



Вищий навчальний заклад  
**«НАЦІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ»**  
Факультет економіки та інформаційних технологій  
Кафедра фінансів, обліку та фундаментальних економічних дисциплін

**ЗАТВЕРДЖЕНО**

Декан факультету економіки та  
інформаційних технологій



Ю.М. Неговська

**РОБОЧА ПРОГРАМА**

**ФІНАНСОВО-ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВА**

(назва навчальної дисципліни)

**підготовки** перший (бакалаврський)  
(назва рівня вищої освіти)

**галузі знань** 07 «Управління та адміністрування»  
(шифр і назва галузі знань)

**Спеціальності** 072 «Фінанси, банківська справа та страхування»  
(код і найменування спеціальності)

**освітньо-професійної програми** «Фінанси, банківська справа та страхування»  
(найменування освітньої програми)

**тип дисципліни** вибіркова дисципліна професійної та практичної підготовки

2020 рік

**ПОГОДЖЕНО:**

Гарант освітньої програми



(підпис)

О.М. Антонова  
(прізвище, ініціали)

**РЕКОМЕНДОВАНО:**

Кафедрою фінансів, обліку та  
фундаментальних економічних дисциплін  
протокол № 1 від «28» серпня 2020 року

Завідувача кафедри



(підпис)

Т.М. Сугак  
(прізвище, ініціали)

**Розробники:**

**Антонова Олена Михайлівна** кандидат економічних наук, доцент кафедри фінансів, обліку та фундаментальних економічних дисциплін

## 1. Опис навчальної дисципліни

**Мова навчання:** українська

**Статус дисципліни:** вибіркова дисципліна, професійної та практичної підготовки

**Передумови вивчення навчальної дисципліни:** «Фінансово-економічна безпека підприємства» для здобувачів вищої освіти є вибірковою дисципліною, яка забезпечує формування вмінь, передбачених освітньо-кваліфікаційною характеристикою. Дисципліна вивчається на основі базової загальноекономічної та правової підготовки з таких дисциплін як «Економічна теорія», «Макроекономіка», «Мікроекономіка», «Економіка підприємства», «Менеджменту», «Господарське право» та набуття ними відповідних фахових компетенцій.

Дисципліна є підґрунтям для подальшого вивчення дисциплін, пов'язаних з галузевою специфікою кожної спеціальності. Знання з даної дисципліни дозволять успішно вивчати такі дисципліни, як: «Фінансовий менеджмент», «Стратегічне управління».

**Предметом** вивчення навчальної дисципліни «Фінансово-економічна безпека підприємства» є наукові основи безпеки підприємницької структури, принципи, методи захисту підприємства в умовах ризику та невизначеності, методичні положення щодо формування системи економічної безпеки підприємства, також комп'ютерні технології, що використовуються в області економіки, організації та планування діяльності підприємства та засоби захисту категоризованої економічної інформації.

**Інформаційний обсяг навчальної дисципліни.** На вивчення навчальної дисципліни відводиться 150 годин 5 кредитів ECTS

## 2. Мета та завдання навчальної дисципліни

**Метою** викладання навчальної дисципліни «Фінансово-економічна безпека підприємства» є формування у здобувачів вищої освіти теоретичних знань та практичних навичок економіко-правового характеру щодо розвитку відносин між зацікавленими особами зовнішнього та внутрішнього середовищ в системі управління підприємством з метою підвищення рівня його економічної безпеки в ринковій економіці.

Основними **завданнями** навчальної дисципліни «Фінансово-економічна безпека підприємства» є оволодіння здобувачами вищої освіти знаннями щодо особливостей діяльності та розвитку підприємств в умовах ризику та невизначеності зовнішнього середовища і навичками щодо забезпечення відповідного рівня економічної безпеки підприємства; одержання знань з основоположних принципів побудови та функціонування систем економічної безпеки; одержання знань про механізми забезпечення інформаційної та економічної безпеки, функціональні складові економічної інформації; підготовка здобувача вищої освіти до подальшого поглибленого вивчення спеціальних дисциплін; вироблення навичок самостійного вивчення різних категорій інформації та проведення їх порівняльного аналізу при забезпеченні її інформаційної та економічної безпеки.

## 3. Компетентності та заплановані результати навчання

Дисципліна «Фінансово-економічна безпека підприємства» забезпечує набуття здобувачами вищої освіти **компетентностей:**

### **Загальні компетентності (ЗК):**

- ЗК02. Здатність застосовувати знання у практичних ситуаціях.
- ЗК05. Навички використання інформаційних та комунікаційних технологій.
- ЗК07. Здатність вчитися і оволодівати сучасними знаннями.
- ЗК08. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
- ЗК09. Здатність бути критичним і самокритичним.

### **Спеціальні (фахові) компетентності:**

- СК03. Здатність до діагностики стану фінансових систем (державні фінанси, у тому числі бюджетна та податкова системи, фінанси суб'єктів господарювання, фінанси домогосподарств, фінансові ринки, банківська система та страхування).
- СК05. Здатність застосовувати знання законодавства у сфері монетарного, фіскального регулювання та регулювання фінансового ринку.
- СК06. Здатність застосовувати сучасне інформаційне та програмне забезпечення для отримання та обробки даних у сфері фінансів, банківської справи та страхування.
- СК09. Здатність здійснювати ефективні комунікації.
- СК10. Здатність визначати, обґрунтовувати та брати відповідальність за професійні рішення.

#### **Програмні результати навчання (ПР)**

- ПР04. Знати механізм функціонування державних фінансів, у т.ч. бюджетної та податкової систем, фінансів суб'єктів господарювання, фінансів домогосподарств, фінансових ринків, банківської системи та страхування.
- ПР05. Володіти методичним інструментарієм діагностики стану фінансових систем (державні фінанси, у т.ч. бюджетна та податкова системи, фінанси суб'єктів господарювання, фінанси домогосподарств, фінансові ринки, банківська система та страхування).
- ПР08. Застосовувати спеціалізовані інформаційні системи, сучасні фінансові технології та програмні продукти.
- ПР09. Формувати і аналізувати фінансову звітність та правильно інтерпретувати отриману інформацію.
- ПР10. Ідентифікувати джерела та розуміти методологію визначення і методи отримання економічних даних, збирати та аналізувати необхідну фінансову інформацію, розраховувати показники, що характеризують стан фінансових систем.
- ПР13. Володіти загальнонауковими та спеціальними методами дослідження фінансових процесів.
- ПР16. Застосовувати набуті теоретичні знання для розв'язання практичних завдань та змістовно інтерпретувати отримані результати.

#### 4. Структура навчальної дисципліни

Назви змістових модулів і тем	Обсяг у годинах											
	денна форма					заочна форма						
	усього	у тому числі					усього	у тому числі				
		л	сем	пз	лаб	с.р		л	сем	пз	лаб	с.р
1	2	3	4	5	6	7	8	9	10	11	12	13
<b>Змістовий модуль 1. Організація фінансово-економічної безпеки підприємства</b>												
Тема 1. Поняття та основні категорії фінансово-економічної безпеки	12	2	2	-	-	8	14	1	-	-	-	13
Тема 2. Індикатори та складові фінансово-економічної безпеки підприємства	18	8	6	-	-	4	18	2	2	-	-	14
Тема 3. Системи фінансово-економічної безпеки підприємства	16	6	4	-	-	6	16	2	2	-	-	12
Тема 4. Особливості діяльності служби безпеки підприємства	16	6	4	-	-	6	16	1	-	-	-	15
Тема 5. Недобросовісна конкуренція та захист комерційної таємниці	16	6	2	-	-	8	16	2	-	-	-	14
Тема 6. Ділова розвідка	12	4	2	-	-	6	12	1	-	-	-	11
<b>Разом за змістовим модулем 1</b>	<b>90</b>	<b>32</b>	<b>20</b>	<b>-</b>	<b>-</b>	<b>38</b>	<b>92</b>	<b>9</b>	<b>4</b>	<b>-</b>	<b>-</b>	<b>77</b>
<b>Змістовий модуль 2. Основи інформаційної безпеки</b>												
Тема 7. Загальні принципи безпеки інформаційних технологій	12	4	-	-	-	8	12	1	-	-	-	11
Тема 8. Канали витоку інформації	12	4	-	-	-	8	12	1	-	-	-	11
Тема 9. Організація інформаційної безпеки на підприємстві	12	4	-	-	-	8	12	1	-	-	-	11
<b>Разом за змістовим модулем 2</b>	<b>36</b>	<b>12</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>24</b>	<b>36</b>	<b>3</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>33</b>
<b>Змістовий модуль 3. Особливості застосування ІБ у бізнесі</b>												
Тема 10. Організація інформаційної безпеки комп'ютерної мережі	12	4	-	-	-	8	12	1	-	-	-	11
Тема 11. Правові основи інформаційної безпеки	12	4	-	-	-	8	12	1	-	-	-	11
<b>Разом за змістовим модулем 3</b>	<b>24</b>	<b>8</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>16</b>	<b>22</b>	<b>2</b>	<b>-</b>	<b>-</b>	<b>-</b>	<b>22</b>
<b>Усього годин</b>	<b>150</b>	<b>52</b>	<b>20</b>	<b>-</b>	<b>-</b>	<b>78</b>	<b>150</b>	<b>14</b>	<b>4</b>	<b>-</b>	<b>-</b>	<b>132</b>

#### 5. Зміст програми навчальної дисципліни

*Змістовий модуль 1. Організація фінансово-економічної безпеки підприємства*

## **Тема 1. Поняття та основні категорії фінансово-економічної безпеки**

Поняття економічної безпеки. Класифікація видів економічної безпеки зовнішнього та внутрішнього середовища системи. Сутність продовольчої, технологічної та соціальної безпеки на національному рівні. Проблеми співвідношення економічної безпеки особистості, підприємства, регіону та держави. Стан безпеки організації. Безпека як функція організації. Джерела негативних впливів на економічну безпеку підприємства. Основна мета економічної безпеки підприємства. Основні функціональні цілі економічної безпеки. Види заходів безпеки: загальні та спеціальні. Економічна безпека підприємства на різних стадіях життєвого циклу. Проблеми сучасного ринку, які обумовлюють необхідність економічно безпечного функціонування підприємства.

Об'єкт та предмет економічної безпеки. Групи суб'єктів економічної безпеки.

Чинники, що формують відповідний рівень економічної безпеки: безпосередні чинники виробництва, стабільний попит на продукцію, надійність постачальників, зовнішня конкуренція, державне економічне регулювання діяльності підприємства, надійний захист комерційної таємниці, компетентність керівництва підприємства.

Види загроз економічній безпеці за місцем, природою, ймовірністю, сферами виникнення, за наслідками, за відношенням до людської діяльності, за об'єктами посягань, за можливістю прогнозування. Економічні загрози. Фізичні загрози. Психологічно-інформаційні загрози. Ризики як фактори загроз економічній безпеці підприємства. Зовнішні та внутрішні джерела загроз: кримінальні структури, промислове шпигунство, фірми-розвідники, конкуренти, корумповані представники органів влади, правоохоронних органів, контролюючих органів, засобів масової інформації, керівники організації, менеджери середньої ланки, працівники підприємства, працівники служби безпеки.

## **Тема 2. Індикатори та складові фінансово-економічної безпеки підприємства**

Структура економічної безпеки підприємства. Внутрішньовиробничі (фінансова, кадрова, технологічна, правова, інформаційна, екологічна, силова) та позавиробничі (ринкова та інтерфейсна) складові економічної безпеки. Поняття індикаторів економічної безпеки підприємства.

Фінансова складова як внутрішньовиробнича функціональна складова економічної безпеки. Свідчення про послаблення фінансової складової. Типова послідовність дій щодо забезпечення фінансової складової економічної безпеки. Показники фінансової складової економічної безпеки. Області фінансової стійкості.

Безпека підприємства в інтелектуальній та кадровій сферах. Характеристика інтелектуальної складової. Особливості кадрової складової. Внутрішні та зовнішні загрози порушення інтелектуальної та кадрової складових економічної безпеки підприємства. Послідовність заходів щодо забезпечення інтелектуальної та кадрової складової. Показники інтелектуальної та кадрової складової. Кадри як внутрішня загроза безпеці підприємства. Зловживання з боку персоналу: дрібні разові розкрадання, систематичні розкрадання, «внутрішнє підприємництво». Функції та завдання кадрової служби в сфері забезпечення економічної безпеки.

Техніко-технологічна складова економічної безпеки підприємства. Загрози послаблення техніко-технологічної безпеки підприємства. Етапи забезпечення техніко-технологічна складова економічної безпеки. Показники техніко-технологічної складової економічної безпеки підприємства.

Політико-правова безпека підприємства. Основні причини виникнення внутрішніх і зовнішніх негативних впливів на політико-правову безпеку. Особливості процесу забезпечення політико-правової складової економічної безпеки. Індикатори оцінки рівня політико-правової безпеки підприємства.

Інформаційна складова безпеки. Показники інформаційної складової. Рівні інформаційної безпеки. Побудова системи інформаційної безпеки. Оцінювання інформаційних ризиків.

Безпека підприємства в екологічній сфері. Алгоритм процесу забезпечення екологічної складової економічної безпеки. Показники безпеки підприємства в екологічній сфері. Рівні екологічної безпеки.

Силова безпека підприємства. Негативні дії щодо силової складової. Показники силової безпеки підприємства. Послідовність дій щодо організації силової складової економічної безпеки.

Ринкова складова економічної безпеки підприємства. Свідчення ослаблення ринкової безпеки. Показники безпеки підприємства на ринку. Організація служби маркетингу як відповідального підрозділу за забезпечення ринкової складової.

Інтерфейсна складова економічної безпеки підприємства. Умови взаємодії з економічними контрагентами. Роль служби маркетингу в забезпеченні інтерфейсної складової.

### **Тема 3. Система фінансово-економічної безпеки підприємства**

Поняття та основні елементи системи економічної безпеки підприємства. Організація системи безпеки підприємства. Завдання, що вирішуються системою гарантування безпеки. Політика безпеки підприємства: поняття, цілі та складові. Програма гарантування безпеки підприємства. Особливості стратегічного управління в сфері безпеки. Тактика гарантування безпеки. Засоби гарантування безпеки: технічні, організаційні, фінансові, інформаційні, правові, кадрові, інтелектуальні. Механізм реалізації безпеки. Функції системи безпеки. Принципи забезпечення економічної безпеки. Режим функціонування системи економічної безпеки.

Концепція безпеки підприємства. Вимоги, що висуваються до концепції безпеки підприємства. Структура концепції економічної безпеки підприємства: опис проблемної ситуації в сфері безпеки підприємства, механізм гарантування безпеки, заходи щодо реалізації заходів безпеки.

### **Тема 4. Особливості діяльності служби безпеки підприємства**

Служба безпеки як підсистема підприємства. Мета та завдання служби безпеки. Типові функції служби безпеки підприємства. Процедура створення та ліквідації служби безпеки підприємства. Кадрове, матеріально-технічне та правове забезпечення діяльності служби безпеки підприємства.

Структура та особливості управління діяльністю служби безпеки підприємства. Особливості підбору персоналу для роботи у службі безпеки. Складові служби безпеки підприємства: сектор охорони, режиму, технічного захисту, оперативної роботи. Завдання служби безпеки щодо гарантування режиму та охорони. Перевірка роботи служби безпеки. Особливості використання послуг зовнішніх охоронних організацій як альтернатива створення служби безпеки підприємства.

### **Тема 5. Недобросовісна конкуренція та захист комерційної таємниці**

Комерційна таємниця підприємства. Відомості, що становлять комерційну таємницю підприємства. Правові аспекти комерційної таємниці.

Механізм визначення переліку інформації, що становить комерційну таємницю. Досвід іноземних підприємств щодо визначення комерційної таємниці. Тотальний, плагіаторський, аналітичний та експертний способи визначення комерційної таємниці.

Поняття та особливості недобросовісної конкуренції. Види недобросовісної конкуренції. Форми недобросовісної конкуренції: економічне, пряме фізичне придушення, промислове шпигунство.

Економічне шпигунство: поняття та особливості. Форми та методи економічного шпигунства. Шпигунство як спосіб добування інформації, що становить комерційну таємницю.

Налагодження охорони комерційної таємниці на підприємстві. Контроль персоналу. Використання технічних засобів.

### **Тема 6. Ділова розвідка**

Поняття ділової розвідки. Історія виникнення та напрями розвитку ділової розвідки. Специфіка трактування ділової розвідки та її відмінність від промислового шпигунства.

Особливості ділової розвідки. Класифікація ділової розвідки за предметом інтересів. Перелік запитань, від яких залежить якість розвідки. Послідовність вирішення певних завдань ділової розвідки. Механізм діяльності ділової розвідки

Роль ділової розвідки у бізнесі. Основні переваги компанії, що має сильну структуру ділової розвідки.

## ***Змістовий модуль 2. Основи інформаційної безпеки***

### **Тема 7. Загальні принципи безпеки інформаційних технологій**

Поняття інформації та її захисту. Основні поняття захисту інформації: речова,

телекомунікаційна та документована. Інформаційні ресурси й процеси. Категорії інформації: державна таємниця, комерційна, службова та банківська тайна, персональна інформація.

Основні характеристики інформації: конфіденційність, цілісність та доступність. Методи порушення конфіденційності, цілісності й доступності інформації.

Загрози ІБ, їх класифікація та основні характеристики. Уразливість інформації. Основні групи загроз: порушення цілісності, порушення конфіденційності та доступності інформації. Аналіз погроз ІБ, проблеми інформаційної війни.

Існуючі стандарти ІБ, їх основні положення щодо використання в інформаційних технологіях. Нормативні документи на підприємстві для організації безпеки економічної інформації. Основні заходи щодо організації спеціального діловодства з носіями інформації.

Роботи, які пов'язані із розробкою й аналізом засобів забезпечення ІБ систем економічної та інформаційної безпеки на основі розроблених програм і методик, у тому числі із забезпеченням вимог, що випливають із документів, що регламентують режим безпеки даних.

Аналіз існуючих методів і засобів, застосовуваних для аудиту й захисту комерційної інформації, і розробка пропозицій по їхньому вдосконаленню й підвищенню ефективності.

Оцінка техніко-економічного рівня й ефективності запропонованих і реалізованих організаційно-технічних рішень, пов'язаних із застосуванням програмно-технічних засобів ІБ, з урахуванням перспектив і напрямків їхнього вдосконалення.

### **Тема 8. Канали витоку інформації**

Історичний аспект виникнення та використання каналів витоку інформації.

Поняття каналу витоку інформації. Класифікація каналів витоку інформації, їх характеристики. Области використання каналів витоку інформації. Методи та засоби захисту каналів витоку інформації.

Поняття інформаційного потоку в каналі витоку інформації. Математичний опис інформаційного потоку.

Способи використання каналів витоку інформації у процесі діяльності підприємства.

Таємні канали витоку інформації. Організація виявлення таємних каналів витоку інформації. Моделі таємних каналів витоку інформації. Організація захисту інформації при визначенні таємних каналів витоку інформації.

Загальні класифікація віддалених мережних атак при використанні електронних каналів витоку інформації. Типові віддалені атаки. Атаки на основі використання стеку протоколів ТСП/ІР.

Основи використання сканерів ІБ в різних каналах витоку інформації. Властивості, достоїнства та недоліки використання сканерів ІБ. Аналіз інформації, отриманої при використанні сканерів ІБ.

Організація проведення різних видів аудиту інформації в різних каналах витоку інформації. Аналіз та подальше використання інформації, отриманої при проведенні аудиту. Формування «динаміки» використання каналів витоку інформації з метою отримання оцінки їх ефективності.

### **Тема 9. Організація інформаційної безпеки на підприємстві**

Поняття політики безпеки (ПБ) на підприємстві. Приклади розроблених ПБ на підприємстві. Служби ІБ на підприємстві. Типові функціональні обов'язки співробітників служби ІБ. Методика розробки ПБ на підприємстві. Основні етапи реалізації ПБ в умовах сучасного бізнесу. Приклади сценаріїв злому ІС на підприємстві.

Багаторівнева структура ПБ. Математичний опис багаторівневої ПБ. Політика захисту цілісності Байба.

Типова структура підсистеми безпеки ОС і функції, які виконуються: ідентифікація й аутентифікація, розмежування доступу, аудит, підзвітність дій, повторне використання об'єктів, точність і надійність обслуговування, захист обміну даних. Реалізація підсистеми ІБ на підприємстві.

Відомі міжнародні стандарти управління ІБ: BS 7799 (ISO/IEC 17799 и ISO/IEC 27001), Orange Book, X.800, критерії Європейських держав, Control Objectives for Information and Related Technology (COBIT), IT Infrastructure Library (ITIL) и Statement on Auditing Standards (SAS) No. 70.

Архітектура систем попередження вторгнення – Intrusion Prevention Systems (IPS).



Організація конфігурування IPS для подальшого використання на підприємстві.

Архітектура систем визначення вторгнення – Intrusion Detection Systems (IDS). Організація конфігурування IDS для подальшого використання на підприємстві. Організація використання обох систем – IPS та IDS для забезпечення комплексного захисту.

Організація оптимального використання парольного захисту інформації на підприємстві. Властивості, достоїнства та недоліки використання парольного захисту. Розрахунок стійкості парольного захисту інформації. Використання парольного захисту інформації в різних системах.

Організація на підприємстві групи улагоджування інцидентів комп'ютерної безпеки (ГУІКБ). Її права, статус, обов'язки. Порядок й організація проведення розслідування за фактом комп'ютерного інциденту.

Системи автентифікації та ідентифікації. Класифікація систем автентифікації та ідентифікації. Особливості електронних систем автентифікації та ідентифікації.

### **Змістовий модуль 3. Особливості застосування ІБ у бізнесі**

#### **Тема 10. Організація інформаційної безпеки комп'ютерних мереж**

Програмно-апаратні засоби забезпечення ІБ в комп'ютерних мережах. Протоколи автентифікації при вилученому доступі. Засоби й методи забезпечення цілісності й конфіденційності. Захист серверів і робочих станцій. Засоби захисту локальних мереж при підключенні до Інтернет. Захисні екрани. Захист віртуальних локальних мереж.

Організація ІБ мережі за допомогою брандмауерів та файрволів. Проектування правил брандмауерів. Апаратні реалізації брандмауерів та файрволів.

ІБ при роботі в мережі Інтернет. Типи ресурсів та сервісів в мережі Інтернет, які використовуються на підприємствах. ІБ при роботі із електронної поштою. Організація ІБ від несанкціонованого доступу при роботі із ресурсами ICQ, IRC, СНАТ. Організація ІБ робочого місця працівника підприємства при роботі в мережі Інтернет. Використання програмних засобів запобігання несанкціонованого доступу.

#### **Тема 11. Правові основи ІБ**

Законодавство України в області ІБ, захисту державної таємниці й конфіденційної інформації. Види інформації, що захищається. Державна таємниця як особливий вид інформації, що захищається. Конфіденційна інформація. Система захисту державної таємниці. Правовий режим захисту державної таємниці. Ліцензійна й сертифікаційна діяльності в області ІБ. Правові основи захисту інформації із використанням застосування технічних засобів (захисту від технічних розвідок, застосування й розробка шифрувальних засобів і т.д.). Захист інтелектуальної власності засобами патентного й авторського права. Правова регламентація охоронної діяльності. Міжнародне законодавство в області ІБ. Злочини в сфері комп'ютерної інформації. Експертиза злочинів в області комп'ютерної інформації. Криміналістичні аспекти проведення розслідувань.

Наслідки порушення ІБ на підприємстві. Основні закони та положення України, які регламентують відповідальність за порушення ІБ.

Правовий статус ГУІКБ на підприємстві. Юридичний аспект функціонування ГУІКБ на підприємстві. Відповідальність членів ГУІКБ.

#### **Підсумковий модульний контроль**

#### **Диференційований залік**

### **6. Теми лекцій**

№ з/п	Назва теми	Обсяг у годинах	
		Денна	Заочна
1	Поняття та основні категорії фінансово-економічної безпеки	2	1
2	Індикатори та складові фінансово-економічної безпеки підприємства	8	2
3	Система фінансово-економічної безпеки підприємства	6	2
4	Особливості діяльності служби безпеки підприємства	6	1
5	Недобросовісна конкуренція та захист комерційної таємниці	6	2
6	Ділова розвідка	4	1

7	Загальні принципи безпеки інформаційних технологій	4	1
8	Канали витоку інформації	4	1
9	Організація інформаційної безпеки на підприємстві	4	1
10	Організація інформаційної безпеки комп'ютерних мереж	4	1
11	Правові основи ІБ	4	1
<b>Усього годин</b>		<b>52</b>	<b>14</b>

### 7. Теми практичних занять

№ з/п	Назва теми	Обсяг у годинах	
		Денна	Заочна
	Не передбачено	-	-
<b>Усього годин</b>		<b>-</b>	<b>-</b>

### 8. Теми лабораторних занять

№ з/п	Назва теми	Обсяг у годинах	
		Денна	Заочна
	Не передбачено навчальним планом	-	-
<b>Усього годин</b>		<b>-</b>	<b>-</b>

### 8. Теми семінарських занять

№ з/п	Назва теми	Обсяг у годинах	
		Денна	Заочна
1	Поняття та основні категорії фінансово-економічної безпеки	2	-
2	Індикатори та складові фінансово-економічної безпеки підприємства	6	2
3	Система фінансово-економічної безпеки підприємства	4	2
4	Особливості діяльності служби безпеки підприємства	4	-
5	Недобросовісна конкуренція та захист комерційної таємниці	2	-
6	Ділова розвідка	2	-
7	Загальні принципи безпеки інформаційних технологій	-	-
8	Канали витоку інформації	-	-
9	Організація інформаційної безпеки на підприємстві	-	-
10	Організація інформаційної безпеки комп'ютерних мереж	-	-
11	Правові основи ІБ	-	-
<b>Усього годин</b>		<b>20</b>	<b>4</b>

#### Тема 1. Поняття та основні категорії фінансово-економічної безпеки

1. Ризики як фактори, що несуть загрози економічній безпеці розвитку підприємства.
2. Втрати в комерційному та виробничому підприємстві, ймовірність їх виникнення в українських умовах господарювання та заходи з їх усунення.
3. Послідовність етапів управління ризиками діяльності підприємства та їх взаємозв'язок з функціями управління.

**Література:** основна [2-10; 17]; додаткова [30; 32; 33; 35; 36; 39; 40].

#### Тема 2. Індикатори та складові фінансово-економічної безпеки підприємства

1. Внутрішні та зовнішні ризики діяльності підприємства та їх вплив на стан функціональних складових економічної безпеки підприємства.
2. Індикатори економічної безпеки особистості, підприємства, регіону та держави, їх порогові значення та напрями зміни.
3. Особливості експертного оцінювання рівня економічної безпеки підприємства за її складовими.

**Література:** основна [2; 6; 8-10; 17]; додаткова [32; 34; 36; 40; 41].

### Тема 3. Система фінансово-економічної безпеки підприємства

1. Стійкість підприємства як важлива складова його економічної безпеки.
2. Адаптація підприємства та її види.
3. Організація інформаційного забезпечення адаптації підприємства.
4. Планування та бюджетування процесу адаптації.

**Література:** основна [2; 6-10; 17]; додаткова [31; 32; 36; 38; 40; 43].

### Тема 4. Особливості діяльності служби безпеки підприємства

1. Ризики та загрози процесів взаємодії з контрагентами підприємства.
2. Інформаційно-психологічна безпека персоналу підприємства.
3. Управління мотивацією персоналу як фактор забезпечення економічної безпеки підприємства.
4. Інформаційна взаємодія служби безпеки з іншими підрозділами підприємства.

**Література:** основна [2-6; 8-10; 17]; додаткова [32; 36; 38; 40].

### Тема 5. Недобросовісна конкуренція та захист комерційної таємниці

1. Обґрунтування складу осіб, яких доцільно залучити в групу з розробки положення про режим доступу до інформації підприємства.
2. Визначення складу відомостей, які слід віднести до категорії конфіденційної та таємної інформації (на прикладі підприємств різних видів економічної діяльності).

**Література:** основна [2; 6; 8-10; 17]; додаткова [32; 36; 40; 42].

### Тема 6. Ділова розвідка

1. Визначення складу осіб, зацікавлених у діяльності підприємства та спроможних порушити його економічну безпеку, кола їх інформаційних потреб.
2. Визначення джерел інформації, якими можливо скористатися з метою порушення економічної безпеки підприємства.
3. Формування переліку економічних рішень, які можуть бути реалізовані різними суб'єктами в напрямі порушення економічної безпеки підприємства.

**Література:** основна [2; 3; 6; 8-10; 17]; додаткова [32; 36; 40].

## 9. Самостійна робота

№ з/п	Назва теми	Обсяг у годинах	
		Денна форма	Заочна форма
1	Поняття та основні категорії фінансово-економічної безпеки	8	13
2	Індикатори та складові фінансово-економічної безпеки підприємства	4	14
3	Система фінансово-економічної безпеки підприємства	6	12
4	Особливості діяльності служби безпеки підприємства	6	15
5	Недобросовісна конкуренція та захист комерційної таємниці	8	14
6	Ділова розвідка	6	11
7	Загальні принципи безпеки інформаційних технологій	8	11
8	Канали витоку інформації	8	11
9	Організація інформаційної безпеки на підприємстві	8	11
10	Організація інформаційної безпеки комп'ютерних мереж	8	11
11	Правові основи ІБ	8	11
Усього годин		78	132

## ПИТАННЯ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ

### Змістовний модуль 1. Організація фінансово-економічної безпеки підприємства

#### Тема 1. Поняття та основні категорії економічної безпеки

1. Передумови виникнення поняття економічної безпеки підприємства та його еволюція.

2. Міжнародна економічна безпека як наслідок глобалізації.
3. Особливості забезпечення національної економічної безпеки.
4. Концепція забезпечення соціально-економічної безпеки регіону.

**Література:** основна [2-10; 17]; додаткова [30; 32; 33; 35; 36; 39].

#### **Тема 2. Індикатори та складові фінансово-економічної безпеки підприємства**

1. Аналіз прибутковості підприємства.
2. Критерії економічної безпеки підприємства.
3. Оцінювання рівня економічної безпеки підприємства.

**Література:** основна [2; 6; 8-10; 17]; додаткова [32; 34; 36; 40; 41].

#### **Тема 3. Система фінансово-економічної безпеки підприємства**

1. Система пріоритетних інтересів підприємства як основа механізму забезпечення його економічної безпеки.
2. Структура механізму забезпечення економічної безпеки підприємства.
3. Адаптація підприємства як спосіб забезпечення його економічної безпеки.
4. Державне регулювання діяльності підприємств у забезпеченні їх економічної безпеки.

**Література:** основна [6-8; 17]; додаткова [31; 32; 36; 38; 40; 41].

#### **Тема 4. Особливості діяльності служби безпеки підприємства**

1. Процедура створення та ліквідації служби безпеки підприємства.
2. Перевірка роботи служби безпеки.
3. Використання послуг державної служби охорони та зовнішніх охоронних підрозділів як альтернатива створення служби безпеки підприємства.

**Література:** основна [2-6; 8-10; 17]; додаткова [32; 36; 38; 40].

#### **Тема 5. Недобросовісна конкуренція та захист комерційної таємниці**

1. Поняття та особливості комерційної інформації підприємства.
2. Загрози інформаційній безпеці підприємства.
3. Напрями підвищення стійкості функціонування інформаційної системи підприємства.
4. Правові аспекти комерційної таємниці.

**Література:** основна [2-6; 8-10; 17]; додаткова [32; 36; 40; 42].

#### **Тема 6. Ділова розвідка**

1. Історія виникнення ділової розвідки.
2. Стратегія безпечного розвитку підприємства в умовах інформаційної війни.

**Література:** основна [1-3; 6; 8-10; 17]; додаткова [32; 36; 40].

### **Змістовний модуль 2. Основи інформаційної безпеки**

#### **Тема 7. Загальні принципи безпеки інформаційних технологій**

1. Дайте визначення інформації, її категорії.
2. Визначте мету використання державної інформаційної політики.
3. У чому полягають принципові відмінності різних категорій інформації.
4. Що дозволяє виявити використання існуючих стандартів ІБ.
5. Назвіть основні принципи побудови ІБ.
6. Назвіть основні загрози ІБ.
7. Дайте визначення національної безпеки.
8. Опишіть загальнометодологічні принципи теорії ІБ.

**Література:** основна [1; 2; 17]; додаткова [26; 28; 30; 32-34].

#### **Тема 8. Канали витоку інформації**

1. Опишіть історію виникнення та використання каналів витоку інформації.
2. Визначте поняття каналу витоку інформації та їх класифікацію.
3. У чому полягають принципові відмінності різних каналів витоку інформації.
4. Опишіть основні характеристики таємних каналів витоку інформації.
5. Основні характеристики сканерів ІБ.
6. Методика проведення різних видів аудиту інформації в різних каналах витоку інформації.

**Література:** основна [1; 17]; додаткова [30; 34; 35].

#### **Тема 9. Організація інформаційної безпеки на підприємстві**

1. Визначте мету використання ПБ на підприємстві.
2. Опишіть процес розробки ПБ на підприємстві.
3. Дайте визначення політики захисту цілісності Байба.
4. У чому полягають принципові відмінності міжнародних стандартів управління ІБ.
5. Області використання систем попередження вторгнення.
6. Назвіть основні принципи побудови систем визначення вторгнення.
7. Приведіть класифікацію систем автентифікації та ідентифікації.

**Література:** основна [1; 2; 3; 17]; додаткова [27; 28; 31; 33; 36; 37].

### Змістовний модуль 3. Особливості застосування іб у бізнесі

#### Тема 10. Організація інформаційної безпеки комп'ютерних мереж

1. Дайте визначення протоколу автентифікації при вилученому доступі.
2. Дайте визначення цілісності й конфіденційності.
3. Дайте визначення вразливості.
4. Класифікуйте основні типи брандмауерів та файрволів.
5. У чому полягають принципи захисту віртуальних локальних мереж.
6. Області використання програмних засобів запобігання несанкціонованого доступу.
7. Назвіть основні принципи побудови технології захисту мережі – IPSec.

**Література:** основна [2; 3; 17]; додаткова [28; 31; 32; 34; 36].

#### Тема 11. Правові основи ІБ

1. Дайте визначення видів інформації, що належать для захисту.
2. Дайте визначення державної таємниці.
3. У чому полягають принципові відмінності ліцензійної й сертифікаційної діяльності в області ІБ.
4. Області використання патентного й авторського права.
5. Основні закони та положення України, які регламентують відповідальність за порушення ІБ.
6. Юридичний аспект функціонування ГУІКБ на підприємстві.

**Література:** основна [1; 3; 17]; додаткова [28; 32; 34; 35].

## КОНТРОЛЬНІ ЗАПИТАННЯ ДО ДИФЕРЕНЦІЙОВАНОГО ЗАЛІКУ

### Змістовний модуль 1. Організація економічної безпеки підприємства

1. Що таке економічна безпека?
2. У чому полягає сутність економічної небезпеки?
3. Який зв'язок можна визначити між економічною небезпекою та економічним правопорушенням?
4. Які є види заходів безпеки?
5. Що таке загрози економічній безпеці?
6. Які є види загроз?
7. Що таке економічна загроза і чим вона відрізняється від економічної небезпеки?
8. Що таке фізичні загрози?
9. Що таке психологічно-інформаційні загрози?
10. Які є джерела загроз?
11. Які економічні загрози та небезпеки існують для підприємства на світовому, національному та індивідуальному рівні?
12. Що таке індикатори економічної безпеки підприємства?
13. Які існують критерії визначення економічної безпеки на макро-, мезо- та мікроекономічному рівнях господарювання, а також на рівні окремої особистості?
14. Які є джерела негативних впливів на економічну безпеку підприємства?
15. Які основні функціональні цілі економічної безпеки?
16. Якою є структура економічної безпеки підприємства?
17. Якими є показники безпеки підприємства у фінансовій сфері?
18. Якими є показники безпеки підприємства у кадровій сфері?
19. Якими є показники безпеки підприємства в інформаційній сфері?

20. Якими є показники безпеки підприємства у силовій сфері?
21. Якими є показники безпеки підприємства у ринковій сфері?
22. Якими є показники безпеки підприємства в інтерфейсній сфері?
23. Якими є показники безпеки підприємства в екологічній сфері?
24. Які існують методичні підходи до оцінювання економічної безпеки підприємства?
25. Що таке система безпеки організації?
26. Яка основна мета системи безпеки?
27. Які основні завдання системи безпеки?
28. Які об'єкти та суб'єкти безпеки?
29. Що є предметом економічної безпеки підприємства?
30. Яким є механізм реалізації безпеки?
31. Які основні функції системи безпеки?
32. Які основні засоби економічної безпеки?
33. Які є режими функціонування системи економічної безпеки?
34. Що таке концепція безпеки підприємства?
35. Яким є алгоритм побудови системи економічної безпеки підприємства?
36. У чому полягає сутність процесу адаптації та формування її бюджету?
37. У чому полягає взаємозв'язок ознак стійкості та адаптивності безпечного стану системи?
38. Чим визначається ефективність системи безпеки підприємства?
39. Які принципи гарантування економічної безпеки?
40. Що таке служба безпеки підприємства?
41. Якими є функції діяльності служби безпеки?
42. Який порядок створення служби безпеки?
43. Який порядок ліквідації служби безпеки?
44. Які ресурси необхідні для ефективної діяльності служби безпеки?
45. Як здійснюється відбір працівників в службу безпеки?
46. Що таке програма забезпечення безпеки підприємства?
47. Які особливості взаємодії служби безпеки на підприємстві з іншими підрозділами та суб'єктами зовнішнього середовища?
48. Які дії служби безпеки можливі у кризовій ситуації?
49. Які заходи загальної безпеки на підприємстві?
50. Які існують заходи протидії рекету?
51. Що таке керівництво службою безпеки підприємства і хто його здійснює?
52. Якими є повноваження начальника служби безпеки підприємства?
53. Якими є основні завдання служби режиму та охорони?
54. У чому сутність та значення комерційної інформації?
55. Що належить до категорії ділової інформації?
56. Як виявляються втрати підприємства через недотримання умов конфіденційності?
57. Що таке комерційна таємниця?
58. Яким є механізм визначення переліку інформації, що становить комерційну таємницю?
59. Якими є методи викрадення таємниць підприємства?
60. Чим державна таємниця відрізняється від комерційної?
61. Що таке недобросовісна конкуренція?
62. Які є форми недобросовісної конкуренції?
63. Які є способи незаконного добування інформації?
64. Що розуміється під незаконним використанням відомостей, які становлять комерційну таємницю?
65. Як визначаються втрати підприємства від порушення комерційної таємниці?
66. Які є форми і методи економічного шпигунства?
67. У чому суть та особливості ділової розвідки?
68. Які існують внутрішні та зовнішні джерела інформації ділової розвідки?
69. Яким чином впливає науково-технічний прогрес на розвиток економічної розвідки?

70. У чому особливості історичного розвитку ділової розвідки?
71. Яка специфіка створення розвідувальних структур у системі безпеки підприємства?
72. У чому суть діяльності ділової розвідки?
73. За якими критеріями доцільно оцінювати джерела та зміст інформації, що отримала ділова розвідка?
74. Які можливі напрями перевірки ділового партнера?
75. Чим відрізняється ділова розвідка від промислового шпигунства?
76. Які основні переваги підприємства з сильною структурою ділової розвідки?
77. Яка роль ділової розвідки у безпеці бізнесу?

### **Змістовний модуль 2. Основи інформаційної безпеки**

1. У чому полягають принципові відмінності категорій інформації.
2. Причини використання ПБ.
3. Назвіть основні принципи побудови теорії ІБ.
4. Назвіть типи загроз ІБ.
5. Назвіть існуючі стандарти ІБ.
6. Приведіть цілі створення комп'ютерних мереж.
7. Що таке комп'ютерна мережа?
8. Який пристрій вперше використовувався для забезпечення доступу до головного комп'ютера з терміналів, віддалених від нього на багато сотень і тисячі кілометрів?
9. В якому році була створена комп'ютерна мережа, яка стала відправною точкою для створення першої і найвідомішої нині глобальної мережі – Інтернет?
10. Що таке мережна технологія?
11. Які мережі відносяться до телекомунікаційних мереж?
12. Які критерії є підставою для класифікації мереж?
13. Які бувають мережі за ступенем географічного розповсюдження?
14. Яка мережа призначена для відносно невеликих за масштабом підприємств, офісів і т.п.?
15. Які бувають комп'ютерні мережі за призначенням?
16. До якого типу мереж відноситься мережа навчальної лабораторії?
17. У чому принципова різниця між доступом до ресурсів «На рівні ресурсів» і «На рівні користувача».
18. Перерахуйте перелік дозволів, які можна встановити для папки. Чи відрізняється він від переліку дозволів для файлів?
19. Які частини URL можна опускати при завданні адреси Web-сторінки?
20. Що таке пошукова машина?
21. Назвіть відомі вам пошукові сервери.
22. Що таке портал? Назвіть адреси URL відомих порталів.
23. Назвіть можливості і переваги електронної пошти.
24. Призначення і взаємодія серверів POP3, SMTP?
25. У яких форматах можуть відправлятися поштові повідомлення? За допомогою якої команди це встановлюється?
26. Назвіть адреси електронної пошти вашої організації, вашого провайдера, вашого комп'ютера в локальній мережі.
27. Для чого служить доменне ім'я?
28. За якою схемою здійснюється перетворення адреси?
29. Для чого застосовується команда ping уа.гу?
30. Якими критеріями характеризується мережа?
31. Що таке ідеальна мережа?
32. Чим характеризується продуктивність мереж?
33. Що дозволяє виявити використання каналів витоку інформації.
34. Назвіть основні принципи побудови каналів витоку інформації.
35. Назвіть типи таємних каналів витоку інформації.
36. Назвіть основні принципи побудови ліцензійної й сертифікаційної діяльності в області ІБ.

37. Назвіть закони та положення України, які регламентують відповідальність за порушення ІБ.
38. Назвіть області використання патентного й авторського права.
39. Назвіть переваги ГУІКБ на підприємстві.
40. Назвіть типи брандмауерів та файерволів.
41. Яку кримінальну відповідальність визначають закони України за комп'ютерні злочини?
42. Що таке цифровий підпис?
43. Назвіть закони України, що визначають статус електронного підпису.
44. Дайте визначення ПБ.
45. Дайте визначення систем попередження вторгнення.
46. У чому полягають принципові відмінності систем визначення вторгнення.
47. Области використання систем автентифікації та ідентифікації.
48. Назвіть основні принципи міжнародних стандартів управління ІБ.
49. Назвіть типи устаткування, використовувані в ПБ.
50. Чому виникла необхідність у захисті комп'ютерів?
51. Що таке інформаційна безпека?
52. Що таке захист інформації?
53. Чому безпека – це процес, а не кінцевий результат?
54. На яких категоріях базується інформаційна безпека?
55. Перерахуйте критерії, за якими можна класифікувати загрози інформації?
56. Що відноситься до шкідливого програмного забезпечення?
57. Які методи захисту інформації ви знаєте?
58. Що таке ідентифікація?
59. Що таке автентифікація користувача?
60. Яким чином здійснюється автентифікація користувача?
61. Які три речі можуть використовуватися для встановлення достовірності особи?
62. Назвіть два типи біометричних систем.
63. Які методи захисту інформації відносяться до формальних засобів?
64. Чим відрізняються методи спонукання від методів примушення. Приведіть приклади засобів, які реалізують ці методи.
65. Чому фізичний захист не може гарантувати безпеку?
66. Що таке електронний документ?
67. Для чого і як здійснюється сертифікація часу?
68. Назвіть основні помилки при виборі паролів.
69. Чому для розшифрування повідомлень, зашифрованих методом перестановки, марно застосовувати частотний аналіз для злочину?
70. Приведіть приклад шифрування по методу перемножування матриць.
71. Назвіть найефективніший метод захисту інформації в бездротових мережах.

### **Змістовний модуль 3. Особливості застосування ІБ у бізнесі**

1. Назвіть типи протоколів автентифікації.
2. Дайте визначення брандмауера.
3. Дайте визначення файервола.
4. У чому полягають принципові відмінності брандмауерів та файерволів.
5. Области використання технології захисту мережі – IPSec.
6. Назвіть основні принципи побудови програмних засобів запобігання несанкціонованого доступу.
7. Назвіть типи брандмауерів та файерволів.
8. Назвіть основні принципи побудови ліцензійної й сертифікаційної діяльності в області ІБ.
9. Назвіть закони та положення України, які регламентують відповідальність за порушення ІБ.
10. Назвіть області використання патентного й авторського права.
11. Назвіть переваги ГУІКБ на підприємстві.



## 10. Індивідуальні завдання

Підготувати доповідь з дослідження конкретної організації з використанням блок-схем, за наступними розділами:

Оцінити рівень економічної безпеки підприємства на основі показників стану економічної і фінансової безпеки підприємства.

Визначити основні загрози економічної безпеки для підприємства.

Сформувати можливу стратегію підвищення рівня економічної безпеки підприємства.

Для закріплення теоретичних знань і практичних навичок з дисципліни здобувачі вищої освіти зобов'язані протягом семестру виконати і до початку екзаменаційної сесії індивідуальну контрольну роботу.

Контрольне завдання видається індивідуально кожному здобувачу вищої освіти з метою перевірити засвоєння теоретичної частини навчальної дисципліни та набуття практичних навиків у вирішенні поставлених задач.

Завдання на контрольну роботу видаються здобувачам вищої освіти відразу ж після прочитання настановних лекцій з дисципліни.

Виконується завдання на аркушах формату А4 на комп'ютері або рукописно з дотриманням вимог нормоконтролю до оформлення матеріалу.

Вимоги нормоконтролю до оформлення матеріалу: робота повинна бути виконана технічно і літературно грамотно: надрукована (або написана) на одній стороні аркуша формату А4; за рукописним способом пояснювальну записку виконують з розрахунку 30-35 рядків на сторінці, за машинним способом шрифтом 14 з міжрядковим інтервалом 1,5; текст слід писати, дотримуючись наступних розмірів полів: лівий – 30 мм, верхній та нижній – 20 мм, правий – 10 мм; всі лінії, букви, цифри і знаки повинні бути одного кольору (чорного, фіолетового або синього) абзацний відступ повинен бути однаковим упродовж усього тексту пояснювальної записки і дорівнювати п'яти знакам; сторінки нумерують арабськими цифрами і проставляють в правому верхньому кутку; ілюстрації і таблиці слід розташовувати в роботі безпосередньо після тексту, в якому вони згадуються вперше, або на наступній сторінці; назва таблиці або рисунка повинна бути короткою і відображати його зміст, і пишеться з великої букви. В кінці назви таблиці або рисунка крапка не ставиться.

Титульний аркуш включається в загальну нумерацію сторінок записки але номер сторінки не проставляється.

При виконанні практичного завдання варто дотримуватися наступних вимог: перед рішенням завдання необхідно навести його умову; рішення завдання варто супроводжувати необхідними формулами, розрахунками, короткими поясненнями; всі розрахунки показників виконуються з точністю від 0,01, до 0,1%; наприкінці роботи вказується перелік використаної літератури, ставиться підпис здобувача вищої освіти та дата.

## 11. Методи навчання

### 1. Методи навчання на лекціях:

- Вербальний метод (лекція, дискусія тощо);
- Методи візуалізації (презентація, метод ілюстрації (графічний, табличний, тощо), метод демонстрацій та інші);
- робота з навчально-методичною літературою (конспектування, тезування, анотування тощо);
- інші методи у сполученні з новітніми інформаційними технологіями та комп'ютерними засобами навчання (дистанційні, мультимедійні, веб-орієнтовані тощо);

### 2. Методи навчання на практичних, семінарських та лабораторних заняттях:

- Вербальний метод (дискусія, співбесіда тощо);
- Практичний метод (практичні, семінарські та лабораторні заняття);
- Метод візуалізації (презентація, метод ілюстрації (графічний, табличний, тощо), метод демонстрацій та інші);

- робота з навчально-методичною літературою (рецензування, підготовка реферату, есе, доповіді тощо);
- інші методи у сполученні з новітніми інформаційними технологіями та комп'ютерними засобами навчання (дистанційні, мультимедійні, веб-орієнтовані тощо);
- кейс-метод (вирішення ситуацій, розв'язання завдань тощо);
- Імітаційний метод
- Дослідницький метод
- Пошуковий метод.
- Метод проблемного виконання.
- Репродуктивний метод

## **12. Методи оцінювання**

У процесі вивчення дисципліни «Фінансово-економічна безпека підприємства» використовуються такі методи оцінювання:

- для поточного контролю у вигляді: *усне та письмове опитування, фронтальне опитування, тестування, вирішення ситуаційних завдань, розв'язування задач, написання есе (рефератів), виконання індивідуальних та групових проектів, творчих завдань, тощо.*
- для модульного контролю у вигляді: *письмова відповідь, тестування, вирішення ситуаційних завдань, розв'язування задач, тощо.*
- для підсумкового контролю у вигляді: *екзамену або заліку у таких формах: усна та/або письмова відповідь, тестування, вирішення ситуаційних завдань, розв'язування задач, тощо.*

## **13. Засоби діагностики результатів навчання**

Робоча програма передбачає застосування засобів діагностики результатів навчання за формами контролю знань:

- *поточний контроль* може передбачати застосування широкого спектру форм та методів оцінювання знань, що проводиться за кожною темою.
- *модульний контроль* передбачає письмове виконання різних видів контрольних завдань.
- *підсумковий контроль* передбачає проведення екзамену або заліку

Завершальним етапом досягнення запланованих програмних результатів навчання з навчальної дисципліни «Фінансово-економічна безпека підприємства» є підсумковий контроль – диференційований залік.

## **14. Критерії та порядок оцінювання результатів навчання**

Рекомендоване оцінювання окремих видів навчальної діяльності здобувача вищої освіти:

№	Вид навчальної діяльності здобувачів вищої освіти*	Кількість балів
1.	Реферат, есе	1-5
2.	Вирішення ситуаційних завдань, розв'язання задач	1-5
3.	Індивідуальне завдання	1-5
4.	Відповідь на практичному, семінарському, лабораторному занятті	1-5
5.	Ділова гра, практичний кейс, тощо.	1-10
6.	Участь у публічних заходах (конференція, олімпіада тощо)	1-10
7.	Модульний контроль (для денної форми здобуття освіти)	1-20
8.	Контрольна робота (для заочної форми здобуття освіти)	1-40

\*види навчальної діяльності здобувачів освіти обираються та оцінюються викладачем за рекомендованою шкалою в залежності від особливостей навчальної дисципліни.

Для визначення ступеня засвоєння навчального матеріалу та поточного оцінювання знань здобувачів вищої освіти оцінюються за такими критеріями:



2	2	2	3	3	3	3	3	3	3	3	10	40	100
Модульний контроль 1 - 10						Модульний контроль 2 - 10							

*Приклад для заочної форми здобуття освіти*

Поточний контроль та самостійна робота		Підсумковий контроль	Сума
Контрольна робота	Самостійна робота		
50	10	40	100

## 16. Методичне забезпечення

Методичне забезпечення дисципліни «Фінансово-економічна безпека підприємства» узагальнено в комплексі навчально-методичного забезпечення, який включає:

- робочу програму навчальної дисципліни;
- методичні вказівки до вивчення дисципліни;
- опорний конспект лекцій;
- варіанти завдань для самостійної та індивідуальної роботи студентів;
- варіанти завдань для модульного контролю;
- варіанти завдань для підсумкового контролю;
- інші матеріали.

## 14.Рекомендована література

### Основна

1. Ареф'єва О.В. Планування економічної безпеки підприємств / О.В. Ареф'єва, Т.Б. Кузенко. К. : видавництво Європейського ун-ту, 2018. 169 с.
2. Васильців Т.Г. Економічна безпека суб'єктів підприємництва: підручник / Варналій З.С., Васильців Т.Г., Лупак Р.Л. та ін. Чернівці: Технодрук, 2020. 458 с.
3. Економічна безпека: Навчальний посібник / за заг. ред. З. С. Варналія. К.: Знання, 2018. – 647 с
4. Варналій З.С., Живко З.Б., Білик Р.Р., Онищенко С.В., Живко М.О. Фінансова безпека: навч.посібник; за ред. З.С. Варналія. Львів: Ліга-Прес, 2018. 300 с.
5. Економічна безпека підприємства: навчально-методичний посібник для студентів вищих навчальних закладів / [уклад. І.В. Ящишина]. Кам'янець-Подільський : МЕДОБОРИ-2006, 2016. 86 с.
6. Іванюта Т.М. Економічна безпека підприємства : Навчальний посібник / Т.М. Іванюта, А.О. Заїчковський. К. : Центр учбової літератури, 2019. – 256 с.
7. Керницький І.С., Живко З.Б., Копитко М.І. Конкурентна розвідка підприємств: курс лекцій. Львів: Ліга-Прес, 2015. 388 с.
8. Обліково-аналітичне забезпечення управління економічною безпекою підприємства: монографія / За заг. ред. А.М. Штангрета. Львів: Укр. акад. друкарства, 2017. 276 с.
9. Штангрет А.М. Економічна безпека підприємства [Текст]: підручник / [А.М. Штангрет та ін.]; за заг. ред. А.М. Штангрета; Укр. акад. друкарства. – Львів: Укр. акад. друкарства, 2016. 292 с.

### Допоміжна

1. Антонова О.М. Формування фінансово-економічного механізму забезпечення економічної безпеки ВНЗ. // Актуальні проблеми економіки. 2016. № 3. С. 117-125.
2. Варналій З.С. Системні проблеми та шляхи забезпечення фінансової безпеки України в умовах гібридної війни / З.С. Варналій, Т.Т. Томашеський// Економічний вісник університету. Збірник наук. праць учених та аспірантів. Випуск 41, Переяслав-Хмельницький, 2019. С.171-179.
3. Варналій З.С. Використання теорії нечітких множин для оцінки рівня фінансової безпеки підприємства / З.С. Варналій, А.М. Мехед // Міжнародний науковий журнал

«Інтернаука», Серія: «Економічні науки». – 2019. № 2 (22). С. 81-87.

4. Варналій З.С. Економічна безпека та конкурентоспроможність регіонів України : монографія / З.С. Варналій, Р.Р. Білик. Чернівці: Технодрук, 2018. 454 с.

5. Варналій З.С. Механізм попередження загроз економічній безпеці України / З.С. Варналій С.В. Онищенко, О.А. Маслій // Економічний часопис ХХІ. 2016. № 159 (5 6). С. 20-24. (Scopus, EBSCOhost, Index Copernicus, Ulrich's Periodicals Directory, С.Е.Е.О.Л., RISC). DOI: <http://dx.doi.org/10.21003/ea.V159-04>

6. Экономическая безопасность / под ред. Е.Л. Олейникова. М.: РЭА им. Плеханова, 2000. 285 с.

7. Економічна безпека підприємства в умовах антикризового управління: концептуальне визначення та механізм забезпечення: монографія / А.М. Штангрет, Я.В. Котляревський, М.М. Караїм. Львів: Укр. акад. друкарства, 2012. 288 с.

8. Живко З.Б., Сердюков В.В., Стаднік О.М., Хорошко В.О. Правові основи охорони інформації. Підручник; за ред.проф.В.О.Хорошка. Вид.2. К.: Вид. ДУІКТ, 2009. 355 с.

9. Козаченко Г.В. Економічна безпека підприємства: сутність та механізм забезпечення: монографія / Козаченко Г.В., Пономарьов В.П., Ляшенко О.М. К.: Лібра, 2003. 280 с.

10. Мунтіян В.І. Економічна безпека України / В.І. Мунтіян. К.: Вид. КВІЦ, 1999. 464 с.

11. Організація перевірок фінансово-господарської діяльності підприємств: підручник [З.Б. Живко, І.О. Ревак, М.О. Живко, С.І. Мельник, Л.М. Плахотнюк]; за заг.ред.З.Б.Живко. Львів: ЛьвДУВС, 2011. 548 с.

12. Організація та управління системою економічної безпеки підприємства: навчально-методичний посібник [З. Б. Живко, О.В. Черевко, Н.В. Зачосова, М. О. Живко, О.Б. Баворовська, В.О. Занора]; за ред. З.Б. Живко. Черкаси : видавець Чабаненко Ю.А., 2019. 120 с.

13. Фінансова безпека підприємства: навч. посібник / З.С. Варналій, З.Б. Живко, Р.Р. Білик, С.В. Онищенко, М.О. Живко; за ред. З.С. Варналія. Львів: Ліга-Прес, 2018. 300 с.

## 15. Інформаційні ресурси, у т.ч. в мережі Інтернет

1. Компания Безопасность [Электронный ресурс]. Режим доступа: <http://bezopasnost.biz>.

2. Державна служба спеціального зв'язку та захисту інформації України [Електронний ресурс]. Режим доступу: <http://dstszi.gov.ua>.

3. International Charity Foundation for History and Development of Computer Science and Technique, ICFCST. Історія розвитку інформаційних технологій в Україні [Електронний ресурс]. Режим доступу: [http://www.icfcst.kiev.ua/MUSEUM/IT\\_u.html](http://www.icfcst.kiev.ua/MUSEUM/IT_u.html).

4. Information Technology Security Evaluation Criteria, v. 1.2. Office for Official publications of the European Communities, 1991 [Електронний ресурс]. Режим доступу: [www.ssi.gouv.fr/IMG/pdf/JILv2.pdf](http://www.ssi.gouv.fr/IMG/pdf/JILv2.pdf)

5. Site of FBI. – Режим доступу: [www.fbi.gov](http://www.fbi.gov).

6. The International PGP Home Page [Electronic resource]. Access mode: [www.pgpi.org](http://www.pgpi.org).

7. Site of SecurityFocus. Access mode: [www.securityfocus.com](http://www.securityfocus.com).

8. Сайт Sysinternals. Режим доступу: [www.sysinternals.com](http://www.sysinternals.com).

9. [Электронный ресурс]. Режим доступа: [www.zdnet.ru](http://www.zdnet.ru).

10. Історія розвитку інформаційних технологій в Україні: нормативні акти України [Електронний ресурс]. Режим доступу: [www.nau.kiev.ua](http://www.nau.kiev.ua).

11. Розвідка України [Електронний ресурс]. Режим доступу: <http://rozvidka.livejournal.com/>.

12. Служба безпеки України [Електронний ресурс]. Режим доступу: <http://www.sbu.gov.ua/>.

13. Служба економічної безпеки [Електронний ресурс]. Режим доступу: <http://sebweb.at.ua/>.

14. Центр информационных технологий [Электронный ресурс]. Режим доступа: <http://www.citmgu.ru>.