НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних систем, мереж та кібербезпеки

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г. Глазунова
"17" 05 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 «КОМП'ЮТЕРНІ МЕРЕЖІ ТА КІБЕРБЕЗПЕКА»

Спеціальність	університетська вибіркова
Освітня програма	**ДЛЯ ВИБІРКОВОЇ СКЛАДОВОЇ ОСВІТНІХ ПРОГРАМ ПІДГОТОВКИ БАКАЛАВРІВ**
Факультет	інформаційних технологій
Розробник:	Гладких В.М.

Київ – 2023

Опис навчальної дисципліни
«КОМП'ЮТЕРНІ МЕРЕЖІ ТА КІБЕРБЕЗПЕКА»

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	Бакалавр	
Галузь знань	**ДЛЯ ВИБІРКОВОЇ СКЛАДОВОЇ ОСВІТНІХ ПРОГРАМ ПІДГОТОВКИ БАКАЛАВРІВ**	
Спеціальність		
Освітня програма		
Характеристика навчальної дисципліни		
Вид	обов'язкова	
Загальна кількість годин	120	
Кількість кредитів ECTS	4	
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	

1. Мета, завдання та компетентності навчальної дисципліни

Мета: вивчення сучасних методів захисту інформації, отримання студентами необхідних базових знань, щодо порядку створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. В рамках курсу передбачено проведення теоретичних та практичних завдань щодо класифікації, шляхів утворення технічних каналів витоку інформації, а також сучасних методів та засобів технічного захисту інформації.

Завдання навчальної дисципліни: є теоретична та практична підготовка студентів до застосування сучасних методів захисту інформації, а також навиків щодо розроблення, впровадження та експлуатації систем технічного захисту інформації на об’єктах інформаційної діяльності.

В результаті вивчення навчальної дисципліни студент повинен

- знати: основні поняття та принципи технічного захисту інформації; загальні аспекти технічного захисту інформації; вимоги щодо розміщення режимних приміщень для функціонування інформації з обмеженим доступом; види технічних каналів витоку інформації, класифікацію та шляхи їх утворення; сучасні методи та засоби технічного захисту інформації; основні положення та сутність створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності; порядок проведення атестації комплексів технічного захисту інформації.

- вміти: застосовувати знання, навички для розв’язування задач аналізу та синтезу визначення загроз інформаційної безпеки; вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах; вміти класифікувати канали витоку інформації; розробляти та впроваджувати заходи з технічного захисту інформації на об’єктах інформаційної діяльності; вирішувати задачі виявлення технічних каналів витоку інформації та запобігання витоку інформації такими каналами; проводити атестацію комплексів технічного захисту інформації.

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	всьо-го	у тому числі					всьо-го	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. Сутність технічного захисту інформації.													
Тема 1. Загальні аспекти кібербезпеки та технічного захисту інформації.	1	8	2		2		4						
Тема 2. Загальні положення та вимоги до кібербезпеки об'єктів інформаційної діяльності (ОІД).	2	8	2		2		4						
Тема 3. Технічні канали витоку інформації та їх класифікація.	3	8	2		2		4						
Тема 4. Основні поняття безпеки. Типи і приклади мережевих атак. Методи забезпечення безпеки. Аутентифікація, авторизація, аудит. Антивіруси. Мережеві екрани. Проксі-сервери.	4	8	2		2		4						
Тема 5. Сутність та шляхи утворення технічних каналів витоку інформації – електромагнітні, електричні, параметричні.	5	8	2		2		4						
Тема 6. Сутність та шляхи утворення технічних каналів витоку інформації – акустичні, акусто-вібраційні, акусто-електричні, акусто-оптичні.	6	8	2		2		4						
Тема 7. Сутність та шляхи утворення технічних каналів	7	8	2		2		4						

витоку інформації – матеріально-речовинні, канали зв'язку, візуальної інформації.													
Тема 8. Сутність та класифікація засобів несанкціонованого перехоплення інформації.	8	8	2		2		4						
Разом за змістовим модулем 1		**64**	**16**		**16**		**32**						
Змістовий модуль 2. Механізми технічного захисту інформації на об'єктах інформаційної діяльності.													
Тема 1. Основні положення та сутність створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності.	9	8	2		2		4						
Тема 2. Проблеми і категорії безпеки мереж. Методи зламу інформації. Захист від атак. Криптографічні засоби захисту. Основні засоби та стратегії захисту комп'ютерних мереж. Фільтрація пакетів і потоків. Міжмережевий екран. Асиметричний трафік. Детектування атак.	10	8	2		2		4						
Тема 3. Розроблення технічного проекту комплексу технічного захисту інформації.	11	8	2		2		4						
Тема 4. Сутність та оформлення моделі загроз при створенні комплексу технічного захисту інформації.	12	8	2		2		4						
Тема 5. Розробка та впровадження заходів з технічного захисту інформації на об'єктах інформаційної діяльності.	13	8	2		2		4						
Тема 6. Безпека мереж.	14	8	2		2		4						

Тема 7. Фізична безпека інформаційних систем та об'єктів інформаційної діяльності.	15	8	2		2		4						
Разом за змістовим модулем 2		**56**	**14**		**14**		**28**						
Всього годин		**120**	**30**		**30**		**60**						

3. 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	

4. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Вирішення завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах.	2
2	Формування вимог щодо розміщення режимних приміщень.	4
3	Вирішення задач виявлення технічних каналів витоку інформації.	4
4	Вирішення задач запобігання витоку інформації технічними каналами.	4
5	Вирішення задач запобігання витоку інформації шляхом несанкціонованого перехоплення.	4
6	Складання розпорядчого документу щодо створення комплексу технічного захисту інформації.	2
7	Розроблення технічного завдання на створення комплексу технічного захисту інформації.	4
8	Розроблення моделі загроз при створенні комплексу технічного захисту інформації.	2
9	Розроблення паспорту на комплекс технічного захисту інформації.	2
10	Оформлення заявки на проведення атестації комплексів технічного захисту інформації.	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.

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

5.1. Питання для перевірки знань студентів:

1. Технічні канали витоку інформації та їх класифікація.
2. Технічні канали витоку інформації, що обробляється в основних технічних засобах і системах.
3. Технічні канали витоку мовної інформації.
4. Витік інформації через засоби несанкціонованого перехоплення.
5. Витік інформації в каналах зв'язку, витік видової інформації та матеріально-речовинні канали витоку інформації.
6. Основні положення та сутність створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності.
7. Передпроектні роботи при створенні комплексів технічного захисту інформації на об'єктах інформаційної діяльності.
8. Сутність та оформлення моделі загроз при створенні комплексу технічного захисту інформації.
9. Розробка та впровадження заходів із захисту інформації на об'єктах інформаційної діяльності.
10. Випробування та атестація комплексів технічного захисту інформації на об'єктах інформаційної діяльності.
11. Основні напрями захисту.
12. Концепція забезпечення захисту інформації.
13. Основні загрози інформації.
14. Політика безпеки інформації.
15. Комплекс засобів захисту і об'єкти комп'ютерної системи.
16. Сутність несанкціонованого доступу.
17. Сутність моделі порушника.
18. Основні принципи забезпечення захисту інформації.
19. Планування захисту і керування системою захисту.
20. Основні принципи керування доступом.
21. Сутність безперервного захисту.
22. Сутність атрибутів доступу.

23. Довірче і адміністративне керування доступом.
24. Забезпечення персональної відповідальності.
25. Сутність послуг безпеки.
26. Сутність гарантій безпеки.
27. Основні принципи реалізації програмно-технічних засобів.
28. Функції і механізми захисту.
29. Реалізація комплексу засобів захисту.
30. Концепція диспетчера доступу.
31. Методи протидії і виявлення троянських програм.
32. Методи протидії і виявлення черв'яків.
33. Методи протидії і виявлення вірусів.
34. Методи нейтралізації шкідливого програмного забезпечення.
35. Методи і засоби сканування і захисту веб-серверів та веб-застосунків.
36. Механізми захисту від DoS/DDoS атак.
37. Захист від SQL-ін'єкцій.
38. Інструменти тестування веб-ресурсів на вразливість до атак.
39. Методи протидії криптографічним атакам.
40. Сутність криптографічного захисту інформації.

5.2. Приклади тестів з дисципліни:

1. Етапи здійснення технічного захисту інформації:

А) визначення й аналіз загроз, розроблення системи захисту інформації, реалізація плану захисту інформації; контроль функціювання та керування системою захисту інформації;

В) визначення завдання захисту інформації, аналіз ризиків, розроблення моделі загроз, розроблення моделі порушника, підготовка до введення в дію, пусконалагоджувальні роботи;

С) визначення загальної структури та складу системи захисту інформації, вимоги до можливих заходів, методів та засобів захисту інформації, допустимі обмеження щодо застосування певних заходів і засобів захисту, введення в дію і функціонування.

2. Комплекс засобів захисту – це ...

А) сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

В) це сукупність всіх програмно-апаратних засобів, в тому числі програм ПЗП, задіяних під час реалізації політики безпеки;

С) взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

3. Технічний захист інформації – це ...

А) вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

B) взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

C) вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

6. Методи навчання

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

7. 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.

8. 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 27.12.2019 р. № 1371):

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): $R_{дис}=R_{НР}+R_{АТ}$.

9. 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.

10. Рекомендована література

Основна:

1. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» // Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. Київ. 1999. – С. 21.

2. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. – К.: ІСЗЗІ НТУУ «КПІ», 2016. – 104 с.

3. Закон «Про інформацію»: Прийнятий 2 жовтня 1992 р. №2657-XII // Відомості Верховної Ради України, 1992. – № 48. – С. 650.

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

5. Указ Президента України від 27 вересня 1999 р. № 1229/99 «Про Положення про технічний захист інформації в Україні».

6. Указ Президента України від 24 вересня 2001 року № 891/2001 «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних».

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