КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з наукової роботи
та міжнародної діяльності
_____ Наталія ВІННІКОВА
«13» січня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ПРИКЛАДНІ АСПЕКТИ ТЕОРІЙ РИЗИКІВ, КОНФЛІКТІВ І КАТАСТРОФ В СИСТЕМАХ БЕЗПЕКИ

для аспірантів

спеціальності 125 Кібербезпека та захист інформації
освітнього рівня третього (освітньо-наукового)
освітньо-наукової програми «Інформаційна безпека держави»

Київ – 2025

Розробник:

Шевченко Світлана Миколаївна, кандидат педагогічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка.

Викладач:

Шевченко Світлана Миколаївна, кандидат педагогічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 03.01.2024 № 1

Завідувач кафедри _____ Павло СКЛАДАННИЙ
(підпис)

Робочу програму погоджено з гарантом освітньо-наукової програми «Інформаційна безпека держави»
03.01.20 1

Гарант освітньо-наукової програми _____ Наталія КОРШУН
(підпис)

Робочу програму перевірено
11.01.2024
Завідувач аспірантури, докторантури _____ Ілона ТРИГУБ
(підпис)

Пролонговано:

на 2024/2025 н.р. Складанний П. (_____), «08» 01 2025 р., протокол №01
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4/120	
Рік навчання	2-3	2-3
Семестр	4,5	4,5
Кількість змістових модулів з розподілом:	4	
Обсяг кредитів	4	4
Обсяг годин, в тому числі:	120	120
Аудиторні	32	16
Модульний контроль	8	-
Самостійна робота	80	104
Семестровий контроль	Залік	

2. Мета та завдання навчальної дисципліни

Мета: формування в аспірантів знань, умінь і навичок з впровадження та застосування теоретичних основ теорій ризиків, конфліктів і катастроф в системи безпеки

Завдання: отримання теоретичних знань та практичних умінь з дослідження теорій ризиків, конфліктів та катастроф в системах інформаційної та кібербезпеки та набуття наступних компетентностей:

– здатність використовувати системний підхід до управління ризиками інформаційної безпеки;

– здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення безпеки систем інформаційної та\або кібербезпеки на основі теорії катастроф;

– здатність до застосування методів сучасних інформаційних конфліктів у сфері захисту інформації.

У результаті вивчення навчальної дисципліни відповідно до освітньо-наукової програми спеціальності формуються фахові компетентності:

Програмні компетентності	**Код**	**Значення компетентності**
Фахові компетентності (ФК)	ФК-3	Здатність застосовувати сучасні ІТ технології при створенні систем інформаційної та/або кібербезпеки і захисту інформації;
	ФК-6	Здатність до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки ІТ систем та мереж, обробки та перетворення інформації.

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни аспірант повинен

знати:

– основні поняття і закони теорії ризиків для їх використання в сучасних кіберсистемах;

– принципи побудови алгоритмів оцінки ризиків у кібербезпеці, основних стандартів оцінки ризиків та їх використання в задачах захисту інформації;

– математичний апарат для визначення оцінки ризиків у професійній діяльності;

– основні моделі катастроф, математичний апарат їх опису та можливості їх застосування в системах безпеки;

– сучасні методи інформаційних конфліктів та способи їх застосування;

вміти:

– застосовувати алгоритми та основні стандарти оцінки ризиків у кібербезпеці з метою ефективного управління ними;

– застосовувати методології, методи та алгоритми теорії катастроф для моделювання систем захисту інформації;

– застосовувати науково-технічний апарат дослідження інформаційного конфлікту в системах безпеки;

– використовувати математичний апарат та програмні засоби, які реалізують основні алгоритми оцінки ризиків, методи інформаційних конфліктів та катастроф для вирішення типових задач захисту інформації.

та досягти наступних програмних результатів навчання:

– знати та розуміти принципи, методології та методи теорії ризиків, теорії конфліктів, теорії катастроф в системах безпеки;

– використовувати методи, технології та інструментальні засоби теорій ризиків, конфліктів та катастроф для моделювання систем захисту інформації;

– забезпечувати інформаційну безпеку держави та неперервність бізнес процесів організації на базі системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів; забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками, конфліктами та катастрофами.

Програмні результати навчання:

Код	Значення програмного результату
ПРН 6	- розробляти та впроваджувати дослідницькі проекти в сфері захисту інформації, інформаційної та кібербезпеки; - розробляти алгоритми, моделі, методи та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки; - здійснювати захист ресурсів і процесів в ІКС на основі моделей безпеки та встановлених режимів їх безпечного функціонування; - забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту, виконувати розробку експлуатаційної документації на КЗЗ;

	- забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками з врахуванням можливих конфліктів і катастроф.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назви змістових модулів і тем	Усього	Розподіл годин між видами робіт			
		Аудиторна			Самостійна
		Лекції	Практичні	Семінарські	
Змістовий модуль І. Прикладні аспекти теорії ризиків в системах безпеки					
Тема 1. Управління ризиками ІБ: основні поняття і нормативне забезпечення	8	2			6
Тема 2. Сучасні методи і засоби аналізу, оцінки та обробки ризиків ІБ	13		4		9
Тема 3. Базові параметри та моделі інформаційних ризиків	8			2	6
Модульний контроль	2				
Разом	**31**	**2**	**4**	**2**	**21**
Змістовий модуль ІІ. Методологія побудови систем інформаційних ризиків					
Тема 4. Система аналізу та оцінювання ризиків втрат інформаційних ресурсів	9	2		2	5
Тема 5. Детермінована система аналізу та оцінювання ризиків безпеки інформаційних ресурсів	8		2		6
Тема 6. Система аналізу та оцінювання ризиків в нечіткому середовищі	8		2		6
Модульний контроль	2				
Разом	**27**	**2**	**4**	**2**	**17**
Змістовий модуль ІІІ. Прикладні аспекти теорії катастроф в системах безпеки					
Тема 7. Теорія катастроф: основні поняття та історичний розвиток	11	2	2		7
Тема 8. Теорія катастроф у Пуанкаре та А. Андронова	9			2	7
Тема 9. Елементарна теорія катастроф та її застосування в системах безпеки	13		2		11
Модульний контроль	2				
Разом	**35**	**2**	**4**	**2**	**25**
Змістовий модуль ІV. Прикладні аспекти теорії конфліктів в системах безпеки					
Тема 10. Інформаційні конфлікти: основні поняття та методи	10	2		2	6
Тема 11. Науково-методичний апарат дослідження інформаційного конфлікту та його застосування в системах безпеки	15	2	2		11
Модульний контроль 4	2				
Разом	**27**	**4**	**2**	**2**	**17**
Усього	**120**	**10**	**14**	**8**	**80**

Тематичний план для заочної форми навчання

Назви змістових модулів і тем	Усього	Розподіл годин між видами робіт			
		Аудиторна			Самостійна
		Лекції	Практичні	Семінарські	
Змістовий модуль І. Прикладні аспекти теорії ризиків в системах безпеки					
Тема 1. Управління ризиками ІБ: основні поняття і нормативне забезпечення	10	2			8
Тема 2. Сучасні методи і засоби аналізу, оцінки та обробки ризиків ІБ	10		2		8
Тема 3. Базові параметри та моделі інформаційних ризиків	10				10
Разом	**30**	**2**	**2**		**26**
Змістовий модуль ІІ. Методологія побудови систем інформаційних ризиків					
Тема 4. Система аналізу та оцінювання ризиків втрат інформаційних ресурсів	10	2			8
Тема 5. Детермінована система аналізу та оцінювання ризиків безпеки інформаційних ресурсів	10			2	8
Тема 6. Система аналізу та оцінювання ризиків в нечіткому середовищі	10				10
Разом	**30**	**2**		**2**	**26**
Змістовий модуль ІІІ. Прикладні аспекти теорії катастроф в системах безпеки					
Тема 7. Теорія катастроф: основні поняття та історичний розвиток	10	2			8
Тема 8. Теорія катастроф у Пуанкаре та А. Андронова	10				10
Тема 9. Елементарна теорія катастроф та її застосування в системах безпеки	10		2		8
Разом за змістовим модулем	**30**	**2**	**2**		**26**
Змістовий модуль ІV Прикладні аспекти теорії конфліктів в системах безпеки					
Тема 10. Інформаційні конфлікти: основні поняття та методи	15	2			13
Тема 11. Науково-методичний апарат дослідження інформаційного конфлікту та його застосування в системах безпеки	15			2	13
Разом	**30**	**2**		**2**	**26**
Усього	**120**	**8**	**4**	**4**	**104**

5. Програма навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ І. Прикладні аспекти теорії ризиків в системах безпеки

Тема 1. Управління ризиками ІБ: основні поняття і нормативне забезпечення

Поняття ризику ІБ, його сутність та складові. Блок-схема процесу управління ризиком ІБ, основні етапи управління ризиком та їх характеристика.

Нормативне забезпечення аналізу та оцінювання ризиків. Міжнародні стандарти забезпечення аналізу та оцінювання ризиків.

Ключові слова: ризик ІБ, управління ризиками ІБ, нормативне забезпечення управління ризиками ІБ.

Література:

1. Архипов О. Є., Муратов О. Є., Бровко В. Д. Основи теорії ризиків : навч. посіб / О. Є. Архипов, О. Є. Муратов, В. Д. Бровко. – Київ : НА СБ України, 2019. – 267 с.

2. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT)

3. http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797

4. Замула О. А., В. І. Черниш. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О. А. Замула, В. І. Черниш // Системи обробки інформації: збірних наукових праць. – Харків : ХУ ПС, 2014. – Вип. 2(92). – С. 53–56.

5. Antonucci D. The Cyber Risk Handbook / Domenic Antonucci. – New Jersey: John Wiley & Sons, 2017. – 433 с.

Тема 2. Сучасні методи і засоби аналізу, оцінки та обробки ризиків ІБ

Методи якісної оцінки ризику (методи PEST-, SWOT-, SNW-аналізу). Методи кількісної оцінки ризику (статистичний, метод аналізу доцільності витрат, аналіз чутливості, аналіз сценаріїв, метод Монте-Карло, метод аналогій, експертні методи оцінювання ризику, нормативний метод).

Засоби якісного та кількісного аналізу та оцінювання ризиків ІБ: ISAMM, EBIOS, Octave, IT-Grundschutz, CRAMM, Magerit, Cobra, RiskWatch, ГРИФ 2006 та інші.

Методи управління ризиками ІБ. Прийоми зниження ризику ІБ. Прийняття ризику ІБ.

Ключові слова: ризик ІБ, ідентифікація ризиків ІБ, аналіз ризиків ІБ, якісна оцінка ризиків ІБ, кількісна оцінка ризиків ІБ, методи якісної оцінки ризиків ІБ, методи кількісної оцінки ризиків ІБ, програмні засоби оцінки ризиків ІБ, обробка ризиків ІБ.

Література:

1. Архипов О. Є., Муратов О. Є., Бровко В. Д. Основи теорії ризиків : навч. посіб / О. Є. Архипов, О. Є. Муратов, В. Д. Бровко. – Київ : НА СБ України, 2019. – 267 с.

2. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT)

http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797

3. Замула О. А., В. І. Черниш. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О. А. Замула, В. І. Черниш // Системи обробки інформації: збірних наукових праць. – Харків : ХУ ПС, 2014. – Вип. 2(92). – С. 53–56.

Тема 3. Базові параметри та моделі інформаційних ризиків

Модель подачі параметрів ризиків. Параметри, що використовуються засобами аналізу та оцінювання ризиків.

Модель «небезпека-ризик». Модель «невизначеність-ризик». Модель «можливості - ризик/шанс».

Ключові слова: параметри ризиків ІБ, модель інформаційного ризику «небезпека-ризик», модель інформаційного ризику «невизначеність-ризик», модель інформаційного ризику «можливості – ризик / шанс».

Література:

1. Архипов О. Є., Муратов О. Є., Бровко В. Д. Основи теорії ризиків : навч. посіб / О. Є. Архипов, О. Є. Муратов, В. Д. Бровко. – Київ : НА СБ України, 2019. – 267 с.

2. Antonucci D. The Cyber Risk Handbook / Domenic Antonucci. – New Jersey: John Wiley & Sons, 2017. – 433 с.

ЗМІСТОВИЙ МОДУЛЬ ІІ. Методологія побудови систем інформаційних ризиків

Тема 4. Система аналізу та оцінювання ризиків втрат інформаційних ресурсів

Вибір методу аналізу та оцінювання ризиків. Ідентифікація ресурсу, дій, подій, оціночних компонент. Формування еталонів для ступеня ризику, формування еталонів для рівня оціночних компонент. Визначення рівня значущості, поточного значення. Класифікація поточних значень. Оцінка ступеня ризику. Інтерпретація ступеня ризику.

Ключові слова: оціночний компонент, еталон для ступеня ризику, оцінка ступеня ризику, інтерпретація ступеня ризику.

Література:

1. Архипов О. Є., Муратов О. Є., Бровко В. Д. Основи теорії ризиків : навч. посіб. / О. Є. Архипов, О. Є. Муратов, В. Д. Бровко. – Київ : НА СБ України, 2019. – 267 с.

2. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT) http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797

3. Antonucci D. The Cyber Risk Handbook / Domenic Antonucci. – New Jersey: John Wiley & Sons, 2017. – 433 с.

Тема 5. Детермінована система аналізу та оцінювання ризиків безпеки інформаційних ресурсів

Структурно-параметрична модель Det-AOP, її підсистеми, модулі та алгоритм дій.

Практика застосування експертних оцінок ризиків ІБ.

Ключові слова: експертна оцінка ризику ІБ, методи експертних оцінок ризику ІБ, структурно-параметрична модель Det-AOP.

Література:

1. Архипов О. Є., Муратов О. Є., Бровко В. Д. Основи теорії ризиків : навч. посіб / О. Є. Архипов, О. Є. Муратов, В. Д. Бровко. – Київ : НА СБ України, 2019. – 267 с.

2. Моделі економічної динаміки : підручник / В. А. Кадієвський, Л. П. Перхун, С. М. Братушка, О. О. Синявська. – Київ : ДП «Інформ.-аналіт. агенство», 2017. – 466 с.

3. Antonucci D. The Cyber Risk Handbook / Domenic Antonucci. – New Jersey: John Wiley & Sons, 2017. – 433 с.

Тема 6. Система аналізу та оцінювання ризиків в нечіткому середовищі

Лінгвістичні змінні та нечіткі множини. Метод FuzM та його застосування для аналізу та оцінювання ризиків.

Інтегрований метод аналізу та оцінювання ризиків інформаційної безпеки.

Ключові слова: нечіткі множини, аналіз ризиків ІБ в нечіткому середовищі, метод FuzM.

Література:

1. Архипов О. Є., Муратов О. Є., Бровко В. Д. Основи теорії ризиків : навч. посіб / О. Є. Архипов, О. Є. Муратов, В. Д. Бровко. – Київ : НА СБ України, 2019. – 267 с.

2. Барибін О. І. Стандартизація та сертифікація в галузі інформаційної безпеки : навч. посіб. / О. І. Барибін. – Вінниця : ДонНУ імені Василя Стуса, 2018. – 238 с.

3. Бурячок В. Л., Хорошко В. О. Технологія прийняття рішень у складних соціотехнічних системах : монографія / В. Л. Бурячок, В. О. Хорошко. – Київ : ДУІКТ, 2012. – 344 с.

4. Економічний ризик: методи оцінки та управління : навч. посібник / Т. А. Васильєва, С. В. Лєонов, Я. М. Кривич та ін. ; під заг. ред. д-ра екон. наук, проф. Т. А. Васильєвої, канд. екон. наук Я. М. Кривич. – Суми : ДВНЗ «УАБС НБУ», 2015. – 208 с.

ЗМІСТОВИЙ МОДУЛЬ ІІІ. Прикладні аспекти теорії катастроф в системах безпеки

Тема 7. Теорія катастроф: основні поняття та історичний розвиток

Стійкість системи. Біфуркації. Математичні основи теорії катастроф. Катастрофічні моделі.

Ключові слова: стійкість системи, біфуркація, катастрофічні моделі.

Література:

1. Бурячок В. Л., Хорошко В. О. Технологія прийняття рішень у складних соціотехнічних системах : монографія / В. Л. Бурячок, В. О. Хорошко. – Київ : ДУІКТ, 2012. – 344 с.

2. Економічний ризик: методи оцінки та управління : навч. посібник / Т. А. Васильєва, С. В. Лєонов, Я. М. Кривич та ін. ; під заг. ред. д-ра екон.

наук, проф. Т. А. Васильєвої, канд. екон. наук Я. М. Кривич. – Суми : ДВНЗ «УАБС НБУ», 2015. – 208 с.

3. Інформаційна безпека держави : навч. посіб. / В. М. Рудницький. С. О. Гнатюк, Н. В. Лада, Р. В. Бреус ; Черкас. держ. технолог. ун-т. – Харків : ДІСА ПЛЮС, 2018. – 359 с.

Тема 8. Теорія катастроф у Пуанкаре та А.Андронова

Основні положення теорії стійкості та біфуркації у Пуанкаре та А. Андронова.

Ключові слова: теорія стійкості Пуанкаре, теорія стійкості у А. Андронова.

Література:

1. Бурячок В. Л., Хорошко В. О. Технологія прийняття рішень у складних соціотехнічних системах : монографія / В. Л. Бурячок, В. О. Хорошко. – Київ : ДУІКТ, 2012. – 344 с.

2. Економічний ризик: методи оцінки та управління : навч. посібник / Т. А. Васильєва, С. В. Лєонов, Я. М. Кривич та ін. ; під заг. ред. д-ра екон. наук, проф. Т. А. Васильєвої, канд. екон. наук Я. М. Кривич. – Суми : ДВНЗ «УАБС НБУ», 2015. – 208 с.

3. Henry K. Risk management and analysis / K. Henry // Information Security Management Handbook / Edited by H. F. Tipton, M. Krauze. – 6th edition. – Boca Raton : Auerbach Publications, 2017. – Part 1, Section 1.4, Ch. 28. – P. 321–329.

Тема 9. Елементарна теорія катастроф та її застосування в системах безпеки

Потенційні функції. Заміна змінних і канонічні форми. Заміна змінних та обурення. Геометрія складки та зборки.

Ключові слова: елементарні математичні катастрофи, потенційні функції, складки, зборки.

Література:

1. Моделі економічної динаміки : підручник / В. А. Кадієвський, Л. П. Перхун, С. М. Братушка, О. О. Синявська. – Київ : ДП «Інформ.-аналіт. агенство», 2017. – 466 с.

2. Alberts C. J. Operationally Critical Threat, Asset and Vulnerability Evaluation / C. J. Alberts, S. G. Behrens, R. D. Pethia, W. R. Wilson. – 2018. – P. 84.

ЗМІСТОВИЙ МОДУЛЬ IV. Прикладні аспекти теорії конфліктів в системах безпеки

Тема 10. Інформаційні конфлікти: основні поняття та методи

Загальні відомості про інформаційні конфлікти. Моделі інформаційних конфліктів та їх застосування в системах безпеки.

Ключові слова: інформаційні конфлікти, моделі інформаційних конфліктів, управління інформаційними конфліктами.

Література:

1. Замула О. А., В. І. Черниш. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О. А. Замула, В. І. Черниш // Системи обробки інформації: збірних наукових праць. – Харків : ХУ ПС, 2014. – Вип. 2(92). – С. 53–56.

2. Моделі економічної динаміки : підручник / В. А. Кадієвський, Л. П. Перхун, С. М. Братушка, О. О. Синявська. – Київ : ДП «Інформ.-аналіт. агенство», 2017. – 466 с.

Тема 11. Науково-методичний апарат дослідження інформаційного конфлікту та його застосування в системах безпеки

Теорія активних систем. Теорія динамічних систем. Теорія ігор. Теорія марковських процесів. Теорія мережі Петрі. Теорія нечітких множин. Теорія логіки.

Ключові слова: теорія ігор, марковські процеси, мережа Петрі, нечіткі множини.

Література:

1. Бурячок В. Л., Хорошко В. О. Технологія прийняття рішень у складних соціотехнічних системах : монографія / В. Л. Бурячок, В. О. Хорошко. – Київ: ДУІКТ, 2012. – 344 с.

6. Контроль навчальних досягнень

6.1. Система оцінювання навчальних досягнень аспірантів денної форми навчання

№ з/п	Вид діяльності аспіранта	Макс. кільк. балів заодиницю	Модуль 1		Модуль 2		Модуль 3		Модуль 4	
			Кільк.один.	Макс. кільк. балів	Кільк.один.	Макс. кільк. балів	Кільк.один.	Макс. кільк. балів	Кільк.один.	Макс. кільк. балів
1	Відвідування лекцій	1	1	1	1	1	1	1	2	2
2	Відвідування практичних занять	1	2	2	2	2	2	2	1	1
3	Відвідування семінарських занять	1	1	1	1	1	1	1	1	1
4	Робота на практичних заняттях	10	2	20	2	20	2	20	1	10
5	Робота на семінарських заняттях	10	1	10	1	10	1	10	1	10
4	Виконання завдань для самостійної роботи	5	3	15	3	15	3	15	2	10
5	Виконання модульної контрольної роботи	25	1	25	1	25	1	25	1	25
6	Макс. кількість балів за видами поточного контролю			**74**		**74**		**74**		**59**
7	Максимальна кількість балів:	**281**								
8	Розрахунок коефіцієнта Бал max / Сума балів max	**100/281=0,36**								

Система оцінювання навчальних досягнень аспірантів заочної форми навчання

№ з/п	Вид діяльності аспіранта	Макс. кільк. балів заодиницю	Модуль 1		Модуль 2		Модуль 3		Модуль 4	
			Кільк.один.	Макс. кільк. балів	Кільк.один.	Макс. кільк. балів	Кільк.один	Кільк.один.	Макс. кільк. балів	Кільк.один.
1	Відвідування лекцій	1	1	1	1	1	1	1	1	1
2	Відвідування практичних занять	1	1	1			1	1		
3	Відвідування семінарських занять	1			1	1			1	1
4	Робота на практичних заняттях	10	1	10			1	10		
5	Робота на семінарських заняттях	10			1	10			1	10
4	Виконання завдань для самостійної роботи	5	3	15	3	15	3	15	2	10
6	Макс. кількість балів за видами поточного контролю			**27**		**27**		**27**		**22**
7	Максимальна кількість балів:	**103**								
9	Розрахунок коефіцієнта Бал max / Сума балів max	**100/103=0,97**								

Умовою зарахування кожного змістовного модулю та отримання аспірантом заліку є здобуття не менше 35% балів (Бал min / Бал max = 35:100=0,35) за результатами всіх видів означених діяльностей в кожному змістовному модулі.

6.2. Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом позааудиторної індивідуальної діяльності аспіранта, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності. В межах кожної теми аспіранти, використовуючи рекомендовану літературу, повинні самостійно опрацювати першоджерела за запропонованою тематикою. Огляд представити у вигляді наукового реферату за вибраною темою з прикладами з предметної області.

№ з/п	Назва теми
Змістовий модуль 1. Прикладні аспекти теорії ризиків в системах безпеки	
1	Системний підхід до управління ризиками ІБ
2	Методи і засоби аналізу та оцінювання ризиків ІБ
3	Моделі інформаційних ризиків
Змістовий модуль 2. Методологія побудови систем інформаційних ризиків	
4	Система аналізу та оцінювання ризиків втрат інформаційних ресурсів
5	Детермінована система аналізу та оцінювання ризиків безпеки інформаційних ресурсів
6	Система аналізу та оцінювання ризиків в нечіткому середовищі
Змістовий модуль 3. Прикладні аспекти теорії катастроф в системах безпеки	
7	Класифікація катастроф по Тому
8	Класифікація катастроф по Арнольду
9	Перспективи використання теорії катастроф у дослідженні інформаційної безпеки організації
Змістовий модуль 4. Прикладні аспекти теорії конфліктів в системах безпеки	
10	Види сучасних інформаційних конфліктів та їх методи вирішення
11	Методи дослідження інформаційного конфлікту та його застосування в системах безпеки

Критерії оцінювання самостійної роботи аспіранта

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2
3	Дотримання вимог щодо технічного оформлення	1
	Разом	5

6.3. Форми проведення модульного контролю та критерії оцінювання

Оцінка за кожний змістовий модуль включає бали за поточну роботу аспіранта на практичних заняттях, за модульну контрольну роботу. Модульний контроль знань аспіранта здійснюється після завершення вивчення навчального матеріалу модуля. Форма проведення – комп'ютерний тест, що складається з 20 питань закритої та відкритої форм. Модульна контрольна робота оцінюється у 25 балів. Критерії оцінювання модульного контролю наведено у таблиці.

Критерії оцінювання модульного контролю

Сума балів	Значення оцінки
22-25	аспірант виявив повне знання програмного матеріалу, успішно виконує передбачені програмою завдання, засвоїв основну літературу рекомендовану програмою, виявив систематичний характер знань з дисципліни і здатний до самостійного доповнення.
13-21	аспірант виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, вміє виконувати завдання, передбачені програмою, знайомий з основною рекомендованою літературою.
0-13	аспірант, що виявив часткове знання основного програмового матеріалу, не завжди вміє виконувати завдання, передбачені програмою, знайомий лише частково з основною рекомендованою літературою.

6.4 Форми проведення семестрового контролю та критерії оцінювання

Семестровий контроль знань аспірантів здійснюється після завершення вивчення навчального матеріалу дисципліни у формі заліку. Підсумкова семестрова (залікова) рейтингова оцінка аспіранта є сумою підсумкових фактичних оцінок аспіранта за змістовими модулями.

6.5. Оцінювання освітніх досягнень аспірантів за системою ECTS

Рейтингова оцінка	Оцінка за стобальною шкалою	Значення оцінки
A	90-100 балів	Відмінно – відмінний рівень знань (умінь) в межах обов'язкового матеріалу з можливими незначними недоліками
B	82-89 балів	Дуже добре - достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	75-81 балів	Добре – в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74 балів	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68 балів	Достатньо – мінімально можливий допустимий рівень знань (умінь)
FX	35-59 балів	Незадовільно з можливістю повторного складання – незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34 балів	Незадовільно з обов'язковим повторним вивченням дисципліни – досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Рекомендовані джерела:

Основна (базова):

1. Архипов О. Є., Муратов О. Є., Бровко В. Д. Основи теорії ризиків : навч. посіб / О. Є. Архипов, О. Є. Муратов, В. Д. Бровко. – Київ : НА СБ України, 2019. – 267 с.
2. Барибін О. І. Стандартизація та сертифікація в галузі інформаційної безпеки : навч. посіб. / О. І. Барибін. – Вінниця : ДонНУ імені Василя Стуса, 2018. – 238 с.
3. Бурячок В. Л., Хорошко В. О. Технологія прийняття рішень у складних соціотехнічних системах : монографія / В. Л. Бурячок, В. О. Хорошко. – Київ : ДУІКТ, 2012. – 344 с.
4. Економічний ризик: методи оцінки та управління : навч. посібник / Т. А. Васильєва, С. В. Лєонов, Я. М. Кривич та ін. ; під заг. ред. д-ра екон. наук, проф. Т. А. Васильєвої, канд. екон. наук Я. М. Кривич. – Суми : ДВНЗ «УАБС НБУ», 2015. – 208 с
5. Замула О. А., Черниш В. І. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О. А. Замула, В. І. Черниш // Системи обробки інформації: збірних наукових праць. – Харків : ХУ ПС, 2014. – Вип. 2(92). – С. 53–56.

6. Моделі економічної динаміки : підручник / В. А. Кадієвський, Л. П. Перхун, С. М. Братушка, О. О. Синявська. – Київ : ДП «Інформ.-аналіт. агенство», 2017. – 466 с.

Додаткова:

1. Інформаційна безпека держави : навч. посіб. / В. М. Рудницький, С. О. Гнатюк, Н. В. Лада, Р. В. Бреус ; Черкас. держ. технолог. ун-т. – Харків : ДІСА ПЛЮС, 2018. – 359 с.

2. Кишакевич Б. Ю., Климкович І. В. Застосування теорії катастроф для моделювання фінансової стійкості банківської системи / Б. Ю. Кишакевич, І. В. Климкович // Науковий вісник НЛТУ України. – 2016. – Вип. 26.6. – С. 312–318.

3. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT)

4. Alberts C. J. Operationally Critical Threat, Asset and Vulnerability Evaluation / C. J. Alberts, S. G. Behrens, R. D. Pethia, W. R. Wilson. – 2018. – P. 84.

5. Antonucci D. The Cyber Risk Handbook / Domenic Antonucci. – New Jersey: John Wiley & Sons, 2017. – 433 с.

6. Endorf C. F. Measuring ROI on security / Carl F. Endorf // Information security management handbook / Edited by H. F. Tipton, M. Krauze. – 6th edition. – Boca Raton : Auerbach Publications, 2017. – Part 1, Section 1.1, Ch. 12. – P. 133–137.

7. Henry K. Risk management and analysis / K. Henry // Information Security Management Handbook / Edited by H. F. Tipton, M. Krauze. – 6th edition. – Boca Raton : Auerbach Publications, 2017. – Part 1, Section 1.4, Ch. 28. – P. 321–329.

http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797

8. ISO/IEC 13335:2000 «Information technology. Guidelines for the management of IT Security. Part 4: Selection of safeguards».

9. ISO/IEC 13335-1:2004 «Information technology. Security techniques. Management of information and communications technology security».

10. ISO/IEC 13335-3:1998 «Information technology. Guidelines for the management of IT Security. Part 3: Techniques for the management of IT Security».

11. ISO/IEC 15408-1:2009 «The Common Criteria for Information Technology Security Evaluation. 1: Introduction and general model».

12. ISO/IEC 15408-2:2008 «The Common Criteria for Information Technology Security Evaluation. Security functional components».

13. ISO/IEC 15408-3:2008 «The Common Criteria for Information Technology Security Evaluation. Security assurance components».

14. ISO/IEC 27001:2005 «Information technology. Security techniques. Information security management systems. Requirements».

15. ISO/IEC 27002:2005 «Information technology. Security techniques. Code of practice for information security management».

16. ISO/IEC Guide 73:2009 «Risk management. Vocabulary. Guidelines for use in standards».

17. ISO/IEC TR 18044:2004 «Information technology. Security techniques. Information security incident management».

18. ISO/TR 13569:2005 «Financial services - Information security guidelines».

19. Landoll D. The security risk assessment handbook: a complete guide for performing security risk assessments / Douglas J. Landoll. – Boca Raton: Auerbach Publications, 2016. – 504 p.

20. Rittinghouse J. W. Business continuity and disaster recovery for infosec managers / John W. Rittinghouse, James F. Ransome. – Oxford: Elsevier, 2015. – 408 p.

21. Spedding L., Rose A. Business risk management handbook: a sustainable approach / L. Spedding, A. Rose. – Oxford : Elsevier, 2018. – 768 p.

Додаткові ресурси:

1. Конституція України [Електронний ресурс] : Закон від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / ВР України. – Режим доступу : http://zakon2.rada.gov.ua/laws/(дата звернення: 08.02.2012).

2. Cybercomply: risk-proof your data : Manage all your cyber security and data privacy obligations in one powerful tool [Electronic resource] // Vigilant : web-site. – Access mode: https://www.vigilantsoftware.co.uk/

3. GeNIe Modeler: Complete Modeling Freedom [Electronic resource] // BayesFusion : web-site. – Access mode: https://www.bayesfusion.com/genie/