Навчальна дисципліна ПРИКЛАДНА КРИПТОЛОГІЯ

1.	Інформація про навчально-науковий інститут	ННІ «Каразінський банківський інститут»
2.	Курс навчання	перший
3.	Спеціальність	F3 Комп'ютерні науки
4.	Назва ОПП	Комп'ютерні науки
5.	Ступень підготовки	Магістр
6.	Мінімальна кількість студентів	10 осіб
7.	Попередні умови вивчення дисципліни	Інформаційні технології
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	оволодіти методами та засобами криптографічного захисту інформації в умовах постійного розвитку інформаційних технологій. Ознайомлення з сучасними та перспективними засобами криптографічного аналізу в умовах визначеної моделі загроз
13.	Очікувані результати навчання	РНД1. Студент має знати основні методи, засоби та алгоритми криптографічного перетворення. РНД2. Студент має знати методи, засоби та алгоритми криптографічного аналізу, які дозволяють оцінити криптографічну стійкість існуючих та перспективних криптографічних систем. РНД3. Студент має вміти розробляти алгоритми та протоколи, що забезпечують потрібний рівень захисту. РНД4. Студент має вміти на основі аналізу моделі загроз розробляти критерії безпеки для криптографічних перетворень в сучасних умовах; РНД5. Студент має вміти застосовувати криптографічні алгоритми для забезпечення цілісності, конфіденційності, спостережливості інформації; обирати параметри для ключів, спираючись на вимоги їх стійкості до відомих криптоаналітичних атак РНД6. Студент має вміти застосовувати стандартизовані криптографічні перетворення для розв'язання прикладних задач.

14.	Теми аудиторних занять	Тема1. Стійкість криптографічних перетворень. Тема2. Генерація псевдовипадкових послідовностей. Тема 3. Управління ключами. Тема 4. Симетричні криптографічні перетворення. Тема 5. Асиметричні криптографічні перетворення. Тема 6. Методи автентифікації в симетричних криптографічних перетвореннях. Тема 7. Методи автентифікації в та асиметричних перетвореннях. Тема 8. Криптографічні протоколи. Тема 9. Криптографічний аналіз симетричних систем. Тема 10. Криптографічний аналіз асиметричних систем.
15.	Теми самостійної роботи	Тема 1. Стійкість криптографічних перетворень. Тема 2. Генерація псевдовипадкових послідовностей. Тема 3. Управління ключами. Тема 4. Симетричні криптографічні перетворення. Тема 5. Асиметричні криптографічні перетворення. Тема 6. Методи автентифікації в симетричних криптографічних перетвореннях. Тема 7. Методи автентифікації в та асиметричних перетвореннях. Тема 8. Криптографічні протоколи. Тема 9. Криптографічний аналіз симетричних систем. Тема 10. Криптографічний аналіз асиметричних систем
16.	Методи контролю результатів навчання	Екзамен – 2 семестр; 60 % – поточний контроль, самостійна робота студента. 40% – екзаменаційна робота студента. Оцінювання відбувається за чотирьохрівневою шкалою ECTS.