МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Львівський національний університет природокористування

Факультет механіки, енергетики та інформаційних технологій

Кафедра Інформаційних технологій

“ЗАТВЕРДЖУЮ”
Проректор з НПР
проф. Віталій БОЯРЧУК
“____” _____ 20__ року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Інформаційна безпека

ОПП «Комп’ютерні науки»

спеціальність 122 «Комп’ютерні науки»

перший (бакалаврський) рівень вищої освіти

Львів 2024

Робоча програма навчальної дисципліни **Інформаційна безпека** для здобувачів першого (бакалаврського) рівня вищої освіти ОП «Комп'ютерні науки» спеціальності **122 «Комп'ютерні науки».**

Розробники: д.т.н. професор Ростислав Ткачук
к.е.н., доцент Володимир Станько.

Робочу програму схвалено на засіданні кафедри «Інформаційних технологій».

Протокол № 1 від 12 серпня 2024 року

Завідувач кафедри Інформаційних технологій

_____ (Тригуба А.М.)
(підпис) (прізвище та ініціали)

Робочу програму схвалено на засіданні методичної комісії (ради) факультету Механіки, енергетики та інформаційних технологій.

Протокол № 1 від 29 серпня 2024 року.

Голова методичної комісії _____ (Ковалишин С.Й.)
(підпис) (прізвище та ініціали)

1. Опис навчальної дисципліни

Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень

Рівень вищої освіти: перший (бакалаврський)

Галузь знань 12 «Інформаційні технології»

Спеціальність 122 «Комп'ютерні науки»

Характеристика навчальної дисципліни: обов'язкова (цикл професійної підготовки)

Кількість кредитів – 5

Загальна кількість годин – 150

Вид контролю: іспит

Тижневих аудиторних годин для денної форми навчання – 5

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить (%):

для денної форми навчання – 67, %

для заочної форми навчання – 15 %

2. Програма навчальної дисципліни

Розділ 1. Теоретичні засади алгоритмізації та програмування.

Тема 1. Концептуальні засади забезпечення інформаційної безпеки України.

1. Мета і завдання курсу.
2. Нормативно-правові основи захисту інформації в Україні.
3. Концепція національної безпеки України, концепція інформаційної безпеки України, доктрина інформаційної безпеки України.
4. Основні поняття, терміни та визначення.

Тема 2. Технічні канали витоку інформації. Способи несанкціонованого зняття інформації.

1. Місце технічного захисту інформації у системі інформаційної безпеки.
2. Сутність та завдання технічного захисту інформації.
3. Основні поняття, терміни та визначення технічного захисту інформації.
4. Види інформації, яка може стати об'єктом злочинних посягань.
5. Поняття технічних каналів витоку інформації та механізм їх утворення.
6. Види та класифікація технічних каналів витоку інформації та способів несанкціонованого зняття інформації.

Тема 3. Методи та засоби блокування технічних каналів витоку інформації.

1. Порядок проведення та складові ТЗ.
2. Методи пасивного та активного захисту інформації.
3. Методи та засоби захисту акустичної інформації.
4. Методи та засіб захисту електромагнітної інформації.
5. Методи захисту від ВЧ-нав'язування.

Тема 4. Основи безпеки даних комп'ютерних системах.

1. Основні поняття щодо захисту інформації в комп’ютерних системах.
2. Загрози безпеки даних та їх особливості.
3. Канали проникнення та принципи побудови систем захисту.
4. Основи фізичного захисту об'єктів.

Розділ 2. Реалізація методів опрацювання даних.

Тема 5. Ідентифікація і аутентифікація користувачів.

1. Поняття про ідентифікацію користувача та її особливості.
2. Основні принципи та методи аутентифікації.

Тема 6. Основи захисту даних.

1. Захист даних від несанкціонованого доступу.
2. Основні принципи захисту даних від несанкціонованого доступу.
3. Моделі управління доступом.
4. Технічні засоби захисту даних від їх витоку.
5. Засоби захисту даних від комп'ютерних вірусів та шкідливих програм.

Тема 7. Основи криптографії.

1. Основні терміни та поняття.
2. Криптографічні методи захисту інформації.
3. Сучасні криптосистеми та їх особливості.
4. Класичні техніки шифрування.
5. Симетричні та асиметричні алгоритми шифрування інформації.
6. Цифрові підписи.
7. Адміністрування ключами.

Тема 8. Стандарти із захисту інформації.

1. Світові стандарти із захисту даних в комп'ютерних системах.
2. Державний стандарт України із захисту інформації.

3. Структура навчальної дисципліни

Назви тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб.	інд.	с.р.		л	п	лаб.	інд.	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
	Рік підготовки 4 Семестр 7						Рік підготовки 4 Семестр 7					
Тема 1.	15	2	4			9	15	1	1			13
Тема 2.	15	2	4			9	15	2	2			11
Тема 3.	15	2	4			9	15	1	1			13
Тема 4.	15	4	4			7	15	1	1			13
Тема 5.	15	4	4			7	15	1	1			13
Тема 6.	15	4	4			7	15	1	1			13
Тема 7.	15	4	6			5	15	2	2			11

Тема 8.	15	2	6			7	15	1	1			13
Іспит	30	0	0			30	30					30
Разом	**150**	**24**	**36**			**90**	**150**	**10**	**10**			**130**

4. Теми практичних занять

№ з/п	Назва теми	Кількість, год.
1	Аналіз інформаційної безпеки в Україні.	2
2	Програмна реалізація і криптоаналіз шифрів з симетричними ключами.	2
3	Основи сучасної криптології. Шифр зсуву; шифр частоколу; шифр одноразового блокноту.	2
4	Класичні методи шифрування.	2
5	Шифрування за допомогою аналітичних перетворень.	2
6	Засоби забезпечення безпеки в операційних системах	4
7	Ідентифікація і аутентифікація користувача	2
8	Захист об'єктів системі	2
9	Алгоритм RSA.	4
10	Модифікація шифру Віженера та загального шифру перестановки.	2
11	Криптоаналіз лінійних шифрів к-го порядку з відомим відкритим текстом.	4
12	Криптоаналіз деяких шифрів з таємним ключем.	2
13	Афінні шифри.	2
14	Стандарти із захисту інформації	4

5. Теми винесені на самостійне вивчення:

№ з/п	Назва теми
1	Концептуальні засади забезпечення інформаційної безпеки
2	Технічні канали витоку інформації.
3	Способи несанкціонованого зняття інформації
4	Методи та засоби блокування технічних каналів витоку інформації
5	Методи захисту інформації у комп’ютерних системах
6	Методи захисту інформації у телекомунікаційних мережах та відкритих каналах зв’язку

7. Методи навчання:

1. Словесні методи (розповідь, пояснення, бесіда, лекція).

2. Наочні методи:

– ілюстрація (картинки, таблиці, моделі, муляжі, схеми тощо);

– демонстрування: навчальне відео чи його фрагменти; інтерактивні презентації, діючий код імітаційної моделі, компілювання та моделювання; експеримент, спостереження, досліди та аналіз результатів тощо.

3. Практичні методи: досліди, вправи, самостійна робота. Лабораторні та практичні роботи, розрахункові, реферати.

8. Методи контролю

1. Усне опитування (фронтальне, індивідуальне).

2. Письмова аудиторна та поза аудиторна перевірка (підготовка різних відповідей, рефератів, контрольні роботи (з конкретних питань тощо).

3. Практична перевірка (виконання практичної роботи, виконання комплексного тематичного завдання).

Види контролю: Поточний контроль, проміжна та семестрова атестація, підсумковий контроль

9. Очікувані результати навчання з дисципліни:

Очікуваними результати навчання з дисципліни «Інформаційна безпека» є набуття студентами ***загальних компетентностей*** – здатність оцінювати та забезпечувати захист інформації в інформаційних системах, здатність оцінювати та забезпечувати якість виконуваних робіт, знання концепції інформаційної безпеки, принципів безпечного проектування ІС а ІТ методології безпечного програмування, погроз і атак, безпеки комп'ютерних мереж. ***Фахових компетентностей*** – володіння навчально-методичними основами і стандартами в області ІТ, уміння їх застосовувати при розробці функціональних профілів ІТ, при побудові та інтеграції систем, продуктів і сервісів ІТ; здатність використовувати сучасні технології проектування в розробці систем захисту інформації; здатність ефективно формувати комунікаційні стратегії у процесі формування концепції обміну інформацією, кодування та вибору каналу комунікації, передачі повідомлень і документів через канал, зберігання та добування документів, реалізації зворотного зв'язку.

Індекс в матриці ОПП	**Програмні компоненти**
ЗК11	Здатність приймати обґрунтовані рішення
СК14	Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне

	програмне забезпечення захисту інформаційних ресурсів об’єктів критичної інформаційної інфраструктури.
ПРН16	Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних.

10. Розподіл балів, які отримують студенти

Поточне тестування та самостійна робота (разом 50 балів)								Підсумковий контроль	Сума
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	іспит	
6	6	6	6	6	6	7	7	50	100

11. Методичне забезпечення

Підручники і навчальні посібники; інструктивно-методичні матеріали до лабораторних занять; контрольні роботи; текстові та електронні варіанти тестів для поточного і підсумкового контролю, методичні матеріали для організації самостійної роботи студентів.

12. Рекомендована література

Базова

1. Рибальський О.В. Основи інформаційної безпеки. Підручник для курсантів ВНЗ МВС України / Рибальський О.В., Смаглюк В.М., Хахановський В.Г. – К.: НАВС, 2013. – 255 с.
2. Коженевський С.Р. Термінологічний довідник з питань захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков. – К.: ДУІКТ, 2007. – 382 с.
3. Рибальський О.В. Захист інформації в інформаційно-комунікаційних системах. Навчальний посібник для курсантів ВНЗ МВС України / О.В. Рибальський, В.Г. Хахановський, В.А. Кудінов, В.М. Смаглюк. – К.: Вид. Національної академії внутріш. справ, 2013. – 118 с.
4. Хорошко В.О. Основи комп’ютерної стеганографії / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук. – Вінниця.: ВДТУ, 2003. – 142 с.
5. Наказ МВС України від 14.07.1998 р. “Про організацію і виконання робіт з технічного захисту інформації з обмеженим доступом в системі МВС України”. – К., 1998.
6. Наказ МВС України № 59 від 14.06.98 р. “Про організацію та виконання робіт з технічного захисту інформації з обмеженим доступом в системі МВС України”.

7. Закон України “Про державну таємницю” від 21.01.1994 // Відомості Верховної Ради України, 1994, № 16. – Ст. 93.
8. Закон України “Про інформацію” // Відомості Верховної Ради, 1992, № 48. – Ст. 650 – 651.
9. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 // Відомості Верховної Ради України, 1994, № 31. – Ст. 286, із змінами 2005 р.
10. Постанова Кабінету Міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” від 08.10.1997 р.
11. Постанова Кабінету Міністрів України “Про затвердження Положення про технічний захист інформації в Україні” від 09.09.1994 р.
12. Постанова Кабінету міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” № 1126 від 08.11.1997 р.

Допоміжна

13. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: «Коло», 2007. – 287 с.
14. Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.
15. ДСанПіН 3.3.6.096-2002 Державні санітарні норми і правила при роботі з джерелами електромагнітних полів
16. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
17. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Проведення робіт.

13. Інформаційні ресурси

18. http://dstszi.gov.ua.
19. Історія розвитку інформаційних технологій в Україні. – http://www.icfcst.kiev.ua/MUSEUM/IT_u.html
20. Нормативні акті Украіn // www.nau.kiev.ua
21. www.rootshell.com.
22. www.securityfocus.com.
23. www.sysinternals.com.