



**ДВНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**  
**ХАРКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**  
**ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ФІНАНСОВИХ ТЕХНОЛОГІЙ**  
**Кафедра ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Навчальна дисципліна	<b>ФВД1 Моделювання (Рівень А - Економіко-математичні методи та моделі)</b>
Офіційна назва освітньої програми	«Кібербезпека у фінансових технологіях»
Спеціальність	125 Кібербезпека
Освітній ступінь	Перший (бакалаврський)
Обсяг дисципліни в кредитах ECTS	6 кредитів
Статус дисципліни	вибіркова дисципліна фахової підготовки
Мета вивчення дисципліни	формування у студентів системи теоретичних знань та практичних навичок побудови та дослідження економіко-математичних моделей, аналізу отриманих результатів та впровадження їх для подальшого розвитку економічних та технічних систем.
Очікувані результати навчання	РНД 1. Студент демонструє знання основних понять, означень, категорій, термінів, закономірностей, принципів економіко-математичного моделювання. РНД 2. Студент показує вміння побудови математичних моделей згідно із загальною логікою економіко-математичного моделювання РНД 3. Студент демонструє навички використання економіко-математичних моделей для дослідження економічних та технічних систем РНД 4. Студент показує вміння оцінювати та аналізувати можливості й обмеженість сучасних економіко-математичних методів та моделей та оцінювати перспективи їх розвитку РНД 5. Студент демонструє знання та навички застосування економіко-математичних методів та моделей в процесі прийняття управлінських рішень. РНД 6. Студент показує вміння застосовувати комп'ютерну техніку, спеціалізоване програмне забезпечення для побудови та аналізу економіко-математичних моделей.
Зміст навчальної дисципліни за темами	Тема 1. Оптимізаційні економіко-математичні моделі Тема 2. Лінійні оптимізаційні моделі Тема 3. Теорія двоїстості Тема 4. Спеціальні розділи задач лінійної оптимізації Тема 5. Постановка задач нелінійної оптимізації Тема 6. Методи аналізу оптимального плану задачі НЛП Тема 7. Основні поняття теорії ігор Тема 8. Проста лінійна економетрична модель Тема 9. Багатофакторна (множинна) регресія Тема 10. Мультиколінеарність та гетероскедастичність Тема 11. Автокореляція в економетричних моделях. Тема 12. Фіктивні змінні в регресійних моделях Тема 13. Нелінійні моделі

	Тема 14. Дистрибутивно-лагові моделі та їх дослідження Тема 15. Авторегресійні моделі та їх оцінка	
Форми поточного та підсумкового контролю	Поточний контроль – 100 балів. Підсумковий контроль – залік	
Мова навчання	українська	
Критерії оцінювання результатів навчання	Форми контролю	Максимальна кількість балів
		Денна форма навчання
	Поточний контроль:	
	Індивідуальна аналітично-розрахункова робота	2 x 10 балів = 20 балів
	Тестування	2 x 10 балів = 20 балів
	Тези та виступ на науковій конференції або Презентація та захист індивідуальних робіт	10 балів
	Модульна контрольна робота	2 x 25 балів = 50 балів
	Всього за результатами поточного контролю:	100
	Підсумковий контроль: залік	0
Викладач/ викладачі	Філатова Л.Д., к.ф.-м.н., доцент	
Забезпечення	1.Мультимедійний проектор, ноутбук; 2.Інтерактивна дошка; 3.Комп'ютери.	



**ДВНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**  
**ХАРКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**  
**ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ФІНАНСОВИХ ТЕХНОЛОГІЙ**  
**Кафедра ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Навчальна дисципліна	<b>ФВД1 Моделювання (Рівень В – Теорія ризиків)</b>
Офіційна назва освітньої програми	«Кібербезпека у фінансових технологіях»
Спеціальність	125 Кібербезпека
Освітній ступінь	Перший (бакалаврський)
Обсяг дисципліни в кредитах ECTS	6 кредитів
Статус дисципліни	Вибіркова дисципліна фахової підготовки
Мета вивчення дисципліни	ознайомитися із сучасними науковими досягненнями в теоретичних питаннях ризику, опанувати наукові досягнення в теоретичних питаннях ризику, способи оцінювання ризикових ситуацій, методи отримання кінцевого результату і вибору оптимальної стратегії в умовах невизначеності, випадковості та конфлікту.
Очікувані результати навчання	<p>РНД1. Студент має знати суттєву характеристику організацій, підприємств та фірм різних форм власності, а також особливості їх функціонування в умовах невизначеності та ризику.</p> <p>РНД2. Студент має знати сутність ризику та причини його виникнення, класифікацію ризиків та специфіку управління ними в умовах ринкових відносин.</p> <p>РНД3. Студент має знати засоби аналізу та кількісної оцінки ризиків з використанням апарата математичної статистики, аналітичних, експертних методів.</p> <p>РНД4. Студент має знати шляхи та заходи зниження ступеню економічних ризиків.</p> <p>РНД5. Студент має вміти ідентифікувати місцезнаходження прогнозованих чи виникаючих в процесі господарської діяльності ризиків в загальній системі їх класифікації.</p> <p>РНД6. Студент має вміти вибирати та використовувати засоби кількісної оцінки ступеня економічних ризиків господарюючих суб'єктів.</p> <p>РНД7. Студент має вміти організувати процес ефективного управління ризиком у випадку його реалізації</p>
Зміст навчальної дисципліни за темами	<p>Змістовий модуль 1. Економічний ризик та методи його оцінки</p> <p>Тема 1. Сутність економічного ризику</p> <p>Тема 2. Оцінка ризику</p> <p>Тема 3. Управління економічним ризиком</p> <p>Змістовий модуль 2. Теоретичні засади моделювання ризику та вибір оптимальної стратегії</p> <p>Тема 4. Економічний ризик і теорія корисності</p> <p>Тема 5. Вибір оптимальної стратегії в умовах ризиків, пов'язаних з конфліктом</p> <p>Тема 6. Вибір оптимальної стратегії в умовах ризиків, пов'язаних з</p>

	невизначеністю навколишнього середовища Тема 7. Оптимальна поведінка в умовах специфічних видів ризику Тема 8. Метод Монте — Карло і його застосування до оцінки стратегій, пов'язаних із ризиком	
Форми поточного та підсумкового контролю	Поточний контроль – 100 балів. Підсумковий контроль – залік	
Мова навчання	українська	
Критерії оцінювання результатів навчання	Форми контролю	Максимальна кількість балів
		Денна форма навчання
	Поточний контроль:	
	Індивідуальна аналітично-розрахункова робота	2 x 10 бали = 20 балів
	Тестування	2 x 10 балів = 20 балів
	Тези та виступ на науковій конференції або Презентація та захист індивідуальних робіт	10 балів
	Модульна контрольна робота	2 x 25 балів = 50 балів
	Всього за результатами поточного контролю:	100
	Підсумковий контроль: залік	0
Викладач/ викладачі	Філатова Л.Д., к.ф.-м.н., доцент	
Забезпечення	1.Мультимедійний проектор, ноутбук; 2.Інтерактивна дошка; 3.Комп'ютери.	



**ДВНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**  
**ХАРКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**  
**ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ФІНАНСОВИХ ТЕХНОЛОГІЙ**  
**Кафедра ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Навчальна дисципліна	<b>ФВД2 Кібербезпека (Рівень F – Основи протидії кіберзлочинності та цифрова криміналістика)</b>
Офіційна назва освітньої програми	«Кібербезпека у фінансових технологіях»
Спеціальність	125 Кібербезпека
Освітній ступінь	Перший (бакалаврський)
Обсяг дисципліни в кредитах ECTS	6 кредитів
Статус дисципліни	Вибіркова дисципліна фахової підготовки
Мета вивчення дисципліни	Ознайомлення з теоретичними положеннями криміналістичної науки, оволодіння криміналістичними засобами, прийомами та методами збирання, дослідження, оцінки та використання доказів під час розслідування та попередження злочинів у цифровому середовищі. Надання цілісного уявлення про процесуальні, організаційні, методичні, наукові і тактичні основи призначення судових експертиз, їх сучасні види й можливості, а також вироблення вмінь з підготовки, призначення судових експертиз та оцінки висновку експерта при розслідуванні злочинів.
Очікувані результати навчання	<p>РНД1. Студент демонструє теоретичні знання і практичне знання спеціальних методів для відновлення, перевірки справжності і аналізу електронних даних, пов'язаних з комп'ютерними злочинами.</p> <p>РНД2. Студент демонструє системне мислення, застосовує методології системного аналізу для дослідження складних проблем різної природи при розкритті кримінальних злочинів в галузі цифрових технологій, методів формалізації та розв'язанні системних задач, що мають суперечливі цілі, невизначеності та ризики</p> <p>РНД3. Студент володіє теоретичними та практичними основами методології комп'ютерних злочинів, надлишкової криміналізації, криміналістична характеристика, статистика, особливостями ймовірного злочинця. Оперативність, пріоритетність розслідування. Онлайн-шахрайство.</p> <p>РНД4. Студент може будувати версії у різних слідчих ситуаціях, планувати й організовувати розслідування злочинів; взаємодіяти з оперативними підрозділами у виконанні завдань розслідування злочинів; аналізувати слідчі ситуації, що складаються на різних етапах розслідування злочинів, і приймати правильні рішення щодо постановки тактичних завдань та визначення засобів їх вирішення – слідчо-оперативних операцій чи комбінацій.</p> <p>РНД5. Студент розуміє механізми скоєння злочинів та їх складові елементи, визначення слідів та їх види, правила виявлення, фіксації, вилучення і використання слідів у розслідуванні злочинів, види</p>

	<p>документів, способи та ознаки їх підробки</p> <p>РНД6. Студент застосовує методології, технології та інструментальні засоби для управління процесами підготовки судово технічної експертизи комп'ютерів та мобільних пристроїв.</p> <p>РНД7. Здобувач застосовує результати аналізу та контролю для прийняття управлінських рішень та вирішення конкретних практичних ситуацій.</p> <p>РНД8. Студент застосовує сучасні статистичні методи для розв'язання задач та навички самостійного використання математичної літератури та прикладних пакетів програм для статистичного аналізу.</p>	
Зміст навчальної дисципліни за темами	<p>Тема1. Введення. Основні аспекти цифрової криміналістики (теоретичні засади).</p> <p>Тема 2. Цифрова криміналістики файлових систем</p> <p>Тема 3. Цифрова криміналістики операційних систем.</p> <p>Тема 4. Криміналістична методика (Загальні положення).</p> <p>Тема 5. Комп'ютерні злочини.</p> <p>Тема 6. Оперативно-розшукові заходи.</p> <p>Тема7. Слідчі дії.</p> <p>Тема 8. Засвідчення контенту.</p> <p>Тема 9. Комп'ютерно-технічна експертиза.</p> <p>Тема 10. Комп'ютерна криміналістика и збір доказів.</p> <p>Тема 11. Міжнародна організація з комп'ютерних доказів.</p> <p>Тема 12. Поведінка комп'ютерних злочинців.</p> <p>Тема 13. Фахівці по розслідуванню інцидентів.</p> <p>Тема 14. Процес проведення комп'ютерної експертизи.</p> <p>Тема 15. Основи криміналістичного обстеження мобільних пристроїв. . ПЗ. Випробування</p>	
Форми поточного та підсумкового контролю	<p>Поточний контроль – 100 балів.</p> <p>Підсумковий контроль – залік</p>	
Мова навчання	українська	
Критерії оцінювання результатів навчання	Форми контролю	Максимальна кількість балів
		Денна форма навчання
	Поточний контроль:	
	Практичні завдання	6 x 5 балів = 30 балів
	Презентація та захист індивідуальної (дослідницько-аналітичної) роботи	до 10 балів
	Письмові тестові роботи	2 x 5 балів = 10 балів
	Всього за результатами поточного контролю:	50
	Підсумковий контроль: екзамен	50
Всього	100	
Викладач/ викладачі	Кобилін А.М., к.т.н.	
Забезпечення	<p>Мультимедійний проектор</p> <p>Електронна дошка</p> <p>Комп'ютери</p>	



**ДВНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**  
**ХАРКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**  
**ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ФІНАНСОВИХ ТЕХНОЛОГІЙ**  
**Кафедра ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Навчальна дисципліна	<b>ФВД2 Кібербезпека (Рівень D – Платіжні системи, технології та сервіси)</b>
Офіційна назва освітньої програми	«Кібербезпека у фінансових технологіях»
Спеціальність	125 Кібербезпека
Освітній ступінь	Перший (бакалаврський)
Обсяг дисципліни в кредитах ECTS	6 кредитів
Статус дисципліни	Вибіркова дисципліна фахової підготовки
Мета вивчення дисципліни	підготовка кваліфікованих фахівців із необхідним обсягом знань про сучасні платіжні технології, формування системи знань з теорії платіжних систем, платіжних інструментів, специфіки побудови національної платіжної системи України
Очікувані результати навчання	<p>РНД1 Студент демонструє знання типів платіжних систем, що використовуються в країнах з розвинутою ринковою економікою.</p> <p>РНД2 Студент розуміє концепцію, принципи функціонування і структуру системи електронного грошового обігу, технологію виконання міжбанківських платежів в Україні засобами СЕП.</p> <p>РНД3 Студент розуміє принципи і методи організації міжбанківських розрахунків.</p> <p>РНД4 Студент володіє теоретичними основами технологій міжбанківських систем розрахунків розвинутих ринкових економік.</p> <p>РНД5 Студент має уявлення про кореспондентські відносини і кореспондентський рахунок та перспективи удосконалення існуючої СЕП в Україні.</p> <p>РНД6 Студент знає основні принципи роботи системи масових електронних платежів на основі платіжних карток різного типу та мобільного інтернету.</p> <p>РНД7 Студент розуміє ризики в платіжних системах, знає бухгалтерські, технічні та технологічні методи організації безпеки платіжних систем. Знає правові основи платіжних систем.</p>
Зміст навчальної дисципліни за темами	<p>Тема 1. Загальна концепція платіжних систем, технологій та сервісів.</p> <p>Тема 2. Технологічна інфраструктура платіжних систем.</p> <p>Тема 3. Безпека платіжних систем.</p> <p>Тема 4. Зарубіжні платіжні системи.</p> <p>Тема 5. система переказу грошових коштів і цінних паперів.</p> <p>Тема 6. система міжбанківських розрахунків.</p> <p>Тема 7. система інтеграції внутрішньо-державних платіжних систем</p> <p>Тема 8. товариство міжнародних міжбанківських фінансових телекомунікацій</p> <p>Тема 9. Система електронних міжбанківських платежів Національного банку України.</p> <p>Тема 10. Загальна технологія розрахунків в СЕП НБУ.</p>

	Тема 11. Системи масових електронних платежів, становлення та розвиток в Україні.	
Форми поточного та підсумкового контролю	Поточний контроль – 50 балів. Підсумковий контроль– екзамен.	
Мова навчання	українська	
Критерії оцінювання результатів навчання	Форми контролю	Максимальна кількість балів
		Денна форма навчання
	Поточний контроль:	
	Підсумкове тестування	1 x 10 балів = 10 балів
	Лабораторні роботи	4 x 10 балів = 40 балів
	Всього за результатами поточного контролю:	50
	Підсумковий контроль: екзамен	50
Всього	100	
Викладач/ викладачі	Ходирев О.І., ст.викл.	
Забезпечення	1.Мультимедійний проектор, ноутбук; 2.Інтерактивна дошка; 3.Комп'ютери.	





**ДВНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**  
**ХАРКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**  
**ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ФІНАНСОВИХ ТЕХНОЛОГІЙ**  
**Кафедра ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Навчальна дисципліна	<b>ФВДЗ Інформаційні технології (Рівень В - Комп'ютерна графіка та веб-дизайн)</b>
Офіційна назва освітньої програми	«Кібербезпека у фінансових технологіях»
Спеціальність	125 Кібербезпека
Освітній ступінь	Перший (бакалаврський)
Обсяг дисципліни в кредитах ECTS	6 кредитів
Статус дисципліни	Вибіркова дисципліна фахової підготовки
Мета вивчення дисципліни	Забезпечення здобувачів бакалаврського рівня вищої освіти необхідними знаннями та практичними навичками щодо формування базових теоретичних понять, що лежать в основі комп'ютерної графіки, дати уявлення про методи геометричного моделювання, моделі графічних даних, набути практичних навичок побудови комп'ютерних зображень, графічної візуалізації даних.
Очікувані результати навчання	РНД 1 Студент демонструє володіння базовими теоретичними знаннями та актуальні проблеми теорії, а так само тенденції розвитку науки і техніки в галузі комп'ютерної графіки РНД 2 Студент демонструє закріплення теоретичних знань, основні методи і алгоритми обробки комп'ютерної графіки РНД 3 Студент демонструє володіння апаратом основних компонент графічної системи комп'ютера, їх загальні характеристики РНД 4 Студент вивчає сучасні програмні види комп'ютерної графіки, способи обробки та області їх застосування РНД 5 Студент демонструє практичні навички способів зберігання графічної інформації в оперативній і зовнішньої пам'яті РНД 6 Здобувач демонструє основні можливості та особливості програмних засобів обробки і відображення комп'ютерної графіки РНД 7 Здобувач застосовує на практиці сучасні методи створювати графічних програм для обробки різних зображень РНД 8 Здобувач користується обраним математичним апаратом для вирішення інженерних і наукових задач
Зміст навчальної дисципліни за темами	Тема 1. Відеосистема комп'ютера Тема 2. Зовнішні графічні пристрої введення зображень Тема 3. Зовнішні графічні пристрої виведення зображень Тема 4. Використання функцій API для відображення графічних примітивів на формі Тема 5. Алгоритми перетворення координат на формі Тема 6. Алгоритми генерації ліній для відображення графіків на формі Тема 7. Фундаментальні методи у графіку. Алгоритми формування анімаційних зображень на формі Тема 8. Афінні перетворення. Алгоритми синтезу цифрових зображень

	Тема 9. По-піксельна обробка зображень. Алгоритм фільтрації зображень Тема 10. Прості кольорові моделі	
Форми поточного та підсумкового контролю	Поточний контроль – 50 балів. Підсумковий контроль – екзамен – 50 балів	
Мова навчання	українська	
Критерії оцінювання результатів навчання		Максимальна кількість балів
	Форми контролю	Денна форма навчання
	Поточний контроль:	
	Практичні завдання	10 x 3 балів = 30 балів
	Письмові тестові роботи	2 x 5 балів= 10 балів
	Презентація та захист індивідуальної (дослідницько-аналітичної) роботи	до 10 балів
	Всього за результатами поточного контролю:	50
	Підсумковий контроль: екзамен	50
Всього	100	
Викладач/ викладачі	Тарасенко О.П., к.т.н., доцент	
Забезпечення	1.Мультимедійний проектор, ноутбук; 2.Інтерактивна дошка; 3.Комп'ютери.	



**ДВНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**  
**ХАРКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**  
**ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ФІНАНСОВИХ ТЕХНОЛОГІЙ**  
**Кафедра ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Навчальна дисципліна	<b>ФВДЗ Фінансові технології (Рівень А - Технології дистанційного банківського обслуговування)</b>
Офіційна назва освітньої програми	«Кібербезпека у фінансових технологіях»
Спеціальність	125 Кібербезпека
Освітній ступінь	Перший (бакалаврський)
Обсяг дисципліни в кредитах ECTS	6 кредитів
Статус дисципліни	Вибіркова дисципліна фахової підготовки
Мета вивчення дисципліни	формування системи знань з теоретичних основ організації та функціонування інформаційних систем дистанційного банківського обслуговування в умовах всесвітньої мережі.
Очікувані результати навчання	<p>РНД 1. Студент демонструє знання основних понять, означень, категорій, термінів, специфіки функціонування різних видів діяльності цифрової економіки</p> <p>РНД 2. Студент показує вміння побудови власної інформаційної безпеки та протистояння маніпулятивним технологіям</p> <p>РНД 3. Студент демонструє навички використання пошукових систем, соціальних мереж та інтернет-сервісів</p> <p>РНД 4. Студент показує вміння оцінювати та аналізувати соціальні та економічні наслідки новітніх технологічних трендів</p> <p>РНД 5. Студент демонструє знання та навички володіння технологіями стартап-діяльності та трансферу технологій</p> <p>РНД 6. Студент показує вміння застосовувати сучасні мобільні технології для розвитку технологічних проєктів</p> <p>РНД 7. Студент вміє побудувати власну кар'єрну траєкторію, персональний бренд, імідж з урахуванням специфіки кіберпростору</p>
Зміст навчальної дисципліни за темами	<p>Тема 1. Основні поняття і технології дистанційного банківського обслуговування (ДБО).</p> <p>Тема 2. Системи дистанційного банківського обслуговування Клієнт-Банк.</p> <p>Тема 3. Основні вимоги до інтегрованих систем комплексного дистанційного банківського обслуговування.</p> <p>Тема 4. Класифікація фінансових послуг у мережі Інтернет.</p> <p>Тема 5. Електронний банкінг як сегмент електронного бізнесу.</p> <p>Тема 6. Системи Internet-banking. Методи та форми організації Internet-banking.</p> <p>Тема 7. Mobil-banking. SMS-Banking. WAP-Banking. Вимоги до Інтернет-сервісу.</p> <p>Тема 8. Стратегічні напрями розвитку банківських Internet-технологій.</p> <p>Тема 9. Інформаційна безпека електронних банківських послуг. Світові стандарти критеріїв оцінки безпеки інформаційних систем.</p> <p>Тема 10. Розвиток Internet-banking в Україні. Інтернет-платежі в on-line</p>

	системах.	
Форми поточного та підсумкового контролю	Поточний контроль – 50 балів. Підсумковий контроль – екзамен – 50 балів	
Мова навчання	українська	
Критерії оцінювання результатів навчання	Форми контролю	Максимальна кількість балів
		Денна форма навчання
	Поточний контроль:	
	Практичні завдання	10 x 3 балів = 30 балів
	Письмові тестові роботи	2 x 5 балів= 10 балів
	Презентація та захист індивідуальної (дослідницько-аналітичної) роботи	до 10 балів
	Всього за результатами поточного контролю:	50
	Підсумковий контроль: екзамен	50
Всього	100	
Викладач/ викладачі	Ходирев О.І., ст.в.	
Забезпечення	1.Мультимедійний проектор, ноутбук; 2.Інтерактивна дошка; 3.Комп'ютери.	



**ДВНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**  
**ХАРКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**  
**ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ФІНАНСОВИХ ТЕХНОЛОГІЙ**  
**Кафедра ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Навчальна дисципліна	<b>ФВД4 Кібербезпека (Рівень G - Організація та проведення тестування на проникнення та соціальна інженерія)</b>
Офіційна назва освітньої програми	«Кібербезпека у фінансових технологіях»
Спеціальність	125 Кібербезпека
Освітній ступінь	Перший (бакалаврський)
Обсяг дисципліни в кредитах ECTS	6 кредитів
Статус дисципліни	Вибіркова дисципліна фахової підготовки
Мета вивчення дисципліни	Забезпечення майбутніх фахівців необхідними знаннями в галузі інформаційних технологій та набуття ними практичних навичок застосування сучасних інформаційних технологій в професійної діяльності.
Очікувані результати навчання	РНД1. Студент демонструє загальні знання в частині захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами; РНД2. Студент демонструє загальні знання теорій та методів захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; РНД3. Студент демонструє практичні навички в частині використання спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах; РНД4. Студент демонструє загальні знання в частині оцінювання можливості реалізації потенційних загроз інформації, РНД5. Студент демонструє загальні знання в частині соціальної інженерії та її інструментів; РНД6. Студент демонструє загальні знання в частині методів захисту від соціальної інженерії;
Зміст навчальної дисципліни за темами	1. Стандартизація проведення тестування на проникнення 2. Тест на проникнення. 3. Методологія проведення робіт 4. Аудит інформаційної безпеки 5. Впровадження систем та процесів оперативного реагування на інциденти 6. Впровадження систем та рішень захисту 7. Засоби тестування на проникнення 8. Соціальна інженерія 9. Причини вразливостей для соціальної інженерії 10. Інструменти соціальної інженерії 11. Фази соціальної інженерії 12. Методи захисту від соціальної інженерії
Форми поточного та підсумкового контролю	Поточний контроль – 50 балів. Підсумковий контроль– екзамен– 50 балів

Мова навчання	українська	
Критерії оцінювання результатів навчання	Форми контролю	Максимальна кількість балів
		Денна форма навчання
	Поточний контроль:	
	Практичні завдання	5 x 10 балів = 50 балів
	Всього за результатами поточного контролю:	50
	Підсумковий контроль: екзамен	50
	Всього	100
Викладач/ викладачі	ст. викладач Чепіга О.О.	
Забезпечення	1.Мультимедійний проектор, ноутбук; 2.Інтерактивна дошка; 3.Комп'ютери.	



**ДВНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**  
**ХАРКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**  
**ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ФІНАНСОВИХ ТЕХНОЛОГІЙ**  
**Кафедра ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

<i>Навчальна дисципліна</i>	<b>ФВД4 Комп'ютерні системи та мережі (Рівень Е - Адміністрування та моніторинг комп'ютерних систем)</b>
Офіційна назва освітньої програми	«Кібербезпека у фінансових технологіях»
Спеціальність	125 Кібербезпека
Освітній ступінь	Перший (бакалаврський)
Обсяг дисципліни в кредитах ECTS	6 кредитів
Статус дисципліни	Вибіркова дисципліна фахової підготовки
Мета вивчення дисципліни	Підготувати фахівців, здатних проектувати, налагоджувати, та обслуговувати комп'ютерні мережі
Очікувані результати навчання	РНД1 Студент демонструє загальні знання в частині комп'ютерних систем, мережевої архітектури РНД2 Студент демонструє знання в частині безпеки інформаційних систем РНД3 Студент демонструє практичні навички в частині налаштуванні доступу до мережевих ресурсів. РНД 4 Студент демонструє практичні навички в частині налаштування систем резервного копіювання. РНД 5 Студент демонструє практичні навички в частині налаштування систем забезпечення безперебійності функціонування інформаційних систем. РНД 6 Студент демонструє практичні навички в частині налаштування систем моніторингу обчислювальних систем РНД 7 Студент демонструє практичні навички в частині налаштування мережевих сервісів
Зміст навчальної дисципліни за темами	Тема 1 - Діагностика і налагодження обладнання. Тема 2 – Встановлення та налаштування програмного забезпечення. Тема 3 – Організація віддаленого доступу до мереж. Тема 4 - Оновлення програмного забезпечення. Тема 5 - Адміністрування користувачів інформаційних систем. Тема 6 - Адміністрування мережевих ресурсів. Тема 7 - Моніторинг обчислювальних систем. Тема 8 - Адміністрування мережевих сервісів (DNS). Тема 9 - Адміністрування мережевих сервісів (WEB). Тема 10 - Адміністрування захисту периметру мережі Тема 11 - Адміністрування антивірусного захисту Тема 12 - Служби резервного копіювання. Тема 13 - Політики безпеки в комп'ютерних системах.) Тема 14 – Відновлення працездатності комп'ютерних систем. Тема 15 – Побудова централізованої системи адміністрування інформаційною інфраструктурою

Форми поточного та підсумкового контролю	Поточний контроль – 50 балів. Підсумковий контроль– екзамен– 50 балів	
Мова навчання	українська	
Критерії оцінювання результатів навчання	Форми контролю	Максимальна кількість балів
		Денна форма навчання
	Поточний контроль:	
	Практичні завдання	5 x 10 балів = 50 балів
	Всього за результатами поточного контролю:	50
	Підсумковий контроль: екзамен	50
	Всього	100
Викладач/ викладачі	ст. викладач Чепіга О.О.	
Забезпечення	1.Мультимедійний проектор, ноутбук; 2.Інтерактивна дошка; 3.Комп'ютери.	





**ДФНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**  
**ХАРКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**  
**ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ФІНАНСОВИХ ТЕХНОЛОГІЙ**  
**Кафедра ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Навчальна дисципліна	<b>ФВД5 Кібербезпека (Рівень Н - Правові основи інформаційної безпеки)</b>
Офіційна назва освітньої програми	«Кібербезпека у фінансових технологіях»
Спеціальність	125 Кібербезпека
Освітній ступінь	Перший (бакалаврський)
Обсяг дисципліни в кредитах ECTS	6 кредитів
Статус дисципліни	Вибіркова дисципліна фахової підготовки
Мета вивчення дисципліни	Навчити студентів спеціалізованим заходам у сферах інформаційної та комп'ютерної безпеки, які забезпечують захист сучасних інформаційних систем у професійній діяльності, пов'язаній з отриманням, обробкою, накопиченням і захистом особистої та юридичної інформації.
Очікувані результати навчання	<p>РНД1 Студент володіє сучасними підходами, методиками, засобами захисту інформаційно-комп'ютерних систем і персональної інформації користувача.</p> <p>РНД2 Студент демонструє знання нормативно-правової бази та основних положень і термінів щодо інформаційної та комп'ютерної безпеки.</p> <p>РНД3 Студент розуміє складові проблеми особистої інформаційної безпеки, безпеки держави та шляхи її вирішення; уразливості інформаційного 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>
Зміст навчальної дисципліни за темами	<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 компютері.</p> <p>Тема 7. Засоби захисту інформації.</p> <p>Тема 8. Комплексний захист інформації.</p>

	Тема 9. Розробка політики безпеки. Тема 10. Міжнародні стандарти безпеки.	
Форми поточного та підсумкового контролю	Поточний контроль – 100 балів. Підсумковий контроль– залік	
Мова навчання	українська	
Критерії оцінювання результатів навчання	Форми контролю	Максимальна кількість балів
		Денна форма навчання
	Поточний контроль:	
	Практичні роботи	6 x 10 балів = 60 балів
	Тестові роботи	4 x 10 балів = 40 балів
	Всього за результатами поточного контролю:	100
	Підсумковий контроль: залік	
	Всього	100
Викладач/ викладачі	Стяглик Н.І., к.п.н.	
Забезпечення	1.Мультимедійний проектор, ноутбук; 2.Інтерактивна дошка; 3.Комп'ютери.	



**ДВНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**  
**ХАРКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**  
**ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ФІНАНСОВИХ ТЕХНОЛОГІЙ**  
**Кафедра ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Навчальна дисципліна	<b>ФВД5 Кібербезпека (Рівень I - Інформаційна безпека держави)</b>
Офіційна назва освітньої програми	«Кібербезпека у фінансових технологіях»
Спеціальність	125 Кібербезпека
Освітній ступінь	Перший (бакалаврський)
Обсяг дисципліни в кредитах ECTS	6 кредитів
Статус дисципліни	Вибіркова дисципліна фахової підготовки
Мета вивчення дисципліни	Сформувати у студентів розуміння сутності явища інформаційна безпека, ознайомити з основними загрозами інформаційній безпеці та виробити уявлення про ефективність інструментів забезпечення інформаційної безпеки держави
Очікувані результати навчання	<p>РНД1 Студент володіє сучасними підходами, методиками, засобами захисту інформаційно-комп'ютерних систем і персональної інформації користувача.</p> <p>РНД2 Студент демонструє знання основних положень та термінів щодо інформаційної та комп'ютерної безпеки, оперує нормативно-правовою базою в сфері забезпечення інформаційної безпеки.</p> <p>РНД3 Студент розуміє складові проблеми особистої інформаційної безпеки, безпеки держави та шляхи її вирішення; уразливості інформаційного 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, відповідальність за порушення інформаційної безпеки.</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>
Зміст навчальної дисципліни за темами	<p>Тема 1. Інформаційна безпека: підходи до концептуалізації та індикатори визначення</p> <p>Тема 2. Загрози інформаційній безпеці.</p> <p>Тема 3. Методики оцінювання загроз інформаційній безпеці в соціальних Інтернет-сервісах.</p> <p>Тема 4. Теорія і практика інформаційно-психологічного протиборства у ХХ – на початку ХХІ ст..</p> <p>Тема 5. Інститути й інструменти забезпечення інформаційної безпеки України.</p>

	Тема 6. Загрози інформаційній безпеці України. Тема 7. Стандарти Європейського Союзу і НАТО у сфері інформаційної безпеки. Тема 8. Розробка політики безпеки.	
Форми поточного та підсумкового контролю	Поточний контроль – 100 балів. Підсумковий контроль – залік	
Мова навчання	українська	
Критерії оцінювання результатів навчання	Форми контролю	Максимальна кількість балів
		Денна форма навчання
	Поточний контроль:	
	Практичні роботи	6 x 10 балів = 60 балів
	Тестові роботи	4 x 10 балів = 40 балів
	Всього за результатами поточного контролю:	100
	Підсумковий контроль: залік	
	Всього	100
Викладач/ викладачі	Стяглик Н.І., к.п.н.	
Забезпечення	1.Мультимедійний проектор, ноутбук; 2.Інтерактивна дошка; 3.Комп'ютери.	



**ДВНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**  
**ХАРКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**  
**ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ФІНАНСОВИХ ТЕХНОЛОГІЙ**  
**Кафедра ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

<i>Навчальна дисципліна</i>	<b>ФВДб Інформаційні технології (Рівень D - Технології проектування та оцінювання людино-машинних інтерфейсів)</b>
Офіційна назва освітньої програми	«Кібербезпека у фінансових технологіях»
Спеціальність	125 Кібербезпека
Освітній ступінь	Перший (бакалаврський)
Обсяг дисципліни в кредитах ECTS	6 кредитів
Статус дисципліни	Вибіркова дисципліна фахової підготовки
Мета вивчення дисципліни	Одержання теоретичних і практичних знань для ефективного використання сучасних інформаційних технологій захисту інформації в фінансових технологіях.
Очікувані результати навчання	РНД 1. Оцінювати якість людино-машинної взаємодії систем критичного застосування РНД 2. Застосовувати сучасні інноваційні програмно-апаратні комплекси для оцінки зручності використання інтерфейсів користувача РНД 3. Проектувати людино-машинні інтерфейси для систем оцінки та забезпечення інформаційної безпеки РНД 4. Проводити дослідження з залученням користувачів програмних додатків
Зміст навчальної дисципліни за темами	Тема 1. Психопатологія звичних речей Тема 2. Психологія звичних дій Тема 3. Зовнішня інформація і внутрішні знання Тема 4. Помилка людини? Ні, поганий дизайн Тема 5. Дизайнерське мислення Тема 6. Процес проектування взаємодії. Тема 7. Визначення потреб Тема 8. Встановлення вимог Тема 9. Проектування, макетування і розробка Тема 10. Орієнтовані на користувача підходи до проектування взаємодії Тема 11. Основи айтрекінга Тема 12. Підготовка до дослідження Тема 13. Планування дослідження Тема 14. Вербальні протоколи Тема 15. Метрики айтрекінга
Форми поточного та підсумкового контролю	Поточний контроль – 100 балів. Підсумковий контроль – залік.
Мова навчання	українська

Критерії оцінювання результатів навчання	Поточний контроль: Перевірка виконання практичних робіт – 15 робіт x 4 бали =60 балів Презентація та захист індивідуальної роботи (проекту) – 2 x 15 балів =30 балів Контрольна робота (тест) 1 x 10 балів = 10 балів Всього за результатами поточного контролю: 100 балів Підсумковий контроль: залік.
Викладач/ викладачі	Тарасенко О.П., к.т.н., доцент
Забезпечення	1.Мультимедійний проектор, ноутбук; 2.Інтерактивна дошка; 3.Комп'ютери.



**ДФНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**  
**ХАРКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**  
**ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ФІНАНСОВИХ ТЕХНОЛОГІЙ**  
**Кафедра ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Навчальна дисципліна	<b>ФВД6 Моделювання (Рівень С – Теорія прийняття рішень)</b>
Офіційна назва освітньої програми	«Кібербезпека у фінансових технологіях»
Спеціальність	125 Кібербезпека
Освітній ступінь	Перший (бакалаврський)
Обсяг дисципліни в кредитах ECTS	6 кредитів
Статус дисципліни	Вибіркова дисципліна фахової підготовки
Мета вивчення дисципліни	Підготувати фахівців, що володіють фундаментальними теоретичними знаннями та здатні вирішувати практичні завдання в області основних методів і розуміння природи прийняття рішень як складової частини управлінської функції, використовують методи експертного оцінювання, призначених для роботи як з кількісною, так і з якісною інформацією, підвищення професіоналізму й ефективності прийнятих рішень у теоретичних і практичних економічних проблемах управління організаційними системами.
Очікувані результати навчання	<p>РНД 1 Студент демонструє знання про основні поняття й категорії прийняття рішень; сучасні моделі розробки та прийняття рішень</p> <p>РНД 2 Студент здійснює аналіз вимог, що до основних принципів й підходів до прийняття рішень в умовах невизначеності</p> <p>РНД 3 Студент володіє основами знань для визначення оптимальної форми подання та реалізації рішень</p> <p>РНД 4 Студент здійснює формалізування практичних задач відповідно до методів теорії прийняття рішень</p> <p>РНД 5 Студент проявляє здатність використовувати розробляти й обґрунтовувати рішення на основі комплексу статистичних методів і моделей, системи показників економічного обґрунтування рішень</p> <p>РНД 6 Студент використовує професійно профільовані знання й уміння в галузі здійснювання ідентифікацій, аналізу та оцінювання невизначеності, використовуючи сучасні економіко-математичні моделі</p> <p>РНД 7 Здобувач застосовує результати аналізу та контролю для прийняття управлінських рішень та вирішення конкретних практичних ситуацій</p> <p>РНД 8 Студент застосовує сучасні методи з формулювання варіантів вибору (альтернатив) для забезпечення прийняття ефективного та адекватного рішення</p>
Зміст навчальної дисципліни за темами	<p>Тема 1. Загальні аспекти прийняття рішень</p> <p>Тема 2. Бінарні відношення та механізми прийняття рішень</p> <p>Тема 3. Метризовані відношення й експертні оцінювання</p> <p>Тема 4. Моделі та методи прийняття рішень за умов багатокритерійності</p> <p>Тема 5. Прийняття рішень методом аналітичної ієрархії</p> <p>Тема 6. Концепція корисності та раціональний вибір</p>

	Тема 7. Моделі та методи прийняття рішень в умовах нечіткої інформації, невизначеності та ризику Тема 8. Моделі та методи багатоособового прийняття рішень Тема 9. Теорія ігор, стратегічні та статистичні ігри Тема 10. Психолінгвістичні аспекти прийняття рішень	
Форми поточного та підсумкового контролю	Поточний контроль – 100 балів. Підсумковий контроль – залік	
Мова навчання	українська	
Критерії оцінювання результатів навчання	Форми контролю	Максимальна кількість балів
		Денна форма навчання
	Поточний контроль:	
	Практичні завдання	6 x 10 балів = 60 балів
	Презентація та захист індивідуальної (дослідницько-аналітичної) роботи	до 10 балів
	Письмові тестові роботи	2 x 15 балів = 30 балів
	Всього за результатами поточного контролю:	100
	Підсумковий контроль: залік	
Всього	100	
Викладач/ викладачі	Чеканова Н.М., к.ф.-м.н., доцент	
Забезпечення	1.Мультимедійний проектор, ноутбук; 2.Інтерактивна дошка; 3.Комп'ютери.	





**ДВНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**  
**ХАРКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**  
**ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ФІНАНСОВИХ ТЕХНОЛОГІЙ**  
**Кафедра ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

<i>Навчальна дисципліна</i>	<b>ФВД7 Програмування (Рівень D - Високорівневе програмування (веб - програмування))</b>
Офіційна назва освітньої програми	«Кібербезпека у фінансових технологіях»
Спеціальність	125 Кібербезпека
Освітній ступінь	Перший (бакалаврський)
Обсяг дисципліни в кредитах ECTS	6 кредитів
Статус дисципліни	Вибіркова дисципліна фахової підготовки
Мета вивчення дисципліни	Підготувати фахівців, що володіють фундаментальними теоретичними знаннями та здатні вирішувати практичні завдання розробки програмного забезпечення мовою Java, ознайомлені з можливостями мови програмування для створення спеціалізованого програмного забезпечення
Очікувані результати навчання	РНД1 демонструє загальні знання в частині проектування структур даних та формування вимог до програмних додатків РНД2 демонструє вміння в частині складання алгоритмів РНД3 демонструє знання та вміння в частині створення програмних функцій та керування пам'яттю РНД4 демонструє навички роботи зі строками та рядками при розробці програмних додатків РНД5 демонструє практичні навички розробки комп'ютерних програм РНД6 демонструє практичні навички при тестуванні та валідації комп'ютерних програм РНД7 демонструє теоретичні знання та практичні навички при аналізі виявлених дефектів та їх виправлення
Зміст навчальної дисципліни за темами	Тема 1. Сучасні технології Web -програмування Тема 2. Введення в XML. Структура XML документа. DOM XML. Створення динамічних Web-сторінок на стороні клієнта. Тема 3. AJAX. Забезпечення безпеки Web -додатків Тема 4. Концепція HTML. Тема 5. Засоби форматування. Тема 6. Списки і таблиці. Графіка та мультимедійна інформація Тема 7. Каскадні таблиці стилів (CSS) Тема 8. Форми Тема 9. Особливості мови PHP. Синтаксичні конструкції та оператори PHP Тема 10 Основи роботи з СУБД MySQL. Обробка запитів засобами PHP Тема 11. Огляд мови JavaScript. Мова ядра JavaScript. Стандартні об'єкти і функції ядра JavaScript Тема 12. Об'єкти клієнта. Обробники подій Тема 13. Динамічний HTML (DHTML)
Форми поточного та підсумкового	Поточний контроль – 50 балів. Підсумковий контроль – екзамен – 50 балів

контролю		
Мова навчання	українська	
Критерії оцінювання результатів навчання	Форми контролю	Максимальна кількість балів
		Денна форма навчання
	Поточний контроль:	
	Практичні завдання	4 x 5 балів = 20 балів
	Презентація та захист індивідуальної (дослідницько-аналітичної) роботи	до 10 балів
	Письмові тестові роботи	2 x 10 балів = 20 балів
	Всього за результатами поточного контролю:	50
	Підсумковий контроль: екзамен	50
	Всього	100
Викладач/ викладачі	Стяглик Н.І., к.п.н.	
Забезпечення	1.Мультимедійний проектор, ноутбук; 2.Інтерактивна дошка; 3.Комп'ютери.	



**ДВНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**  
**ХАРКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**  
**ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ФІНАНСОВИХ ТЕХНОЛОГІЙ**  
**Кафедра ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Навчальна дисципліна	<b>ФВД7 Фінансові технології (Рівень С - Безпека фінансових ринків)</b>
Офіційна назва освітньої програми	«Кібербезпека у фінансових технологіях»
Спеціальність	125 Кібербезпека
Освітній ступінь	Перший (бакалаврський)
Обсяг дисципліни в кредитах ECTS	6 кредитів
Статус дисципліни	Вибіркова дисципліна фахової підготовки
Мета вивчення дисципліни	формування комплексу теоретичних і практичних знань з основних принципів, методів і технологій сучасного математичного моделювання, розвинення навичок практичного застосування перспективних математичних методів та моделей для аналізу безпеки фінансових ринків.
Очікувані результати навчання	<p>РНД 1. Студент демонструє знання сучасних технологій математичного моделювання безпеки фінансових ринків, розуміє перспективи застосування математичних методів та моделей в дослідженні об'єктів, процесів і явищ на фінансових ринках.</p> <p>РНД 2. Студент показує вміння розробки та побудови математичних моделей для дослідження безпеки фінансових ринків згідно із загальною логікою математичного моделювання.</p> <p>РНД 3. Студент демонструє знання та навички застосування математичних методів та моделей в процесі прогнозування та прийняття управлінських рішень при дослідженні фінансових ринків.</p> <p>РНД 4. Студент показує вміння оцінювати та аналізувати можливості й обмеженість застосування сучасних математичних методів та моделей при вивченні фінансових ринків.</p> <p>РНД 5. Студент демонструє навички здійснювати презентацію результатів дослідження, вести дискусію з прикладних питань математичного моделювання безпеки фінансових ринків на різних наукових рівнях, порівнювати власні наукові результати з актуальними світовими досягненнями.</p> <p>РНД 6. Студент показує вміння застосовувати комп'ютерну техніку, спеціалізоване програмне забезпечення для побудови та аналізу математичних моделей безпеки фінансових ринків..</p>
Зміст навчальної дисципліни за темами	<p>Тема 1. Сучасний стан проблеми</p> <p>Тема 2. Регресійна модель в дослідженні фінансових ринків</p> <p>Тема 2. Моделі з фіктивними змінними</p> <p>Тема 3. Моделі з лаговими змінними</p> <p>Тема 4. Моделі з дискретними залежними змінними</p> <p>Тема 5. Методи кластерного аналізу.</p> <p>Тема 6. Методи дискримінантного аналізу.</p>

	Тема 7. Моделі панельних даних Тема 8. Векторні авторегресійні технології Тема 9. Методи експертних оцінок Тема 10. Методи оцінки ризику Тема 11. Теоретико-ігрові моделі Тема 12. Імітаційне моделювання	
Форми поточного та підсумкового контролю	Поточний контроль – 50 балів. Підсумковий контроль – екзамен – 50 балів	
Мова навчання	українська	
Критерії оцінювання результатів навчання	Форми контролю	Максимальна кількість балів
		Денна форма навчання
	Поточний контроль:	
	Практичні завдання	4 x 5 балів = 20 балів
	Презентація та захист індивідуальної (дослідницько-аналітичної) роботи	20 балів
	Письмові тестові роботи	1 x 10 балів = 40 балів
	Всього за результатами поточного контролю:	50
	Підсумковий контроль: екзамен	50
Всього	100	
Викладач/ викладачі	Філатова Л.Д., к.ф.-м.н., доцент	
Забезпечення	1.Мультимедійний проектор, ноутбук; 2.Інтерактивна дошка; 3.Комп'ютери.	



**ДВНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**  
**ХАРКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**  
**ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ФІНАНСОВИХ ТЕХНОЛОГІЙ**  
**Кафедра ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Навчальна дисципліна	<b>ФВД8 Інформаційні технології (Рівень С - Організація баз даних та знань)</b>
Офіційна назва освітньої програми	«Кібербезпека у фінансових технологіях»
Спеціальність	125 Кібербезпека
Освітній ступінь	Перший (бакалаврський)
Обсяг дисципліни в кредитах ECTS	6 кредитів
Статус дисципліни	Вибіркова дисципліна фахової підготовки
Мета вивчення дисципліни	забезпечення здобувачів вищої освіти знаннями з основ теорії побудови та функціонування баз даних та знань реляційного типу, а також вміннями їх проектування на основі вивчення предметної області та керування ними за допомогою систем керування базами даних та знань при створенні та експлуатації інформаційних систем
Очікувані результати навчання	<p>РНД1. Студент демонструє знання про моделі подання даних та знань для відображення у комп'ютерних системах та мережах предметних областей, що є об'єктами професійної діяльності</p> <p>РНД2. Студент демонструє знання теорій побудови та оптимізації реляційних баз даних.</p> <p>РНД3. Студент демонструє знання про функції, склад та інформаційні процеси систем керування реляційними базами даних</p> <p>РНД4. Студент демонструє знання про сучасні архітектури систем баз даних та знань і вміння їх ідентифікації та аналізу за даними технічної документації</p> <p>РНД5. Студент володіє знаннями та вміннями аналізувати та складати мовою структурованих запитів інструкції системі керування базами даних для створення, корегування та використання баз даних та знань</p> <p>РНД6. Студент вміє будувати та досліджувати бази даних та знань засобами систем керування базами даних та знань</p> <p>РНД7. Студент застосовує сучасні програмні засоби для розробки та використання баз даних та знань</p>
Зміст навчальної дисципліни за темами	<p>Тема 1. Вступ до дисципліни.</p> <p>Тема 2. Архітектура реляційних баз даних.</p> <p>Тема 3. Таблиці.</p> <p>Тема 4. Запити.</p> <p>Тема 5. Форми.</p> <p>Тема 6. Звіти.</p> <p>Тема 7. Створення баз даних.</p> <p>Тема 8. Дatalogічне проектування баз даних.</p> <p>Тема 9. Реляційна алгебра.</p> <p>Тема 10. Системи баз даних.</p> <p>Тема 11. Мова структурованих запитів SQL.</p>

	Тема 12. Бази знань.	
Форми поточного та підсумкового контролю	Поточний контроль – 100 балів. Підсумковий контроль – залік	
Мова навчання	українська	
Критерії оцінювання результатів навчання	Форми контролю	Максимальна кількість балів
		Денна форма навчання
	<i>Поточний контроль:</i>	
	Практичні завдання	8 x 10 балів = 80 балів
	Письмові контрольні роботи	2 x 10 балів = 20 балів
	<i>Всього за результатами поточного контролю:</i>	
	<i>Підсумковий контроль: екзамен</i>	
	<i>Всього</i>	100 балів
Викладач/ викладачі	Шаповал С. О., к.т.н., доцент	
Забезпечення	1.Мультимедійний проектор, ноутбук; 2.Інтерактивна дошка; 3.Комп'ютери.	



**ДВНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**  
**ХАРКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**  
**ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ФІНАНСОВИХ ТЕХНОЛОГІЙ**  
**Кафедра ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Навчальна дисципліна	<b>ФВД8 Програмування (Рівень С – Кросплатформне програмування)</b>
Офіційна назва освітньої програми	«Кібербезпека у фінансових технологіях»
Спеціальність	125 Кібербезпека
Освітній ступінь	Перший (бакалаврський)
Обсяг дисципліни в кредитах ECTS	6 кредитів
Статус дисципліни	Вибіркова дисципліна фахової підготовки
Мета вивчення дисципліни	формування системи теоретичних і практичних знань з основ створення крос-платформного програмування, опанування студентами фундаментальних теоретичних знань і практичних навичок компонентного програмування, опанування навиками створення крос-платформних додатків на мові програмування JAVA, та розробка крос-платформних інтерфейсів
Очікувані результати навчання	РНД1 студент має знати архітектуру та стандарти компонентних моделей, комунікаційних засобів і розподілених обчислень. РНД2 студент має знати стратегії інтеграції програмних компонентів; основні платформи проміжного рівня та компонентні моделі. РНД3 студент має знати формальні та візуальні методи конструювання компонентів; РНД4 студент має вміти розробляти вимоги та специфікації компонентів інформаційних систем і об'єктів професійної діяльності. РНД5 студент має вміти проектувати компоненти крос-платформного програмного забезпечення; проектувати людино-машинний інтерфейс інформаційних систем. РНД6 студент має вміти реалізовувати прототипи архітектури програмного забезпечення; РНД7 студент має вміти інтегрувати компоненти в систему; установлювати, налаштовувати та обслуговувати системне, інструментальне і прикладне програмне забезпечення та інформаційні системи
Зміст навчальної дисципліни за темами	Тема 1. Графічні засоби. Технологія GDI+ Тема 2. Розробка крос-платформних програм. Тема 3. Компонентні технології. Тема 4. Методи створення компонентів Тема 5. Архітектура та проектування компонентних систем Тема 6. Проміжне програмне забезпечення Тема 7. Особливості компонентних технологій
Форми поточного та підсумкового контролю	Поточний контроль – 100 балів. Підсумковий контроль – залік
Мова навчання	українська

Критерії оцінювання результатів навчання	Форми контролю	Максимальна кількість балів
		Денна форма навчання
	Поточний контроль:	
	Практичні завдання	8 x 10 балів = 80 балів
	Письмові контрольні роботи	2 x 10 балів = 20 балів
	Всього за результатами поточного контролю:	
	Підсумковий контроль: екзамен	
	Всього	100 балів
Викладач/ викладачі	Тарасенко О.П., к.т.н., доцент	
Забезпечення	1.Мультимедійний проектор, ноутбук; 2.Інтерактивна дошка; 3.Комп'ютери.	