НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

Навчально-науковий інститут фінансів, економіки, управління та права
Кафедра фінансів, банківського бізнесу та оподаткування

ЗАТВЕРДЖЕНО
Проректор з науково-педагогічної роботи
_____ Богдан КОРОБКО
«__» _____ 2026 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ЗАХИСТ ФІНАНСОВОЇ ІНФОРМАЦІЇ»

(назва навчальної дисципліни)

Підготовки: Магістр
(назва ступеня вищої освіти)

Освітньої програми: Фінанси, банківська справа та страхування
(назва освітньої програми)

Спеціальності: D2 Фінанси, банківська справа, страхування та фондовий ринок
(код і назва спеціальності)

Полтава
2026 рік

Робоча програма навчальної дисципліни «Захист фінансової інформації» розроблена для здобувачів вищої освти спеціальності D2 Фінанси, банківська справа, страхування та фондовий ринок другого (магістерського) рівня вищої освіти.
Складена відповідно до освітньо-професійної програми «Фінанси, банківська справа та страхування» другого (магістерського) рівня вищої освіти 2026 року.

Розробник: Баран А., доктор філософії з права, доцент кафедри публічного управління, адміністрування та права

Погоджено

Гарант освітньої програми _____ Людмила СВИСТУН

Робоча програма затверджена на засіданні кафедри публічного управління, адміністрування та права

Протокол від «27» серпня 2026 року № 1

Завідувач кафедри публічного управління, адміністрування та права

_____ Інна КУЛЬЧІЙ

«27» серпня 2026 року

Схвалено навчально-методичною комісією навчально-наукового інституту фінансів, економіки, управління та права

Протокол від «28» серпня 2026 року № 1

Голова навчально-методичної комісії _____ Євгенія КАРПЕНКО

«28» серпня 2026 року

© Баран А., 2026 рік
© Національний університет
імені Юрія Кондратюка, 2026 рік

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="3">Найменування показників</td><td rowspan="3">Галузь знань, спеціальність, ступінь вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td colspan="2">форма здобуття освіти</td></tr>
<tr><td>денна</td><td>заочна</td></tr>
<tr><td>Кількість кредитів – 3</td><td rowspan="2">Галузь знань
D Бізнес, адміністрування та право</td><td colspan="2" rowspan="2">вибіркова</td></tr>
<tr><td>Загальна кількість годин – 90</td></tr>
<tr><td rowspan="2">Модулів – 1</td><td rowspan="4">Спеціальність
D2 Фінанси, банківська справа, страхування та фондовий ринок</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">1-й</td></tr>
<tr><td rowspan="2">Змістових модулів – 2</td><td colspan="2">Семестр</td></tr>
<tr><td colspan="2">2-й</td></tr>
<tr><td rowspan="11">Індивідуальне завдання – не передбачено</td><td rowspan="11">Ступінь вищої освіти

другий (магістерськкий)</td><td colspan="2">Лекції</td></tr>
<tr><td>12 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>12 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>66 год.</td><td>82 год.</td></tr>
<tr><td colspan="2">Індивідуальна робота:
0 год.</td></tr>
<tr><td colspan="2">Вид контролю: диференційований залік</td></tr>
</table>

Примітка.
Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми здобуття освіти – 24/66
для заочної форми здобуття освіти – 8/82

2. Мета навчальної дисципліни

Метою викладання навчальної дисципліни «Захист фінансової інформації» є формування у здобувачів системи знань і практичних умінь щодо правового режиму фінансової інформації, банківської, комерційної та професійної таємниці, організації захисту персональних даних і кібербезпеки фінансових операцій, управління інформаційними ризиками на рівні суб'єкта господарювання та реагування на інциденти витоку даних як складової фінансової безпеки бізнесу.

Вивчення дисципліни передбачає формування та розвиток компетентностей, визначених освітньою програмою, зокрема:

– Здатність розв'язувати складні задачі і проблеми у професійній діяльності або у процесі навчання у сфері фінансів, банківської справи та страхування, що передбачає проведення досліджень та/або здійснення інновацій і характеризується невизначеністю умов і вимог.

– Вміння виявляти, ставити та вирішувати проблеми.

– Здатність приймати обґрунтовані рішення.

– Здатність діяти на основі етичних міркувань (мотивів).

– Здатність до пошуку, використання та інтерпретації інформації, необхідної для вирішення професійних і наукових завдань у сфері фінансів, банківської справи та страхування.

– Здатність застосовувати теоретичні знання, практичні навички та інструментарій антикризового управління для оцінювання, забезпечення та підвищення рівня фінансової безпеки в умовах ризиків і загроз.

3. Передумови для вивчення дисципліни

Передумовами для вивчення навчальної дисципліни є попередньо опановані дисципліни другого (магістерського) рівня вищої освіти.

4. Очікувані результати навчання з дисципліни

Результатами вивчення дисципліни є формування програмних результатів освітньої програми:

– Відшуковувати, обробляти, систематизувати та аналізувати інформацію, необхідну для вирішення професійних та наукових завдань у сфері фінансів, банківської справи та страхування.

– Вирішувати етичні дилеми з опорою на норми закону, етичні принципи та загальнолюдські цінності.

– Здійснювати діагностику і моделювання фінансової діяльності суб'єктів господарювання.

– Обґрунтовувати вибір варіантів управлінських рішень у сфері фінансів, банківської справи та страхування й оцінювати їх ефективність з урахуванням цілей, наявних обмежень, законодавчих та етичних аспектів.

– Вміти застосовувати теоретичні знання, практичні навички та інструментарій антикризового управління для оцінювання, забезпечення та підвищення рівня фінансової безпеки в умовах ризиків і загроз.

Здобувач повинен знати поняття і види фінансової інформації, режими банківської, комерційної та професійної таємниці, вимоги законодавства про захист персональних даних і кібербезпеку; уміти класифікувати дані, виявляти інформаційні ризики, формувати політику захисту інформації на підприємстві та оформлювати реагування на інцидент у межах закону.

5. Критерії оцінювання результатів навчання

Критерієм успішного проходження здобувачем освіти підсумкового оцінювання може бути досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом вивчення навчальної дисципліни.

Мінімальний порогів рівень оцінки варто визначати за допомогою якісних критеріїв і трансформувати в мінімальну позитивну оцінку числової (рейтингової) шкали.

Сума балів	Значення ЄКТС	Оцінка за національною шкалою	Критерій оцінювання	Рівень компетентності
90 – 100	**A**	**Відмінно**	Здобувач демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Власні пропозиції Здобувача в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін.	**Високий**, що повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни.
82 – 89	**B**	**Добре**	Здобувач демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною.	**Достатній**, що забезпечує Здобувачу самостійне вирішення основних практичних задач.
74 - 81	**C**	**Добре**	Здобувач загалом добре володіє матеріалом, знає основні положення матеріалу, що відповідають робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та використовує для рішення характерних/типових практичних завдань на професійному рівні. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають ускладнення.	**Достатній**, конкретний рівень, за вивченим матеріалом робочої програми дисципліни.
64 - 73	**D**	**Задовільно**	Здобувач засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.	**Середній**, що забезпечує достатньо надійний рівень відтворення основних положень дисципліни.
60 –	**E**	**Достатньо**	Здобувач засвоїв основний теоретичний	**Середній,** що є

63			матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. володіє основними положеннями на рівні, який визначається як мінімально допустимий. Правила вирішення практичних завдань з використання м основних теоретичних положень пояснюються з труднощами. Виконання практичних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	мінімально допустимим у всіх складових навчальної дисципліни.
35 - 59	**FX**	**Незадовільно** з можливістю повторного складання екзамену/ заліку	Здобувач може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни Здобувач виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у здобувача відсутні.	**Низький**, не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни.
0 – 34	**F**	**Незадовільно** з обов'язковим повторним вивченням дисципліни	Здобувач повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Здобувач не допущений до здачі екзамену/заліку.	**Незадовільний**, Здобувач не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни.

6. Засоби діагностики результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання можуть бути:
1) поточний контроль
• усне опитування
• виконання практичних робіт
• виконання завдань самостійної роботи
• тестування
2) модульний контроль (тестування)
3) підсумковий контроль
• диференційований залік

7. Програма навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1. ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ЗАСАДИ ЗАХИСТУ ФІНАНСОВОЇ ІНФОРМАЦІЇ

Тема 1. Поняття, види та правовий режим фінансової інформації

Поняття інформації та фінансової інформації. Відкрита, конфіденційна, службова і таємна інформація. Банківська таємниця, комерційна таємниця, професійна таємниця аудитора, адвоката, нотаріуса. Фінансова звітність як об'єкт охорони. Відмінність режиму доступу від режиму захисту. Принципи законності, пропорційності, мінімізації даних і підзвітності. Кримінальна, адміністративна та цивільно-правова відповідальність за незаконне збирання, використання і розголошення фінансової інформації.

Практичне заняття № 1.

Тема 2. Нормативно-правове та інституційне забезпечення захисту фінансової інформації

Конституція України. Закони України «Про інформацію», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних», «Про банки і банківську діяльність», «Про бухгалтерський облік та фінансову звітність в Україні», «Про платіжні послуги», «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення». Конвенція 108+, Загальний регламент про захист даних, акти Європейського Союзу щодо цифрової операційної стійкості. Національний банк України, Національна комісія з цінних паперів та фондового ринку, Державна служба спеціального зв'язку та захисту інформації України, Уповноважений Верховної Ради України з прав людини, Державна податкова служба, Державна служба статистики, Державна служба фінансового моніторингу. Галузеві вимоги Національного банку України до кіберстійкості банків і первинного фінансового моніторингу. Взаємодія регуляторів і суб'єктів господарювання.

Практичне заняття № 2.

Тема 3. Організація захисту фінансової інформації та перевірка контрагента (OSINT, Orbis)

Політика інформаційної безпеки. Класифікація активів і даних. Розмежування доступу, принцип службової необхідності. Ролі власника інформації, адміністратора безпеки, користувача. Договірні застереження про конфіденційність. Інвентаризація інформаційних систем. Карта інформаційних ризиків. Взаємодія підрозділів інформаційних технологій, комплаєнсу, юридичної служби та служби безпеки. Перевірка контрагента як елемент організаційного захисту. Законні джерела: Єдиний державний реєстр, Єдиний реєстр судових рішень, санкційні переліки, публічна фінансова звітність. База Orbis: фінансова звітність, структура власності, кінцеві бенефіціарні власники, керівництво, судові спори, показники кредитоспроможності, зв'язки між особами та компаніями. Збір інформації з відкритих джерел для оцінки фінансової стійкості та репутаційних ризиків. Правові й етичні межі OSINT.

Практичне заняття № 3.

ЗМІСТОВИЙ МОДУЛЬ 2. ПЕРСОНАЛЬНІ ДАНІ, КІБЕРБЕЗПЕКА ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ

Тема 4. Захист персональних даних у фінансовій сфері

Персональні дані клієнта банку, страховика, учасника фондового ринку. Правові підстави обробки: згода, договір, законний інтерес, виконання обов'язку суб'єкта первинного фінансового моніторингу. Права суб'єкта даних. Транскордонна передача. Відповідальна особа з питань захисту персональних даних. Відмінності Закону України «Про захист персональних даних» і Загального регламенту про захист даних. Типові порушення: надмірний збір, зберігання «про запас», передача третім особам без підстави. Співвідношення відкритих джерел, Orbis і режиму персональних даних під час ідентифікації клієнта.

Практичне заняття № 4.

Тема 5. Кібербезпека цифрових фінансових послуг, інциденти та розслідування витоків

Вимоги до захисту платіжних даних. Міжнародний стандарт захисту даних платіжних карток як орієнтир для еквайрингу та інтернет-еквайрингу. Багатофакторна автентифікація. Фішинг, соціальна інженерія, компрометація облікових записів. Хмарні сервіси: розподіл відповідальності. Резервне копіювання та безперервність діяльності. Класифікація загроз:

зовнішня атака, внутрішній порушник, помилка персоналу, ланцюг постачання. Ознаки інциденту. Повідомлення регулятора та постраждалих осіб. Внутрішнє розслідування: фіксація, збереження доказів, межі збору інформації. Допустиме використання відкритих джерел і спеціалізованих баз, зокрема Orbis, під час розслідування. Взаємодія з урядовою командою реагування на комп'ютерні надзвичайні події України, Національним банком України та правоохоронними органами. Відновлення режиму захисту.

Практичне заняття № 5.

Тема 6. Захист фінансової інформації в умовах воєнного стану та міжнародні стандарти

Обіг фінансової інформації під час воєнного стану. Резервні майданчики, виведення критичних систем, обмеження оприлюднення чутливих даних. ISO/IEC 27001, рамка кібербезпеки Національного інституту стандартів і технологій США, вимоги Європейського Союзу до цифрової операційної стійкості. Документування системи захисту та оцінка відповідності. Етичні межі моніторингу працівників і клієнтів. OSINT і перевірка контрагента в умовах санкційних та воєнних ризиків.

Практичне заняття № 6.

8. Структура навчальної дисципліни

а) для денної форми здобуття освіти

Назви змістових модулів і тем	Кількість годин					
	Усього	у тому числі				
		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7
Змістовий модуль 1. Правові та організаційні засади захисту фінансової інформації						
Тема 1. Поняття, види та правовий режим фінансової інформації	15	2	2	-	-	11
Тема 2. Нормативно-правове та інституційне забезпечення захисту фінансової інформації	15	2	2	-	-	11
Тема 3. Організація захисту фінансової інформації та перевірка контрагента (OSINT, Orbis)	15	2	2	-	-	11
Разом за змістовним модулем 1	**45**	**6**	**6**	-	-	**33**
Змістовий модуль 2. Персональні дані, кібербезпека та реагування на інциденти						
Тема 4. Захист персональних даних у фінансовій сфері	15	2	2	-	-	11
Тема 5. Кібербезпека цифрових фінансових послуг, інциденти та розслідування витоків	15	2	2	-	-	11
Тема 6. Захист фінансової інформації в умовах воєнного стану та міжнародні стандарти	15	2	-	-	-	11
Разом за змістовним модулем 2	**45**	**6**	**6**	-	-	**33**
Усього годин	**90**	**12**	**12**	-	-	**66**

б) для заочної форми здобуття освіти

Назви змістових модулів і тем	Кількість годин					
	Усього	у тому числі				
		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7
Змістовий модуль 1. Правові та організаційні засади захисту фінансової інформації						
Тема 1. Поняття, види та правовий режим фінансової інформації	15	-	-	-	-	15
Тема 2. Нормативно-правове та інституційне забезпечення захисту фінансової інформації	15	-	-	-	-	15
Тема 3. Організація захисту фінансової інформації та перевірка контрагента (OSINT, Orbis)	15	2	2	-	-	11
Разом за змістовним модулем 1	**45**	**2**	**2**	-	-	**41**
Змістовий модуль 2. Персональні дані, кібербезпека та реагування на інциденти						
Тема 4. Захист персональних даних у фінансовій сфері	15	-	-	-	-	15
Тема 5. Кібербезпека цифрових фінансових послуг, інциденти та розслідування витоків	15	-	-	-	-	15
Тема 6. Захист фінансової інформації в умовах воєнного стану та міжнародні стандарти	15	2	2	-	-	11
Разом за змістовним модулем 2	**45**	**2**	**2**	-	-	**41**
Усього годин	**90**	**4**	**4**	-	-	**82**

9. Перелік питань для семінарських занять

№ з/п	Тема заняття та перелік питань	Кількість	
		годин для денної форми	для заочної форми
	Семінарські заняття не передбачені*	-	-

10. Перелік питань для практичних занять

№ з/п	Тема заняття та перелік питань	Кількість годин	
		для денної форми	для заочної форми
Змістовий модуль 1. Правові та організаційні засади захисту фінансової інформації			
1	**Тема 1. Поняття, види та правовий режим фінансової інформації** 1. Ознаки фінансової інформації та підстави її охорони. 2. Розмежування відкритої, конфіденційної, службової і таємної інформації на прикладі банку та страховика. 3. Відмінність банківської таємниці, комерційної таємниці і професійної таємниці аудитора, адвоката, нотаріуса. 4. Співвідношення режиму доступу і режиму захисту на прикладі фінансової звітності. 5. Застосування принципів законності, пропорційності, мінімізації даних і підзвітності під час збирання фінансової інформації. 6. Розмежування кримінальної, адміністративної та цивільно-правової відповідальності за незаконне збирання, використання і розголошення фінансової інформації.	2	-
2	**Тема 2. Нормативно-правове та інституційне забезпечення захисту фінансової інформації** 1. Конституційні межі збирання і поширення фінансової інформації. 2. Співвідношення Законів України «Про інформацію», «Про доступ до публічної інформації» і «Про захист інформації в інформаційно-комунікаційних системах». 3. Обов'язки щодо фінансової інформації за законами «Про банки і банківську діяльність», «Про бухгалтерський облік та фінансову звітність в Україні» і «Про платіжні послуги». 4. Роль законодавства про фінансовий моніторинг у захисті фінансової інформації. 5. Розподіл повноважень Національного банку України, НКЦПФР, Держспецзв'язку, Уповноваженого Верховної Ради України з прав людини, ДПС, Держстату і Держфінмоніторингу. 6. Галузеві вимоги Національного банку України до кіберстійкості банків і завдання внутрішньої служби безпеки.	2	-
3	**Тема 3. Організація захисту фінансової інформації та перевірка контрагента (OSINT, Orbis)** 1. Склад політики інформаційної безпеки фінансової установи. 2. Класифікація активів і даних та розмежування доступу за принципом службової необхідності. 3. Розподіл відповідальності власника інформації,	2	2

	адміністратора безпеки і користувача. 4. Договірні застереження про конфіденційність у відносинах з контрагентом і підрядником. 5. Складання карти інформаційних ризиків для типової фінансової операції. 6. Законні джерела перевірки контрагента та межі такого збору. 7. Можливості бази Orbis для оцінки структури власності, кінцевих бенефіціарних власників, кредитоспроможності і зв'язків між особами. 8. Межа між допустимим OSINT і незаконним збиранням інформації.		
	Змістовий модуль 2. Персональні дані, кібербезпека та реагування на інциденти		
4	**Тема 4. Захист персональних даних у фінансовій сфері** 1. Розмежування персональних даних клієнта банку, страховика і учасника фондового ринку та відомостей, що становлять фінансову таємницю. 2. Порівняння згоди, договору, законного інтересу і виконання обов'язку суб'єкта первинного фінансового моніторингу як підстав обробки. 3. Права суб'єкта даних і порядок реагування фінансової установи. 4. Умови допустимості транскордонної передачі персональних даних. 5. Типові порушення: надмірний збір, зберігання «про запас», передача третім особам без підстави, та способи їх уникнення 6. Співвідношення відкритих джерел, Orbis і режиму персональних даних під час ідентифікації клієнта.	2	-
5	**Тема 5. Кібербезпека цифрових фінансових послуг, інциденти та розслідування витоків** 1. Вимоги Закону України «Про платіжні послуги» до захисту платіжних даних. 2. Застосування міжнародного стандарту захисту даних платіжних карток до еквайрингу та інтернет-еквайрингу. 3. Ризики фішингу, соціальної інженерії і компрометації облікових записів та роль багатофакторної автентифікації. 4. Розподіл відповідальності між фінансовою установою і постачальником хмарних послуг. 5. Класифікація загроз: зовнішня атака, внутрішній порушник, помилка персоналу, ланцюг постачання, та ознаки інциденту. 6. Порядок повідомлення регулятора і постраждалих осіб. 7. Внутрішнє розслідування витоку: фіксація, збереження доказів, межі збору інформації, допустиме використання відкритих джерел і Orbis. 8. Межі взаємодії з CERT-UA, Національним банком України і правоохоронними органами після інциденту.	2	-
6	**Тема 6. Захист фінансової інформації в умовах воєнного стану та міжнародні стандарти** 1. Обмеження обігу і оприлюднення фінансової інформації під час воєнного стану. 2. Призначення резервних майданчиків і виведення критичних	2	2

	систем; склад даних, які не залишають на основному майданчику. 3. Порівняння ISO/IEC 27001, рамки кібербезпеки NIST і вимог Європейського Союзу до цифрової операційної стійкості з погляду доцільності впровадження українською фінансовою установою. 4. Документування системи захисту та оцінка її відповідності. 5. Етичні межі моніторингу працівників і клієнтів. 6. Використання OSINT і Orbis для перевірки контрагента в умовах санкційних і воєнних ризиків у правових межах.		
Усього годин		**12**	**4**

11. Перелік питань лабораторних занять

№ з/п	Тема заняття та перелік питань	Кількість годин	
		для денної форми	для заочної форми
	Лабораторні заняття не передбачені*		

12. Самостійна робота

Мета самостійної роботи – навчитися працювати з нормативно-правовими актами, аналітикою Держфінмоніторингу, матеріалами FATF, рішеннями судів і внутрішніми політиками комплаєнсу, формувати висновки щодо системи запобігання на рівні підприємства.

Види самостійної роботи здобувача вищої освіти:

- опрацювання лекційного матеріалу;
- підготовка до практичних занять;
- опрацювання тем курсу, які виносяться на самостійне вивчення, за списками літератури, рекомендованими в робочій навчальній програмі дисципліни;
- підготовка до виконання модульної контрольної роботи (тестування);
- відвідування консультацій (згідно графіку консультацій кафедри);
- підготовка до складання диференційованого заліку за контрольними питаннями.

Питання
для самостійного вивчення здобвачами

№ з/п	Тема заняття та перелік питань	Кількість годин	
		для денної форми	для заочної форми
Тема 1. Поняття, види та правовий режим фінансової інформації			
1	Поняття інформації в Законі України «Про інформацію» та його застосування до фінансової сфери	6	8
2	Фінансова звітність як об’єкт охорони: склад, строки зберігання, коло осіб з доступом	5	7
Тема 2. Нормативно-правове та інституційне забезпечення захисту фінансової інформації			
3	Акти Європейського Союзу щодо цифрової операційної стійкості: предмет регулювання і значення для України.	6	8
4	Внутрішні підрозділи інформаційної безпеки банку, страховика і професійного учасника ринку	5	7
Тема 3. Організація захисту фінансової інформації та перевірка контрагента (OSINT, Orbis)			
5	Інвентаризація інформаційних систем: мета, склад відомостей, періодичність	6	6

6	Взаємодія підрозділів інформаційних технологій, комплаєнсу, юридичної служби та служби безпеки	5	5
Тема 4. Захист персональних даних у фінансовій сфері			
7	Статус і функції відповідальної особи з питань захисту персональних даних	6	8
8	Строки зберігання даних клієнта і підстави їх видалення	5	7
Тема 5. Кібербезпека цифрових фінансових послуг, інциденти та розслідування витоків			
9	Резервне копіювання і забезпечення безперервності діяльності. Відновлення режиму захисту після інциденту: документування і зміна політики доступу	6	8
10	Ознаки компрометації облікового запису працівника фінансової установи. Відмінність інциденту інформаційної безпеки від операційного збою.	5	7
Тема 6. Захист фінансової інформації в умовах воєнного стану та міжнародні стандарти			
11	Особливості обігу фінансової інформації в умовах воєнного стану	6	6
12	Обмеження оприлюднення чутливих відомостей і вимоги щодо прозорості діяльності установи.	5	5
	Усього	**66**	**82**

13. Індивідуальні завдання

Не передбачено планом

14. Методи навчання

При викладанні навчальної дисципліни «Захист фінансової інформації» застосовуються словесні, наочні та практичні методи навчання, які поєднуються з сучасними інтерактивними технологіями. Це сприяє не лише засвоєнню теоретичних знань про правовий режим фінансової інформації, інституційну систему її захисту, організацію захисту на рівні суб'єкта господарювання, обробку персональних даних, кібербезпеку платіжних сервісів і реагування на інциденти, а й формуванню практичних навичок та соціально-комунікативних умінь, необхідних майбутнім фахівцям у сфері фінансів, банківської справи, страхування та забезпечення фінансової безпеки. Для забезпечення ефективності освітнього процесу використовуються сучасні інструменти та обладнання, серед яких мультимедійні засоби (проектор, інтерактивна дошка, комп'ютери, веб-камери, мікрофони), а також спеціалізоване програмне забезпечення. Під час занять застосовуються Microsoft Teams і Zoom для дистанційного навчання та консультацій, система Moodle – для організації навчального процесу, тестування та взаємодії зі здобувачами освіти. Для аналізу сучасної практики захисту фінансової інформації використовуються портал законодавства України, інформаційно-правова система «Ліга:Закон», офіційні ресурси Національного банку України, Національної комісії з цінних паперів та фондового ринку, Державної служби спеціального зв'язку та захисту інформації України, Уповноваженого Верховної Ради України з прав людини, Державної служби фінансового моніторингу України, Державної податкової служби України, Державної служби статистики України, урядової команди реагування на комп'ютерні надзвичайні події України, а також портал відкритих даних. Важливим елементом є робота з відкритими реєстрами, публічною фінансовою звітністю, санкційними переліками та аналітичними платформами перевірки контрагентів (зокрема базою даних Orbis та аналогами) в межах, дозволених законодавством про захист персональних даних і режимами банківської, комерційної та професійної таємниці, а також з електронними бібліотеками (DOAJ, ResearchGate, Національна бібліотека України імені В. І. Вернадського).

Словесні методи навчання застосовуються під час лекцій та практичних занять для формування базових знань. Серед них – розповідь, що дає змогу викладачеві логічно і доступно викладати матеріал із прикладами з практики банків, страховиків і професійних

учасників ринку капіталу; пояснення для розкриття складних категорій (режим доступу і режим захисту, банківська таємниця, персональні дані, інцидент витоку, принцип службової необхідності); бесіда та дискусія, що забезпечують активну взаємодію зі здобувачами. Наочні методи включають демонстрацію схем видів фінансової інформації, інституційної системи захисту, карти інформаційних ризиків установи, моделі розмежування доступу, алгоритму перевірки контрагента та порядку реагування на інцидент.

Практичні методи орієнтовані на формування професійних навичок і включають аналіз відкритих рішень судів у справах про розголошення банківської та комерційної таємниці, розгляд типових порушень законодавства про захист персональних даних, моделювання класифікації інформаційних активів, розробку елементів політики інформаційної безпеки та карти ризиків, розв'язання ситуаційних завдань щодо перевірки контрагента за відкритими державними джерелами та базою даних Orbis, оформлення аналітичного висновку внутрішньої перевірки, а також відпрацювання алгоритму дій при ознаках витоку фінансової інформації. Дисципліна не передбачає відпрацювання способів несанкціонованого збору чи розголошення відомостей; акцент робиться на розпізнаванні ризиків, побудові превентивних механізмів захисту та етично коректній роботі з відкритими джерелами.

Методи, що дозволяють формувати soft skills, ґрунтуються на роботі в малих групах, де здобувачі відпрацьовують командну взаємодію, розподіл ролей між підрозділом інформаційних технологій, комплаєнсом, юридичною службою та службою безпеки і спільне прийняття рішень. Ділові ігри та моделювання професійних ситуацій (надання доступу за принципом службової необхідності, оцінка запиту на розкриття банківської таємниці, підготовка повідомлення регулятора про інцидент, взаємодія з компетентними органами в межах закону), а також дебати й дискусії розвивають навички публічного виступу, аргументації та розв'язання етичних дилем щодо меж моніторингу працівників і клієнтів. Мозковий штурм під час побудови карти інформаційних ризиків стимулює аналітичне мислення, а метод конкретних ситуацій дає змогу опрацьовувати публічно відомі випадки витоків і визначати шляхи відновлення режиму захисту.

Застосування поєднання традиційних і сучасних методів навчання у викладанні дисципліни «Захист фінансової інформації» дає змогу сформувати у здобувачів не лише ґрунтовні теоретичні знання, а й практичні навички класифікації інформації, організації захисту, ідентифікації ризиків витоку, критичне мислення, доброчесність і здатність до аргументованої професійної комунікації, що є важливими для роботи у фінансових установах, службах комплаєнсу та підрозділах інформаційної і фінансової безпеки.

15. Методи контролю

Поточний контроль успішності засвоєнням здобувачами навчального матеріалу може здійснюватися шляхом опитування й оцінювання знань здобувачів під час практичних занять, оцінювання виконання самостійної роботи, тестування або в ході індивідуальних співбесід зі здобувачами під час консультацій. Вибір конкретних форм і методів поточного контролю знань здобувачів залежить від викладача і доводиться до їхнього відома на першому практичному занятті.

Модульний контроль має на меті перевірку засвоєння здобувачами певної сукупності знань та вмінь, що формують відповідний модуль. Модульний контроль реалізується шляхом узагальнення результатів поточного контролю знань і проведення спеціальних контрольних заходів (у формі тестування), проводиться наприкінці кожного змістового модулю за рахунок аудиторних занять. На підставі результатів модульного контролю здійснюється міжсесійний контроль (атестація).

Підсумковий контроль здійснюється у формі диференційованого заліку.

16. Розподіл балів, які отримують здобувачі: Схема нарахування балів* з навчальної дисципліни «Захист фінансової інформації» за видами робіт

а) для здобувачів денної форми здобуття освіти

Види робіт/контролю	Перелік тем					
	Тема 1	Тема 2	Тема 3.	Тема 4.	Тема 5	Тема 6.
	Практичне заняття					
	1	2	3	4	5	6
Усне опитування	4	4	4	4	4	4
Виконання практичних завдань	3	3	3	3	3	3
Тестування	2	2		2	2	
Виконання завдань самостійної роботи	2	2	2	2	2	2
Модульний контроль			4			4
Всього за темами	11	11	13	11	11	13
Диф. залік	**30**					
Всього за результатами вивчення навчальної дисципліни	**100**					

б) для здобувачів заочної форми здобуття освіти

Види робіт/контролю	Перелік тем					
	Тема 1	Тема 2	Тема 3.	Тема 4.	Тема 5	Тема 6.
	Практичне заняття					
			1			2
Усне опитування			10			10
Виконання практичних завдань			10			10
Виконання завдань самостійної роботи	3	3	3	3	3	3
Модульний контроль			6			6
Всього за темами	3	3	29	3	3	29
Диф. залік	**30**					
Всього за результатами вивчення навчальної дисципліни	**100**					

Шкала та критерії оцінювання відповіді за результатами усного опитування:

Бали для форми здобуття освіти		Критерії оцінювання
денної	заочної	
4	10	Питання розкрито повністю, що свідчить про відмінне засвоєння матеріалу відповідно вказаних програмних результатів навчання. Здобуач вільно володіє науково-понятійним апаратом.
2	5	Механічне відтворення матеріалу з деякими помилками, неточності у використанні науково-понятійного апарату.
0	0	Відсутність відповіді на теоретичне питання, що не дає можливість оцінити формування компетентностей та отримання програмних результатів навчання у здобувача вищої освіти.

Шкала та критерії оцінювання виконання практичних завдань:

Бали для форми здобуття освіти		Критерії оцінювання
денної	заочної	
3	10	Завдання практичної роботи виконано в повному обсязі, оформлено належним чином, у висновках відображено здатність до практичного застосування отриманих знань.
1,5	5	Завдання виконано не повністю або з несуттєвими помилками, висновки оформлені, але лише частково розкривають практичне завдання.
0	0	Практична робота не виконана або виконана з суттєвими помилками, висновки відсутні чи не мають практичного значення.

Оцінювання тестування для денної форми здобуття освіти:

- кожна правильна відповідь оцінюється у фіксовану кількість балів *(0,2×10=2);*
- правильність відповідей перевіряється відповідно до ключа тестів.

Шкала та критерії оцінювання виконання завдань самостійної роботи:

Бали для денної форми здобуття освіти	Бали для заочної форми здобуття освіти	Критерії оцінювання
2	3	Виконання завдань самостійної роботи здійснене у повному обсязі, не містить помилок, що дає можливість оцінити формування компетентностей та отримання програмних результатів навчання у здобувача вищої освіти на високому рівні.
1	1,5	Виконання завдань самостійної роботи здійснене не у повному обсязі, містить несуттєві помилки, що дає можливість оцінити рівень формування компетентностей та отримання програмних результатів навчання у здобувача вищої освіти як достатній.
0	0	Завдання самостійної роботи не виконано та/або результати не відповідають поставленим завданням та/або завдання виконано із суттєвими помилками.

Шкала та критерії оцінювання виконання модульного контролю (тестування) для денної форми здобуття освіти:

- кожна правильна відповідь оцінюється у фіксовану кількість балів (0,4×10=4,0);
- правильність відповідей перевіряється відповідно до ключа тестів.

Шкала та критерії оцінювання виконання модульного контролю (тестування) для заочної форми здобуття освіти:

- кожна правильна відповідь оцінюється у фіксовану кількість балів (0,6×10=6,0);
- правильність відповідей перевіряється відповідно до ключа тестів.

Шкала та критерії оцінювання знань здобувачів вищої освіти за результатами складання диф. заліку

Завдання	Бали	Критерії оцінювання
1. Тест ування	0-30	Кожна правильна відповідь оцінюється у фіксовану кількість балів (1×30=30), правильність відповідей перевіряється відповідно до ключа тестів.

Шкала оцінювання: національна та ECTS

100-бальна рейтингова система оцінювання	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою для екзамену, диференційованого заліку, курсового проекту (роботи), практики
90 – 100	**A** – відмінно	**5** – відмінно
82 – 89	**B** – дуже добре	**4** – добре
74 – 81	**C** – добре	
64 – 73	**D** – задовільно	**3** – задовільно
60 – 63	**E** – достатньо	
35 – 59	**FX** – незадовільно з можливістю повторного складання	**2 –** незадовільно
0 – 34	**F** – незадовільно з обов'язковим повторним вивченням дисципліни	

Правила модульно-рейтингового оцінювання знань

Загальна трудомісткість дисципліни – 100 балів, із них:

– при семестровому контролі у вигляді диференційованого заліку на поточний контроль може бути відведено від 70 до 100 балів (для допуску до диференційованого заліку необхідно мати не менше 35 балів поточної успішності).

1. Поточний контроль. Бали, отримані впродовж семестру, за видами навчальної діяльності розподіляються наступним чином (розподіл орієнтовний):

- робота на практичних, заняттях (відповіді на практичних, виконання практичних завдань, а в разі їх пропусків з поважної причини – індивідуальні співбесіди на консультаціях за темами відповідних занять) – до 70 балів.

Присутність на лекціях і практичних заняттях не оцінюється в балах. Пропуски занять підлягають обов'язковому відпрацюванню в індивідуальному порядку під час консультацій. Пропущене заняття має бути відпрацьоване впродовж двох наступних тижнів, при тривалій відсутності зобувача на заняттях з поважної причини встановлюється індивідуальний графік відпрацювання пропусків, але не пізніше початку екзаменаційної сесії.

Здобувач, який повністю виконав програму навчальної дисципліни і отримав достатню рейтингову оцінку (не менше 35 балів у випадку диференційованого заліку), допускається до підсумкового контролю з дисципліни.

2. Підсумковий контроль Підсумковим контролем є диференційований залік. Він здійснюється відповідно до вимог «Положення про організацію освітнього процесу в Національному університеті «Полтавська політехніка імені Юрія Кондратюка»

17. Методичне забезпечення

1. Баран А. Методичні рекомендації для підготовки до практичних занять та самостійної роботи навчальної дисципліни «Захист фінансової інформації» для здобувачів вищої освіти другого (магістерського) рівня вищої освіти за спеціальністю D2 «Фінанси, банківська справа та страхування та фондового ринку». Полтава, 2025, с. 25.

18. Рекомендована література

Базова

1. Gore A. Global Financial Investigations: Forensic Accounting in Practice. London; New York: Routledge, 2025. 206 p. URL: https://www.routledge.com/Global-Financial-Investigations-Forensic-Accounting-in-Practice/Gore/p/book/9781032493763
2. Hopton D. Money Laundering: A Concise Guide for All Business. 2nd ed. London; New York: Routledge, 2009. 232 p. URL: https://www.routledge.com/Money-Laundering-A-Concise-Guide-for-All-Business/Hopton/p/book/9781032838601
3. Naz F., Karim S. (Eds.). Safeguarding Financial Data in the Digital Age. Hershey : IGI Global, 2024. 330 p. URL: https://doi.org/10.4018/979-8-3693-3633-5
4. Білінський Д. О. Правове регулювання публічної фінансової системи : монографія. Харків : Право, 2017. 296 с.
5. Зачосова Н. В. Фінансова безпека: проблеми оперативного та стратегічного управління : монографія. Черкаси, 2019. 160 с.
6. Ковалів М. В., Єсімов С. С., Проць І. М., Скриньковський Р. М., Лозинський Ю. Р. Фінансове право України : навч. посіб. Львів : СПОЛОМ, 2022. 394 с. URL: https://vstup.htek.com.ua/wp-content/uploads/2024/10/11.6-financial.pdf
7. Кравченко О. М. Охорона комерційної таємниці та конфіденційної інформації бізнесу в Україні : наук.-метод. посіб. для бізнесу. Київ : ФОП Жукова І. В., 2025. 275 с. URL: https://perspectives.pp.ua/public/site/print-kravchenko.pdf
8. Латковська Т., Сідор М., Голоядова Т. Фінансове право : навч.-метод. посіб. (для здобувачів вищої освіти). 2-ге вид., доопр. і доп. Одеса : Фенікс, 2023. 140 с. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/dfa9c4b9-b797-4634-98ef-2d1d43d23ad4/content
9. Макаренко А. П. Державний фінансовий контроль : навч. посіб. Запоріжжя : ЗДІА, 2017. 279 с.
10. Макух О. В. Фінансові правовідносини: теорія, сучасний стан і тенденції розвитку : монографія. Харків : Право, 2016. 304 с.
11. Фінансове право : підручник / за ред. М. П. Кучерявенка і О. О. Дмитрик. Харків : Право, 2019. 416 с.
12. Фінансове право : підручник / за ред. Т. Є. Кагановської та М. П. Кучерявенка ; Харків. нац. ун-т ім. В. Н. Каразіна ; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право,

2022. 432 с. URL: https://library.nlu.edu.ua/novi-nadkhodzhennia/item/3066-finansove-pravo.html

13. Фінансове право : підручник / О. О. Дмитрик, Є. О. Алісов, Д. А. Кобильнік та ін. ; за ред. О. О. Дмитрик. Одеса : Юридика, 2022. 466 с. URL: https://dspace.nlu.edu.ua/jspui/handle/123456789/19568

Допоміжна

1. Andrej BARAN Advanced Tools in Financial Investigations: Orbis and Ukraine's Legal Reforms. Council of Europe, 2025. 80 с.

2. Бойко В. В., Мирошниченко А. І. Фінансові правопорушення в системі виконання державного бюджету: правова природа та законодавчі виклики. Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування. 2025. № 17. DOI: https://doi.org/10.54929/2786-5746-2025-17-01-07. URL: https://reposit.nupp.edu.ua/item/19825

3. Бюджетний кодекс України : Закон України від 08.07.2010 р. № 2456-VI. URL: https://zakon.rada.gov.ua/laws/show/2456-17

4. Жигалкевич Ж.М., Кам'янська О.В. Фінансовий менеджмент: навч. посіб. для здобувачів другого (магістерського) рівня вищої освіти спеціальності 073 «Менеджмент». Київ : КПІ ім. Ігоря Сікорського, 2022. 214 с. URL:https://duikt.edu.ua/uploads/l_1598_88405701.pdf

5. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр

6. Мирошниченко А. І. ORBIS як сучасний інструмент забезпечення економічної безпеки суб'єктів господарювання. Геополітика України: історія і сучасність. 2025. № 1 (34). С. 134–142. DOI: https://doi.org/10.24144/2078-1431.2025.1(34).134-142. URL: https://reposit.nupp.edu.ua/handle/PoltNTU/19566

7. Олюха В., Шепелюк В., Юнацький М. Судово-бухгалтерська експертиза та фінансовий моніторинг у боротьбі з економічними злочинами в Україні та ЄС. Наука і техніка сьогодні. 2025. № 3 (44). С. 123–141. DOI: https://doi.org/10.52058/2786-6025-2025-3(44)-123-141

8. Піпко Ю. В. Поняття фінансового правопорушення: проблематика наукового підходу. Право і суспільство. 2023. № 5. С. 142–148. URL: http://pravoisuspilstvo.org.ua/archive/2023/5_2023/22.pdf

9. Податковий кодекс України : Закон України від 02.12.2010 р. № 2755-VI. URL: https://zakon.rada.gov.ua/laws/show/2755-17

10. Про Бюро економічної безпеки України : Закон України від 28.01.2021 р. № 1150-IX. URL: https://zakon.rada.gov.ua/laws/show/1150-20

11. Про запобігання корупції : Закон України від 14.10.2014 р. № 1700-VII. URL: https://zakon.rada.gov.ua/laws/show/1700-18

12. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 06.12.2019 р. № 361-IX. URL: https://zakon.rada.gov.ua/laws/show/361-20

13. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17

14. Про Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів : Закон України від 10.11.2015 р. № 772-VIII. URL: https://zakon.rada.gov.ua/laws/show/772-19

15. Про основні засади здійснення державного фінансового контролю в Україні : Закон України від 26.01.1993 р. № 2939-XII. URL: https://zakon.rada.gov.ua/laws/show/2939-12

16. Фінансовий менеджмент: конспект лекцій : навч. посіб. для здобувачів ступеня магістра за освітньою програмою «Економіка і бізнес» спец. 051 «Економіка» / КПІ ім. Ігоря Сікорського ; уклад.: С. О. Тульчинська. Київ : КПІ ім. Ігоря Сікорського, 2025. –

130 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/53ae6d5f-8a5e-414f-a1b8-e1b0fbfb7afc/content

17. Шевченко Н. В., Мельник С. І.Фінансовий менеджмент : навчальний посібник у схемах і таб-лицях. Львів : Львівський державний університет внутрішніхсправ, 2022. 224 с. URL: https://www.researchgate.net/publication/367023192_Finansovij_menedzment_navcalnij_posibnik_-_Sevcenko_NV_Melnik_SI_VIDANIJ.

19. Інтернет ресурси

1. Сторінка курсу на платформі Moodle URL: https://dist.nupp.edu.ua/course/view.php?id=7540
2. Законодавство України. URL: http://zakon1.rada.gov.ua
3. Міністерство юстиції України. URL: http://www.minjust.gov.ua
4. Національна бібліотека України ім. В. І. Вернадського. URL: http://www.nbuv.gov. ua/
5. Офіційне інтернет-представництво Президента України. URL: http://www.president.gov.ua
6. Офіційний веб-сайт Верховної Ради України. URL: http://portal.rada.gov.ua/
7. Сайт Державної аудиторської служби України. URL: https://dasu.gov.ua/
8. Сайт Державної податкової служби України. URL: https://tax.gov.ua/
9. Сайт Міністерства фінансів України. URL: https://www.mof.gov.ua/uk
10. Сайт Національного банку України. URL: https://bank.gov.ua/
11. Урядовий портал (Кабінет Міністрів України). URL: http://www.kmu.gov.ua
12. Юридична газета. URL: http://www.yur-gazeta.com/
13. Неформальна освіта. Курс «Фінансова грамотність» URL: https://prometheus.org.ua/prometheus-free/finansova-gramotnist-dlya-veteraniv
14. Неформальна освіта. Курс «Управління фінансами для власників і керівників» URL: https://prometheus.org.ua/prometheus-plus/finance-management-leaders/