МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Львівський національний університет природокористування

Факультет механіки, енергетики та інформаційних технологій

Кафедра Інформаційних технологій

ЗАТВЕРДЖЕНО

Гарант освітньо-професійної програми «Комп'ютерні науки» першого (бакалаврського) рівня вищої освіти

к.т.н., доцент В.В. Пташник

СИЛАБУС
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ІНФОРМАЦІЙНА БЕЗПЕКА»

освітньо-професійна програма «Комп’ютерні науки»

спеціальність 122 «Комп’ютерні науки»

перший (бакалаврський) рівень вищої освіти

ВИКЛАДАЧ **ТКАЧУК РОСТИСЛАВ ЛЬВОВИЧ**

E-mail: tkachukrl@lnup.edu.ua

Доктор технічних наук, професор. Викладач з понад 23-річним досвідом, автор та співавтор понад 40 наукових статей та понад 35 навчально-методичних розробок.

Читає курс: *Інформаційна безпека, теорія інформації та кодування, технології захисту інформації.*

Сфера наукових інтересів: *Інформаційні системи безпеки та захисту інформації.*

ЛЬВІВ 2025

Галузь знань: ***12 «Інформаційні технології»***
Спеціальність: ***122 «Комп'ютерні науки»***
Освітньо-професійна програма ***«Комп'ютерні науки»***
Рівень вищої освіти – ***перший (бакалаврський)***
Кількість кредитів – ***4***
Рік підготовки, семестр – ***4 рік, 7 семестр***
Компонент освітньої програми: ***обов'язкова***
Мова викладання: ***українська***

Опис дисципліни

Інформаційна складова життя суспільства, активно впливає на стан політичної, економічної, оборонної й інших складових національної безпеки України.

Сьогодні, як ніколи, відбувається безперервна боротьба за контроль над інформаційними потоками. Виграє той, хто не лише вміє їх формувати та регулювати у своїх власних інтересах, але й здатний забезпечити цілісність свого інформаційного ресурсу.

Основою сучасного суспільства є інформаційні технології та інформація, яка в таких умовах стає товаром й основним продуктом виробництва та створення додаткової вартості.

Зворотнім боком цієї "медалі" є тотальні незаконні зазіхання на чужу інформацію, що, в свою чергу, вимагає її захисту. Особливу небезпеку складають спроби викрадення інформації, що є власністю держави та містить державну або іншу таємницю.

Міждисциплінарні зв'язки: вивчення дисципліни «Інформаційна безпека» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів: «Вища математика», «Теорія ймовірності та математична статистика», «Алгоритми та структури даних», «Програмування», «Основи штучного інтелекту»

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

Предметом вивчення освітньої компоненти «Інформаційна безпека» є теоретичні, методичні та практичні аспекти передбачені освітньо-кваліфікаційною характеристикою, технологічними умовами, нормами законодавства та правилами суспільства

Метою вивчення освітньої компоненти «Інформаційна безпека» це – захистити інтереси суб'єктів інформаційних відносин. Інтереси ці різноманітні, але всі вони концентруються навколо трьох основних аспектів:

- доступність;
- цілісність;
- конфіденційність.

Основними завданнями освітньої компоненти «Інформаційна безпека» є набуття здобувачами вищої освіти теоретичних знань щодо оцінювання та

забезпечення захисту інформації в інформаційних системах, принципів безпечного проектування ІС а ІТ методології безпечного програмування, погроз і атак, безпеки комп’ютерних мереж, 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.

№п/п	Теми	Результати навчання
ЗМІСТОВИЙ МОДУЛЬ 1		
1	Тема 1. Концептуальні засади забезпечення інформаційної безпеки України.	Знати: Нормативно-правові основи захисту інформації в Україні. Концепцію національної інформаційної безпеки України. Основні поняття, терміни та визначення технічного захисту інформації. Поняття технічного захисту інформації у системі інформаційної безпеки. Сутність та завдання технічного захисту інформації. Види та класифікація технічних каналів витоку інформації. Основні поняття щодо захисту інформації в автоматизованих системах. Вміти: Працювати з нормативно-правовими актами. Застосовувати заходи щодо попередження несанкціонованого доступу до інформації. Використовувати методи пасивного та активного захисту інформації. Визначати загрози безпеки даних та їх особливості. Розрізняти і класифікувати канали проникнення та принципи побудови систем захисту.
2	Тема 2. Технічні канали витоку інформації. Способи несанкціонованого зняття інформації	
3	Тема 3. Методи та засоби блокування технічних каналів витоку інформації	
4	Тема 4. Основи безпеки даних комп'ютерних системах	
ЗМІСТОВИЙ МОДУЛЬ 2		
5	Тема 5. Ідентифікація і аутентифікація користувачів	Знати: Поняття про ідентифікацію користувача та її особливості. Основні принципи та методи аутентифікації. Основні принципи захисту даних від несанкціонованого доступу. Моделі управління доступом. Криптографічні методи захисту інформації.
6	Тема 6. Основи захисту даних	
7	Тема 7. Основи криптографії	

8	Тема 8. Стандарти із захисту інформації	Світові стандарти із захисту даних в комп'ютерних системах. Державний стандарт України із захисту інформації Вміти: Проводити ідентифікацію та аутентифікацію користувачів. Захищати дані від несанкціонованого доступу. Використовувати технічні засоби захисту даних від їх витоку. Застосовувати засоби захисту даних від комп'ютерних вірусів та шкідливих програм. Супроводжувати та підтримувати криптосистеми та алгоритми шифрування інформації. Здійснювати адміністрування ключами та цифровими підписами.

Навчальний контент
Формування програмних компетентностей

Інтегральна компетентність	Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі комп’ютерних наук або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов.
Загальні компетентності	ЗК13. Здатність діяти на основі етичних міркувань
Фахові (спеціальні) компетентності	ФК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об’єктів критичної інформаційної інфраструктури.
Програмні результати навчання	ПРН15. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних. ПРН16. Виконувати паралельні та розподілені обчислення, застосовувати чисельні методи та алгоритми для паралельних структур, мови паралельного програмування при розробці та експлуатації паралельного та розподіленого програмного забезпечення

Літературні джерела

1.Правове забезпечення інформаційної безпеки : курс лекцій / В. Фурашев, О. Радзієвська ; ДНУ «Ін-т інформ., безпеки і права Нац. акад. прав. наук України». – Київ; Одеса : Фенікс, 2022. 158 с. URL: https://ippi.org.ua/pravove-zabezpechennya-informatsiinoi-bezpeki

2. Правові засади забезпечення кібербезпеки в умовах цифрової трансформації: навчальний посібник / О. Довгань , Н. Ткачук , Т. Ткачук , В. Петров. – К., Артек. 2022. 171 с. URL: https://ippi.org.ua/pravovi-zasadi-zabezpechennya-kiberbezpeki-v-umovakh-tsifrovoi-transformatsii

3. Захист прав, приватності та безпеки людини в інформаційну епоху / Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін. : монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. – Київ-Одеса : Фенікс, 2020. 260 с. URL: https://ippi.org.ua/zakhist-prav-privatnosti-ta-bezpeki-lyudini-v-informatsiinu-epokhu

4. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. URL: https://ippi.org.ua/kiberbezpeka-v-informatsiinomu-suspilstvi

Допоміжна

1. ДСНІП 3.3.6.096-2002 Державні санітарні норми і правила при роботі з джерелами електромагнітних полів
2. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
3. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Проведення робіт.
4. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: «Коло», 2007. – 287 с.
5. 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.

13. Інформаційні ресурси

6. http://dstszi.gov.ua.
7. Історія розвитку інформаційних технологій в Україні. – http://www.icfcst.kiev.ua/MUSEUM/IT_u.html
8. Нормативні акті Україн // www.nau.kiev.ua
9. www.rootshell.com.
10. www.securityfocus.com.
11. www.sysinternals.com.

КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Успішність студента оцінюється шляхом проведення поточного та підсумкового контролю.

Максимальна кількість балів з дисципліни «Інформаційна безпека», яку може отримати студент протягом семестру за всі види роботи, становить 100, при цьому 50 балів за результатами поточного оцінювання, та 50 – за результатами екзаменаційного контролю.

Результати **поточного контролю** оцінюються за чотирибальною («2», «3», «4», «5») шкалою. В кінці семестру обчислюється середнє арифметичне значення (САЗ) усіх отриманих студентом оцінок з наступним переведенням його у 50-ти бальну шкалу за формулою:

ПК = 10•САЗ

Критерії поточного оцінювання знань студентів

Оцінка	Критерії оцінювання
5 («відмінно»)	У повному обсязі володіє навчальним матеріалом, вільно, самостійно та аргументовано його викладає, глибоко і всебічно розкриває зміст, використовуючи обов'язкову та додаткову літературу. Правильно вирішив 90% тестових завдань.
4 («добре»)	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає, в основному розкриває зміст завдань, використовуючи обов'язкову літературу. При викладанні окремих питань не вистачає достатньої глибини та аргументації, допускаються несуттєві неточності й незначні помилки. Правильно вирішив більшість тестових завдань.
3 («задовільно»)	У цілому володіє навчальним матеріалом, викладає його основний зміст, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи окремі суттєві неточності та помилки. Правильно вирішив близько половини тестових завдань.
2 («незадовільно»)	Не в повному обсязі володіє навчальним матеріалом. Викладає матеріал фрагментарно та поверхово, без аргументації й обґрунтування, недостатньо розкриває зміст теоретичних і практичних завдань, допускає суттєві неточності. Правильно вирішив меншість тестових завдань.

Переведення підсумкових рейтингових оцінок з дисципліни, виражених у балах за 100-бальною шкалою, у оцінки за національною шкалою та шкалою ECTS

Таблиця 1 – **Шкала оцінювання: національна та ECTS**

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Оцінка ECTS</td><td colspan="2">Оцінка за національною шкалою</td></tr>
<tr><td>для екзамену, диференційованого заліку, курсового проєкту (роботи), практики</td><td>для заліку</td></tr>
<tr><td>90–100</td><td>A</td><td>відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82–89</td><td>B</td><td rowspan="2">добре</td></tr>
<tr><td>74–81</td><td>C</td></tr>
<tr><td>64–73</td><td>D</td><td rowspan="2">задовільно</td></tr>
<tr><td>60–63</td><td>E</td></tr>
<tr><td>35–59</td><td>FX</td><td>незадовільно з можливістю повторного складання</td><td>не зараховано з можливістю повторного складання</td></tr>
<tr><td>0–34</td><td>F</td><td>незадовільно з обов’язковим повторним вивченням дисципліни</td><td>не зараховано з обов’язковим повторним вивченням дисципліни</td></tr>
</table>

До Силабусу також готуються матеріали навчально-методичного комплексу:

1) Навчальний контент (розширений план лекцій)
2) Тематика та зміст лабораторних робіт
3) Питання на іспит
4) Електронне навчання у системі MOODLE.