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
_____ Наталія ВІННІКОВА
«__» _____ 2024 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 – 2024

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 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)

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	3/90	
Рік навчання	2-3	2-3
Семестр	4,5	4,5
Кількість змістових модулів з розподілом:	3	
Обсяг кредитів	3	3
Обсяг годин, в тому числі:	90	90
Аудиторні	24	12
Модульний контроль	6	-
Самостійна робота	60	78
Форма семестрового контролю	Залік	

2. Мета та завдання навчальної дисципліни

Мета: формування у здобувачів 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 спеціальні (фахові, предметні) компетентності:

Програмні компетентності	**Код**	**Значення компетентності**
Спеціальні компетентності (СК)	СК-1	Здатність оцінювати фізичні, технологічні, інформаційні, соціологічні, етичні та інші процеси інформаційного і кіберпросторів.
	СК-3	Здатність застосовувати сучасні IT технології при створенні систем інформаційної та/або кібербезпеки і захисту інформації, електронні інформаційні ресурси, спеціалізоване

		програмне забезпечення у науковій та навчальній діяльності; здійснювати проєктну діяльність на засадах лідерства.
	СК-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 здобувач 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
РН 4	Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів; здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності; проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД; обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах; використовувати сучасні

	техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів, зокрема дотичних міждисциплінарних напрямів.
РН 6	Розробляти та впроваджувати науково-дослідницькі та інноваційні проєкти 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.
РН 7	Вирішувати задачі централізованого і децентралізованого адміністрування доступом до ІР і процесів в ІКС та реалізовувати заходи з протидії отриманню несанкціонованого доступу до них; володіти науково-організаційними основами проведення аудиту безпеки ІКС, а також науковими методами та практичними навичками щодо створення систем моніторингу безпеки в ІТ системах та мережах.

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	10	4			6
Тема 2. Сучасні методи і засоби аналізу, оцінки та обробки ризиків ІБ	10		4		6
Тема 3. Базові параметри та моделі інформаційних ризиків	10			2	8
Модульний контроль 1	2				
Разом за змістовим модулем 1	32	4	4	2	20
Змістовий модуль ІІ. Прикладні аспекти теорії катастроф в системах безпеки					
Тема 4. Теорія катастроф: основні поняття та історичний розвиток	12	2			10
Тема 5. Елементарна теорія катастроф та її застосування в системах безпеки	14	2	2		10
Модульний контроль 2	2				
Разом за змістовим модулем 2	28	4	2		20

Змістовий модуль ІІІ. Прикладні аспекти теорії конфліктів в системах безпеки					
Тема 6. Інформаційні конфлікти: основні поняття та методи	14	2		2	10
Тема 7. Науково-методичний апарат дослідження інформаційного конфлікту та його застосування в системах безпеки	14	2	2		10
Модульний контроль 3	2				
Разом за змістовим модулем 3	30	4	2	2	20
Разом	**90**	**12**	**8**	**4**	**60**

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		1		9
Тема 3. Базові параметри та моделі інформаційних ризиків	10		1		9
Разом за змістовим модулем	30	2	2		26
Змістовий модуль ІІ. Прикладні аспекти теорії катастроф в системах безпеки					
Тема 4. Теорія катастроф: основні поняття та історичний розвиток	12	2			10
Тема 5. Елементарна теорія катастроф та її застосування в системах безпеки	18			2	16
Разом за змістовим модулем	30	2		2	26
Змістовий модуль ІІІ. Прикладні аспекти теорії конфліктів в системах безпеки					
Тема 6. Інформаційні конфлікти: основні поняття та методи	12	2			10
Тема 7. Науково-методичний апарат дослідження інформаційного конфлікту та його застосування в системах безпеки	18		2		16
Разом за змістовим модулем	30	2	2		26
Разом	**90**	**6**	**4**	**2**	**78**

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.https://drive.google.com/file/d/1YyY2JE6SmFPpEEdWBB9MZZR4sPFqXNgn/view?usp=sharing
2. Стандарт NIST 800-30 https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf
3. BSI-Standard 200-3 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-3-Risikomanagement/bsi-standard-200-3-risikomanagement_node.html
4. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks
5. ДСТУ ISO/IEC 27005:2023 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT)
6. Antonucci D. The Cyber Risk Handbook / Domenic Antonucci. – New Jersey: John Wiley & Sons, 2017. – 433 c.

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. https://drive.google.com/file/d/1YyY2JE6SmFPpEEdWBB9MZZR4sPFqXNgn/view?usp=sharing

2. Стандарт NIST 800-30
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf
3. BSI-Standard 200-3 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-3-Risikomanagement/bsi-standard-200-3-risikomanagement_node.html
4. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks
5. ДСТУ ISO/IEC 27005:2023 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT)
6. Shevchenko H., Shevchenko S., Zhdanova Y., Spasiteleva S. and O. Negodenko (2021) *Information Security Risk Analysis SWOT* - Cybersecurity Providing in Information and Telecommunication Systems, 2923. С. 309-317. ISSN 1613-0073
7. Шевченко С.М. Модель захисту інформації на основі оцінки ризиків інформаційної безпеки для малого та середнього бізнесу / С.М. Шевченко, Ю.Д. Жданова, К.В. Кравчук // Кібербезпека: освіта, наука, техніка. – 2021, Том 2, № 14. – С. 158-175.
8. Antonucci D. The Cyber Risk Handbook / Domenic Antonucci. – New Jersey: John Wiley & Sons, 2017. – 433 с.

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.
3. Rotshtein A. Risk Analysis: Fuzzy Cognitive Map vs Fault Tree, Journal of Computer and Systems Sciences International, 2019, 2: 200–211.
https://link.springer.com/article/10.1134/S1064230719020163
4. Shevchenko S., Zhdanova Y., Shevchenko H., Nehodenko O. and Spasiteleva S. (2023) *Information Security Risk Management using Cognitive Modeling* Cybersecurity Providing in Information and Telecommunication Systems, 3550. с. 297-305. ISSN 1613-0073.

ЗМІСТОВИЙ МОДУЛЬ ІІ. Прикладні аспекти теорії катастроф в системах безпеки

Тема 4. 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. 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.
2. Arnold, Vladimir Igorevich. Catastrophe Theory, 3rd ed. Berlin: Springer-Verlag, 1992.
3.Gilmore Robert. Catastrophe Theory of Scientists and Engineers. New York: Dover, 1993.
4. Sanns, Werner. Catastrophe Theory with Mathematica: A Geometric Approach. Germany: DAV, 2000
5. Шевченко С.М., Жданова Ю.Д., Спасітєлєва С.О. (2023) *Математичні методи в кібербезпеці: теорія катастроф.* Кібербезпека: освіта, наука, техніка, 2023, 3 (19). с. 165-175.

Тема 5. 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: ктастрофи в системах безпеки, елементарні математичні катастрофи, потенційні функції, складки, зборки.

Література:

1. 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.
2. Arnold, Vladimir Igorevich. Catastrophe Theory, 3rd ed. Berlin: Springer-Verlag, 1992.
3.Gilmore Robert. Catastrophe Theory of Scientists and Engineers. New York: Dover, 1993.
4. Sanns, Werner. Catastrophe Theory with Mathematica: A Geometric Approach. Germany: DAV, 2000
5. Шевченко С.М., Жданова Ю.Д., Спасітєлєва С.О. (2023) *Математичні методи в кібербезпеці: теорія катастроф.* Кібербезпека: освіта, наука, техніка, 2023, 3 (19). с. 165-175.

ЗМІСТОВИЙ МОДУЛЬ ІІІ. Прикладні аспекти теорії конфліктів в системах безпеки

Тема 6. 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. Kononovich, I., Mayevskiy, D., Podobniy, R. (2015). Models of system of the cibersecurity providing with delay of reaction on incidents. Informatics and Mathematical Methods in Simulation, 5 (4), 339–346. Available at: http://immm.opu.ua/files/archive/ n4_v5_2015/n4_v5_2015.pdf
2. Musman S, Turner A. A game theoretic approach to cyber security risk management. *The Journal of Defense Modeling and Simulation*. 2018;15(2):127-146. doi:10.1177/1548512917699724
3. Yevseiev, S., Pohasii, S., Milevskyi, S., Milov, O., Melenti, Y., Grod, I., Berestov, D., Fedorenko, R., & Kurchenko, O. (2021). Development of a method for assessing the security of cyber-physical systems based on the Lotka–Volterra model. Eastern-

European Journal of Enterprise Technologies. https://www.semanticscholar.org/paper/Development-of-a-method-for-assessing-the-security-Yevseiev-Pohasii/721cd765a5b00f1b2b647a40a739ba88f926a9e3
4. Шевченко С.М. Дослідження прикладних аспектів теорії конфліктів у системах безпеки / С.М. Шевченко, Складанний П.М., Негоденко О.В., Негоденко В.П. // Кібербезпека: освіта, наука, техніка. – 2022, Том 2, № 18. – С. 150-162.
5. Кошманенко В.Д. Спектральна теорія динамічних систем конфлікту. – Київ: Наукова думка, 2016. – 288 с.

Тема 7. Науково-методичний апарат дослідження інформаційного конфлікту та його застосування в системах безпеки

Теорія ігор. Теорія марковських процесів. Мережі Петрі. Теорія нечітких множин. Теорія диференціальних рівнянь.

Ключові слова: конфлікти в системах безпеки, теорія ігор, марковські процеси, мережа Петрі, нечіткі множини, диференціальні рівняння

Література:

1. Shevchenko S., Zhdanova Y., Shevchenko H., Nehodenko O. and Spasiteleva S. (2023) *Conflict Analysis in the Information Security System: Subject - Subject* CEUR Workshop Proceedings., 3421. pp. 56-66 . ISSN 1613-0073
2. Bebeshko B., Malyukov V., Lakhno M., Skladannyi P., Sokolov V., Shevchenko S. and Zhumadilova M. (2022) *Application of Game Theory, Fuzzy Logic and Neural Networks for Assessing Risks and Forecasting Rates of Digital Currency* Journal of Theoretical and Applied Information Technology, 100 (24). c. 7390-7404. ISSN 1817-3195.
3. Шевченко С., Жданова Ю., Складанний П., & Бойко С. (2023). *Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки*. Кібербезпека: освіта, наука, техніка, 2(22), с.168–178. https://doi.org/10.28925/2663-4023.2023.22.168178
4. Yevseiev S., Milov O., Milevskyi S., Voitko O., Kasianenko M., Melenti Y., Pohasii S., Stepanov H., Turinskyi O. & Faraon S. (2020). Development and analysis of game-theoretical models of security systems agents interaction. Eastern-European Journal of Enterprise Technologies. 2. 15-29. 10.15587/1729-4061.2020.201418.
5. Кошманенко В.Д. Спектральна теорія динамічних систем конфлікту. – Київ: Наукова думка, 2016. – 288 с.

6. Контроль навчальних досягнень

6.1.1. Система оцінювання навчальних досягнень аспірантів денної форми навчання

№ з/п	Вид діяльності аспіранта	Макс. кількість балів за одиницю	Модуль 1		Модуль 2		Модуль 3	
			Кількість одиниць	Максимальна кількість	Кількість одиниць	Максимальна кількість	Кількість одиниць	Максимальна кількість
1	Відвідування лекцій	1	2	2	2	2	2	2
2	Відвідування практичних занять	1	2	2	1	1	1	1
3	Відвідування семінарських занять	1	1	1			1	1
4	Виконання завдань для самостійної роботи	5	2	10	1	5	2	10
5	Робота на практичних заняттях	10	2	20	1	10	1	10
6	Робота на семінарських заняттях	10	1	10			1	10
7	Виконання модульної контрольної роботи	25	1	25	1	25	1	25
Разом				**70**		**43**		**59**
Максимальна кількість балів: **172**								
Розрахунок коефіцієнта: **100/172=0.58**								

6.1.2. Система оцінювання навчальних досягнень аспірантів заочної форми навчання

№ з/п	Вид діяльності аспіранта	Макс. кількість балів за одиницю	Модуль 1		Модуль 2		Модуль 3	
			Кількість одиниць	Максимальна кількість	Кількість одиниць	Максимальна кількість	Кількість одиниць	Максимальна кількість
1	Відвідування лекцій	1	1	1	1	1	1	1
2	Відвідування практичних занять	1	1	1			1	1
3	Відвідування семінарських занять	1			1	1		
4	Виконання завдань для самостійної роботи	5	2	10	1	5	2	10
5	Робота на практичних заняттях	10	1	10			1	10
6	Робота на семінарських заняттях	10			1	10		
Разом				**22**		**17**		**22**
Максимальна кількість балів: **61**								
Розрахунок коефіцієнта: **100 / 61=1.63**								

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	Кількість годин (денна/ заочна)	Бали
Змістовий модуль 1. Прикладні аспекти теорії ризиків в системах безпеки			
1	Системний підхід до управління ризиками ІБ	12/17	5
2	Методи і засоби аналізу та оцінювання ризиків ІБ	8/9	5
Змістовий модуль 3. Прикладні аспекти теорії катастроф в системах безпеки			
3	Перспективи використання теорії катастроф у дослідженні інформаційної безпеки організації	20/26	5
Змістовий модуль 4. Прикладні аспекти теорії конфліктів в системах безпеки			
4	Види сучасних інформаційних конфліктів	10/10	5
5	Методи вирішення інформаційного конфлікту в системах кібербезпеки	10/16	5
	Разом	60/78	25

Критерії оцінювання самостійної роботи.

Критерії	**Обґрунтування критеріїв**	**Бали**
Розуміння завдання	- робота демонструє точне розуміння завдання	1
	- включені матеріали, що безпосередньо розкривають теми або опосередковані до неї	0,5
	- включені матеріали, що не мають безпосереднього відношення до теми, зібрана інформація не аналізується і не оцінюється	0
Повнота розкриття теми	- тема розкрита повністю	1
	- часткове розкриття теми	0,5
	- виконане завдання не відповідає темі	0
Логіка викладу інформації	- логічне й структуроване викладення матеріалу	1
	- порушення логіки й структури викладу	0,5
Креативність	- унікальність роботи, велика кількість оригінальних прикладів, у роботі присутні авторські знахідки	1
	- стандартна робота, не містить авторської індивідуальності	0,5
Культура змістового наповнення відповідей	- орфографічно правильно оформлена робота з точки зору граматики, стилістики	1
	- присутні не грубі помилки з точки зору граматики, стилістики, орфографії	0,5
	- грубі помилки з точки зору граматики, стилістики, орфографії	0
	Разом	**5 балів**

6.3 Критерії оцінювання практичних та семінарських робіт 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.	4
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	4
3	Дотримання вимог щодо технічного оформлення	2
	Разом	**10 балів**

6.4. Форми проведення модульного контролю та критерії оцінювання

Оцінка за кожний змістовий модуль включає бали за поточну роботу аспіранта на практичних заняттях, за виконання домашніх завдань, 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.

6.5 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.

6.6. 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 курсу – досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Рекомендована література

Основна (базова) 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. Стандарт NIST 800-30 https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf
3. BSI-Standard 200-3 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-3-Risikomanagement/bsi-standard-200-3-risikomanagement_node.html
4. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks
5. ДСТУ ISO/IEC 27005:2023 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT)
6. Antonucci D. The Cyber Risk Handbook / Domenic Antonucci. – New Jersey: John Wiley & Sons, 2017. – 433 с.
7. Shevchenko H., Shevchenko S., Zhdanova Y., Spasiteleva S. and O. Negodenko (2021) Information Security Risk Analysis SWOT - Cybersecurity Providing in Information and Telecommunication Systems, 2923. С. 309-317. ISSN 1613-0073
8. Шевченко С.М. Модель захисту інформації на основі оцінки ризиків інформаційної безпеки для малого та середнього бізнесу / С.М. Шевченко, Ю.Д. Жданова, К.В. Кравчук // Кібербезпека: освіта, наука, техніка. – 2021, Том 2, № 14. – С. 158-175.

9. Rotshtein A. Risk Analysis: Fuzzy Cognitive Map vs Fault Tree, Journal of Computer and Systems Sciences International, 2019, 2: 200–211.
https://link.springer.com/article/10.1134/S1064230719020163
10. Shevchenko S., Zhdanova Y., Shevchenko H., Nehodenko O. and Spasiteleva S. (2023) Information Security Risk Management using Cognitive Modeling Cybersecurity Providing in Information and Telecommunication Systems, 3550. с. 297-305. ISSN 1613-0073.
11. Шевченко С.М., Жданова Ю.Д., Спасітєлєва С.О. (2023) Математичні методи в кібербезпеці: теорія катастроф. Кібербезпека: освіта, наука, техніка, 2023, 3 (19). с. 165-175.
12. Shevchenko S., Zhdanova Y., Shevchenko H., Nehodenko O. and Spasiteleva S. (2023) Conflict Analysis in the Information Security System: Subject - Subject CEUR Workshop Proceedings., 3421. pp. 56-66 . ISSN 1613-0073
13. Bebeshko B., Malyukov V., Lakhno M., Skladannyi P., Sokolov V., Shevchenko S. and Zhumadilova M. (2022) Application of Game Theory, Fuzzy Logic and Neural Networks for Assessing Risks and Forecasting Rates of Digital Currency Journal of Theoretical and Applied Information Technology, 100 (24). с. 7390-7404. ISSN 1817-3195.
14. Шевченко С., Жданова Ю., Складанний П., & Бойко С. (2023). Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки. Кібербезпека: освіта, наука, техніка, 2(22), с.168–178. https://doi.org/10.28925/2663-4023.2023.22.168178
15. Yevseiev S., Milov O., Milevskyi S., Voitko O., Kasianenko M., Melenti Y., Pohasii S., Stepanov H., Turinskyi O. & Faraon S. (2020). Development and analysis of game-theoretical models of security systems agents interaction. Eastern-European Journal of Enterprise Technologies. 2. 15-29. 10.15587/1729-4061.2020.201418.

Додаткова література.

1. Барибін О. І. Стандартизація та сертифікація в галузі інформаційної безпеки: навч. посіб. / О. І. Барибін. – Вінниця : ДонНУ імені Василя Стуса, 2018. – 238 с.
2. 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.
3. Кошманенко В.Д. Спектральна теорія динамічних систем конфлікту. – Київ: Наукова думка, 2016. – 288 с.
4. Rittinghouse J. W. Business continuity and disaster recovery for infosec managers / John W. Rittinghouse, James F. Ransome. – Oxford: Elsevier, 2015. – 408 p.
5. 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.
6. Antonucci D. The Cyber Risk Handbook / Domenic Antonucci. – New Jersey: John Wiley & Sons, 2017. – 433 c.
7. 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.
8. Gilmore Robert. Catastrophe Theory of Scientists and Engineers. New York: Dover, 1993.
9. 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://sccs.intelgr.com/archive/2016-03/04-Makarenko.pdf
10. 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.
11. 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/
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/