Робоча програма дисципліни «Безпека банківської діяльності з використанням управлінських інформаційних систем і технологій»

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

БАКАЛАВР

90

Годин

Загальний обсяг дисципліни

3

Кредити ЄКТС

Відповідно до стандарту

3

Модулі

Змістовних блоки курсу

Загальна інформація про дисципліну

Ідентифікація

Назва: Безпека банківської діяльності

Спеціальність: 123 Комп'ютерна інженерія

ОП: Фінанси, банківська справа та страхування в управлінських інформаційних системах і технологіях

Ступінь: Бакалавр

Обсяг: 90 годин / 3 кредити ЄКТС

Модулів: 3 змістовних блоки

Підсумковий контроль: Іспит

Призначення дисципліни

Дисципліна «Безпека банківської діяльності з використанням управлінських інформаційних систем і технологій» формує у студентів системне розуміння теоретичних і практичних засад забезпечення безпеки банківських установ в умовах цифровізації та інформаційних загроз. Курс охоплює організаційно-правові основи банківської безпеки, методи захисту банківської інформації, протидію кіберзагрозам, фінансовий моніторинг та управління ризиками безпеки.

Дисципліна є профільною для підготовки бакалаврів зі спеціальності 123 «Комп'ютерна інженерія» в межах освітньої програми «Фінанси, банківська справа та страхування в управлінських інформаційних системах і технологіях» та забезпечує формування необхідних загальних і фахових компетентностей у сфері IT-безпеки фінансового сектору.

Загальні компетентності

Аналітичне мислення

Здатність до аналізу, синтезу та критичного оцінювання інформації в контексті безпеки банківських інформаційних систем: виявлення суттєвих загроз, порівняння методів захисту, формування обґрунтованих висновків і висловлення власної позиції.

Самоорганізація

Уміння самостійно навчатися, планувати роботу та організовувати виконання завдань у визначені строки, зокрема під час підготовки аналітичних звітів, практичних кейсів та презентацій у сфері банківської безпеки.

Комунікація

Здатність до усної та письмової професійної комунікації: чітко пояснювати поняття інформаційної та фінансової безпеки, аргументовано відповідати на запитання, оформлювати технічні звіти, аналітичні записки та висновки аудиту безпеки.

Командна робота

Відповідальність, ініціативність, дисциплінованість та готовність працювати в команді під час групового аналізу інцидентів інформаційної безпеки, моделювання кіберзагроз та спільного розроблення заходів захисту банківських систем.

Студент повинен вміти: аналізувати навчальну, нормативну та технічну інформацію у сфері банківської безпеки; виділяти головне та узагальнювати результати оцінки загроз; планувати власну діяльність і дотримуватися дедлайнів; коректно спілкуватися з викладачами та одногрупниками; брати участь у командній роботі при моделюванні загроз та розробленні політик безпеки.

Фахові компетентності

Розуміння банківської безпеки

Розуміння сутності безпеки банківської діяльності, її складових та ролі в захисті фінансово-інформаційного простору. Знання принципів функціонування систем безпеки банків, організаційно-правових засад їх забезпечення, видів загроз та механізмів прийняття рішень у сфері захисту.

Аналіз загроз і ризиків

Здатність аналізувати загрози та ризики безпеки банківських установ: кіберзагрози, шахрайство, витоки даних, несанкціонований доступ, операційні та фінансові ризики, загрози банківській таємниці та персональним даним клієнтів.

Захист та моніторинг

Знання основ кібербезпеки банків, фінансового моніторингу, протидії легалізації доходів (AML/KYC), використання інформаційних технологій у системах безпеки та стандартів захисту банківської інформації (ISO 27001, PCI DSS, SWIFT).

Студент повинен вміти: оцінювати стан безпеки банківської установи за ключовими індикаторами; ідентифікувати та класифікувати загрози банківській діяльності; характеризувати правове регулювання банківської безпеки в Україні та ЄС; орієнтуватися в основах фінансового моніторингу та AML-процедур; застосовувати технічні засоби захисту банківських інформаційних систем.

Результати навчання

Пояснення категорій банківської безпеки

Пояснювати сутність категорій та явищ у сфері банківської безпеки: загроза, ризик, вразливість, банківська таємниця, фінансовий моніторинг, кіберінцидент, AML/KYC, шахрайство та інсайдерська загроза.

Аналіз загроз та інцидентів безпеки

Аналізувати основні загрози та інциденти безпеки банківських установ для виявлення слабких місць системи захисту та розроблення рекомендацій щодо її вдосконалення.

Організаційно-технічні засоби захисту

Характеризувати організаційні та технічні засоби захисту банківських систем; застосовувати методи оцінки ефективності заходів безпеки; визначати відповідність систем захисту стандартам ISO 27001, PCI DSS та вимогам НБУ.

Нормативно-правова база

Орієнтуватися в нормативно-правовій базі у сфері банківської та інформаційної безпеки; використовувати нормативні документи НБУ, законодавство України та міжнародні стандарти для прийняття обґрунтованих рішень у сфері захисту.

МОДУЛЬ 1

Організаційно-правові засади безпеки банківської діяльності

Тема 1.1

Сутність та складові безпеки банківської діяльності. Концепція безпеки комерційного банку, її цілі, функції та місце в системі банківського менеджменту.

Тема 1.2

Нормативно-правове регулювання банківської безпеки в Україні та ЄС. Роль НБУ, ДССЗЗІ та інших регуляторів у забезпеченні безпеки банківського сектору.

Тема 1.3

Загрози та ризики банківської діяльності. Класифікація загроз, методи їх ідентифікації та оцінки. Система управління ризиками безпеки банку.

Тема 1.1 — Лекційний матеріал

Сутність та складові безпеки банківської діяльності

Лекція 1 (2 год.): Поняття безпеки банківської діяльності як комплексної системи захисту інтересів власників, клієнтів, персоналу та держави. Складові безпеки банку: фінансова безпека, інформаційна безпека, кадрова безпека, фізична безпека, правова безпека. Місце служби безпеки у структурі банку.

Концепція безпеки комерційного банку: принципи побудови (комплексність, превентивність, законність, економічна доцільність), суб'єкти та об'єкти захисту, внутрішні та зовнішні загрози. Взаємозв'язок безпеки банку з національною фінансовою безпекою держави.

Ключові питання лекції

- Поняття та складові системи безпеки банку
- Класифікація загроз банківській діяльності (внутрішні та зовнішні)
- Принципи побудови системи безпеки банківської установи
- Суб'єкти та об'єкти захисту у банківській сфері
- Роль та функції служби безпеки банку
- Зв'язок банківської безпеки з економічною безпекою держави

Нормативна база: Закон України «Про банки і банківську діяльність», Закон «Про Національний банк України», Положення НБУ про організацію систем управління ризиками.

Тема 1.1 — Практичне заняття та СРС

Практичне заняття (1 год.)

Завдання 1. Порівняльний аналіз складових безпеки банківської установи: заповнення порівняльної таблиці за критеріями (об'єкт захисту, основні загрози, методи забезпечення, відповідальні підрозділи).

Завдання 2. Кейс: визначення слабких місць у системі безпеки умовного банку на основі опису його організаційної структури та виявлених інцидентів. Обґрунтування пропозицій щодо вдосконалення.

Завдання 3. Тестування за ключовими термінами теми (10 питань).

Самостійна робота (4 год.)

- Опрацювання Закону України «Про банки і банківську діяльність» (розділи щодо банківської таємниці та безпеки) та конспектування ключових положень
- Підготовка порівняльної характеристики систем безпеки двох українських банків (за відкритими даними та річними звітами)
- Складання схеми «Складові системи безпеки банку» з прикладами загроз
- Опрацювання: Зубок М. І. «Безпека банківської діяльності» — розділ 1. Концепція безпеки комерційного банку

Очікуваний результат: студент вміє характеризувати складові системи безпеки банку, ідентифікувати загрози та обґрунтовувати організаційні заходи захисту.

Тема 1.2 — Лекційний матеріал

Нормативно-правове регулювання банківської безпеки

Лекція 2 (2 год.): Система правового регулювання банківської безпеки в Україні. Закон України «Про банки і банківську діяльність»: вимоги до організації управління ризиками, внутрішнього аудиту та банківської таємниці. Закон «Про захист персональних даних» у контексті банківської діяльності. Закон «Про основні засади забезпечення кібербезпеки України».

Роль НБУ в регулюванні безпеки: нормативні акти НБУ щодо управління операційними та кіберризиками (Постанова № 64, Постанова № 95). Вимоги до систем управління інформаційною безпекою банків. Банківський нагляд як інструмент забезпечення стабільності. Міжнародні стандарти: Базель III, DORA (ЄС), PCI DSS.

Ключові питання лекції

- Законодавча база безпеки банківської діяльності в Україні
- Повноваження НБУ у сфері банківського нагляду та безпеки
- Вимоги до систем управління ризиками банків за НБУ
- Захист банківської таємниці та персональних даних
- Міжнародні стандарти кібербезпеки у банківській сфері
- Регуляторна відповідальність за порушення вимог безпеки
- Регламент DORA (ЄС): вимоги до цифрової операційної стійкості

Тема 1.2 — Практичне заняття та СРС

Практичне заняття (1 год.)

Завдання 1. Аналіз нормативної бази: визначення вимог НБУ до систем управління інформаційною та кіберризиками (на основі Постанови НБУ № 64 від 2023 р.). Структурування ключових вимог у вигляді таблиці.

Завдання 2. Визначення застосовності міжнародних стандартів (ISO 27001, PCI DSS, DORA) до діяльності українських банків. Порівняння вимог стандартів за обраними критеріями.

Завдання 3. Міні-дискусія: «Чи є вимоги НБУ щодо кібербезпеки достатніми в умовах воєнного стану?» — аргументація позиції.

Самостійна робота (4 год.)

- Опрацювання Постанови НБУ № 64 «Про організацію управління операційним ризиком в банках України» та конспектування вимог до систем безпеки
- Підготовка аналітичної записки: «Порівняння вимог НБУ та стандарту ISO 27001 щодо управління інформаційною безпекою банків» (1–2 сторінки)
- Складання порівняльної таблиці: вимоги до безпеки банків в Україні vs. ЄС (DORA)
- Пошук актуальних даних на офіційному сайті НБУ (bank.gov.ua) щодо вимог до кібербезпеки банків

Очікуваний результат: студент вміє орієнтуватися в нормативно-правовій базі банківської безпеки, характеризувати вимоги регуляторів та порівнювати їх з міжнародними стандартами.

Тема 1.3 — Лекційний матеріал

Загрози та ризики банківської діяльності

Лекція 3 (2 год.): Поняття загрози, ризику та вразливості у банківській безпеці. Класифікація загроз: зовнішні (кібератаки, шахрайство, рейдерство, кризові явища) та внутрішні (інсайдерські загрози, помилки персоналу, корупція). Класифікація ризиків безпеки: операційний, кредитний, ринковий, репутаційний, правовий, кіберризик.

Система управління ризиками безпеки

1. Ідентифікація ризиків та загроз (реєстр ризиків)
2. Оцінка ймовірності та потенційного збитку (матриця ризиків)
3. Розроблення заходів реагування (уникнення, зниження, передача, прийняття)
4. Впровадження контрольних заходів (превентивні, детективні, коригувальні)
5. Моніторинг та перегляд системи управління ризиками
6. Звітування перед наглядовими органами та керівництвом
7. Безперервне вдосконалення системи захисту

Тема 1.3 — Практичне заняття та СРС

Практичне заняття (2 год.)

Завдання 1. Розробка спрощеного реєстру ризиків безпеки для умовного комерційного банку (за варіантами): ідентифікація загроз, їх класифікація, оцінка ймовірності та впливу.

Завдання 2. Побудова матриці ризиків безпеки («ймовірність × вплив») для обраного банку та визначення пріоритетних ризиків для управління.

Завдання 3. Презентація та захист реєстру ризиків (3–5 хвилин на групу). Взаємооцінювання за критеріями.

Самостійна робота (4 год.)

- Опрацювання матеріалів НБУ щодо управління операційними ризиками банків та конспектування вимог до реєстру ризиків
- Підготовка реферату: «Класифікація загроз безпеці банківської діяльності та методи їх мінімізації» (3–4 сторінки)
- Аналіз реального кейсу банківського кіберінциденту (за відкритими публікаціями): виявлення причин та наслідків
- Опрацювання: Попов О. Г. «Теоретичні основи забезпечення банківської безпеки держави». Економіка, управління та адміністрування. — 2023. — № 3(105)

Очікуваний результат: студент вміє ідентифікувати та класифікувати ризики безпеки банку, будувати матрицю ризиків та пропонувати заходи реагування.

МОДУЛЬ 2

Кібербезпека та захист інформації в банківській сфері

Тема 2.1

Інформаційна безпека банку: принципи, стандарти, засоби захисту банківських інформаційних систем та мереж.

Тема 2.2

Кіберзагрози у банківській сфері. Класифікація кібератак, методи їх виявлення та протидії. Захист платіжних систем та систем дистанційного банківського обслуговування.

Тема 2.3

Банківська таємниця та захист персональних даних. Правові засади, організаційні заходи, технічні засоби захисту конфіденційної інформації.

Тема 2.4

Фінансовий моніторинг та протидія легалізації доходів (AML/KYC). Процедури ідентифікації клієнтів, виявлення підозрілих операцій та звітування.

Тема 2.1 — Лекційний матеріал

Інформаційна безпека банку

Лекція 4–5 (4 год.): Поняття інформаційної безпеки банку та її складові. Тріада CIA (Confidentiality, Integrity, Availability) у банківському контексті. **Стандарти інформаційної безпеки:** ISO/IEC 27001 (СУІБ — система управління інформаційною безпекою), PCI DSS (стандарт безпеки платіжних карток), SWIFT Customer Security Programme (CSP). Сертифікація банків за міжнародними стандартами.

Засоби захисту банківських ІС: управління доступом (IAM, PAM), криптографічний захист (шифрування каналів, даних у спокої), міжмережеві екрани (NGFW), системи виявлення та запобігання вторгненням (IDS/IPS), SIEM-системи для моніторингу подій безпеки.

Захист банківської інфраструктури

Захист мережевої інфраструктури банку: сегментація мереж, DMZ, VPN для захищених каналів, захист АРМ операціоністів, серверної інфраструктури та банкоматів. Резервне копіювання та відновлення даних (RPO, RTO). Забезпечення безперервності діяльності (BCP/DRP).

Ключові поняття

- СУІБ за ISO 27001: PDCA-цикл (Plan-Do-Check-Act)
- Управління інцидентами інформаційної безпеки (IRM)
- Тестування на проникнення (Penetration Testing) банківських систем
- Хмарна безпека у банківській сфері (Cloud Security)

Тема 2.1 — Практичне заняття та СРС

Практичне заняття (1 год.)

Задача 1. Аналіз відповідності умовного банку вимогам стандарту ISO 27001: заповнення чек-листа за ключовими доменами стандарту, визначення рівня зрілості СУІБ.

Задача 2. Розробка матриці доступу (RBAC) для типових ролей банківської установи: операціоніст, системний адміністратор, керівник відділу, аудитор. Обґрунтування прав доступу.

Задача 3. Розробка плану реагування на інцидент інформаційної безпеки (витік клієнтських даних): кроки виявлення, стримування, ліквідації та відновлення.

Самостійна робота (4 год.)

- Опрацювання стандарту ISO/IEC 27001:2022 (основні домени та вимоги до СУІБ) та конспектування ключових контролів для банківської сфери
- Виконання аналітичного завдання: порівняння засобів захисту інформації двох українських банків (за відкритими звітами та публікаціями)
- Підготовка таблиці «Засоби захисту банківської ІС: призначення та ефективність»
- Пошук даних про стан кібербезпеки банківського сектору України на сайті bank.gov.ua та cert.gov.ua

Очікуваний результат: студент вміє характеризувати засоби захисту банківських ІС, оцінювати рівень відповідності ISO 27001 та розробляти матриці доступу.

Тема 2.2 — Лекційний матеріал

Кіберзагрози у банківській сфері

Лекція 6 (2 год.): Класифікація кібератак на банки: фішинг та спір-фішинг, атаки типу «людина посередині» (MitM), DDoS-атаки на банківські сервіси, APT (Advanced Persistent Threats), атаки на банкомати (Jackpotting, Skimming), атаки на SWIFT-систему, програми-вимагачі (Ransomware).

Захист платіжних систем: безпека карткових транзакцій (PCI DSS), двофакторна автентифікація (2FA/MFA), токенізація платіжних даних, захист систем дистанційного банківського обслуговування (інтернет-банкінг, мобільний банкінг). Моніторинг транзакцій у режимі реального часу.

Виявлення та протидія кібератакам

Методи виявлення кіберінцидентів: аналіз журналів подій (Log Management), поведінковий аналіз (UEBA), threat intelligence (розвідка загроз), SOC (Security Operations Center) у банках.

- Еластичність попиту на банківські послуги до кіберінцидентів
- Оцінка збитків від кібератак: прямі та репутаційні втрати
- Державне регулювання кібербезпеки фінансового сектору (CERT-UA, НБУ)
- Страхування кіберризиків у банківській практиці

Тема 2.2 — Практичне заняття та СРС

Практичне заняття (2 год.)

Задача 1. Аналіз реального кейсу кібератаки на банківську установу (наприклад, атака на банківський сектор України у 2022–2024 рр.): ідентифікація типу атаки, вектора проникнення, завданої шкоди та вжитих заходів реагування.

Задача 2. Розробка плану захисту системи інтернет-банкінгу від фішингових атак та атак типу MitM: технічні та організаційні заходи, навчання персоналу та клієнтів.

Задача 3. Порівняльний аналіз засобів виявлення кіберзагроз (IDS, SIEM, UEBA) для банківської установи. Обґрунтування вибору оптимального рішення.

Самостійна робота (4 год.)

- Опрацювання матеріалів CERT-UA (cert.gov.ua) та НБУ щодо актуальних кіберзагроз для банківського сектору України (2023–2024 рр.)
- Підготовка аналітичної записки: «Кіберзахист банківської системи України в умовах воєнного стану» (за даними відкритих публікацій)
- Складання порівняльної таблиці типів кібератак на банки та методів протидії
- Розв'язання ситуаційних задач на виявлення ознак фішингу та соціальної інженерії (4 задачі)

Очікуваний результат: студент вміє класифікувати кіберзагрози банківській діяльності, аналізувати кіберінциденти та розробляти заходи захисту платіжних систем.

Тема 2.3 — Лекційний матеріал

Банківська таємниця та захист персональних даних

Лекція 7 (2 год.): Банківська таємниця: поняття, об'єкти (інформація про клієнта, стан рахунків, операції), суб'єкти зобов'язання дотримання таємниці. Підстави для розкриття банківської таємниці: судовий запит, органи державної влади, ДСФМ. Відповідальність за розголошення (кримінальна, цивільна, адміністративна).

Захист персональних даних у банках: Закон України «Про захист персональних даних», GDPR (для банків з операціями в ЄС). Категорії персональних даних у банківській діяльності. Принципи обробки даних: законність, мінімізація, точність, обмеження зберігання. Технічні та організаційні заходи захисту (шифрування, псевдонімізація, контроль доступу).

Організація захисту конфіденційної інформації

DLP-системи (Data Loss Prevention) у банках: принципи роботи, канали контролю (мережевий трафік, кінцеві пристрої, хмарні сервіси), реагування на витоки. Управління інсайдерськими загрозами: контроль привілейованого доступу (PAM), моніторинг дій персоналу.

- Класифікація інформації за рівнями конфіденційності у банку
- Комерційна та банківська таємниця: відмінності у правовому режимі
- Безпека передачі банківської інформації (протоколи TLS, S/MIME)

Тема 2.3 — Практичне заняття та СРС

Практичне заняття (1 год.)

Задача 1. Аналіз ситуаційних кейсів щодо розголошення банківської таємниці: визначення правомірності розкриття інформації та відповідальності банку у конкретних ситуаціях.

Задача 2. Порівняльний аналіз вимог Закону України «Про захист персональних даних» та GDPR щодо обробки клієнтських даних банку. Виявлення ключових відмінностей та спільних вимог.

Задача 3. Розробка переліку організаційних і технічних заходів захисту персональних даних клієнтів для умовного банку.

Самостійна робота (4 год.)

- Опрацювання Закону України «Про захист персональних даних» та виписування ключових вимог до банківської діяльності
- Підготовка аналітичної записки: «Практика захисту банківської таємниці та персональних даних в Україні: актуальні проблеми» (1–2 сторінки)
- Аналіз публічних звітів про витоки персональних даних у фінансовому секторі
- Розв'язання задач на застосування норм про банківську таємницю (4 задачі)

Очікуваний результат: студент вміє застосовувати норми про банківську таємницю та захист персональних даних, розробляти організаційні заходи захисту конфіденційної інформації.

Тема 2.4 — Лекційний матеріал

Фінансовий моніторинг та протидія легалізації доходів (AML/KYC)

Лекція 8–9 (4 год.): Поняття фінансового моніторингу та легалізації доходів, одержаних злочинним шляхом. Правова база: Закон України «Про запобігання та протидію легалізації (відмиванню) доходів». Стадії відмивання: розміщення, розшарування, інтеграція. Типові схеми відмивання через банківський сектор. Фінансові санкції (FATF Recommendations 2023).

Процедури KYC (Know Your Customer): ідентифікація та верифікація клієнта (фізичної особи, юридичної особи, ПЕП), поглиблена перевірка (EDD), ризик-орієнтований підхід (RBA). Процедури CDD (Customer Due Diligence) та Enhanced Due Diligence для клієнтів підвищеного ризику.

Виявлення підозрілих операцій

- **Індикатори підозрілих операцій:** незвична сума, нетипова частота, невідповідність профілю клієнта, операції з офшорними юрисдикціями
- **Автоматизований моніторинг транзакцій (TMS):** системи виявлення аномалій на основі правил та машинного навчання
- **Звітування:** повідомлення Державній службі фінансового моніторингу (ДСФМ), формування SAR (Suspicious Activity Report)
- **Список санкцій:** перевірка клієнтів за списками РНБО, ЄС, OFAC, ООН

Відповідальність банку за порушення AML-законодавства: штрафні санкції НБУ, кримінальна відповідальність посадових осіб, відкликання ліцензії.

Тема 2.4 — Практичне заняття та СРС

Практичне заняття (2 год.)

Задача 1. Проведення ідентифікації та верифікації умовного клієнта банку (фізична особа та юридична особа): перелік необхідних документів, визначення ризик-категорії, рішення щодо встановлення ділових відносин.

Задача 2. Аналіз операцій умовного клієнта: виявлення ознак підозрілих транзакцій за встановленими індикаторами ДСФМ. Підготовка спрощеного повідомлення про підозрілу операцію (SAR).

Задача 3. Факторний аналіз ризику клієнта: оцінка клієнта за ризик-профілем (географія, вид діяльності, обсяги операцій). Визначення рівня ризику та необхідних заходів CDD/EDD.

Самостійна робота (4 год.)

- Опрацювання Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом» — розділи щодо обов'язків банків
- Аналіз Рекомендацій FATF 2023 щодо вимог до банків у сфері AML/CFT
- Підготовка аналітичної записки: «Стан фінансового моніторингу в банківській системі України: сучасні виклики» (за даними ДСФМ та НБУ)
- Розв'язання комплексного завдання з визначення ризик-категорії клієнта та відповідних заходів KYC

Очікуваний результат: студент вміє проводити процедури KYC/CDD, виявляти ознаки підозрілих операцій, формувати повідомлення ДСФМ та оцінювати ризики клієнта з позицій AML.

МОДУЛЬ 3

Управління безпекою банку та захист від шахрайства

Тема 3.1

Шахрайство у банківській діяльності: види, схеми, методи виявлення та протидії. Захист від карткового шахрайства та шахрайства у сфері ДБО.

Тема 3.2

Фізична та кадрова безпека банку: організація фізичного захисту, робота з персоналом, превентивні заходи щодо внутрішніх загроз.

Тема 3.3

Безперервність діяльності та антикризове управління в банку. Плани BCP/DRP, стрес-тестування, відновлення після кіберінцидентів.

Тема 3.4

Аудит та оцінка ефективності системи безпеки банку. Методи внутрішнього та зовнішнього аудиту, ключові показники ефективності (KPI) безпеки.

Тема 3.1 — Лекційний матеріал

Шахрайство у банківській діяльності

Лекція 10–11 (4 год.): Банківське шахрайство: поняття, масштаби та тенденції. Класифікація видів шахрайства: зовнішнє шахрайство (скімінг, фішинг, підробка документів, кіберкрадіжки) та внутрішнє шахрайство (привласнення активів, маніпуляції зі звітністю, зловживання повноваженнями). Схеми шахрайства у сфері кредитування: шахрайство з кредитами, страховими виплатами, іпотекою.

Методи виявлення шахрайства: системи fraud detection на основі правил (rule-based), статистичних методів та машинного навчання. Поведінковий аналіз транзакцій. Ознаки шахрайства у документах та операціях.

Захист від карткового шахрайства та ДБО

- Картковий фрод: CNP-шахрайство (Card Not Present), підробка карток, несанкціоновані операції
- Захист: 3D Secure 2.0, токенізація, динамічний CVV, геолокаційний контроль
- Шахрайство у мобільному та інтернет-банкінгу: соціальна інженерія, OTP-перехоплення, SIM-свопінг
- Чарджбек: процедура, зловживання та захист банку
- Відповідальність банку та клієнта за несанкціоновані операції
- Кримінальна відповідальність за банківське шахрайство (ст. 190, 200 КК України)

Тема 3.1 — Практичне заняття та СРС

Практичне заняття (2 год.)

Завдання 1. Аналіз кейсу банківського шахрайства: ідентифікація схеми шахрайства, вектора атаки, задіяних вразливостей та збитків. Розробка заходів превенції.

Завдання 2. Налаштування правил fraud-моніторингу: розробка набору правил виявлення підозрілих карткових транзакцій для умовного банку (пороги суми, частота, географія).

Завдання 3. Кейс: аналіз конкретного випадку внутрішнього шахрайства у банку та розроблення рекомендацій щодо посилення внутрішнього контролю.

Самостійна робота (4 год.)

- Опрацювання матеріалів НБУ та звітів платіжних систем VISA/Mastercard щодо тенденцій карткового шахрайства в Україні (2023–2024 рр.)
- Підготовка аналітичної записки: «Банківське шахрайство в умовах цифровізації: сучасні виклики та методи протидії»
- Проведення аналізу реального випадку шахрайства (за відкритими даними): виявлення причин та наслідків
- Опрацювання статті про фінансову безпеку банків в умовах цифровізації (Галицький економічний вісник, № 4 (89), 2024)

Очікуваний результат: студент вміє класифікувати схеми банківського шахрайства, налаштовувати правила fraud-моніторингу та розробляти заходи превенції.

Тема 3.2 — Лекційний матеріал

Фізична та кадрова безпека банку

Лекція 12–13 (4 год.): Фізична безпека банківської установи: захист приміщень (системи контролю доступу, відеоспостереження, охорона, сейфи та сховища), безпека банкоматів та POS-терміналів (антискімінгові пристрої, захисні кожухи, GPS-трекінг), безпека інкасації. Стандарти фізичного захисту об'єктів критичної інфраструктури.

Кадрова безпека: загрози з боку персоналу (інсайдерські загрози, навмисне та ненавмисне розголошення інформації). Превентивні заходи: перевірка кандидатів при прийомі на роботу, підписання NDA, розмежування обов'язків (Segregation of Duties), ротація персоналу на критичних посадах.

Навчання персоналу та культура безпеки

Програми навчання персоналу безпеки: антифішинговий тренінг, навчання розпізнаванню соціальної інженерії, правил роботи з конфіденційною інформацією, порядку дій при виявленні інциденту. Тестування рівня обізнаності (Security Awareness Testing).

- Джерела інсайдерських загроз та їх ознаки
- Моніторинг поведінки персоналу (UEBA) та правові обмеження
- Формування корпоративної культури безпеки у банку
- Відповідальність персоналу за порушення безпекових вимог

Тема 3.2 — Практичне заняття та СРС

Практичне заняття (2 год.)

Завдання 1. Розробка системи фізичного захисту відділення банку: визначення зон доступу, засобів контролю (СКУД, відеоспостереження, тривожна кнопка), процедур реагування на фізичні загрози.

Завдання 2. Оцінка рівня кадрових ризиків безпеки умовного банку: складання матриці інсайдерських ризиків (посада × тип доступу × рівень ризику) та розроблення заходів реагування.

Завдання 3. Кейс: розробка антикризового плану для банку, що зазнав фізичного нападу чи крадіжки. Обґрунтування запропонованих заходів.

Самостійна робота (4 год.)

- Опрацювання стандартів фізичної безпеки критичної інфраструктури (Постанова КМУ щодо захисту об'єктів критичної інфраструктури) та їх застосування до банківської сфери
- Підготовка аналітичної записки: «Кадрова безпека банків: інсайдерські загрози та методи протидії в умовах воєнного стану в Україні»
- Ознайомлення з методичними рекомендаціями НБУ щодо управління операційними ризиками (zakon.rada.gov.ua)
- Підготовка таблиці «Засоби фізичного захисту банківської установи: переваги та обмеження»

Очікуваний результат: студент вміє проектувати систему фізичного захисту банківської установи, оцінювати кадрові ризики безпеки та розробляти заходи превенції інсайдерських загроз.

Тема 3.3 — Лекційний матеріал

Безперервність діяльності та антикризове управління в банку

Лекція 14 (2 год.): Забезпечення безперервності діяльності банку (BCP — Business Continuity Plan): поняття, структура, ключові елементи. Аналіз бізнес-впливу (BIA) для банківських процесів. Відновлення після катастрофи (DRP — Disaster Recovery Plan): RPO (Recovery Point Objective), RTO (Recovery Time Objective), резервні центри обробки даних. Сценарії загроз: кібератака, природна катастрофа, збої в енергопостачанні, збройний конфлікт.

Стрес-тестування систем безпеки банку: методологія, регуляторні вимоги НБУ до стрес-тестів, сценарний аналіз кіберінцидентів. Навчання персоналу та регулярні перевірки BCP/DRP.

Антикризове управління в банку

Кризові явища у банківській діяльності: ознаки кризи (відтік депозитів, зниження капіталу, кіберінцидент, паніка клієнтів, проблеми з ліквідністю). Антикризові заходи: стабілізаційні (обмеження операцій, залучення рефінансування НБУ) та стратегічні (реструктуризація, злиття, продаж проблемних активів).

- Показники фінансової стійкості банку як індикатори кризи (нормативи НБУ)
- Процедури виведення неплатоспроможного банку з ринку (ФГВФО)
- Тимчасова адміністрація: поняття, умови введення та наслідки

Тема 3.3 — Практичне заняття та СРС

Практичне заняття (2 год.)

Завдання 1. Розробка спрощеного плану забезпечення безперервності діяльності (BCP) для умовного банку: ідентифікація критичних процесів, визначення RPO та RTO, розподіл ролей у команді реагування.

Завдання 2. Розрахунок показників фінансової стійкості та ліквідності умовного банку за нормативами НБУ. Діагностика ознак фінансової кризи та виявлення критичних відхилень.

Завдання 3. Кейс: розробка плану реагування на DDoS-атаку на банківські IT-системи: виявлення, стримування, відновлення, комунікація з клієнтами та регулятором.

Самостійна робота (4 год.)

- Опрацювання Постанови НБУ щодо вимог до планів забезпечення безперервності діяльності банків та конспектування ключових вимог
- Підготовка аналітичної записки: «Безперервність діяльності банків України в умовах воєнного стану: досвід та висновки»
- Ознайомлення з матеріалами ФГВФО щодо виведення банків з ринку (fg.gov.ua)
- Підготовка таблиці «Заходи антикризового управління банком: оперативні та стратегічні»

Очікуваний результат: студент вміє розробляти плани BCP/DRP для банку, діагностувати ознаки банківської кризи та пропонувати антикризові заходи реагування.

Тема 3.4 — Лекційний матеріал

Аудит та оцінка ефективності системи безпеки банку

Лекція 15 (2 год.): Аудит системи безпеки банку: поняття, цілі, види (внутрішній, зовнішній, регуляторний). Внутрішній аудит безпеки: функції підрозділу внутрішнього аудиту, методологія перевірок, звітування перед спостережною радою. Зовнішній аудит та пентест: залучення спеціалізованих компаній, методологія тестування на проникнення (Black Box, White Box, Grey Box).

Показники ефективності (KPI) безпеки банку: кількість інцидентів безпеки, середній час виявлення (MTTD) та реагування (MTTR), рівень відповідності нормативним вимогам, відсоток навченого персоналу, покриття моніторингом критичних активів. Системи звітності: звіт про стан інформаційної безпеки перед керівництвом та НБУ.

Стратегія розвитку системи безпеки банку

Стратегічне планування безпеки: модель зрілості кібербезпеки (CMMI, NIST CSF), дорожня карта розвитку СУІБ. Тенденції та інновації у банківській безпеці: ШІ та машинне навчання у fraud-detection та виявленні аномалій, безпека Open Banking та API, Zero Trust Architecture у банках.

- Перспективи безпеки: технологічна, регуляторна, операційна, стратегічна
- KPI безпеки як інструмент моніторингу та звітування
- Стратегічний контроль та актуалізація планів безпеки

Тема 3.4 — Практичне заняття та СРС

Практичне заняття (2 год.)

Завдання 1. Розробка системи KPI безпеки для умовного банку: визначення ключових показників, методів їх вимірювання, відповідальних осіб та цільових значень. Порівняльний аналіз ефективності систем безпеки двох банків.

Завдання 2. Розробка дорожньої карти (roadmap) розвитку системи безпеки умовного банку на 3 роки: визначення пріоритетів, ключових ініціатив та показників успіху.

Завдання 3. Підсумкова дискусія: «Які підходи до забезпечення безпеки банківської діяльності є найбільш актуальними в умовах цифровізації та воєнного стану в Україні?»

Самостійна робота (5 год.)

- Опрацювання методології NIST Cybersecurity Framework (CSF 2.0, 2024) та її застосування до оцінки зрілості кібербезпеки банку
- Підготовка комплексного аналітичного завдання: оцінка ефективності системи безпеки реального банку за публічними даними (річний звіт, звіт про стан безпеки)
- Підготовка презентації: «Стратегія розвитку системи кібербезпеки обраного банку» (10–12 слайдів)
- Систематизація матеріалу всього курсу для підготовки до підсумкового іспиту

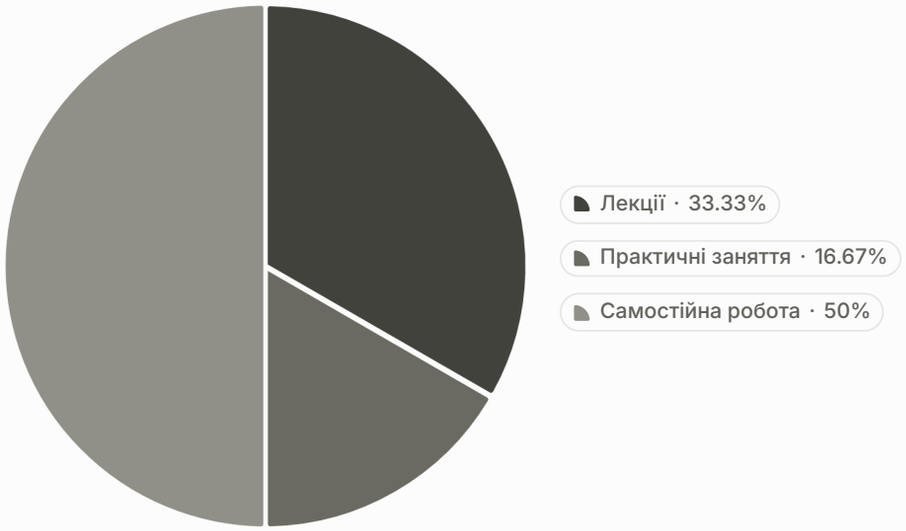
Очікуваний результат: студент вміє оцінювати ефективність системи безпеки банку, формувати KPI безпеки, розробляти стратегічні плани розвитку СУІБ та аудиторські програми перевірки.

Розподіл навчального часу — 90 годин

Модуль	Тема	Лекції (год.)	Практичні (год.)	СРС (год.)
Модуль 1	Тема 1.1 — Сутність та складові безпеки банку	2	1	4
	Тема 1.2 — Нормативно-правове регулювання	2	1	4
	Тема 1.3 — Загрози та ризики банківської діяльності	2	2	4
Модуль 2	Тема 2.1 — Інформаційна безпека банку	4	1	4
	Тема 2.2 — Кіберзагрози та захист платіжних систем	2	2	4
	Тема 2.3 — Банківська таємниця та захист даних	2	1	4
	Тема 2.4 — Фінансовий моніторинг та AML/KYC	4	2	4
Модуль 3	Тема 3.1 — Шахрайство у банківській діяльності	4	2	4
	Тема 3.2 — Фізична та кадрова безпека	4	2	4
	Тема 3.3 — Безперервність діяльності та антикриза	2	2	4
	Тема 3.4 — Аудит та ефективність системи безпеки	2	2	5
Разом		**30**	**15**	**45**

Загальний обсяг: **90 годин = 3 кредити ЄКТС**. Підсумковий контроль — іспит. Розподіл є орієнтовним і може коригуватися відповідно до специфіки навчального процесу.

Структура навчального часу



Коментар до розподілу

Загальний обсяг — **90 годин (3 кредити ЄКТС)** — розподілено між трьома формами роботи для забезпечення балансу між теоретичною підготовкою та практичними навичками у сфері банківської безпеки.

Лекції — 30 год. (33,33%)

Системне подання ключового теоретичного матеріалу з використанням схем, таблиць і реальних прикладів кіберінцидентів та банківських загроз.

Практичні — 15 год. (16,67%)

Відпрацювання навичок, розв'язання задач і кейсів, моделювання загроз, аналіз інцидентів безпеки та захист міні-проектів.

Самостійна робота — 45 год. (50%)

Поглиблене вивчення, підготовка аналітичних завдань, робота з нормативними документами та фаховими джерелами. Самостійна робота становить **50% обсягу дисципліни**.

Самостійна робота студентів — Детальний опис

Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за підручниками та посібниками з безпеки банківської діяльності (Зубок М. І., Корченко А. О., Хорошко В. О. та ін.), нормативними документами НБУ, законодавством України, стандартами ISO 27001 та матеріалами FATF. Студент конспектує ключові положення та порівнює підходи різних авторів.

Робота з інформаційними ресурсами

Опрацювання офіційних сайтів: НБУ (bank.gov.ua), ДСФМ (fiu.gov.ua), CERT-UA (cert.gov.ua), ФГВФО (fg.gov.ua), Верховна Рада (zakon.rada.gov.ua). Аналіз річних звітів банків, публікацій НБУ та міжнародних регуляторів (FATF, EBA, ENISA) щодо стану безпеки фінансового сектору.

Індивідуальні завдання

Виконання аналітичних завдань (оцінка системи безпеки банку, аналіз кіберінцидентів, KYC/AML кейси); практичних завдань (налаштування правил моніторингу, розробка BCP, матриці ризиків); творчих завдань — есе, аналітичні записки, міні-дослідження з актуальних питань банківської безпеки.

Підготовка до занять

Підготовка до практичних занять (опрацювання умов кейсів, повторення теорії); підготовка до тестувань (ключові терміни, нормативні вимоги); підготовка до контрольних робіт за кожним модулем та систематизація знань для підготовки до підсумкового іспиту.

Форми контролю знань

1	2	3
Поточний контроль Завдання: аналітичні та практичні вправи за темами змістовного модуля (кейси інцидентів, розробка матриць ризиків, завдання з AML/KYC). Оцінюються регулярність виконання, якість відповідей і рівень засвоєння матеріалу. Поточний контроль формує накопичувальну оцінку протягом семестру. Проводиться після кожної теми у формі тестування (10–15 питань) або усного опитування.	**Проміжний контроль** Самостійна робота — комплексне ситуаційне завдання або реферат, які охоплюють теми змістовних модулів (теоретичні питання, аналіз загроз, розробка заходів захисту). Оцінюються повнота відповіді, правильність аналізу та обґрунтованість висновків. Проводиться після завершення кожного змістовного модуля.	**Підсумковий контроль** Іспит відповідно до навчального плану. Форма проведення — письмовий іспит (теоретичні питання та практичні завдання / кейси). Підсумкова оцінка враховує результати поточного, проміжного та підсумкового контролю відповідно до встановленої шкали: **100-бальна система** з переведенням у національну шкалу та ЄКТС (A, B, C, D, E, FX, F).

Методи викладання

Викладання дисципліни «Безпека банківської діяльності» поєднує класичні академічні та інтерактивні методи, що забезпечує формування не лише міцної теоретичної бази, а й практичних навичок у сфері захисту банківських систем та управління ризиками безпеки.

Лекції

Системне подання теоретичного матеріалу з використанням наочних схем, таблиць і реальних прикладів кіберінцидентів та банківських загроз; студенти ведуть конспекти та задають уточнювальні запитання.

Кейс-стаді

Аналіз реальних інцидентів безпеки банківських установ; студенти ідентифікують загрозу, аналізують заходи реагування та формулюють рекомендації щодо превенції.

Практичні завдання

Розробка матриць ризиків, планів BCP/DRP, реєстрів ризиків, KYC-процедур; відпрацювання алгоритмів реагування на кіберінциденти та fraud-моніторингу.

Дискусії

Обговорення актуальних проблем безпеки банківського сектору України (кіберзагрози, AML, захист даних, безпека в умовах воєнного стану); розвиток критичного мислення та аргументації.

Нормативні документи

Опрацювання Закону «Про банки і банківську діяльність», постанов НБУ, рекомендацій FATF та стандартів ISO 27001, PCI DSS; формування навичок роботи з технічною та правовою базою.

Самостійне дослідження

Підготовка аналітичних записок, рефератів і презентацій за обраною темою; розвиток навичок самостійного пошуку та систематизації інформації у сфері банківської безпеки.

Усі методи спрямовані на формування компетентностей, передбачених освітньо-професійною програмою спеціальності 123 «Комп'ютерна інженерія» (ОП «Фінанси, банківська справа та страхування в управлінських інформаційних системах і технологіях»).

Рекомендована література та ресурси

Підручники та навчальні посібники (2022–2024 рр.)

1 **Корченко А. О., Скачек Л. М., Хорошко В. О.**
Банківська безпека : підручник / за заг. ред. В. О. Хорошка. — К. : ПВП «Задруга», 2022. — 185 с.

2 **Попов О. Г.**
Теоретичні основи забезпечення банківської безпеки держави. Економіка, управління та адміністрування. — 2023. — № 3(105). — С. 195–202.

3 **Трусова Н. В., Чкан І. О. та ін.**
Кіберзахист банківської системи України в умовах воєнного часу. Збірник наукових праць ТДАТУ імені Дмитра Моторного (економічні науки). — 2023. — № 1(47).

4 **Висоцька І. та ін.**
Банківська система : навчальний посібник у схемах і таблицях. — Київ, 2024. — (ResearchGate. DOI: 10.13140/RG.2.2.17012).

5 **Фінансова безпека банківських установ в умовах цифровізації**
Колектив авторів. Економіка та суспільство : журнал. — 2024. — (economyandsociety.in.ua). DOI: 10.32782/2524-0072.

6 **Цифровізація та кібербезпека у забезпеченні фінансової безпеки банків в умовах війни**
Галицький економічний вісник. — 2024. — № 4 (89). — DOI: 10.33108/galicianvisnyk_tntu2024.04.

7 **FATF Recommendations**
Financial Action Task Force. Updated FATF Recommendations on Anti-Money Laundering and Counter-Terrorist Financing. — Paris : FATF/OECD, 2023.

8 **NIST Cybersecurity Framework 2.0**
National Institute of Standards and Technology. Cybersecurity Framework (CSF) 2.0. — Gaithersburg : NIST, 2024.

9 **ISO/IEC 27001:2022**
International Organization for Standardization. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. — Geneva : ISO, 2022.

10 **European Banking Authority (EBA)**
EBA Guidelines on ICT and Security Risk Management. — London : EBA, 2023. — (eba.europa.eu).

11 **Regulation (EU) 2022/2554 — DORA**
Digital Operational Resilience Act (DORA). — Brussels : European Parliament, 2022. — (eur-lex.europa.eu).

12 **Стойко О. Я., Дема Д. І.**
Фінанси : підручник. — Житомир : Університет «Полісся», 2024. — 317 с.

Нормативно-правова база

- **Закон «Про банки і банківську діяльність»**
  zakon.rada.gov.ua/laws/show/2121-14
- **Закон «Про основні засади забезпечення кібербезпеки України»**
  zakon.rada.gov.ua/laws/show/2163-19
- **Закон «Про запобігання та протидію легалізації доходів»**
  zakon.rada.gov.ua/laws/show/361-20

Офіційні ресурси та фахові видання

Національний банк України
bank.gov.ua

CERT-UA (Держспецзв'язку)
cert.gov.ua

Державна служба фінансового моніторингу
fiu.gov.ua

Фонд гарантування вкладів фізичних осіб
fg.gov.ua

Верховна Рада України
zakon.rada.gov.ua

Журнал «Економіка та суспільство»
economyandsociety.in.ua

Галицький економічний вісник (ТНТУ)
galicianvisnyk.tntu.edu.ua