МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Львівський національний університет природокористування

Факультет механіки, енергетики та інформаційних технологій

Кафедра Інформаційних технологій

"ЗАТВЕРДЖУЮ"
Проректор з НПР
проф. Віталій ПОЯРЧУК
"____" _____ 20__ року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Інформаційна безпека

ОПП «Автоматизація та комп'ютерно-інтегровані технології»

спеціальність 151 «Автоматизація та комп'ютерно-інтегровані технології»

перший (бакалаврський) рівень вищої освіти

Львів 2024

Робоча програма навчальної дисципліни **Інформаційна безпека** для здобувачів першого (бакалаврського) рівня вищої освіти ОП «Автоматизація та комп'ютерно-інтегровані технології» спеціальності **151 «Автоматизація та комп'ютерно-інтегровані технології».**

Розробники: к.е.н., доц. Станько В.Ю.

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

Галузь знань: 15 «Автоматизація та приладобудування»

Спеціальність: 151 «Автоматизація та комп'ютерно-інтегровані технології»

Освітньо-професійна програма «Автоматизація та комп'ютерно-інтегровані технології»

Компонент освітньої програми: вибірковий (цикл професійної підготовки)

Рівень вищої освіти – перший (бакалаврський)

Кількість кредитів – 4 (іспит)

Загальна кількість годин – 120

Вид контролю: іспит

Тижневих аудиторних годин для денної форми навчання – 3

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

для денної форми навчання – 48,8 %;

для заочної форми навчання – 16 %.

2. Програма навчальної дисципліни

Розділ 1. Теоретичні засади інформаційної безпеки та захисту інформації

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 автоматизованих 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 криптографії та захисту даних.

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

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.	12	2	4			6	8			1		
Тема 2.	12	2	4			6	12	1		1		8
Тема 3.	12	2	4			6	12	1		1		10
Тема 4.	12	2	4			6	12	1		1		10
Тема 5.	14	2	4			8	12	1		1		10
Тема 6.	14	2	4			8	12	1		1		10
Тема 7.	14	2	4			8	12	1		2		8
Іспит	30	0	0			30	30					30
Разом	**120**	**14**	**28**			**86**	**120**	**6**		**10**		**100**

4. Теми лабораторних 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	2
7	Ідентифікація і аутентифікація користувача	2
8	Захист об'єктів системі	2
9	Алгоритм RSA.	2
10	Модифікація шифру Віженера та загального шифру перестановки.	2
11	Криптоаналіз лінійних шифрів к-го порядку з відомим відкритим текстом.	2
12	Криптоаналіз деяких шифрів з таємним ключем.	2
13	Афінні шифри.	2
14	Стандарти із захисту інформації	2

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 автоматизованих 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, 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, побудові та інтеграції систем, продуктів і сервісів ІТ; здатність використовувати сучасні технології захисту інформації; здатність ефективно формувати комунікаційні стратегії у процесі формування концепції обміну інформацією, кодування та вибору каналу комунікації, передачі повідомлень і документів через канали комунікації.

Індекс в матриці ОПП	**Програмні компоненти**
ЗК01	Здатність застосовувати знання у практичних ситуаціях
ЗК04	Навички використання інформаційних і комунікаційних технологій
ЗК05	Здатність до пошуку, опрацювання та аналізу інформації з різних джерел
ЗК06	Навички здійснення безпечної діяльності
ПРН03	Вміти застосовувати сучасні інформаційні технології та мати навички розробляти алгоритми та комп'ютерні програми з використанням мов високого рівня та технологій об'єктно-орієнтованого програмування, створювати бази даних та використовувати інтернет-ресурси
ПРН14	Вміти використовувати у виробничій і соціальній діяльності фундаментальні поняття і категорії державотворення для обґрунтування власних світоглядних позицій та політичних переконань з урахуванням процесів соціально-політичної історії України, правових засад та етичних норм

10. Розподіл балів, які отримують студенти

Поточне тестування та самостійна робота (разом 50 балів)							Підсумковий контроль	Сума
Т1	Т2	Т3	Т4	Т5	Т6	Т7	іспит	
7	7	7	7	7	7	8	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

Літературні джерела

1. 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.
2. Закон України “Про інформацію” // Відомості Верховної Ради, 1992, № 48. – Ст. 650 – 651.
3. 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.
4. Постанова Кабінету міністрів України “Про затвердження Концепції технічного захисту інформації в Україні” № 1126 від 08.11.1997 р.

Допоміжна

5. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
6. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Проведення робіт.
7. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: «Коло», 2007. – 287 с.
8. 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.

Інформаційні ресурси

9. http://dstszi.gov.ua.
10. William Stallings. "Cryptography and Network Security: Principles and Practice." Pearson, 2016. (784 p.) - https://www.pearson.com/us/highereducation/program/Stallings-Cryptography-and-Network-Security-Principles-and-Practice-7th-Edition/PGM335896.html
    2. Ross Anderson. "Security Engineering: A Guide to Building Dependable Distributed Systems." Wiley, 2020. (1024 p.) - https://www.wiley.com/enus/Security+Engineering%3A+A+Guide+to+Building+Dependable+Distributed+Systems%2C+3rd+Edition-p-9781119642787
11. ISO/IEC 27001:2013. "Information technology — Security techniques — Information security management systems — Requirements." - https://www.iso.org/standard/54534.html

12. NIST Special Publication 800-53. "Security and Privacy Controls for Federal Information Systems and Organizations." - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
13. "National Cyber Security Centre (NCSC)" - Various publications and recommendations. - https://www.ncsc.gov.uk/
14. Brian Krebs. "Krebs on Security" - Online blog focusing on cybersecurity. - https://krebsonsecurity.com/
15. Virtual Hacking Labs - Practical labs for ethical hacking and penetration testing. - https://www.virtualhackinglabs.com/
16. Coursera: "Cybersecurity Specialization" - Various courses from leading universities. - https://www.coursera.org/specializations/intro-cyber-security
17. www.rootshell.com.
18. www.securityfocus.com.
19. www.sysinternals.com.