



КИЇВСЬКИЙ ІНСТИТУТ БІЗНЕСУ ТА ТЕХНОЛОГІЙ

КАФЕДРА ЕКОНОМІКИ ТА ПІДПРИЄМНИЦТВА

ЗАТВЕРДЖЕНО

Вчена рада

Протокол № 1 від 31.08.2024

Голова вченої ради

О. В. Яковлева



Інформаційна безпека економічних систем

ВАРІАТИВНА ДИСЦИПЛІНА

СИЛАБУС

для підготовки фахівців другого (магістерського) рівня вищої освіти

за спеціальністю 051 "Економіка"

за освітньою програмою

"Економіка"

С.М. Чімишенко, 2024 рік

chimyshenko@kibit.edu.ua

СХВАЛЕНО

Кафедра економіки та підприємництва

Протокол № 1 від 20.09.2024

Зав. каф. Т.І. Пішеніна

Київ 2024

Силабус вибіркової освітньої компоненти “Інформаційна безпека економічних систем” для студентів для студентів освітньої програми «Економіка» другого (магістерського) рівня вищої освіти за спеціальностями 051 Економіка, галузі знань 05 Соціальні і поведінкові науки.

Розробник: С.М. Чімишенко, к.е.н., доцент, доцент кафедри економіки та підприємництва Київського інституту бізнесу та технологій

Силабус затверджений на засіданні кафедри економіки та підприємництва

Протокол № 1 від «30» 08 2024 року

Завідувач кафедри  Т.І. Пішеніна

© С.М. Чімишенко, 2024 рік,
© КІБІТ, 2024 рік

1. Анотація курсу

Навчальна дисципліна «Інформаційна безпека економічних систем» в програмі навчання є варіативною за вибором здобувачів освіти.

Засоби оцінювання – підсумковий залік, який здійснюється за тестовими завданнями.

Форма навчання	Семестр	Кредити ECTS	Години	Лекції	Практичні (семінарські) заняття	СРС	Залік
Денна	2	4	120	18	8	84	4
Заочна	2	4	120	6	6	108	

Мова навчання: українська.

Передреквізити – Інформатика. Комп'ютерна і технічна грамотність. Інформаційний менеджмент. Міжнародна економіка. Глобальна економіка.

Постреквізити – Науково-дослідне стажування. Підготовка кваліфікаційної роботи та захист.

2. Мета курсу

Предметом вивчення навчальної дисципліни є основні терміни, поняття та визначення в галузі безпеки інформаційних систем в економіці; головні завдання безпеки ІС; моделі загроз інформації, механізми та сервіси її захисту; криптографічні методи забезпечення конфіденційності, цілісності та нонрепудіації (унеможливлення відмови від виконаних дій, або обов'язків, що були прийняті) в інформаційних системах економічних суб'єктів; аутентифікації суб'єктів та об'єктів інформаційної діяльності в інформаційних системах; електронний цифровий підпис (ЕЦП).

Метою дисципліни "Інформаційна безпека економічних систем" є систематизація знань студентів в галузі інформаційної безпеки економічних суб'єктів різних форм власності та вивчення прикладних особливостей застосування методів та засобів захисту інформації.

Згідно з вимогами освітньої програми студенти повинні освоїти наступні **компетентності**:

- Здатність використовувати сучасні інформаційні технології, методи та прийоми дослідження економічних та соціальних процесів, адекватні встановленим потребам дослідження.
- Здатність оцінювати можливі ризики, соціально-економічні наслідки управлінських рішень.
- Застосовувати інноваційні інструменти та технології в економіці, виконувати аналітичну обробку економічної інформації в різних сферах цифрової економіки
- Здатність формулювати професійні задачі в сфері економіки та розв'язувати їх, обираючи належні напрями і відповідні методи для їх розв'язання, беручи до уваги наявні ресурси.

- Здатність планувати і розробляти проекти у сфері економіки, здійснювати її інформаційне, методичне, матеріальне, фінансове та кадрове забезпечення.
- Знати методи захисту інформації, моделі безпеки інформаційних систем, методи проектування, розробки та реалізації вимог до забезпечення якості інформаційних систем в економіці та використовувати ці знання при створенні захищених інформаційних систем.

Програма навчальної дисципліни складається з **7 тем**.

3. План лекційних та семінарських занять та завдання до СРС

Основні підручники цього курсу:

- Кавун С. В. Економічна та інформаційна безпека підприємств у системі консолідованої інформації : навчальний посібник / С. В. Кавун, А. А. Пилипенко, Д. О. Ріпка. – Х. : Вид. ХНЕУ, 2013. – 364 с.
- Economic and cyber security: collective monograph. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 196 p

Тема заняття	Питання на семінарські заняття	Література
<p>Тема 1. Основні аспекти інформаційної безпеки економічних систем.</p> <p>Лекція</p> <p>1. <i>Поняття та основні категорії економічної безпеки</i></p> <p>2. <i>Система економічної безпеки підприємства</i></p> <p>3. <i>Загальні принципи безпеки інформаційних технологій</i></p>	<p>1. <i>Як зміна економічного середовища впливає на підходи до забезпечення економічної безпеки підприємства?</i></p> <p>2. <i>Які основні загрози для економічної безпеки підприємства існують в умовах сучасної цифрової економіки?</i></p> <p>3. <i>Чи достатньо сучасних заходів безпеки інформаційних технологій для забезпечення економічної безпеки підприємства?</i></p> <p>4. <i>Як можна інтегрувати принципи економічної безпеки у загальну стратегію розвитку підприємства?</i></p> <p>5. <i>Яка роль законодавства та нормативних актів у забезпеченні інформаційної безпеки економічних систем?</i></p>	<p>1. "Економічна безпека підприємства: теорія, методологія, практика" / За заг. ред. О.В. Савчук, О.М. Подсолонко.</p> <p>2. "Інформаційна безпека в умовах цифрової економіки" / В.І. Подвальний, О.С. Фурсов</p> <p>3. "Національна безпека України: виклики та загрози в інформаційній сфері" / За ред. В.Г. Крисача.</p>
<p>Тема 2 Поняття інформаційних загроз та їх види.</p> <p>Лекція</p> <p>1. <i>Загрози економічній безпеці та джерела їх виникнення.</i></p>	<p>1. <i>Які фактори найбільше впливають на виникнення загроз економічній безпеці підприємства в умовах глобалізації?</i></p> <p>2. <i>Як підприємства можуть ефективно управляти ризиками, що виникають через інформаційні загрози?</i></p>	<p>1. "Інформаційна безпека економічних систем: методологія та практика" / За ред. О.М. Герасименко</p> <p>2. "Кібербезпека в умовах сучасної економіки" / А.О. Дегтярьов, Л.В. Паламарчук</p>

<p>2. Ризики як фактори, що несуть загрози економічній безпеці підприємства, та управління ними.</p> <p>3. Класифікація атак та вірусів.</p>	<p>3. Які типи атак і вірусів найбільш небезпечні для економічної безпеки підприємств, і чому?</p> <p>4. Як розвиток нових технологій впливає на зміну типології інформаційних загроз?</p> <p>5. Які основні виклики існують для класифікації інформаційних атак та вірусів у контексті економічної безпеки?</p>	<p>3.</p> <p>"Економічна безпека підприємства: інформаційні аспекти" / О.В. Череп, Н.В. Попова</p>
<p>Тема 3. Принципи побудови системи інформаційної безпеки.</p> <p>Лекція</p> <p>1. Стандарти інформаційної безпеки.</p> <p>2. Ідентифікація та автентифікації у комп'ютерних мережах.</p> <p>3. Методи та засоби інформаційної безпеки в комп'ютерних мережах</p>	<p>1. Як впровадження міжнародних стандартів інформаційної безпеки впливає на економічну безпеку підприємства?</p> <p>2. Які економічні ризики виникають при недостатньому контролі ідентифікації та автентифікації в комп'ютерних мережах?</p> <p>3. Наскільки виправдані інвестиції в сучасні методи та засоби інформаційної безпеки з точки зору економічної вигоди для підприємства?</p> <p>4. Як порушення стандартів інформаційної безпеки може вплинути на репутацію та фінансову стабільність підприємства?</p> <p>5. Які економічні наслідки можуть виникнути через компрометацію системи автентифікації в умовах цифрової трансформації?</p>	<p>1. "Інформаційна безпека: теорія і практика" / І.В. Гура, О.А. Ковтун</p> <p>2. "Управління інформаційною безпекою на підприємствах України" / В.П. Жовнір, О.В. Кузьмін.</p> <p>3. "Економічні аспекти кібербезпеки: український контекст" / М.М. Колесніков, Л.М. Романенко</p>
<p>Тема 4. Організація систем захисту інформації економічних систем.</p> <p>Лекція</p> <p>1. Моделі систем безпеки</p> <p>2. Методика розробки політики безпеки</p> <p>3. Методи оцінки втрат</p> <p>4. Методи оцінки ризиків</p> <p>5. Служба інформаційної безпеки. Організація її аудиту.</p>	<p>1. Яким чином вибір моделі системи безпеки впливає на економічну стабільність підприємства?</p> <p>2. Які економічні наслідки можуть виникнути через недосконалу політику безпеки?</p> <p>3. Як точність методів оцінки втрат впливає на управлінські рішення та фінансове планування в контексті інформаційної безпеки?</p> <p>4. Які підходи до оцінки ризиків є найбільш економічно ефективними для підприємств різних розмірів і галузей?</p>	<p>1. "Інформаційна безпека та управління ризиками в економічних системах" / В.О. Пашко, О.М. Литвиненко.</p> <p>2. "Організація інформаційної безпеки: стандарти, політики та аудит" / О.В. Шквір, І.В. Ігнатенко.</p> <p>3. "Економічна безпека підприємств: організаційні та інформаційні аспекти" / О.М. Гаврилюк, Т.В. Ковальчук</p>

	<p>5. Як ефективна організація служби інформаційної безпеки та регулярний аудит впливають на довгострокову економічну безпеку підприємства?</p>	
<p>Тема 5. Інформаційна безпека систем на макроекономічному рівні. Лекція 1. Вплив інформаційної безпеки на стабільність національної економіки та її конкурентоспроможність на глобальному ринку. 2. Основні загрози інформаційній безпеці та їх вплив на економічну безпеку держави. 3. Механізми та політики для забезпечення інформаційної безпеки національної економіки.</p>	<p>1. Як нестача інформаційної безпеки може вплинути на довгострокову економічну стабільність та міжнародну репутацію держави? 2. Яким чином інформаційні загрози на макроекономічному рівні можуть підривати конкурентоспроможність національної економіки на глобальному ринку? 3. Наскільки ефективними є поточні державні політики і механізми щодо забезпечення інформаційної безпеки національної економіки? 4. Які довгострокові економічні наслідки можуть виникнути через невчасну адаптацію національної стратегії інформаційної безпеки до нових глобальних викликів? 5. Яку роль відіграють міжнародні співпраці та угоди в забезпеченні інформаційної безпеки національної економіки, і які економічні вигоди та ризики вони можуть нести?</p>	<p>1. "Інформаційна безпека та економічна стабільність: Національний та глобальний контексти" / В.С. Шаповал, О.В. Костенко 2. "Економічні аспекти інформаційної безпеки: Тенденції та виклики" / І.М. Гаврилюк, Т.С. Ковальчук 3. "Національна інформаційна безпека України: Стратегії та реалізація" / О.М. Литвиненко, М.В. Гуров</p>
<p>Тема 6. Інформаційна безпека автоматизованих банківських систем. Лекція 1. Оцінка і управління ризиками в автоматизованих банківських системах. 2. Захист і шифрування даних у банківських системах. 3. Ризик-менеджмент та реагування на кіберзагрози в банківських системах</p>	<p>1. Яким чином неефективне управління ризиками в автоматизованих банківських системах може вплинути на фінансову стабільність банку та довіру клієнтів? 2. Які економічні наслідки можуть виникнути у випадку компрометації даних у банківських системах через недосконалість захисту і шифрування? 3. Наскільки ефективний ризик-менеджмент і швидке реагування на кіберзагрози впливають на зниження економічних збитків банку під час кіберінцидентів? 4. Які фінансові ресурси необхідно інвестувати в інформаційну безпеку банківських систем, щоб</p>	<p>1. "Інформаційна безпека банківських систем: ризики та захист" / А.В. Чеботаренко, О.М. Сидоренко 2. "Кіберзагрози в банківських системах: оцінка та реагування" / В.С. Коваленко, Л.М. Герасимчук 3. "Інформаційна безпека в банківському секторі України: теорія і практика" / О.М. Тищенко, В.П. Литвин</p>

	запобігти значним економічним втратам у разі кіберзагроз?	
Тема 7. Інформаційна безпека електронної комерції Лекція 1. Захист даних користувачів і забезпечення конфіденційності в електронній комерції 2. Управління ризиками та протидія шахрайству в електронній комерції 3. Інформаційна безпека мобільної комерції та багатоканальних продажів	1. Як недостатній захист даних користувачів впливає на економічні показники компанії та її репутацію на ринку електронної комерції? 2. Які основні економічні ризики пов'язані з шахрайством в електронній комерції, і як ефективно управління ризиками може мінімізувати ці втрати? 3. Як безпека мобільної комерції впливає на розширення ринку та економічний розвиток компанії, що використовує багатоканальні продажі? 4. Які економічні наслідки можуть виникнути у компаній через невчасне впровадження стандартів і технологій інформаційної безпеки в електронній комерції?	1. "Інформаційна безпека та електронна комерція: виклики та рішення" / О.М. Литвин, І.В. Гончар 2. "Кібербезпека в електронній комерції: захист даних і економічна стабільність" / С.О. Зубченко, В.В. Колесник 5. "Електронна комерція та кіберзагрози: стратегічні підходи до безпеки" / М.В. Петров, А.І. Ковальчук
Залік (підсумковий контроль)		

План занять та СРС для заочної форми

Тема заняття	Практичне/кейсове завдання для самостійного вивчення і виконання	Література
Тема 1. Основні аспекти інформаційної безпеки економічних систем. Лекція 1. Система економічної безпеки підприємства 2. Загальні принципи безпеки інформаційних технологій	Дайте письмову відповідь на питання: 1. Як зміна економічного середовища впливає на підходи до забезпечення економічної безпеки підприємства? 2. Які основні загрози для економічної безпеки підприємства існують в умовах сучасної цифрової економіки? 3. Як можна інтегрувати принципи економічної безпеки у загальну стратегію розвитку підприємства?	1. "Економічна безпека підприємства: теорія, методологія, практика" / За заг. ред. О.В. Савчук, О.М. Подсолонко. 2. "Інформаційна безпека в умовах цифрової економіки" / В.І. Подвальний, О.С. Фурсов 1. "Національна безпека України: виклики та загрози в інформаційній сфері" / За ред. В.Г. Крисача.

<p>Тема 2 Поняття інформаційних загроз та їх види.</p> <p>Лекція</p> <p>1. Загрози економічній безпеці та джерела їх виникнення.</p> <p>2. Ризики як фактори, що несуть загрози економічній безпеці підприємства, та управління ними.</p>	<p>Підготуйте презентацію на одне з питань:</p> <p>1. Які фактори найбільше впливають на виникнення загроз економічній безпеці підприємства в умовах глобалізації?</p> <p>2. Як підприємства можуть ефективно управляти ризиками, що виникають через інформаційні загрози?</p> <p>3. Як розвиток нових технологій впливає на зміну типології інформаційних загроз?</p>	<p>1. "Інформаційна безпека економічних систем: методологія та практика" / За ред. О.М. Герасименко</p> <p>2. "Кібербезпека в умовах сучасної економіки" / А.О. Дегтярьов, Л.В. Паламарчук</p> <p>3. "Економічна безпека підприємства: інформаційні аспекти" / О.В. Череп, Н.В. Попова</p>
<p>Тема 3. Принципи побудови системи інформаційної безпеки.</p> <p>Лекція</p> <p>1. Ідентифікація та автентифікації у комп'ютерних мережах.</p> <p>2. Методи та засоби інформаційної безпеки в комп'ютерних мережах</p>	<p>Написати реферат та розкрити одне з питань:</p> <p>1. Які економічні ризики виникають при недостатньому контролі ідентифікації та автентифікації в комп'ютерних мережах?</p> <p>2. Наскільки виправдані інвестиції в сучасні методи та засоби інформаційної безпеки з точки зору економічної вигоди для підприємства?</p> <p>3. Які економічні наслідки можуть виникнути через компрометацію системи автентифікації в умовах цифрової трансформації?</p>	<p>1. "Інформаційна безпека: теорія і практика" / І.В. Гура, О.А. Ковтун</p> <p>2. "Управління інформаційною безпекою на підприємствах України" / В.П. Жовнір, О.В. Кузьмін.</p> <p>3. "Економічні аспекти кібербезпеки: український контекст" / М.М. Колесніков, Л.М. Романенко</p>
<p>Тема 4. Організація систем захисту інформації економічних систем.</p> <p>Лекція</p> <p>1. Методика розробки політики безпеки</p> <p>2. Методи оцінки втрат та ризиків.</p> <p>3. Служба інформаційної безпеки.</p>	<p>Дати письмову відповідь на одне з питань з наведенням конкретних прикладів:</p> <p>1. Які економічні наслідки можуть виникнути через недосконалу політику безпеки?</p> <p>2. Як точність методів оцінки втрат впливає на управлінські рішення та фінансове планування в контексті інформаційної безпеки?</p> <p>3. Як ефективна організація служби інформаційної безпеки та регулярний аудит впливають на довгострокову економічну безпеку підприємства?</p>	<p>1. "Інформаційна безпека та управління ризиками в економічних системах" / В.О. Пашко, О.М. Литвиненко.</p> <p>2. "Організація інформаційної безпеки: стандарти, політики та аудит" / О.В. Шквір, І.В. Ігнатенко.</p> <p>3. "Економічна безпека підприємств: організаційні та інформаційні аспекти" / О.М. Гаврилюк, Т.В. Ковальчук</p>

<p>Тема 5. Інформаційна безпека систем на макроекономічному рівні.</p> <p>Лекція</p> <p>1. Основні загрози інформаційній безпеці та їх вплив на економічну безпеку держави.</p> <p>2. Механізми та політики для забезпечення інформаційної безпеки національної економіки.</p>	<p>Підготувати презентацію на одне з питань:</p> <p>1. Наскільки ефективними є поточні державні політики і механізми щодо забезпечення інформаційної безпеки національної економіки?</p> <p>2. Які довгострокові економічні наслідки можуть виникнути через невчасну адаптацію національної стратегії інформаційної безпеки до нових глобальних викликів?</p> <p>3. Яку роль відіграють міжнародні співпраці та угоди в забезпеченні інформаційної безпеки національної економіки, і які економічні вигоди та ризики вони можуть нести?</p>	<p>1. "Інформаційна безпека та економічна стабільність: Національний та глобальний контексти" / В.С. Шаповал, О.В. Костенко</p> <p>2. "Економічні аспекти інформаційної безпеки: Тенденції та виклики" / І.М. Гаврилюк, Т.С. Ковальчук</p> <p>3. "Національна інформаційна безпека України: Стратегії та реалізація" / О.М. Литвиненко, М.В. Гурав</p>
<p>Тема 6. Інформаційна безпека автоматизованих банківських систем.</p> <p>Лекція</p> <p>1. Оцінка і управління ризиками в автоматизованих банківських системах.</p> <p>2. Захист і шифрування даних у банківських системах.</p>	<p>Написати реферат та розкрити одне з питань:</p> <p>1. Яким чином неефективне управління ризиками в автоматизованих банківських системах може вплинути на фінансову стабільність банку та довіру клієнтів?</p> <p>2. Які економічні наслідки можуть виникнути у випадку компрометації даних у банківських системах через недосконалість захисту і шифрування?</p> <p>3. Які фінансові ресурси необхідно інвестувати в інформаційну безпеку банківських систем, щоб запобігти значним економічним втратам у разі кіберзагроз?</p>	<p>1. "Інформаційна безпека банківських систем: ризики та захист" / А.В. Чеботаренко, О.М. Сидоренко</p> <p>2. "Кіберзагрози в банківських системах: оцінка та реагування" / В.С. Коваленко, Л.М. Герасимчук</p> <p>3. "Інформаційна безпека в банківському секторі України: теорія і практика" / О.М. Тищенко, В.П. Литвин</p>
<p>Тема 7. Інформаційна безпека електронної комерції</p> <p>Лекція</p> <p>1. Управління ризиками та протидія шахрайству в електронній комерції</p> <p>2. Інформаційна безпека мобільної комерції та багатоканальних продажів</p>	<p>1. Які основні економічні ризики пов'язані з шахрайством в електронній комерції, і як ефективно управління ризиками може мінімізувати ці втрати?</p> <p>2. Як безпека мобільної комерції впливає на розширення ринку та економічний розвиток компанії, що використовує багатоканальні продажі?</p> <p>3. Які економічні наслідки можуть виникнути у компанії через невчасне впровадження стандартів і технологій інформаційної безпеки в електронній комерції?</p>	<p>1. "Інформаційна безпека та електронна комерція: виклики та рішення" / О.М. Литвин, І.В. Гончар</p> <p>2. "Кібербезпека в електронній комерції: захист даних і економічна стабільність" / С.О. Зубченко, В.В. Колесник</p> <p>3. "Електронна комерція та кіберзагрози: стратегічні підходи до безпеки" / М.В. Петров, А.І. Ковальчук</p>

Залік (підсумковий контроль)		
-------------------------------------	--	--

4. Засоби діагностики результатів навчання

Перелік питань для підсумкового контролю

1. Нормативно-правове забезпечення національної безпеки.
2. Держава і економічна політика.
3. Захист національного виробника.
4. Економічна безпека як складова національної безпеки держави
5. Взаємодія правоохоронних органів при забезпеченні економічної безпеки держави.
6. Сутність тіньової економіки.
7. Причини існування тіньової економіки.
8. Види та сутність державних обмежень і вимог та їх соціально-економічні наслідки.
9. Структура тіньової економіки.
10. Сутність економічної злочинності, її види.
11. Рівні тінізації економіки та їх соціально-економічні наслідки.
12. Класифікація тіньової економічної злочинності.
13. Сутність організованої економічної злочинності, її структурні елементи.
14. Зміст і кримінологічні ознаки "п'ятої влади". Обставини, що сприяли виникненню "п'ятої влади" в Україні.
15. Сучасна банківська система України.
16. Органи, які наділені повноваженнями по здійсненню документальної ревізії комерційних банків.
17. Порядок отримання правоохоронними органами інформації, що має статус банківської таємниці.
18. Основні види банківських операцій.
19. Механізм функціонування "фіктивних" фірм.
20. Сутність банківського кредиту, його види.
21. Основні етапи кредитного процесу.
22. Загальна характеристика зловживань, пов'язаних з незаконним отриманням та неповерненням кредитів.
23. Місце і значення бюджету в загальній системі фінансових відносин.
24. Функції бюджету.
25. Принципи побудови бюджетної системи.
26. Характеристика доходів бюджету держави.
27. Характеристика видатків бюджету держави
28. Позабюджетні загальнодержавні фонди.
29. Використання бюджетних коштів не за цільовим призначенням.
30. Використання бюджетних коштів в обсягах, що перевищують затверджені межі видатків.
31. Видання нормативних актів, що змінюють доходи і видатки бюджету всупереч встановленому законом порядку.
32. Зловживання з використанням позабюджетних фондів.
33. Характеристика основних видів злочинів у бюджетній сфері.
34. Варіанти приватизації об'єктів державної власності.

- 35.Юридична відповідальність за правопорушення у ході приватизації об'єктів державної власності.
- 36.Способи вчинення зловживань у сфері приватизації.
- 37.Причини та умови, що сприяють скоєнню злочинів в процесі приватизації.
- 38.Попередження злочинів та інших правопорушень у ході приватизації.
- 39.Загальна правова характеристика видів цінних паперів. Ознаки, за якими класифікується ринок цінних паперів.
- 40.Учасники ринку цінних паперів. Складові інфраструктури ринку цінних паперів.
- 41.Основні державні органи, що здійснюють регулювання ринку цінних паперів, їх функції. Система нормативно-правового регулювання ринку цінних паперів.
- 42.Різновиди злочинів, що скоюються на вексельному ринку.
- 43.Характеристика паливно-енергетичного комплексу України.
- 44.Кримінологічна характеристика функціонування ринку лікєро-горілкової та тютюнової продукції в Україні.
- 45.Виявлення злочинної діяльності в паливно-енергетичному комплексі.
- 46.Характеристика основних видів скоюваних злочинів в ПЕК.
- 47.Зміст та сучасний стан зовнішньоекономічної діяльності в Україні.
- 48.Суб'єкти зовнішньоекономічної діяльності.
- 49.Порядок здійснення зовнішньоекономічних операцій.
- 50.Способи зловживань, що здійснюються при проведенні експортно-імпорнтних операцій.
- 51.Зловживання при здійсненні зовнішньоекономічних операцій з давальницькою сировиною.
- 52.Способи ухилень від сплати податків суб'єктами ЗЕД.
- 53.Характеристика АПК України та його структура
- 54.Сучасні організаційно-правові форми господарюючих суб'єктів.
- 55.Використання бюджетних коштів не за цільовим призначенням суб'єктами аграрної сфери.
- 56.Механізм зловживання при проведенні взаємозаліків щодо погашення заборгованості суб'єктам АПК по компенсації вартості побудованих ними об'єктів соціально-культурного призначення.
- 57.Основні види правопорушень, що скоюються в процесі реформування власності в АПК.
- 58.Зловживання при сплаті фіксованого сільськогосподарського податку.
- 59.Злочини у сфері спиртової галузі.
- 60.Злочини у сфері інтелектуальної власності.
- 61.Поняття інтелектуальної власності. Норми права, що регулюють відносини в сфері інтелектуальної власності.

- 62.Сутність відмивання доходів незаконного походження.
- 63.Загальні стадії відмивання грошей.
- 64.Види відмивання "брудних" грошей.
- 65.Стан боротьби з відмиванням коштів незаконного походження в Україні.
- 66.Страховання як форма ризик-менеджменту.
- 67.Морально-психологічний аспект бізнесу.
- 68.Зовнішня безпека підприємства.
- 69.Внутрішня безпека підприємства.
- 70.Захист комерційної таємниці.
- 71.Сутність підприємницької діяльності; нелегальність у підприємницькій діяльності.
- 72.Ризик у підприємницькій діяльності. Класифікація ризиків.
- 73.Кримінальний тиск на бізнес (форми і методи).
- 74.Конкуренція як основа ринкових відносин.
- 75.Недобросовісна конкуренція.
- 76.Засоби протидії недобросовісній конкуренції.
- 77.Комп'ютерна безпека як елемент економічної безпеки бізнесу.
- 78.Сутність і система економічної безпеки підприємства.
- 79.Управління ризиками підприємницької діяльності.
- 80.Види порушень антимонопольного законодавства.
- 81.Протидія комерційному шпигунству.
- 82.Правове регулювання захисту підприємців від незаконних дій представників органів влади.
- 83.Інформаційні технології і безпека бізнесу.
- 84.Поняття та класифікація інформації із обмеженим доступом.
- 85.Банківська таємниця. Випадки надання інформації, що містить банківську таємницю правоохоронним органам.
- 86.Організаційно-економічні заходи захисту комерційної таємниці.
- 87.Система неправохоронних контролюючих органів у сфері підприємницької діяльності.
- 88.Органи спеціального контролю у сфері підприємницької діяльності.

5. Оцінювання

Правила набору балів – протягом курсу студент може набрати до 100 балів, з яких до 80 балів набирається за рахунок виконання самостійних завдань та виступів на заняттях, і до 20 балів – на підсумковому контролі.

Студенти допускаються до підсумкового контролю за умов набору протягом семестру не менше 50 балів.

Якщо студент набрав більше 90 балів, то за його бажанням і за рішенням кафедри він може бути звільнений від іспиту.

По кожній темі можна набрати наступну максимальну кількість балів:

Теми	Завдання теми	Максимальна оцінка на семінарському занятті	Максимальна оцінка за СРС для очної форми навчання	Максимальна оцінка за СРС для заочної форми навчання
1	Тема 1. Основні аспекти інформаційної безпеки економічних систем.	10	3	13
2	Тема 2. Поняття інформаційних загроз та їх види.	9	3	12
3	Тема 3. Принципи побудови системи інформаційної безпеки.	10	3	13
4	Тема 4. Організація систем захисту інформації економічних систем.	9	4	13
5	Тема 5. Інформаційна безпека систем на макроекономічному рівні.	9	4	13
6	Тема 6. Інформаційна безпека автоматизованих банківських систем.	9	4	13
7	Тема 7. Інформаційна безпека електронної комерції	9	4	13
	Підсумок	65	25	90
ЗАЛІК			90+10	100

Шкала оцінювання

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
90-100	відмінно	A	відмінне виконання
82-89	добре	B	вище середнього рівня
75-81		C	загалом хороша робота
67-74	задовільно	D	непогано
60-66		E	виконання відповідає мінімальним критеріям
35-59	незадовільно	FX	незадовільно з можливістю повторного складання
0-34	незадовільно	F	незадовільно з обов'язковим повторним вивченням дисципліни

6. Політика курсу

1. Завдання на самостійну роботу студентів, як індивідуальні, так і загальні, мають бути здані у вказаний час: на відповідному семінарському занятті чи у зазначений термін в Гугл-класі. В разі несвоєчасного виконання завдання на автора (групу авторів) накладається штраф балів залежно від строку запізнення.
2. Під час дискусії та під час представлення групових робіт участь у ній обов'язкова для всіх членів групи. Необхідно вміти не лише виконати поставлене завдання, а й обґрунтувати його, пояснити особливості та висновки. Окрім того, участь у дискусії беруть як викладач, так і інші студенти академічної групи.
3. Самостійна домашня робота є обов'язковою для всіх студентів. Студенти виконують її в об'ємі, необхідному для набрання достатньої кількості балів.
4. Студентам рекомендується вести зошит з підготовки до занять, у який заносяться основні позиції лекційного заняття та представлено конспекти рекомендованих першоджерел з тем, питань, що виносяться на семінарські заняття. Представлений у зошиті матеріал має бути чітко структурований відповідно до питань, які розглядаються на семінарі.
5. Поведінка на заняттях регламентується загальними правилами поведіння в учбових закладах та соціальними нормами взаємодії (не дозволяється застосовувати нецензурну лексику, перебивати викладача та одногрупників, самостійно без дозволу пересуватися по аудиторії, розмовляти під час занять по мобільному телефону або спілкуватися в соцмережах).
6. Консультативну допомогу здобувачі вищої освіти можуть отримати у науково-педагогічних працівників кафедри економіки та підприємництва, який безпосередньо проводить заняття, або звернувшись з письмовим запитом на електронну пошту за адресою: dekanat@kibit.edu.ua