

**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА**

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра інформаційних систем та технологій

«ЗАТВЕРДЖУЮ»
Заступник декана з навчально-виховної роботи
Наталія ТМЄНОВА
_____ 2025 року



РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Системи банкової безпеки»

для студентів

галузь знань	12 «Інформаційні технології»
спеціальність	126 «Інформаційні системи та технології»
освітній рівень	бакалавр
освітня програма	« Програмні технології інтернет речей»
вид дисципліни	вибіркова
Форма навчання	денна

Навчальний рік	2025/2026
Семестр	5
Кількість кредитів ECTS	4
Мова викладання, навчання та оцінювання	українська
Форма заключного контролю	залік

Викладачі: професор кафедри, д.т.н. Трембовецький М.П.

Пролонговано: на 20__/20__ н.р. _____ (_____) «__» ____ 20__ р.
(підпис, ПШБ, дата)

на 20__/20__ н.р. _____ (_____) «__» ____ 20__ р.
(підпис, ПШБ, дата)

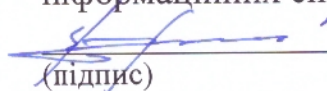
КИЇВ – 2025

Розробник: Трембовецький Максим Петрович д.т.н., професор кафедри інформаційних систем та технологій

ЗАТВЕРДЖЕНО

Зав. кафедри

інформаційних систем та технологій

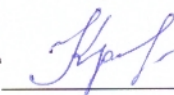

(підпис)

Володимир ДРУЖИНІН
(прізвище та ініціали)

Протокол № 17_24/25 від 25 червня 2025 р

Схвалено науково - методичною комісією факультету інформаційних технологій
Протокол № 10 від 27 червня 2025 року

Голова науково-методичної комісії ФІТ



Ганна КРАСОВСЬКА

Програму перевірено


« _____ » _____ 2025 року

ВСТУП

1. Мета дисципліни - надати студентам знання про методи та засоби захисту інформації у банківських системах, джерела і канали поширення інформації, що становить банківську таємницю для їх практичного застосування та втілення у процесі фахової діяльності майбутнього спеціаліста з інформаційної безпеки. Ознайомлення зі станом та тенденціями забезпечення безпеки інформації у сучасних банківських системах, оволодіння організаційно-правовими та економічними основами захисту банківської таємниці; засвоєння сутності банківських операцій.

2. Попередні вимоги до опанування або вибору навчальної дисципліни: успішне опанування базових положень у галузі банківської справи, відповідними методами, інструментарієм для обґрунтування рішень щодо функціонування банківської системи та окремих банківських установ, теорією та методами організації і функціонування фінансово-кредитних установ. *Вміти* застосовувати отримані знання в практичних ситуаціях, виявляти, ставити та вирішувати завдання у сфері банкової професійної діяльності, та виконувати фінансово-економічні розрахунки, які пов'язані з аналізом та обґрунтуванням раціональних та ефективних рішень. *Володіти* навичками ідентифікації та аналізу загроз, застосування сучасних методів захисту, управління ризиками й розробки комплексних заходів забезпечення інформаційної та фінансової безпеки банківських установ..

3. Анотація навчальної дисципліни:

Дисципліна спрямована на формування у студентів цілісного уявлення про сучасні підходи, методи та інструменти забезпечення безпеки банківської діяльності. У курсі розглядаються теоретичні основи банківської безпеки, нормативно-правова база та міжнародні стандарти у сфері захисту фінансової та інформаційної інфраструктури. Особлива увага приділяється аналізу ризиків, методам протидії шахрайству, організації системи внутрішнього контролю та фінансового моніторингу, а також управлінню інформаційною безпекою та кіберзахистом банківських установ.

Практична частина курсу зосереджена на застосуванні сучасних технологій і програмних засобів для запобігання інцидентам безпеки та реагування на них, впровадженні багаторівневих систем захисту, управлінні ризиками та створенні політики безпеки банку. Вивчення дисципліни дозволяє студентам оволодіти навичками розробки та реалізації комплексних заходів із забезпечення стабільності банківських операцій, підвищення довіри клієнтів і дотримання вимог регуляторів, що є критично важливим для ефективного функціонування фінансової системи в умовах зростання кіберзагроз.

4. Завдання (навчальні цілі): завданням дисципліни «Системи банківської безпеки» є формування у студентів теоретичних знань та практичних навичок з ідентифікації й оцінювання ризиків у банківській сфері, засвоєння методів захисту інформаційних і фінансових ресурсів, опанування принципів побудови комплексної системи безпеки банку, здатності застосовувати сучасні технології кіберзахисту, протидії шахрайству та фінансовим злочинам, а також вироблення умінь приймати обґрунтовані управлінські рішення для забезпечення стійкості та надійності банківської діяльності..

5. Результати навчання за дисципліною:

Результат навчання (1. знати; 2. Вміти; 3. Комунікація; 4. Автономність та відповідальність)		Методи викладання і навчання	Методи оцінювання	Відсоток у підсумковій оцінці з дисципліни
Код	Результат навчання			
1.1	Знати основні положення безпеки банків, та безпеку автоматизованих систем обробки інформації банку.	Лекції курсу	Питання на тестування для МКР, усне опитування, дискусія	10%
1.2	Знати та застосовувати криптографічні та програмні засоби захисту інформації.			10%
1.3	Знати блокчейн технології у банківській сфері.			10%
1.4	Знати і застосовувати методи оцінки фінансово-економічної безпеки банку.			10%
2.1	Вміти використовувати програми протидії комп'ютерних злочинів. Вміти формулювати стратегічні завдання управління безпекою банківських установ.	Лабораторні роботи та практичні роботи з курсу	Звіт з лабораторних робіт, презентація за практичним завданням	15%
2.2	Вміти використовувати результати моніторингу загроз в управлінні безпекою банківських установ.			15%
2.3	Вміти формувати структуру інформаційно-аналітичного забезпечення діяльності банківських установ			20%
3.1	Здатність працювати в команді, вироблення у студентів практичних навиків групової роботи з застосуванням відповідних методів і прийомів отримання, зберігання й обробки даних та їх представлення сучасними технічними можливостями.	Практичні заняття, групова доповідь та реферативні сповіщення	Виконання групових досліджень за додатковою тематикою курсу	10%

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання (необов'язково для вибірових дисциплін)

Результати навчання дисципліни (код)	1.1	1.2	1.3	1.4	2.1	2.2	2.3	3.1
Програмні результати навчання (назва)								
ПР 2. Застосовувати знання фундаментальних і природничих наук, системного аналізу та технологій моделювання, стандартних алгоритмів при розв'язанні задач і у сфері фінансів, та банківської безпеки.	+	+		+			+	
ПР 3. Використовувати базові знання інформатики і сучасних інформаційних систем та технологій для розв'язання задач зовнішніх та внутрішніх загроз та ризиків у сфері банкової безпеки.		+			+	+	+	+

ПР 10. Розуміти і враховувати соціальні, економічні аспекти для прийняття управлінських рішень щодо доцільності діяльності банківських установ з урахуванням виявлених загроз і небезпек, захисту отриманої інформації.			+	+			+	+
---	--	--	---	---	--	--	---	---

7. Схема формування оцінки.

7.1. Форми оцінювання: рівень досягнення всіх результатів навчання визначається за результатами написання модульної контрольної роботи у тестовій формі за допомогою системи Microsoft Teams та Moodle, опитуванні під час лекційних занять або доповненні при обговоренні проблемного питання та під час виконання лабораторних робіт та практичних робіт.

Питома вага результатів навчання у підсумковій оцінці за умови її опанування на належному рівні наступні:

- результати навчання – 1 (знання) РН 1.1- РН 1.8. - до 40%;
- результати навчання – 2 (вміння) – РН 2.1- РН 2.9. - до 50%;
- результати навчання – 3 (комунікація) – РН 3 - до 10%.

7.2 Організація оцінювання.

Розрахунок балів ведеться з загальної суми 100 балів за семестр. Окрема залікова робота не передбачається. Студенти набирають бали протягом семестру за різні види робіт.

Упродовж семестру на лекціях здобувачі освіти приймають участь у дискусіях та усних опитуваннях за результатами тем лекцій та питань, що виносилися на самостійну підготовку. Кількість виступів обмежена до 3. Одна доповідь оцінюється до 2 балів, а доповнення 0.5-1 бал. Загальна кількість балів, що здобувач може обрати на лекціях 5 балів. За результатами набутих знань проводиться одна МКР у формі тестування та оцінюється до 25 балів. Також, передбачено виконання 6 практичних робіт, що оцінюються від 2 до 5 балів за роботу (всього від 12 до 30 балів). За планом здобувачі освіти виконують 10 лабораторних робіт, що оцінюються від 2 до 4 балів за роботу (всього від 20 до 40 балів).

Предмет закінчується **заліком**.

На заліку обраховується сума набрана студентом за виконані завдання протягом семестру та виставляється як підсумкове оцінювання. При отриманні студентом мінімальних 60 балів у підсумку виконання запланованих робіт, ставиться оцінка **зараховано**.

Якщо студент не набрав необхідних мінімальних балів, то йому надається можливість отримати додаткові бали у формі виконання індивідуального практичного завдання за тематикою практичних або лабораторних робіт.

Шкала відповідності

Зараховано/Passed	60-100
Не зараховано / Fail	0-59

8 8. Структура навчальної дисципліни. Тематичний план занять.

№ п/п	Назва теми	Кількість годин			
		лекції	ПЗ	ЛЗ	С/Р
1	Тема 1. Вступ до банківської безпеки (поняття безпеки та її місце в банківській діяльності; банківська безпека як складова національної та економічної безпеки держави; історичні приклади: банківські кризи XX–XXI ст.; еволюція загроз: від фізичних пограбувань до кібератак; суб'єкти та об'єкти банківської безпеки; актуальні виклики сучасної фінансової системи)	2		2	7
2	Тема 2. Правові основи банківської безпеки (законодавча база України у сфері банківської діяльності; норми міжнародного права (Базельські угоди, FATF, ISO 27001); роль НБУ та інших регуляторів у забезпеченні безпеки; судова практика банківських злочинів (українські та світові приклади); вимоги до комплаєнс-контролю та внутрішнього аудиту; проблеми гармонізації національного та міжнародного права).	2	2	2	7
3	Тема 3. Загрози банківській діяльності (класифікація загроз: внутрішні, зовнішні, комбіновані; банківське шахрайство: класичні та сучасні схеми; рейдерство та корпоративні конфлікти; терористичні загрози та фінансування тероризму; кіберзагрози: фішинг, DDoS, атаки на платіжні системи; реальні кейси з української та світової практики).	2		2	7
4	Тема 4. Фінансова та економічна безпека банку (основи фінансової стійкості банку: ліквідність і капіталізація; кредитні та процентні ризики; базельські угоди II–III: сутність та значення; фінансові кризи XX–XXI ст. та їх вплив на банки; валютні ризики та проблеми глобалізації фінансових ринків; інструменти моніторингу економічної безпеки банку).	2	2	2	7
5	Тема 5. Інформаційна безпека банків (поняття банківської інформації та принципи її захисту; технічні канали витоку інформації; соціальна інженерія як фактор ризику; кібератаки на банківські IT-системи: історичні приклади (Stuxnet, SWIFT); сучасні методи автентифікації та криптографічного захисту; перспективи застосування штучного інтелекту в кіберзахисті).	2		4	14
6	Тема 6. Організаційна та кадрова безпека банку (людський фактор у банківській безпеці; служба безпеки банку: структура, функції, компетенції; персонал як об'єкт і суб'єкт ризику; внутрішні шахрайства: кейси та профілактика; психологічні аспекти кадрових ризиків; культура безпеки в банківських установах).	2	2	2	7
7	Тема 7. Фізична безпека банків (принципи організації фізичної безпеки банків; технічні засоби охорони: сейфи, системи доступу, сигналізації; відеоспостереження та сучасні біометричні системи; організація охорони банківських відділень і інкасації; пограбування банків у XX–XXI ст.: аналіз резонансних випадків; інноваційні рішення у сфері фізичної безпеки).	2	2	2	7
8	Тема 8. Системи управління ризиками в банку (основи ризик-менеджменту в банківській діяльності; ідентифікація та оцінка банківських ризиків; моделі ризик-менеджменту та міжнародний досвід; аналітичні інструменти: VaR, стрес-тести, сценарний аналіз; вплив макроекономічних факторів на ризики банків; використання цифрових технологій у ризик-менеджменті).	2	2	2	7
9	Тема 9. Антикризове управління та дії банків в екстремальних умовах (принципи антикризового управління; кіберзагрози та протидія кібератакам; дії банку під час фінансової кризи;	2	2	2	7

	планування безперервності бізнесу (ВСП); український досвід функціонування банків під час воєнного стану; майбутні виклики та сценарії розвитку банківської безпеки).				
	Модульна контрольна робота			2	
	Всього за семестр	18	12	20	70

Загальний обсяг – 120 год., в тому числі:

Лекцій – **18 год.**

Практичні заняття - **12 год.**

Лабораторні заняття - **20 год.**

Самостійна робота – **70 год.**

9. Рекомендовані джерела:

Основна: (Базова)

1. Закон України «Про основні засади забезпечення кібербезпеки України», 2017 р.
2. Карась П.М. Банківська система: навчальний посібник . Херсон: ОЛДПЛЮС, 2015. 292 с.
3. Л. О. Примостка, М. І. Діба, І. В. Краснова Банківська система України : інституційні зміни та інновації : монографія/ за заг. ред. О. Примостки. К. : КНЕУ, 2015.434 с.
4. Зубок М. І. Забезпечення економічної безпеки банків : навч. посіб. / М. І. Зубок; Ун-т "КРОК". – Київ : Ун-т "КРОК", 2018. – 257 с.
5. Отенко І. П. Організація та управління фінансово-економічною безпекою банківських установ : навч. посіб. / І. П. Отенко, О. Ю. Мішин, С. В. Мішина. – Харків : ХНЕУ ім. С. Кузнеця, 2015. – 240 с.

Додаткова:

15. Настанови з кібербезпеки від експертів [Електронний ресурс]. – Режим доступу: <http://www.isaca.org.ua/index.php/press-center/news/191-translation-of-guidelines-on-cybersecurity> .
16. Основні функції структурних підрозділів центрального апарату НБУ [Електронний ресурс]. – Режим доступу : <https://bank.gov.ua/doccatalog/document?id=24604231>.
17. Концепція ISO/IEC 27001. "Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью.
18. ISO/IEC 27002. «Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью.»
19. ISO/IEC 27005. «Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности»
<https://exebit.files.wordpress.com/2013/11/iso-27005-2011-ru-v1.pdf>
20. Аналітичний огляд банківської системи України за 9 місяців 2019 рік.К.: Національне рейтингове агентство «Рюрік», 2019.URL: <http://rurik.com.ua/ourresearch/branch-reviews/1187/>
21. Урядовий портал.URL: <http://www.kmu.gov.ua>
22. Офіційний сайт Національного банку України.URL: <http://www.bank.gov.ua/>
23. Офіційний портал Верховної Ради України. URL: <http://portal.rada.gov.ua>
24. Офіційний сайт Державного комітету статистики України: <http://www.ukrstat.gov.ua>
25. Гладка М.В., Лісневський Р.В., Костіков М. П. USING THE INTERNET OF THINGS WHEN INTRODUCING CRM SYSTEMS IN THE BANKING SECTOR. “Information Technology and Interactions” (IT&I-2020).December 02-04, 2020 Taras Shevchenko National University of Kyiv.