

Навчальна дисципліна ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

1.	Інформація про навчально-науковий інститут	ННІ «Каразінський банківський інститут»
2.	Курс навчання	четвертий
3.	Спеціальність	122 Комп'ютерні науки
4.	Назва ОПП	Комп'ютерні науки та інформаційні технології в бізнесі
5.	Ступень підготовки	Бакалавр
6.	Мінімальна кількість студентів	15 осіб
7.	Попередні умови вивчення дисципліни	«Вища математика», «Статистика у.т.ч. теорія ймовірності»»
8.	Семестр (осінній/весняний)	Перший (осінній)
9.	Кафедра, що забезпечує викладання	Інформаційних технологій та математичного моделювання
10.	Контактні дані розробників робочої програми навчальної дисципліни	Кандидат технічних наук, доц. Петренко О.Є.
11.	Науково-педагогічні працівники, залучені до викладання	Кандидат технічних наук, доц. Петренко О.Є.
12.	Мета дисципліни	полягає в підготовки фахівців, здатних вирішувати практичні проблеми з реалізації методів, принципів, політик безпеки інформаційних технологій.
13.	Очікувані результати навчання	<p>РНД 1 Студент демонструє знання загальних законів, методів та принципів забезпечення інформаційною безпекою в конкретних проблемних ситуаціях</p> <p>РНД 2 Студент демонструє системне мислення, застосовує методології побудування політик безпеки підприємств та організацій.</p> <p>РНД 3 Студент володіє теоретичними та практичними основами методології та технології моделювання для забезпечення політики інформаційної безпеки</p> <p>РНД 4 Студент демонструє здатність забезпечувати захист інформації, що обробляється в інформаційно телекомунікаційних системах.</p> <p>РНД 5 Студент застосовує програмне</p>

		<p>та програмно-апаратне комплекси засобів захисту інформації в інформаційних телекомунікаційних системах.</p> <p>РНД 6 Студент демонструє здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою.</p> <p>РНД 7 Студент вміє вибирати основні методи та способи захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії інформаційної безпеки.</p> <p>РНД 8 Студент теоретичними та практичними основами захисту від вірусів.</p>
14.	Теми аудиторних занять	<p>Тема 1. Огляд безпеки системи</p> <p>Тема 2. Механізми і політики розмежування доступу.</p> <p>Тема 3. Методи та пристрої забезпечення захисту і безпеки.</p> <p>Тема 4. Захист, доступ та аутентифікація.</p> <p>Тема 5. Моделі захисту. Захист пам'яті.</p> <p>Тема 6. Шифрування даних.</p> <p>Тема 7. Управління відновленням.</p> <p>Тема 8. Основні напрямки розвитку сучасної криптографії.</p> <p>Тема 9. Механізми та протоколи керування ключами в ІВК інформаційної системи.</p> <p>Тема 10. Алгоритми з відкритим ключом</p> <p>Тема 11. Основні види атак, принципи криптоаналізу. Основи криптографії.</p> <p>Тема 12. Алгоритми з секретним ключом.</p> <p>Тема 13. Протоколи аутентифікації</p> <p>Тема 14. Цифрові підписи.</p> <p>Тема 15. Використання паролів і механізмів контролю за доступом</p>
15.	Теми самостійної роботи	<p>Тема 1. Концепція інформаційної безпеки (ІБ) в розподілених інформаційних системах. Задачі ІБ підприємства та рівні їх вирішення.</p> <p>Тема 2. Основні загрози. Фактори уразливості та канали витоку інформації. Модель загроз та порушника</p>

		<p>Тема 3. Апаратні та програмні засоби захисту інформації.</p> <p>Тема 4. Методи автентифікації з використанням асиметричних криптоалгоритмів.</p> <p>Тема 5. Захист від комп'ютерних вірусів</p> <p>Тема 6. Асиметричні та симетричні алгоритми шифрування.</p> <p>Тема 7. Управління відновленням, орієнтоване на своєчасне виявлення втрат інформації і відмовлень компонентів мережі.</p> <p>Тема 8. Основні напрямки розвитку асиметричних криптоалгоритмів.</p> <p>Тема 9. Компоненти та сервіси інфраструктури відкритих ключів.</p> <p>Тема 10 Диференціальний криптоаналіз та лінійний криптоаналіз.</p> <p>Тема 11. Алгоритми симетричного шифрування. Структура, методи, функціональні можливості.</p> <p>Тема 12. Структура алгоритму асиметричного шифрування та дешифрування, галузі застосування.</p> <p>Тема 13. Протоколи захисту та цілісності IPSec, SSL, TLS, їх сутність.</p> <p>Тема 14. Класифікація стандартів електронних цифрових підписів</p> <p>Тема 15. Варіанти побудови VPN-каналів</p> <p>Самостійне опрацювання лекційного матеріалу.</p>
16.	Методи контролю результатів навчання	<p>Екзамен – 7 семестр;</p> <p>60 % – поточний контроль та самостійна робота студентів;</p> <p>40 % – підсумковий контроль: екзамен в письмовій формі (3 ак. години)</p> <p>Оцінювання відбувається за чотирьохрівневою шкалою ECTS..</p>