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

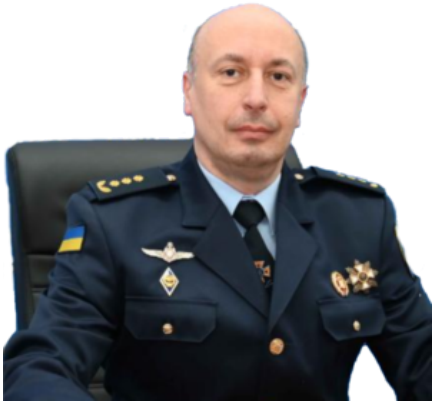
к.т.н., доцент В.В. Пташник

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 2024

Галузь знань: ***12 «Інформаційні технології»***
Спеціальність: ***122 «Комп'ютерні науки»***
Освітньо-професійна програма ***«Комп'ютерні науки»***
Рівень вищої освіти – ***перший (бакалаврський)***
Кількість кредитів – ***5***
Рік підготовки, семестр – ***4 рік, 8 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», «Алгоритмізація та програмування», «Інженерія даних та знань», «Основи проектування інформаційних систем», «Системи 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

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.

Літературні джерела

1. Закон України “Про державну таємницю” від 21.01.1994 // Відомості Верховної Ради України, 1994, № 16. – Ст. 93.
2. 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.
3. Закон України “Про інформацію” // Відомості Верховної Ради, 1992, № 48. – Ст. 650 – 651.

4. 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.
5. 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".
6. 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.
7. Постанова Кабінету Міністрів України "Про затвердження Концепції технічного захисту інформації в Україні" від 08.10.1997 р.
8. Постанова Кабінету міністрів України "Про затвердження Концепції технічного захисту інформації в Україні" № 1126 від 08.11.1997 р.
9. Постанова Кабінету Міністрів України "Про затвердження Положення про технічний захист інформації в Україні" від 09.09.1994 р.
10. 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.
11. 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.
12. Хорошко В.О. Основи комп'ютерної стеганографії / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук. – Вінниця.: ВДТУ, 2003. – 142 с.

Допоміжна

13. ДСНІП 3.3.6.096-2002 Державні санітарні норми і правила при роботі з джерелами електромагнітних полів
14. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.
15. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Проведення робіт.
16. Русин Б.П. Біометрична аутентифікація та криптографічний захист / Б.П. Русин, Я.Ю. Варецький. – Львів: «Коло», 2007. – 287 с.
17. 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

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

22.www.securityfocus.com.
23.www.sysinternals.com.

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 вісьмох тем. Теми від першої до шостої оцінюються по 6 балів, сьома і восьма теми оцінюються по 6 балів (6 х 6 + 7 х 2 = 50).

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

Т1, Т2 ... Т8 – теми

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 віртуальному навчальному середовищі ЛНУП