НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних систем, мереж та кібербезпеки

«ЗАТВЕРДЖУЮ»

Декан факультету
інформаційних технологій

_____ проф. О.Г. Глазунова
«___» _____ 2022р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем,
мереж та кібербезпеки
Протокол №12 від «11» травня» 2022р.
Завідувач кафедри
(проф. Лахно В.А.)

РОЗГЛЯНУТО
Гарант ОП «Кібербезпека»

_____ (Лахно В.А.)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ПРИКЛАДНІ АСПЕКТИ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ»

Спеціальність	125 «Кібербезпека»
Освітня програма	«Кібербезпека»
Факультет	інформаційних технологій
Розробник:	Мамченко С.М., д.пед.н., професор

Київ – 2023

1. Опис навчальної дисципліни
«Прикладні аспекти побудови систем захисту інформації»

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	2	
Семестр	4	
Лекційні заняття, год.	30	
Практичні, семінарські заняття	-	
Лабораторні заняття, год.	30	
Самостійна робота, год.	60	
Індивідуальні завдання	-	
Кількість тижневих аудиторних годин для денної форми навчання	4	

2. Мета, завдання та компетентності навчальної дисципліни

Мета навчальної дисципліни “Прикладні аспекти побудови системи захисту інформації” є навчання студентів принципам побудови комплексних систем захисту інформації на основі синтезу організаційних і технічних заходів щодо забезпечення захисту інформації з обмеженим доступом, основ ведення електронного документообігу в умовах сучасних кіберзагроз та витоку технічними каналами, забезпечення захисту інформації від несанкціонованого доступу на основі вимог міжнародних стандартів з інформаційної безпеки, державних нормативних документів з технології захисту інформації.

Навчальна дисципліна забезпечує формування ряду фахових компетентностей:

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.

КЗ 8. Здатність до абстрактного і системного мислення, аналізу та синтезу.

Спеціальні (фахові, предметні) компетентності (СК):

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

СК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

СК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

СК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

У результаті вивчення навчальної дисципліни студент набуде певні програмні результати, а саме

ПРН 4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;

ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (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;

ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;

ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

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 «Комплексні системи захисту інформації» є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма дисципліни «Комплексні системи захисту інформації» розроблена на підставі наступних документів:

- освітня програма підготовки фахівців за спеціальністю 125 «Кібербезпека»;
- навчальний план підготовки фахівців 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 «Комплексні системи захисту інформації» є курси «Організаційне забезпечення захисту інформації» та «Інформаційна безпека держави».

Курс «Прикладні аспекти побудови систем захисту інформації» є вибірковим.

3.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
Модуль 1. Порядок проведення робіт із створення комплексної системи захисту інформації підприємства АПК.													
Тема 1. Організаційні, технічні та програмно-апаратні засоби комплексної системи захисту корпоративної інформації.	1	8	2		2		4						
Тема 2. Автоматизовані системи АПК.	2	8	2		2		4						
Тема 3. Формування загальних вимог до КСЗІ в ІТС АПК.	3	8	2		2		4						
Тема 4. Оцінка загроз та джерел загроз безпеці інформації, що циркулює на об'єкті інформаційної діяльності в АПК .	4	8	2		2		4						
Тема 5. Сутність моделі порушника інформаційної безпеки в ІТС підприємств АПК.	5	8	2		2		4						
Тема 6. Вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій, які регламентують використання захищених технологій обробки інформації в ІТС.	6	8	2		2		4						
Тема 7. Визначення вимог із захисту оброблюваної в ІТС інформації.	7	8	2		2		4						
Тема 8. Обґрунтування і прийняття проектних рішень, які дають змогу реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію різних компонентів КСЗІ.	8	8	2		2		4						
Разом за змістовим модулем 1		**64**	**16**		**16**		**32**						
Змістовий модуль 2. Визначення відповідності комплексної системи захисту інформації технічному завданню.													
Тема 1. Введення КСЗІ в дію та оцінка захищеності інформації в ІТС	9	8	2		2		4						
Тема 2. Захист інформації WEB-сторінки від НСД.	10	8	2		2		4						
Тема 3. Розробка програми та методики державної	11	8	2		2		4						

експертизи комплексної системи захисту інформації.													
Тема 4. Етапи проведення експертизи комплексної системи захисту інформації.	12	8	2		2		4						
Тема 5. Декларація про відповідність, порядок розробки та відмінності в застосуванні.	13	8	2		2		4						
Тема 6. Порядок створення та впровадження організаційно-технічного рішення на комплексну систему захисту інформації.	14	8	2		2		4						
Тема 7. Організація служби захисту інформації (СЗІ) та організаційне проектування діяльності СЗІ.	15	8	2		2		4						
Разом за змістовим модулем 2		**56**	**14**		**14**		**28**						
Всього годин		**120**	**30**		**30**		**60**						

4. Теми практичних занять

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

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	Особливості побудови та розгортання сучасного веб-сайту на базі системи управління вмістом (CMS).	2
2	Засоби безпеки рівня серверної інфраструктури.	2
3	Особливості застосування технології віртуалізації рівня операційної системи.	2
4	Архітектура веб-систем. Об’єкти захисту/атаки.	2
5	REST-інтерфейс та його безпека.	2
6	Відкритий проект по забезпеченню безпеки веб-додатків (OWASP).	2
7	Вразливості веб-ресурсів та додатківта атаки на них.	2
8	Міжсайтовий скриптинг (XSS) та засоби захисту від нього.	4
9	SQL-ін’єкції: характеристика вразливості та засоби захисту.	2
10	Основи методології та безпеки веб-ресурсів та додатків.	2
11	Методологія тестування безпеки: OSSTMM.	2
12	Методологія тестування безпеки: Testing Guide.	4
13	Методологія тестування безпеки: PTES, OWASP.	2
	Всього	**30**

Курсове проектування - Не передбачено робочим навчальним планом

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

6.1. Питання для перевірки знань студентів:

1. Етапи створення КСЗІ.
2. Формування загальних вимог до КСЗІ в ІТС.
3. Обґрунтування необхідності створення КСЗІ.
4. Порядок обстеження середовищ функціонування ІТС.
5. Формування завдання на створення КСЗІ.
6. Порядок розробки політики безпеки інформації в ІТС.
7. Вибір варіанту КСЗІ.
8. Порядок розробки плану захисту інформації.
9. Порядок розробки технічного завдання на створення КСЗІ.
10. Порядок розробки проекту КСЗІ.
11. Сутність ескізного проекту КСЗІ.
12. Сутність технічного проекту КСЗІ.
13. Сутність робочого проекту КСЗІ.
14. Порядок підготовки КСЗІ до введення в дію.
15. Навчання користувачів КСЗІ і ІТС.
16. Оцінка захищеності інформації в ІТС.
17. Комплектування КСЗІ.
18. Будівельно-монтажні роботи при побудові КСЗІ.
19. Пусконалагоджувальні роботи КСЗІ.
20. Порядок проведення попередніх випробувань КСЗІ.
21. Порядок проведення дослідної експлуатації КСЗІ.
22. Порядок проведення державної експертизи КСЗІ.
23. Організація служби захисту інформації.
24. Організаційне проектування діяльності служби захисту інформації.
25. Порядок створення служби захисту інформації.
26. Склад нормативних документів, що регламентують діяльність служб захисту інформації.
27. Сутність декларації про відповідність.
28. Порядок розробки декларації про відповідність.
29. Порядок розробки програми державної експертизи комплексної системи захисту інформації.
30. Порядок розробки методики державної експертизи комплексної системи захисту інформації.
31. Сутність моделі загроз.
32. Сутність моделі порушника.

33. Сутність автоматизованих систем.
34. Класифікація автоматизованих систем.
35. Типи інформації, які обробляються в автоматизованих системах.
36. Визначення об'єктів захисту.

7. Методи навчання

Виконання лабораторних робіт з використанням ПЗ; виконання індивідуальних навчально-дослідних завдань.

8. 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.

9. 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): $R_{дис}=R_{НР}+R_{АТ}$.

10. Методичне забезпечення

1. Електронний навчальний курс на платформі Moodle вміщує повне методичне забезпечення включаючи: лекції, презентації до лекцій, методичні вказівки до виконання лабораторних робіт, глосарій термінів тощо.

11. Рекомендована література

Основна:

1. НД ТЗІ 3.7-003 -2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» // Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. Київ. 2005. – С. 22.

2. Закон України «Про захист інформації в автоматизованих системах» // Відомості Верховної Ради України, 1994. - № 31. – С. 286.

3. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.].Вінниця : ВНТУ, 2018. - 118 с.

4. Проєктування комплексних систем захисту інформації. Підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. 320 с.

.

Допоміжна

1. Кузнецов О.О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2011. – 510 с.

Інформаційні ресурси

1. АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=81998&cat_id=38835
2. Законодавча база України, [Електронний ресурм] – Режим доступу: https://zakon.rada.gov.ua/laws/main/index