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.)

«ПРОДУКТИ ТА ПОСЛУГИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Спеціальність	125 - Кібербезпека
Освітня програма	Кібербезпека
Факультет	інформаційних технологій
Розробник:	Сагун А.В., к.т.н., доцент

Київ – 2023

Опис навчальної дисципліни

«ПРОДУКТИ ТА ПОСЛУГИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	Бакалавр	
Галузь знань	12 – Інформаційні технології	
Спеціальність	125 – Кібербезпека	
Освітня програма	Кібербезпека	
Характеристика навчальної дисципліни		
Вид	Вибіркова	
Загальна кількість годин	150	
Кількість кредитів ECTS	5	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
Форма контролю	екзамен	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	4	
Семестр	8	
Лекційні заняття, год.	24	
Практичні, семінарські заняття	-	
Лабораторні заняття, год.	24	
Самостійна робота, год.	102	
Індивідуальні завдання	-	
Кількість тижневих аудиторних годин для денної форми навчання	4 (15 тижнів)	

1. Мета, завдання та компетентності навчальної дисципліни

Мета: ознайомлення з теорією та практикою проектування та реалізації продуктів та послуг інформаційної безпеки на базі компонент мережевих ОС, криптографічних та мережевих засобів та протоколів.

Завдання навчальної дисципліни: вивчення та вміння проектувати та налаштовувати продукти та послуги ІБ, забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.

В результаті вивчення навчальної дисципліни студент повинен

знати:

- механізми автентифікації захищених вузлів та сервісів ІБ;
- основні напрямки розвитку та застосування продуктів та послуг ІБ;
- методи аудиту продуктів та послуг у відповідності до ДСТУ та ISO/IEC 27003;
- методи захисту в продуктах та послугах ІБ та прийоми перешкоджання спробам несанкціонованого доступу (НСД).

вміти:

– аналізувати взаємодію сервісів в мережі Internet;

– користуватися інструментальними засобами аналізу проектування та аналізу вразливостей захищених вузлів та сервісів;

– Володіти раціональними прийомами адміністрування захищених вузлів та сервісів в Internet;

– синтезувати на основі компонентів мережевих операційних систем портали, сервіси для розв'язку галузевих задач різного рівню складності в якості адміністратора безпеки.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням

Спеціальні (фахові, предметні) компетентності (СК):

СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

СК2. Здатність до використання інформаційно - комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

СК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

СК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

В результаті вивчення навчальної дисципліни студент набуде певні програмні результати (РН), а саме

ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;

ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.

В контексті зазначених вище компетентностей та програмних результатів навчання задачі викладання дисципліни визначають необхідний комплекс знань і вмінь, що отримують студенти під час вивчення дисципліни.

Навчальна програма розрахована на студентів, які навчаються за освітньою програмою підготовки бакалавра за спеціальністю «Кібербезпека».

Програма побудована за вимогами кредитно-модульної системи організації навчального процесу у закладах вищої освіти і використанням академічної системи оцінювання досягнень студентів та шкали оцінок Європейської кредитно-трансферної системи (ECTS).

Робоча навчальна програма з курсу є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма дисципліни розроблена на підставі наступних документів:

- освітня програма підготовки бакалаврів за спеціальністю 125 «Кібербезпека»;
- навчальний план підготовки бакалаврів за спеціальністю 125 «Кібербезпека».
- освітньо-професійної програми «Кібербезпека» першого (бакалаврського)рівня вищої освіти за спеціальністю 125 «Кібербезпека».

Навчальна програма характеризує шляхи перетворення інформації, що одержується студентом впродовж вивчання курсу, і відбиває зміст курсу, розподілення його на розділи та їх обсяги, дані про форми вивчення та контролю знань.

Теоретичною базою для вивчення курсу «Продукти та послуги інформаційної безпеки» є курси «Основи криптографічного та стеганографічного захисту інформації", «Методи та засоби захисту інформації», «Захист інформації в комп'ютерних системах» ОПП першого (бакалаврського) рівня вищої освіти.

2. Програма та структура навчальної дисципліни

– повного терміну денної (заочної) форми навчання;

Назви змістових модулів і тем	Кількість годин												
	денна форма							Заочна форма					
	тиж-ні	всього	у тому числі					всього	у тому числі				
			л	п	лр	інд	с.р.		л	п	лр	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Змістовий модуль 1. Методики проектування та використання продуктів та послуг інформаційної безпеки													
Тема 1. Етапи та алгоритми проектування ППІБ. Методика синтезу ППІБ на базі існуючих мережних компонент.	1	20	2		-		18						
Тема 2. Завантаження та налаштування компонент ППІБ та конфігураційних файлів.	3	28	4		6		18						
Тема 3. Проектування та реалізація захищених каналів передачі на базі алгоритмів та вимог стандарту ДСТУ ISO/IEC 27033-5:2016 для VPN-мереж	6	32	6		6		20						
Разом за змістовим модулем 1		**80**	**12**		**12**		**56**						
Змістовий модуль 2. Проектування послуг інформаційної безпеки, пов'язаних з моніторингом та реагуванням на загрози серверних платформ													
Тема 4. Проектування послуг реагування на потенційні загрози безпеці серверів на базі ОС Linux	8	18	4		4		10						
Тема 5. Проектування та реалізація ППІБ мережевої ідентифікації на базі *nix	10	24	4		4		16						
Тема 6. Автоматизація обробки ведення журналів безпеки серверних ОС на базі ОС Linux	13	28	4		4		20						
Разом за змістовим модулем 2		**70**	**12**		**12**		**46**						
Всього годин		**150**	**24**		**24**		**102**						

3. Теми практичних занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

4. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Компіляція та модифікація ядра ОС Linux серверної платформи	6
2	Проектування захищеного VPN-тунелю по ДСТУ ISO/IEC 27033-5:2016	6
3	Розробка сервісу реагування на потенційні загрози серверній платформі на базі bash-script	4
4	Розробка та конфігурування PAM-сервісу мережевої автентифікації	4
5	Автоматизоване формування та аналіз log-файлів в ОС Linux	4
	Разом	**24**

Курсове проектування - Не передбачено робочим навчальним планом

6. САМОСТІЙНА РОБОТА СТУДЕНТІВ

Самостійна робота студентів передбачає:

– систематичне відвідання усіх видів аудиторних занять і ведення конспекту лекцій;

– систематичне вивчення лекційного матеріалу і навчальної літератури, що рекомендуються;

– сумлінну підготовку до лабораторних занять;

– вчасне і якісне оформлення звітів про лабораторні роботи.

6.1.Теми самостійної роботи

№	Тема	Кількість годин
1	Оптимізація процесу формування складу системи захисту вузла в Internet	8
2	Аналіз статистики та характеру загроз для вузлів та сервісів в середовищі Linux	10
3	Характерні вразливості вузлів та сервісів в Internet, заснованих на базі *nix	8
4	Реалізація розмежування доступу для мережевого вузла в Internet	10
5	Системні виклики та алгоритми їх взаємодії з процесами користувачів в мережевій ОС	8
6	Атаки на програмні порти та методи їх попередження засобами скріптового програмування	12
7	Використання дискрипторів та файлів потоків вводу/виводу периферійних пристроїв в задачах захисту інформації на bash	10
8	Організація кешування в середовищі *.nix	8

9	Програмування резидентних модулів в мережевих ОС	8
10	Консольне адміністрування віддалених компонентів мережевої ОС	12
11	Практичні реалізація кластерних обчислень на базі Linux	8
Всього:		**102**

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

7.1. Питання для перевірки знань студентів

1. Поняття та склад продуктів та послуг інформаційної безпеки. Етапи та алгоритми проектування ППІБ.
2. Методика синтезу ППІБ на базі існуючих мережних та криптографічних компонент.
3. Привілейований та user- режим роботи послуги ІБ. Завантаження та налаштування компонент ППІБ та конфігураційних файлів.
4. Криптографічні компоненти для побудови продуктів та послуг інформаційної безпеки.
5. Мережеві компоненти та протоколи для побудови продуктів та послуг інформаційної безпеки.
6. Проектування та реалізація захищених каналів передачі на базі алгоритмів та вимог стандарту ДСТУ ISO/IEC 27033-5:2016 для vpn-мереж.
7. Проектування послуг реагування на потенційні загрози безпеці серверів на базі ОС Linux.
8. Проектування та реалізація ППІБ мережевої ідентифікації на базі *nix – ОС.
9. Автоматизація обробки ведення журналів безпеки серверних ОС на базі ОС Linux
10. Компіляція та модифікація ядра ОС Linux серверної платформи. Версії ядра. Створення та застосування patch-файлів.
11. Алгоритм проектування захищеного vpn-тунелю по ДСТУ ISO/IEC 27033-5:2016.
12. Засоби автоматизації адміністрування послуг ІБ на базі bash та powershell.
13. Етапи розробки сервісу реагування на потенційні загрози серверній платформі на базі bash-script.
14. Послуги ІБ на базі open-source компонет *nix типу PAM. Стеки PAM-конфігурування.
15. Розробка та конфігурування PAM-сервісу мережевої автентифікації.
16. Автоматизоване формування та аналіз log-файлів в ОС Linux.

8. Методи навчання

Виконання лабораторних робіт з використанням ОС Linux та Windows; виконання індивідуальних навчально-дослідних завдань.

9. Форми контролю

Систематичний контроль за самостійною роботою студентів і якістю засвоєння ними поточного навчального матеріалу:

– на лабораторних роботах шляхом перевірки підготовки до виконання роботи;

– роботу над індивідуальними завданнями до лабораторних робіт;

– вивчення літератури, що рекомендувалася, та конспекту лекцій;

– оформлення звітів про виконання лабораторним роботам.

Поточний контроль знань студентів проводиться:

– на лабораторних роботах оцінюється підготовка до роботи, обсяг її виконання, результати захисту звіту;

– на лекційних заняттях виконується вибіркове опитування студентів;

– шляхом проведення модульних контролів знань студентів та виставлення рейтингових оцінок знань студентів по усім видам занять.

10. 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 здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзамен	**Залік**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

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

11. Методичне забезпечення

1. Конспект лекцій з курсу "Продукти та послуги інформаційної безпеки". - Київ, НУБіП, 2022 (elearn.nubip.edu.ua/course/view.php?id)

12. Рекомендовані джерела інформації

Основні

1. Остапов С. Е. Технології захисту інформації: навч. посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2013. – 476 с. – URL: http://kist.ntu.edu.ua/textPhD/tzi.pdf

2. Прикладна криптологія: системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с. – URL: https://er.nau.edu.ua/handle/NAU/32583

3. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р.

4. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СВ України від 28.04.99 р. № 22.

5. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000 № 63.