентності (КЗ): *КЗ2. Знання та розуміння предметної області та розуміння професії; КЗ4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням; КЗ5. Здатність до пошуку, оброблення та аналізу інформації; КЗ8. Здатність до абстрактного і системного мислення, аналізу та синтезу.*

фахові (спеціальні) компетентності (СК): *СК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки; СК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.); СК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку; СК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.*

3. Програма та структура навчальної дисципліни для:

– повного терміну денної форми навчання.

Назви змістових модулів і тем	Кількість годин						
	денна форма						
	Тижні	Усього	у тому числі				
			л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8
Змістовий модуль 1.							
Тема 1. Вступ, мета та цілі дисципліни. Аудити інформаційної безпеки	1	20	2				18
Тема 2. Системи менеджменту інформаційної безпеки (СМІБ) за вимогами ISO/IEC 27001.	1	22	4		4		14
Тема 3. Комплексний аудит інформаційної безпеки. Реалізація програми аудиту	1	22	4		4		14
Тема 4. Оцінка діяльності з управління інформаційною безпекою організації.	1	22	4		4		14
Тема 5. Системи менеджменту інцидентами інформаційної безпеки. Етапи управління інцидентами інформаційної безпеки ISO/IEC 27035	1	22	4		4		14
Тема 6. Концепція та структура автоматизованої системи управління інцидентами інформаційної безпеки	1	20	2		4		14
Тема 7. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT. Програмні рішення у розслідуваннях інцидентів інформаційної безпеки \ кібербезпеки	1	22	4		4		14
Разом за змістовим модулем 1		**150**	**24**		**24**		**102**
Усього годин		**150**					

4. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
-	-	-

5. Теми практичних занять

№ з/п	Назва теми	Кількість годин
-	-	-

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Аудити інформаційної безпеки.	4
2	Реалізація програми комплексного аудиту.	4
3	Оцінка діяльності з управління інформаційною безпекою організації.	4
4	Етапи управління інцидентами інформаційної безпеки.	4
5	Автоматизованої системи управління інцидентами.	4
6	Програмні рішення у розслідуваннях інцидентів інформаційної безпеки \ кібербезпеки.	4
	Разом за семестр	**24**
	Разом	**24**

7. Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Види аудиту інформаційної безпеки.	17
2	Реалізація програми комплексного аудиту.	17
3	Оцінка діяльності з управління інформаційною безпекою організації.	17
4	Етапи управління інцидентами інформаційної безпеки.	17
5	Автоматизованої системи управління інцидентами та проведення аудиту ІБ.	17
6	Програмні рішення у розслідуваннях інцидентів інформаційної безпеки \ кібербезпеки.	17
	Разом	**102**

1. Контрольні питання, комплекти тестів для визначення рівня засвоєння знань студентами.

1. Аудити інформаційної безпеки.
2. Системи менеджменту інформаційної безпеки . Приклад використання.
3. Реалізація програми комплексного аудиту. Приклад використання.
4. Оцінка діяльності з управління інформаційною безпекою організації.
5. Прокоментувати етапи управління інцидентами інформаційної безпеки.
6. Структура автоматизованої системи управління інцидентами.
7. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT.

2. Методи навчання.

Під час викладання курсу використовуються наступні методи навчання:

– розповідь – для оповідної, описової форми розкриття навчального матеріалу;

– пояснення – для розкриття сутності певного явища, закону, процесу;

– бесіда – для усвідомлення, за допомогою діалогу, нових явищ, понять;

– ілюстрація – для розкриття предметів і процесів через їх символічне зображення (рисунки, схеми, графіки);

– лабораторна робота – для використання набутих знань при виконанні лабораторних завдань;

– аналітичний метод – для мисленнєвого або практичного розкладу цілого на частини з метою вивчення їх суттєвих ознак;

– проблемний виклад матеріалу – для створення проблемної ситуації.

3. Форми контролю.

Наприкінці кожного змістовного модуля проводиться контрольна робота.

Перший змістовий модуль – захист п’яти лабораторних робіт, усне опитування, контрольна робота, залік.

4. Розподіл балів, які отримують студенти.

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл. 1 «ПОЛОЖЕННЯ про екзамени та заліки у НУБіП України» (наказ про уведення в дію від «26» квітня 2023 р. протокол № 10):

Рейтинг студента, бали	Оцінка національна за результати складання	
	екзаменів	заліків
90-100	Відмінно	Зараховано
74-89	Добре	
60-73	Задовільно	
0-59	Незадовільно	Не зараховано

Для визначення рейтингу студента (слухача) із засвоєння дисципліни $\mathbf{R_{ДИС}}$ (до 100 балів) одержаний рейтинг з атестації (до 30 балів) додається до рейтингу студента (слухача) з навчальної роботи $\mathbf{R_{НР}}$ (до 70 балів): $\mathbf{R_{ДИС} = R_{НР} + R_{АТ}}$.

11. Методичне забезпечення

Презентації, слайди лекцій, методичні рекомендації до лабораторних робіт.

12. Рекомендовані джерела інформації

– основні:

1. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 «Кібербезпека» / Корченко О.Г., Шелест М.Є., Казмірчук С.В. та ін. – Ніжин: ТПК «Орхідея», 2019. – 408 с.

2. Аудит та управління інцидентами інформаційної безпеки: навч. посіб / Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін. – К: НА СБУ, 2014. – 190 с.

– допоміжна:

1. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.
2. ISO/IEC 27001:2013 «Система управління інформаційною безпекою. Вимоги».
3. ISO/IEC 27032:2012 «Інформаційні технології – Методи забезпечення безпеки - Керівництво з кібербезпеки».
4. ISO/IEC 27035:2011 «Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки».

13. Інформаційні ресурси

1. Сайт системи дистанційного навчання НУБіП (https://elearn.nubip.edu.ua/)