МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет природокористування
Факультет механіки, енергетики та інформаційних технологій
Кафедра інформаційних технологій

ЗАТВЕРДЖЕНО
Гарант освітньо-професійної програми «Інформаційні системи та технології» другого (магістерського) рівня вищої освіти:
зав. каф. ІТ, д.т.н., проф.

А.М. Тригуба

СИЛАБУС
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ»

освітньо-професійна програма «Інформаційні системи та технології»
спеціальність 126 «Інформаційні системи та технології»
другий (магістерський) рівень вищої освіти

ВИКЛАДАЧ **Ткачук Ростислав Львович**

Електронна пошта: rlvtk@ukr.net

Телефон +380507342271

Викладач кафедри інформаційних технологій Львівського національного університету природокористування, доктор технічних наук, професор. Викладач з 27-річним досвідом, автор та співавтор 185 наукових статей, 45 монографій та 65 навчально-методичних розробок.

Читає курси: Основи кібербезпеки; Ведення документів з грифом секретно та для службового користування; Методи та моделі в управлінні інформаційною безпекою; Технології захисту інформації; Методи захисту економічної інформації. Сфера наукових інтересів: інформаційно-логічні та когнітивні технології прийняття рішень в умовах ризику; інформаційні технології у підготовці особового складу до дій в екстремальних умовах; інформаційна безпека.

ЛЬВІВ 2023

Рівень вищої освіти – ***другий (магістерський)***
Галузь знань: ***12 «Інформаційні технології»***
Спеціальність: ***126 «Інформаційні системи та технології»***
Освітньо-професійна програма ***«Інформаційні системи та технології»***
Кількість кредитів – ***5***
Рік підготовки, семестр – ***1 рік, 1 семестр***
Компонент освітньої програми: ***обов'язкова***
Мова викладання: ***українська***

Опис дисципліни

Дисципліна «Технології захисту інформації» вивчає теоретичну та практичну основу сукупності знань та вмінь, що формують профіль фахівця в області інформаційних комп'ютерних систем та технологій для забезпечення у студентів цілісності сприйняття методології і методів захисту інформації, аспекти котрих знаходять широке застосування при використанні сучасних інформаційних систем. Висвітлює основні поняття й подає визначення, які стосуються процесу захисту інформації та формують політику безпеки. Розглядає критерії оцінки захищеності комп'ютерних систем, основ криптографічного захисту інформації, захисту інформації від несанкціонованого доступу в сучасних операційних системах, подає комплексні системи захисту в корпоративних інформаційних системах.

Програма дисципліни «Технології захисту інформації» відноситься до дисциплін професійної підготовки та складена відповідно до освітньо-професійної програми «Інформаційні системи та технології» другого (магістерського) рівня вищої освіти.

Міждисциплінарні зв'язки: освітня компонента «Технології захисту інформації» є складовою частиною циклу професійної підготовки для здобувачів освітньо-професійної програми «Інформаційні системи та технології» другого (магістерського) рівня вищої освіти. Вивчення дисципліни передбачає наявність систематичних та ґрунтовних знань із суміжних курсів – «Вища математика», «Теорія ймовірності та математична статистика», «Алгоритмізація та програмування», «Інженерія даних та знань», «Основи проектування інформаційних систем», «Інформаційна безпека», «Теорія інформації та кодування».

Вимоги до знань та умінь визначаються галузевими стандартами вищої освіти України.

Предметом вивчення освітньої компоненти «Технології захисту інформації» є процес навчання і підготовки фахівця за освітньо-професійною програмою «Інформаційні системи та технології» другого (магістерського) рівня вищої освіти, який дозволить використовувати методи захисту інформації, проводити аналіз систем стосовно їхньої безпеки, застосувати сучасні рішення для захисту інформації.

Метою вивчення освітньої компоненти «Технології захисту інформації» є теоретична та практична підготовка здобувачів вищої освіти, ознайомлення з принципами побудови та використання програмних та програмно-апаратних засобів для захисту програмного забезпечення та інформації в комп'ютерних системах.

Основними завданнями освітньої компоненти «Технології захисту інформації» є: надання комплексу знань, умінь та навичок на рівні новітніх досягнень у розв'язуванні задач використання технологій захисту інформаційно-комунікаційних систем, забезпечення цілісності, доступності та конфіденційності інформації, використання принципів функціонування систем захисту інформації.

Структура курсу

Години аудиторних занять (лек./ практ.)	Тема	Результати навчання	Завдання
2/-	Тема 1. Вступ. Термінологія. Базові поняття про інформацію, інформаційну безпеку та захист інформації.	Розуміти основні поняття інформація, види та властивості інформації, носії та захист інформації. Знати термінологію, основні поняття про загрози для даних в комп'ютерних системах, способи та методи перевірки достовірності інформації.	Питання, робота у ВНС
2/-	Тема 2. Механізми і політики розмежування прав доступу.	Розуміти основні поняття «Оранжевої книги», європейський стандарт у галузі оцінки захищеності комп'ютерних систем. Знати функціональні вимоги безпеки, вимоги довіри, критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу.	Питання, робота у ВНС
2/4	Тема 3. Основи криптографії та шифрування даних.	Розуміти основні поняття теорії зв'язку в секретних системах, симетричні, асиметричні та комбіновані криптосистеми. Знати вимоги до сучасних криптосистем та їх класифікацію, математичні основи асиметричної криптографії	Питання, практична робота
2/-	Тема 4. Стандарти шифрування та алгоритми з секретним ключем.	Розуміти DES – стандарт шифрування даних, основні модифікації DES та алгоритм криптографічного перетворення ГОСТ 28147-89. Знати послідовність перетворень окремого раунду, операції шифрування та розшифрування, алгоритм DES	Питання, робота у ВНС
2/4	Тема 5. Алгоритми з відкритим ключем.	Розуміти алгоритм RSA, його криптостійкість, алгоритм Ель-Гамаля. Знати можливості безпеки та швидкодії RSA, криптостійкість системи Ель-Гамаля	Питання, практична робота
2/4	Тема 6. Протоколи автентифікації.	Розуміти поняття про гешувальні алгоритми, їх призначення. Знати колізійно-стійкі функції гешування Whirpool та SHA-256, SHA-384, SHA-512	Питання, практична робота
2/4	Тема 7. Цифрові підписи.	Розуміти поняття про цифровий та вимоги до нього. Знати основні алгоритми електронного цифрового підпису, український алгоритм ЕЦП ДСТУ 4145	Питання, практична робота
2/-	Тема 8. Основні види атак, принципи криптоаналізу.	Розуміти диференціальний та лінійний криптоаналіз. Знати класифікацію атак на симетричні та асиметричні криптоалгоритми.	Питання, робота у ВНС
2/-	Тема 9. Основні напрями розвитку сучасної криптографії.	Розуміти нові асиметричні алгоритми на основі еліптичних кривих, проблеми генерування випадкових та псевдовипадкових послідовностей. Знати вимоги до генераторів	Питання, робота у ВНС

		випадкових та псевдовипадкових послідовностей, криптографічно стійкі генератори псевдовипадкових послідовностей.	
2/4	Тема 10. Механізми та протоколи керування ключами (PKI).	Розуміти основні положення керування ключами на основі симетричних та асиметричних методів. Знати життєвий цикл криптографічного ключа, Стандарти і специфікації PKI.	Питання, практична робота
4/4	Тема 11. Методи та пристрої забезпечення захисту і безпеки	Розуміти основні принципи захисту інформації при підключені до мережі Інтернет, можливості захисту інформації на мережному рівні. Знати принципи роботи протоколів IPSec, SSL, TLS	Питання, практична робота
4/4	Тема 12. Моделі захисту. Технологія блокчейн	Розуміти умови функціонування та загрози інформації в комп'ютерних системах та мережах. Знати принципи побудови моделі загроз у сучасних комп'ютерних мережах та системах, забезпечення безпеки даних за рахунок децентралізації, шифрування та контролю доступу використовуючи технологію блокчейн.	Питання, практична робота

Навчальний контент

Формування програмних компетентностей

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.
ЗК03	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).
ЗК05	Здатність оцінювати та забезпечувати якість виконуваних робіт.
СК03	Здатність проектувати інформаційні системи з урахуванням особливостей їх призначення, неповної / недостатньої інформації та суперечливих вимог.
СК04	Здатність розробляти математичні, інформаційні та комп'ютерні моделі об'єктів і процесів інформатизації.
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.
РН09	Розробляти і використовувати сховища даних, здійснювати аналіз даних для підтримки прийняття рішень.
РН10	Забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації.

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.

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 за вид діяльності балів). Перескладання модулів відбувається за наявності поважних причин (наприклад, лікарняний).

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

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 ведучим викладачем

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).

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

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

До Силабусу також готуються матеріали навчально-методичного комплексу:

1) Навчальний контент (розширений план лекцій)
2) Тематика та зміст практичних робіт
3) Завдання для підсумкової роботи, питання на іспит
4) Електронне навчання у системі MODLE.