Міністерство освіти і науки України
Львівський національний університет природокористування
Факультет механіки, енергетики та інформаційних технологій
Кафедра інформаційних технологій

"ЗАТВЕРДЖУЮ"
Перший
проректор
доц. Федів І.М.
_____
"___"_____20___ року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ»

ОПП «Інформаційні системи та технології»
спеціальність 126 «Інформаційні системи та технології»
другий (магістерський) рівень вищої освіти

Львів 2023

Робоча програма **«Технології захисту інформації»**
для здобувачів спеціальності: **126 «Інформаційні системи та технології», другий (магістерський) рівень вищої освіти**

Розробник: Ткачук Р.Л., д.т.н., професор, Станько В.Ю., к.е.н.

Робочу програму схвалено на засіданні кафедри інформаційних технологій

Протокол № 1 від 28 серпня 2023 року

Завідувач кафедри інформаційних технологій

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

Робочу програму схвалено на засіданні методичної комісії факультету механіки, енергетики та інформаційних технологій

Протокол № 1 від 30 серпня 2023 року

Голова методичної комісії факультету механіки, енергетики та інформаційних технологій

_____ (Ковалишин С.Й.)
(підпис) (прізвище та ініціали)

1. Опис навчальної дисципліни

Галузь знань, освітній ступень
Рівень вищої освіти: другий (магістерський)
Освітній ступень: магістр
Галузь знань 12 Інформаційні технології
(шифр і назва)

Спеціальність 126 «Інформаційні системи та технології»
(шифр і назва)

Характеристика навчальної дисципліни:
Обов'язкова
Кількість кредитів 5
Загальна кількість годин – 150
Індивідуальне завдання _____
(назва)

Вид контролю: екзамен
Тижневих аудиторних годин для денної форми навчання – 4
Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить (%):
для денної форми навчання – 60%
для заочної форми навчання – 21%

2. Програма навчальної дисципліни

Тема 1. Вступ. Термінологія. Базові поняття про інформацію, інформаційну безпеку та захист інформації.
Тема 2. Механізми і політики розмежування прав доступу.
Тема 3. Основи криптографії та шифрування даних.
Тема 4. Стандарти шифрування та алгоритми з секретним ключем.
Тема 5. Алгоритми з відкритим ключем.
Тема 6. Протоколи автентифікації.
Тема 7. Цифрові підписи.
Тема 8. Основні види атак, принципи криптоаналізу.
Тема 9. Основні напрями розвитку сучасної криптографії.
Тема 10. Механізми та протоколи керування ключами (PKI).
Тема 11. Методи та пристрої забезпечення захисту і безпеки
Тема 12. Моделі захисту. Технологія блокчейн

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 1 Семестр 1						Рік підготовки 1 Семестр 1					
Тема 1	8	2	–	–	–	6	8	1	–	–	–	7
Тема 2	8	2	–	–	–	6	8	1	–	–	–	7
Тема 3	10	2	4	–	–	4	10	1	2	–	–	7
Тема 4	8	2	–	–	–	6	8	1	–	–	–	7
Тема 5	10	2	4	–	–	4	10	1	2	–	–	7
Тема 6	10	2	4	–	–	4	10	1	2	–	–	7
Тема 7	10	2	4	–	–	4	10	1	2	–	–	7
Тема 8	8	2	–	–	–	6	8	1	–			7
Тема 9	8	2	–	–	–	6	8	1	–			7
Тема 10	12	2	4	–	–	6	12	1	2			9
Тема 11	14	4	4	–	–	6	14	1	2	–	–	11
Тема 12	14	4	4	–	–	6	14	1	2			11
Іспит	30	–	–	–	–	30	30	–	–	–	–	30
Разом за семестр	150	28	28	0	0	94	150	12	14	0	0	124
Індивідуальні завдання												
–	–	–	–	–	–	–	–	–	–	–	–	–
Усього годин	150	28	28	0	0	94	150	12	14	0	0	124

4. Перелік практичних занять

№ з/п	Назва теми	Кількість годин
1	Основи криптографії та шифрування даних	4
2	Алгоритми з відкритим ключем	4
3	Протоколи автентифікації	4
4	Цифрові підписи	4
5	Механізми та протоколи керування ключами (PKI)	4
6	Методи та пристрої забезпечення захисту і безпеки	4
7	Моделі захисту. Технологія блокчейн	4
	Разом	28

5. Теми, питання та завдання, винесені на самостійне вивчення

№ з/п	Назва теми
1	Вступ. Термінологія. Базові поняття про інформацію, інформаційну безпеку та захист інформації
2	Механізми і політики розмежування прав доступу
3	Основи криптографії та шифрування даних
4	Стандарти шифрування та алгоритми з секретним ключем
5	Алгоритми з відкритим ключем
6	Протоколи автентифікації
7	Цифрові підписи
8	Основні види атак, принципи криптоаналізу
9	Основні напрями розвитку сучасної криптографії
10	Механізми та протоколи керування ключами (PKI)
11	Методи та пристрої забезпечення захисту і безпеки
12	Моделі захисту. Технологія блокчейн

6. Індивідуальні завдання

7. Методи навчання

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

2. Наочні методи

- ілюстрація (ілюстративно-репродуктивний, презентації, слайди, діаграми, відеоматеріали тощо),

- демонстрування засобу демонстрування: навчальна телепередача або кіно-відеофільм чи його фрагмент; діюча модель, дослід; експеримент, спостереження та досліди в практичних умовах тощо,

3. Словесні та дослідницькі (вербальний, дискусійний), дослідницький, аналіз, синтез, індукція, дедукція.

4. Практичні методи: практичні та самостійні роботи (тренінги тощо).

8. Методи контролю

Політика оцінювання

Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (75% від можливої максимальної кількості балів). Перескладання проміжних модулів відбувається за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Списування під час тестування, виконання контрольних робіт або підсумкового заліку заборонені (в т.ч. із використанням мобільних девайсів). Мобільні пристрої дозволяється технічно використовувати лише під час он-лайн тестування та підготовки практичних завдань.

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, хвороба, працевлаштування, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.

Оцінювання

Остаточна оцінка за курс розраховується наступним чином: поточний контроль оцінюється в 50 балів, та складається із двох модулів. В суму балів кожного модуля входять бали за підготовку, виконання та захисту 7 практичних робіт по 6 за кожну роботу (7 х 6 = 42) та по 4 бали за самостійну роботу, яка оцінюється усна компонента під час здачі кожного модуля (співбесіда із лектором) (4 х 2 = 8).

Поточне тестування та самостійна робота (разом 50 балів)				Підсумковий контроль	Сума
Модуль 1 (22 бали)		Модуль 2 (28 балів)		екзамен	
П1- П3	СР	П4- П7	СР		
3 х 6 =18	4	4 х 6 =24	4	50	100

П1, П2 ... П7 – практичні роботи; СР – самостійна робота.

9. Результати навчання

У результаті засвоєння тем із дисципліни ***Технології захисту інформації*** здобувачі другого (магістерського) рівня вищої освіти набувають знання, уміння та компетентності, що відповідають вимогам ОП «***Інформаційні системи і технології***» спеціальності 126 «***Інформаційні системи і технології***».

Індекс в матриці ОПП	**Програмні компоненти**
ІНТ	Здатність розв'язувати задачі дослідницького та інноваційного характеру у сфері інформаційних систем та технологій.
ЗК01	Здатність до абстрактного мислення, аналізу та синтезу.
ЗК05	Здатність оцінювати та забезпечувати якість виконуваних робіт.
СК01	Здатність розробляти та застосувати ІСТ, необхідні для розв'язання стратегічних і поточних задач.
СК02.	Здатність формулювати вимоги до етапів життєвого циклу сервіс-орієнтованих інформаційних систем.
СК03	Здатність проектувати інформаційні системи з урахуванням особливостей їх призначення, неповної / недостатньої інформації та суперечливих вимог.
СК05	Здатність використовувати сучасні технології аналізу даних для оптимізації процесів в інформаційних системах.
СК06	Здатність управляти інформаційними ризиками на основі концепції інформаційної безпеки.

РН01	Відшуковувати необхідну інформацію в науковій і технічній літературі, базах даних, інших джерелах, аналізувати та оцінювати цю інформацію.
РН03	Приймати ефективні рішення з проблем розвитку інформаційної інфраструктури, створення і застосування ІСТ.
РН06	Обґрунтовувати вибір технічних та програмних рішень з урахуванням їх взаємодії та потенційного впливу на вирішення організаційних проблем, організовувати їх впровадження та використання.
РН10	Забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації.

11. Методичне забезпечення

Підручники і навчальні посібники; інструктивно-методичні матеріали до практичних занять; індивідуальні навчально-дослідні завдання; контрольні роботи; текстові та електронні варіанти тестів для поточного контролю, методичні матеріали для організації самостійної роботи студентів, виконання індивідуальних завдань.

12. Рекомендована література

Літературні джерела

1. Закони України: «Про інформацію». Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650

2. Закони України: «Про доступ до публічної інформації». Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314

3. Закон України «Про захист персональних даних». (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481)

4. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”. (Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286)

5. Постанова Кабінету Міністрів України від 25.05.2011 № 616 "Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення". від 25 травня 2011 р. N 616 Київ.

6. Браіловський М.М., Зибін С.В., Пискун І.В., Хорошко В.О., Хохлачова Ю.Є.. Технології захисту інформації: підручник. – К.: ЦП «Компринт», 2021. – 296 стр.

7. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.

8. Литвин В. В., Пасічник В. В., Нікольський Ю. В. Аналіз даних та знань : навчальний посібник. Львів: «Магнолія 2006», 2015. 276 с.

9. Основи інформаційної безпеки / С. В. Кавун, О. А. Смірнов, В. Ф. Столбов – Кіровоград : Вид. КНТУ, 2012. – 414 с.

10. 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.

11. Пономаренко В. С. Основи захисту інформації. Навчальний посібник/ В. С. Пономаренко, І. В. Журавльова. – Харків: Вид. ХДЕУ, 2003. – 176 с.

12. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

13. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.

14. Фаль О. М. Криптографія: основні ідеї та застосування/ О. М. Фаль. – К,: Вид-во НТТУ КПІ, 2004.

15. Хлобистова, О. А. Технології захисту інформації [Електронний ресурс] : навч. посіб. / О. А. Хлобистова, Ю. Г. Савченко, М. В. Гладка – К.: НУХТ, 2014. – 84 с.

16. Alp Ustundag, Emre Cevikcan. Industry 4.0: Managing The Digital Transformation. – Springer Series in Advanced Manufacturing, 2018. 286 pp.

17. Матеріали відкритого курсу OpenDataScience [Електронний ресурс]. Електрон. дан. Режим доступа: World Wide Web. URL: https://habr.com/ru/company/ods/blog/344044.

18. Портал відкритих даних України. [Електронний ресурс]. Режим доступу: https://data.gov.ua/

19. Комплект методичних посібників виданих кафедрою, конспект лекцій.

Інформаційні ресурси в Інтернеті

20. Матеріали відкритого курсу OpenDataScience [Електронний ресурс]. Електрон. дан. Режим доступа: World Wide Web. URL: https://habr.com/ru/company/ods/blog/344044.

21. The latest in machine learning. Papers With Code [Електронний ресурс]. Електрон. дан. Режим доступу: World Wide Web. URL: https://paperswithcode.com/.

22. Портал відкритих даних України. [Електронний ресурс]. Режим доступу: https://data.gov.ua/

23. Weka Machine learning software to solve data mining problems [Електронний ресурс]. – Режим доступу: https://sourceforge.net/projects/weka/?source=typ_redirect.