Навчальна дисципліна УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

1.	Інформація про навчально-науковий інститут	ННІ «Каразінський банківський інститут»
2.	Курс навчання	третій
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)	Другий (весняний)
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 задачі з управління інформаційною безпекою та реалізації політик безпеки інформаційних технологій.
13.	Очікувані результати навчання	РНД 1 Студент демонструє знання загальних законів, методів та принципів забезпечення інформаційною безпекою в конкретних проблемних ситуаціях РНД 2 Студент демонструє системне мислення, застосовує методології побудування політик безпеки підприємств та організацій. РНД 3 Студент володіє теоретичними та практичними основами методології та технології моделювання для забезпечення політики інформаційної безпеки РНД 4 Студент демонструє здатність забезпечувати захист інформації, що обробляється в інформаційно телекомунікаційних системах.

		РНД 6 Студент демонструє здатність формувати комплекс заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою. 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.
14.	Теми аудиторних занять	Тема 1. Основні положення інформаційної безпеки Тема 2. Компоненти моделі безпеки. Тема 3. Законодавчий рівень інформаційної безпеки. Тема 4. Адміністративний рівень політики безпеки. Тема 5. Організаційний рівень інформаційної безпеки. Тема 6. Система управління інформаційною безпекою «Матриця»в банківських структурах України. Система управління інцидентами інформаційної безпеки. Тема 7. Аудит інформаційної безпеки Тема 8. Криптографічний захист інформації. Алгоритми з секретним ключом. Тема 8. Криптографічний захист інформації. Алгоритми з відкритим ключом. Тема 9. Основні види атак, принципи криптоаналізу. Тема 11. Ідентифікація та автентифікація. Тема 11. Електронні цифрові підписи.
15.	Теми самостійної роботи	Тема 1. Основні положення інформаційної безпеки. Тема 2. Компоненти моделі безпеки Тема 3 Законодавчий рівень інформаційної безпеки Тема 4. Адміністративний рівень політики безпеки. Тема 5. Організаційний рівень інформаційної безпеки

		Тема 6. Система управління інцидентами інформаційної безпеки. Тема 7. Аудит інформаційної безпеки. Тема 8. Алгоритми з секретним ключом. Система Вернама. Тема 9. Алгоритми з відкритим ключом. . Алгоритм RSA. Тема 10. Лінійний, диференційний криптоаналіз. Тема 11. Біометричні методи автентифікації. Тема 12. Класифікація стандартів цифрових підписів
16.	Методи контролю результатів навчання	залік – 6 семестр; 100 % – поточний контроль та самостійна робота студентів; Оцінювання відбувається за чотирьохрівневою шкалою ECTS.