

Навчальна дисципліна ПРАВОВІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.	Інформація про навчально-науковий інститут	ННІ «Каразінський банківський інститут»
2.	Курс навчання	четвертий
3.	Спеціальність	125 Кібербезпека
4.	Назва ОПП	Кібербезпека у фінансових технологіях
5.	Ступень підготовки	Бакалавр
6.	Мінімальна кількість студентів	10 осіб
7.	Попередні умови вивчення дисципліни	«Основи кібербезпеки», «Проектування інформаційних систем безпеки», «Основи протидії кіберзлочинності та цифрова криміналістика»
8.	Семестр (осінній/весняний)	восьмий (весняний)
9.	Кафедра, що забезпечує викладання	Інформаційних технологій та математичного моделювання
10.	Контактні дані розробників робочої програми навчальної дисципліни	Кандидат педагогічних наук, зав.каф. Стяглик Н.І. 066-749-67-63
11.	Науково-педагогічні працівники, залучені до викладання	Кандидат педагогічних наук, зав.каф. Стяглик Н.І.
12.	Мета дисципліни	Навчити студентів спеціалізованим заходам у сферах інформаційної та комп'ютерної безпеки, які забезпечують захист сучасних інформаційних систем у професійній діяльності, пов'язаної з отриманням, обробкою, накопиченням і захистом особистої та юридичної інформації.
13.	Очікувані результати навчання	РНД1 Студент володіє сучасними підходами, методиками, засобами захисту інформаційно-комп'ютерних систем і персональної інформації користувача. РНД2 Студент демонструє знання нормативно-правової бази та основних положень і термінів щодо інформаційної та комп'ютерної безпеки. РНД3 Студент розуміє складові проблеми особистої інформаційної безпеки, безпеки держави та шляхи її вирішення; уразливості інформаційного

		<p>простору сучасного суспільства і методи протидії та захисту цього простору.</p> <p>РНД4 Студент усвідомлює загальні принципи, стан та шляхи вирішення проблеми боротьби із комп'ютерними злочинами.</p> <p>РНД5 Студент використовує засоби протидії у втручання в персональну інформацію у віртуальному середовищі Інтернет і в комп'ютері користувача; найважливіші програмно-технічні та криптографічні методи та засоби захисту інформації від несанкціонованого доступу</p> <p>РНД6 Студент вміє аналізувати інформаційні погрози та протидіяти діям порушників; захищати технічні канали витоку інформації; вирішувати практичні завдання із захисту інформації в комп'ютерних системах</p>
14.	Теми аудиторних занять	<p>Тема 1. Основні поняття, визначення. Основні нормативно-правові документи України у сфері інформаційної безпеки.</p> <p>Тема 2. Загрози безпеки. Класифікація загроз. Класифікаційна політика в сфері інформації.</p> <p>Тема 3. Механізми реалізації безпеки.</p> <p>Тема 4. Забезпечення безпеки об'єктів інформаційної сфери держави.</p> <p>Тема 5. Характеристика стандартів по забезпеченню інформаційної безпеки.</p> <p>Тема 6. Ризики роботи на персональному комп'ютері.</p> <p>Тема 7. Засоби захисту інформації.</p> <p>Тема 8. Комплексний захист інформації.</p> <p>Тема 9. Розробка політики безпеки.</p> <p>Тема 10. Міжнародні стандарти безпеки.</p>
15.	Теми самостійної роботи	<p>Тема 1. Нормативна база інформаційної безпеки.</p> <p>Тема 2. Поняття стандартів інформаційної безпеки.</p> <p>Тема 3. Кіберпростір.</p> <p>Тема 4. Кіберзагрози та кібератаки.</p> <p>Тема 5. Методика забезпечення інформаційної безпеки.</p>

16.	Методи контролю результатів навчання	Залік – 8 семестр; 100 % – поточний контроль, самостійна робота студентів; Оцінювання відбувається за чотирьохрівневою шкалою ECTS.
-----	--------------------------------------	---