

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

СПЕЦІАЛЬНІСТЬ 123 · КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

БАКАЛАВР

90 годин · 3 кредити ЄКТС · 3 змістовних модулі



Загальна інформація про дисципліну

Ідентифікація

Назва: Безпека банківської діяльності з використанням управлінських інформаційних систем і технологій

Спеціальність: **123** Комп'ютерна інженерія

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

Ступінь: Бакалавр

90

Годин

загальний обсяг дисципліни

3

Кредити ЄКТС

відповідно до стандарту

3

Модулі

змістовних блоки курсу

Компетентності та результати навчання

Загальні компетентності

Здатність до аналізу, синтезу та критичного оцінювання інформації у сфері інформаційної та фінансової безпеки банківських установ: виявлення загроз, порівняння методів захисту, формування обґрунтованих висновків і вироблення власної позиції. Уміння самотійно навчатися, планувати роботу та організовувати виконання завдань у визначені строки, зокрема під час підготовки аналітичних звітів, практичних завдань і презентацій.

Здатність до усної та письмової професійної комунікації: чітко пояснювати поняття безпеки банківської діяльності, аргументовано відповідати на запитання, оформлювати звіти, висновки та аналітичні записки.

Відповідальність, ініціативність, дисциплінованість та готовність працювати в команді під час групового аналізу кейсів у сфері кібербезпеки та захисту банківської інформації.

- аналізувати навчальну, нормативну та технічну інформацію з питань банківської безпеки;
- виділяти ключові загрози та узагальнювати методи протидії;
- планувати власну діяльність і дотримуватися дедлайнів;
- коректно спілкуватися з викладачами та одногрупниками;
- брати участь у командній роботі та розподіляти обов'язки під час виконання групових проєктів.

Фахові компетентності

Розуміння сутності безпеки банківської діяльності, її складових та ролі в забезпеченні стабільності фінансової системи. Знання принципів організації захисту банківських інформаційних систем, методів оцінки ризиків та механізмів прийняття рішень у сфері безпеки банку.

Здатність аналізувати стан інформаційної, кібернетичної та фінансової безпеки банківської установи: виявляти загрози, оцінювати вразливості, застосовувати методи захисту даних, електронних платежів і банківських систем. Знання основ фінансового моніторингу, протидії відмиванню коштів та антикризового управління в банківництві.

- оцінювати рівень безпеки банківської установи за ключовими індикаторами;
- визначати роль і функції підрозділів безпеки банку;
- характеризувати загрози банківській системі та методи їх нейтралізації;
- орієнтуватися в основах кіберзахисту банківських інформаційних систем;
- пояснювати механізми фінансового моніторингу та протидії шахрайству в банківництві.

Результати навчання

Пояснювати сутність понять та явищ у сфері банківської безпеки: загрози, ризики, вразливості, фінансовий моніторинг, кіберінциденти, захист персональних даних та банківської таємниці.

Аналізувати основні показники захищеності банківських установ для виявлення слабких місць та потенційних загроз.

Характеризувати організаційно-правові засади забезпечення безпеки банківської діяльності, застосовувати методи оцінки захищеності інформаційних систем, визначати основні тенденції кіберзагроз та робити висновки щодо ефективності захисних заходів.

- пояснювати зміст ключових понять банківської безпеки та захисту інформації;
- аналізувати загрози та вразливості банківських систем;
- визначати показники фінансової стійкості та безпеки банківської установи;
- застосовувати базові методи оцінки захищеності банківських інформаційних ресурсів;
- використовувати нормативні та інформаційні джерела НБУ для прийняття обґрунтованих рішень у сфері безпеки.

Основи безпеки банківської діяльності

Тема 1.1

Банківська безпека як система.

Сутність і зміст безпеки банківської діяльності, її місце в системі фінансової та економічної безпеки держави, основні складові та принципи організації.

Тема 1.2

Загрози та ризики банківської діяльності: класифікація загроз, внутрішні та зовнішні ризики банку, методи їх ідентифікації та оцінки, ризик-орієнтований підхід у банківській безпеці.

Тема 1.3

Нормативно-правове забезпечення безпеки банківської діяльності.

Законодавство України у сфері банківської безпеки, роль НБУ як регулятора, міжнародні стандарти та вимоги Базельського комітету.

Інформаційна та кібернетична безпека банку

Тема 2.1

Інформаційна безпека банківської установи: склад банківської інформації, загрози конфіденційності, цілісності та доступності даних, захист банківської таємниці та персональних даних клієнтів.

Тема 2.2

Кібербезпека банківських систем. Основні кіберзагрози та методи захисту: шкідливе програмне забезпечення, фішинг, DDoS-атаки, захист автоматизованих банківських систем і мереж.

Тема 2.3

Безпека електронних банківських платежів та дистанційного обслуговування. Захист платіжних систем, криптографічні методи, електронний підпис, безпека інтернет-банкінгу та мобільних додатків.

Тема 2.4

Фінансовий моніторинг і протидія відмиванню коштів. Система фінансового моніторингу в банку, ризик-орієнтований підхід, виявлення підозрілих операцій, вимоги антилегалізаційного законодавства.

Управління ризиками та захист активів банку

Тема 3.1

Фізична та технічна безпека банківської установи: системи охорони, контроль доступу, засоби відеоспостереження, захист сховищ і банківських цінностей.

Тема 3.2

Кадрова безпека банку та протидія внутрішньому шахрайству: добір і перевірка персоналу, запобігання корупції, виявлення інсайдерських загроз та зловживань.

Тема 3.3

Антикризове управління та забезпечення безперервності банківської діяльності. Плани відновлення після інцидентів, стрес-тестування, управління операційними ризиками.

Тема 3.4

Оцінка ефективності системи безпеки банку та стратегічний розвиток захисних механізмів. Аудит безпеки, показники захищеності, сучасні тенденції банківської безпеки в умовах цифровізації.

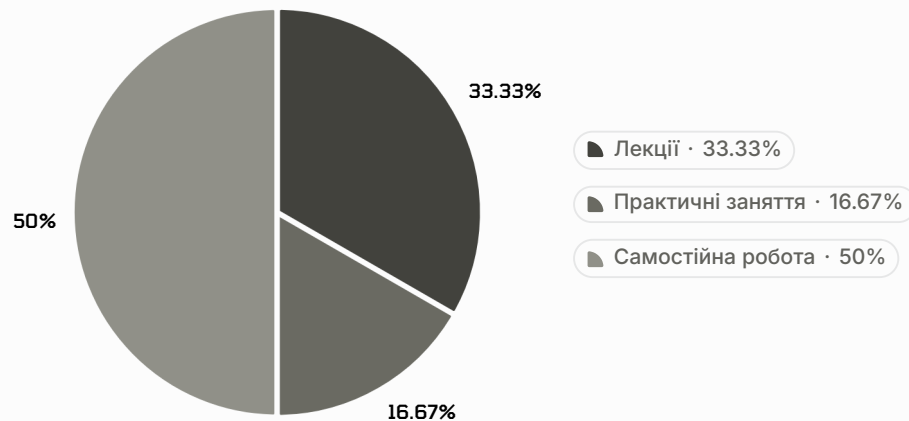
Розподіл навчального часу – 90 годин

Модуль	Тема	Лекції (год.)	Практичні (год.)	Самостійна робота (год.)
Модуль 1	Тема 1.1 – Банківська безпека як система	2	1	4
	Тема 1.2 – Загрози та ризики	2	1	4
	Тема 1.3 – Нормативно-правове забезпечення	2	2	4
Модуль 2	Тема 2.1 – Інформаційна безпека банку	4	1	4
	Тема 2.2 – Кібербезпека банківських систем	2	2	4
	Тема 2.3 – Безпека електронних платежів	2	1	4
	Тема 2.4 – Фінансовий моніторинг	4	2	4
Модуль 3	Тема 3.1 – Фізична та технічна безпека	4	2	4
	Тема 3.2 – Кадрова безпека та протидія шахрайству	4	2	4
	Тема 3.3 – Антикризове управління	2	2	4
	Тема 3.4 – Аудит безпеки та стратегія	2	2	5
Разом		30	15	45

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



Примітки до розподілу часу



Структура навчального часу

Загальний обсяг — **90 годин (3 кредити ЄКТС)** — розподілено між трьома формами роботи для забезпечення балансу між теорією та практикою.

- **Лекції (30 год.):** подача ключового теоретичного матеріалу з безпеки банківської діяльності
- **Практичні (15 год.):** відпрацювання навичок аналізу загроз, розв'язання задач з оцінки ризиків
- **Самостійна робота (45 год.):** поглиблене вивчення, підготовка завдань, опрацювання нормативних документів

□ Самостійна робота становить **50% обсягу дисципліни** — студенти навчаються самостійно опрацьовувати джерела та нормативні акти у сфері банківської безпеки.

Самостійна робота студентів



Опрацювання літератури

Поглиблене вивчення теоретичного матеріалу за навчальними посібниками з безпеки банківської діяльності (Усік, Буравченко, Стрельбицька та ін.), нормативно-правовими актами (Закон України «Про банки і банківську діяльність», Закон про ПВК/ФТ, постанови НБУ), науковими статтями у фахових виданнях. Студент має вміти конспектувати ключові положення, виділяти основні загрози та методи захисту, порівнювати підходи різних авторів до забезпечення безпеки банківських систем.



Робота з інформаційними ресурсами

Опрацювання офіційних сайтів Національного банку України (bank.gov.ua), Верховної Ради України (zakon.rada.gov.ua), Державної служби фінансового моніторингу (sdfm.gov.ua), Держспецзв'язку (cip.gov.ua) та Мінцифри (diia.gov.ua). Аналіз нормативних актів, звітів НБУ про фінансову стабільність, матеріалів щодо кіберінцидентів у банківській сфері. Результат — розвиток навичок роботи з офіційними джерелами та формування інформаційної грамотності в сфері банківської безпеки.



Індивідуальні завдання

Виконання аналітичних завдань з оцінки рівня захищеності банківської установи, виявлення кіберзагроз та розробки заходів протидії; розрахункових завдань з оцінки ризиків та індикаторів фінансової безпеки банку; творчих завдань — підготовка есе, аналітичних записок, міні-досліджень з актуальних питань кібербезпеки та протидії банківському шахрайству. Очікуваний результат — уміння застосовувати теорію на практиці, інтерпретувати результати та обґрунтовувати висновки.



Підготовка до занять

Підготовка до практичних занять шляхом опрацювання умов задач, повторення теоретичного матеріалу та алгоритмів аналізу загроз; підготовка до тестувань через вивчення ключових термінів і визначень у сфері банківської безпеки; підготовка до контрольних робіт за кожним змістовним модулем через систематизацію знань, повторення прикладів кіберінцидентів і методів захисту. Очікуваний результат — готовність до активної роботи на заняттях і впевнене виконання контрольних завдань.

Форми контролю знань

1

Поточний контроль

Завдання: аналітичні та розрахункові вправи за темами змістовного модуля у сфері банківської безпеки. Оцінюються регулярність виконання завдань, якість відповідей і рівень засвоєння матеріалу. Поточний контроль формує накопичувальну оцінку протягом семестру.

2

Проміжний контроль

Самостійна робота — комплексне ситуаційне завдання або реферат, що охоплює теми змістовних модулів (теоретичні питання з безпеки банківської діяльності, аналіз загроз і вразливостей, оцінка заходів захисту). Оцінюються повнота відповіді, правильність аналізу та обґрунтованість висновків.

3

Підсумковий контроль — Іспит

Іспит відповідно до навчального плану. Форма проведення — тестування та/або письмові завдання. Підсумкова оцінка враховує результати поточного, проміжного та підсумкового контролю відповідно до встановленої шкали оцінювання: 100-бальна система з переведенням у національну шкалу та ЄКТС.

Методи викладання

Підходи до навчання

Викладання дисципліни «Безпека банківської діяльності» поєднує класичні академічні та інтерактивні методи, що забезпечує формування не лише міцної теоретичної бази, а й практичних навичок, необхідних для майбутньої професійної діяльності у сфері комп'ютерної інженерії та фінансових інформаційних систем. Такий підхід сприяє глибшому розумінню механізмів банківської безпеки, розвитку аналітичного мислення та вмінню застосовувати набуті знання під час вирішення фахових завдань у сфері захисту банківських систем і даних.

Лекції Системне подання теоретичного матеріалу з використанням наочних схем, таблиць і прикладів кіберінцидентів та реальних кейсів банківської безпеки; студенти ведуть конспекти та задають уточнювальні запитання.	Кейс-стаді Аналіз реальних інцидентів безпеки у банківській сфері; студенти виявляють вразливості, пропонують заходи захисту та обґрунтовують висновки щодо запобігання повторним інцидентам.	Практичні задачі Розрахункові та аналітичні вправи за темами (оцінка ризиків, аналіз загроз, моделювання сценаріїв кібератак та методів захисту); відпрацювання алгоритмів вирішення задач безпеки.
Дискусії Обговорення актуальних проблем кібербезпеки банків України (сучасні кіберзагрози, захист від DDoS-атак, протидія фішингу); розвиток критичного мислення та аргументації.	Робота з нормативними документами Опрацювання Закону «Про банки і банківську діяльність», постанов НБУ щодо фінансового моніторингу, вимог законодавства у сфері кіберзахисту; формування навичок роботи з правовою базою.	Самостійне дослідження Підготовка аналітичних записок, міні-рефератів і презентацій з питань захисту банківських інформаційних систем; розвиток навичок самостійного пошуку та систематизації інформації.
Тестування та опитування Перевірка рівня засвоєння матеріалу після кожної теми; формування навичок чіткого та лаконічного формулювання відповідей у сфері банківської безпеки.		
 Усі методи спрямовані на формування компетентностей, передбачених освітньою програмою «Фінанси, банківська справа та страхування в управлінських інформаційних системах і технологіях» спеціальності 123 «Комп'ютерна інженерія».		

Рекомендована література та ресурси

1. Усік П. С., Буравченко К. О. Безпека банківських систем : навч. посіб. — Кропивницький : ЦНТУ, 2022. — 194 с.
2. Закон України «Про банки і банківську діяльність» від 07.12.2000 № 2121-III (зі змінами). — URL: <https://zakon.rada.gov.ua/laws/show/2121-14>
3. Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» від 06.12.2019 № 361-IX (зі змінами). — URL: <https://zakon.rada.gov.ua/laws/show/361-20>
4. Гудзь О. Є., Захаржевська А. А. Управління ризиками підприємств в умовах цифровізації : навч. посіб. — Кропивницький : Видавець Лисенко В. Ф., 2023. — 176 с.
5. Борисова Л., Волкова М. Управління банківськими ризиками в умовах воєнного стану в Україні. Економіка та суспільство. — 2024. — № 67. — DOI: <https://doi.org/10.32782/2524-0072/2024-67-113>
6. Постанова НБУ від 19.05.2020 № 65 «Про затвердження Положення про здійснення банками фінансового моніторингу» (зі змінами, редакція від 08.10.2024). — URL: <https://zakon.rada.gov.ua/go/v0065500-20>
7. Фінансова безпека банківських установ в умовах цифровізації. Економіка та суспільство. — 2024. — № 60. — DOI: <https://doi.org/10.32782/2524-0072/2024-60-117>
8. Усік П. С., Смірнова Т. В., Буравченко К. О. та ін. Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту. Кібербезпека: освіта, наука, техніка. — 2025. — Т. 1. — № 29. — С. 704–716. — URL: <https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/930>
9. Петик Л. О., Кравченко Б. О. Управління ризиками у банківській сфері. Економіка і регіон. — 2024. — № 3(34). — С. 122–132.
10. Попов О. Г. Теоретичні основи забезпечення банківської безпеки держави. Економіка, управління та адміністрування. — 2023. — № 3(105). — С. 195–202.
11. Стойко О. Я., Дема Д. І. Фінанси : підручник. — Житомир : Університет «Полісся», 2024. — 317 с.
12. Hudoliy Yu. S., Andriiets T. R. Zabezpechennia kiberbezpeky bankivskoi systemy Ukrainy u period voiennoho stanu. Ekonomichna bezpeka: derzhava, rehion, pidpriemstvo : materialy VII Mizhnar. nauk.-prakt. Internet-konf. — Poltava, 2023. — S. 58–61.
13. Постанова НБУ від 05.09.2023 № 110 «Про затвердження Змін до Положення про здійснення банками фінансового моніторингу». — URL: <https://bank.gov.ua/ua/news/all/vstanovleno-dodatkovі-vimogi-schodo-zdiysnennya-bankami-finansovogo-monitoringu>
14. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII (зі змінами). — URL: <https://zakon.rada.gov.ua/laws/show/2163-19>
15. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР (зі змінами). — URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>
16. Офіційний сайт Національного банку України. — URL: <https://bank.gov.ua/>
17. Офіційний сайт Верховної Ради України. — URL: <https://zakon.rada.gov.ua/>
18. Офіційний сайт Державної служби фінансового моніторингу України. — URL: <https://sdfm.gov.ua/>
19. Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України. — URL: <https://cip.gov.ua/>
20. Офіційний сайт Міністерства цифрової трансформації України. — URL: <https://thedigital.gov.ua/>
21. Офіційний сайт Кабінету Міністрів України. — URL: <https://www.kmu.gov.ua/>
22. Офіційний сайт Міністерства фінансів України. — URL: <https://mof.gov.ua/>
23. Банківська система : навч. посіб. у схемах і таблицях. — Київ, 2024.
24. Журнал «Економіка та суспільство» (електронне видання). — URL: <https://economyandsociety.in.ua/>
25. Журнал «Кібербезпека: освіта, наука, техніка» (електронне видання). — URL: <https://www.csecurity.kubg.edu.ua/>