НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
Кафедра комп'ютерних систем, мереж та кібербезпеки

ЗАТВЕРДЖЕНО
Факультет інформаційних технологій
02 червня 2025 р

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Ризики інформаційної безпеки»

Галузь знань _____12 Інформаційні технології
Спеціальність ___123 Кібербезпека_____
Освітня програма _____«Кібербезпека»_____
Факультет (ННІ)_____інформаційних технологій_____
Розробники: _____доцент, к.т.н., доцент, Сагун А.В._____
(посада, науковий ступінь, вчене звання)

Київ – 2025 р.

Опис навчальної дисципліни

Дисципліна вивчає основи ідентифікації та управління ризиками інформаційної безпеки в інформаційно-телекомунікаційних (автоматизованих) системах. При вивченні теоретичних та практичних моментів управління ризиками даний аспект розглядається в межах встановленої політики безпеки відповідно та рекомендації нормативних документів серій ДСТУ ISO/IEC 27000 та 310000.

Вивчаються методики управління ризиками (CRAMM, OCTAVE), нормативні документи на міжнародні стандарти по управлінню ризиками в контексті ризик – орієнтованого підходу забезпечення кібербезпеки, експертні методи оцінки ризиків, засоби автоматизованої обробки та керування ризиками.

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	*бакалавр*	
Спеціальність	*125 – Кібербезпека та захист інформації*	
Освітня програма	*Кібербезпека*	
Характеристика навчальної дисципліни		
Вид	обов'язкова	
Загальна кількість годин	120	
Кількість кредитів ECTS	4	
Кількість змістових модулів	2	
Курсовий проект (робота) (за наявності)	-	
Форма контролю	*екзамен*	
Показники навчальної дисципліни для денної та заочної форм здобуття вищої освіти		
	Форма здобуття вищої освіти	
	денна	**заочна**
Курс (рік підготовки)	2	-
Семестр	4	-
Лекційні заняття	*30 год.*	*год.*
Практичні, семінарські заняття	*30 год.*	*год.*
Лабораторні заняття	*год.*	*год.*
Самостійна робота	*60 год.*	*год.*
Кількість тижневих аудиторних годин для денної форми здобуття вищої освіти	*4 год.*	

1. Мета, компетентності та програмні результати навчальної дисципліни

Мета вивчення дисципліни «Ризики інформаційної безпеки» є формування комплексу знань щодо основ ідентифікації та управління ризиками інформаційної безпеки на підприємствах та організаціях різних форм власності, набуття студентом теоретичних знань та практичних навичок щодо ідентифікації та управління ризиками інформаційної безпеки в інформаційно-телекомунікаційних (автоматизованих) системах в межах встановленої

політики безпеки відповідно до рекомендацій нормативних документів серій ДСТУ ISO/IEC 27000 та 31000 та опанування методиками управління ризиками (типу OCTAVE, CRAMM тощо).

Набуття компетентностей:

інтегральна компетентність (ІК): здатність комплексно застосовувати теоретичні знання, професійні навички та законодавчо-нормативну базу для аналізу, оцінювання та обробки ризиків в інформаційно-телекомунікаційних системах, забезпечуючи ефективний захист інформації відповідно до державних та міжнародних стандартів у сфері кібербезпеки.

загальні компетентності (ЗК): здатність застосовувати знання у практичних ситуаціях; знання та розуміння предметної області та розуміння професії; вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням; здатність до абстрактного і системного мислення, аналізу та синтезу.

спеціальні (фахові) компетентності (СК): здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки; здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

Програмні результати навчання (ПРН): критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем; вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів; вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;

2. Програма та структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин												
	денна форма							заочна форма					
	тижні	усього	у тому числі					усього	у тому числі				
			л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
Змістовий модуль 1. Оцінка та аналіз ризиків та основи управління ризиками по ISO/IEC													
Тема 1. Основні поняття, терміни і означення загальної теорії ризиків	1	4	2		-		2						
Тема 2. Класифікація та оцінки ризиків, вимірювання ризиків ІБ. Стандарт методів загального оцінювання ризиків ДСТУ IEC/ISO 31010:2013	2	14	4		4		6						
Тема 3. Основи управління ризиками. Методи управління ризиками. Міжнародні стандарти по управлінню ризиками (ISO/IEC 27001:2013)	3	12	2		-		6						
Тема 4. Ризик – орієнтований підхід забезпечення кібербезпеки та його задачі. Стратегії обробки ризиків. Вимоги до оцінки і обробки ризиків інформаційної безпеки з урахуванням потреб організації, стандарт ISO/IEC 27001:2022	4	8	2		4		2						
Тема 5. Оцінка та моделювання ризикованих ситуацій. Калібрування шкали оцінки ризиків з використанням рекомендацій ДСТУ ISO/IEC 27005.	5	20	4		4		8						
Разом за модулем 1		**54**	**14**		**12**		**24**						
Змістовий модуль 2. Ризик-орієнтований підхід на підприємстві. Методи оцінки та обробки ризиків з використанням автоматизованих програмних засобів													
Тема 6. Експертні методи оцінки ризиків. Метод Дельфі. Метод бальної оцінки ризиків.	7	12	2		4		6						
Тема 7. Система управляння ризиками в загальні концепції Політики інформаційної безпеки підприємства.	8	10	2		-		8						
Тема 8. Моделі аналізу ризиків інформаційної безпеки. Моделі ALE, SLE. Якісні та кількісні методики оцінювання ризиків.	9	12	2		4		6						
Тема 9. План реагування на ризики: реалізація заходів з реагування на ризики; оцінка ефективності реалізованих заходів.	11	12	4		-		8						

Керування ризиками у комплексних системах безпеки діяльності банківських та фінансово-кредитних установ.													
Тема 10. Системи автоматизованого оцінювання та керування ризиками. Програмні продукти для аналізу ризиків інформаційної безпеки: CRAMM, RiskWatch.	13	18	4		6		8						
Тема 11. Ризик-менеджмент. Документування в систем управління ризиками.	15	6	2		4		-						
Разом за модулем 2		**66**	**16**		**18**		**36**						
Усього годин		**120**	**30**		**30**		**60**						

3. Теми лекцій

№ з/п	Назва теми	Кількість годин
1	Основні поняття, терміни і означення загальної теорії ризиків	2
2	Класифікація та оцінки ризиків, вимірювання ризиків ІБ (ISO/IEC 27001:2013)	4
3	Ризики ІБ. Основи управління ризиками	4
4	Ризик –орієнтований підхід забезпечення кібербезпеки.	4
5	Експертні оцінки при аналізі ризиків. Метод Дельфі. Якісний аналіз ризиків з використанням методу Дельфі	2
6	Експертні методи оцінки ризиків. Методики визначення та експертної оцінки ризикованих активів з використанням засобів пен-тестування. Розробка та впровадження заходів з реагування на ризики в рамках обраної стратегії керування ризиками	2
7	Система управляння ризиками в загальні концепції Політики інформаційної безпеки підприємства	2
8	Якісні та кількісні методи управління ризиками	4
9	Ризики та керування ризиками у банківській діяльності	4
10	Регламенти та плани управління ризиками на підприємств. Система документування ризиків та планів обробки ризиків	2

4. Теми лабораторних (практичних, семінарських) занять

№ з/п	Назва теми	Кількість годин
1	Аналіз та класифікація ризикованих активів ІБ	4
2	Оцінка та моделювання ризикованих ситуацій	4
3	Калібровка шкали оцінки ризиків з використанням рекоменацій ДСТУ ISO/IEC 27005	4
4	Якісний аналіз ризиків з використанням методів експертної оцінки	4
5	Стратегії керування ризиками в практичних ситуаціях	4
6	Автоматизована оцінка та управління ризиками	6
7	Документування в системі управління ризиками	4

5. Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Методики визначення ваги та ціни ризикованих активів та процесів	2
2	Сучасні методи і засоби контролю ризиків на підприємствах і в організаціях	6
3	Нормативні документи в галузі оцінки та обробки ризиків. Фази обробки ризиків	8
4	Моделі ранжування ризиків за показниками ALE, SLE	8
5	Методи обробки ризиків та планування протидії ризикам	6
6	Залишкові ризики та методи обробки залишкових ризиків в різних методиках	8
7	Роль та місце ризиків в політиці безпеки підприємства	6
8	Принципи роботи та застосування стандарту NIST Special Publication 800-30 Revision 1 для оцінки ризиків	8
9	Методи та засоби оцінки та управління ризиками ІБ: OCTAVE Allegro, MEHARY, Magerit, CRAMM	8
	Разом	**60**

6. Методи та засоби діагностики результатів навчання:

(вибрати необхідне чи доповнити)

- усне або письмове опитування;
- співбесіда;
- тестування;
- захист лабораторних робіт;
- пірінгове оцінювання, самооцінювання.

7. Методи навчання *(вибрати необхідне чи доповнити):*

- метод проблемного навчання;
- метод практико-орієнтованого навчання;
- метод командної роботи, мозкового штурму
- метод гейміфікованого навчання.

8. Оцінювання результатів навчання.

Оцінювання знань здобувача вищої освіти відбувається за 100-бальною шкалою і переводиться в національну оцінку згідно чинного «Положення про екзамени та заліки у НУБіП України»

8.1. Розподіл балів за видами навчальної діяльності

Вид навчальної діяльності	Результати навчання	Оцінювання
Змістовий модуль 1. Оцінка та аналіз ризиків та основи управління ризиками по ISO/IEC		
Лабораторна робота 1. Аналіз та класифікація ризикованих активів ІБ	здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних	9

	систем;	
Лабораторна робота 2. Оцінка та моделювання ризикованих ситуацій	критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;	9
Лабораторна робота 3. Калібровка шкали оцінки ризиків з використанням рекомендацій ДСТУ ISO/IEC 27005	застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.	10
Модульна контрольна робота 1	Контроль засвоєння матеріалу	6
Всього за модулем 1		**34**
Змістовий модуль 2. Ризик-орієнтований підхід на підприємстві. Методи оцінки та обробки ризиків з використанням автоматизованих програмних засобів		
Лабораторна робота 4. Якісний аналіз ризиків з використанням методів експертної оцінки	вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;	8
Лабораторна робота 5. Стратегії керування ризиками в практичних ситуаціях	здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.	8
Лабораторна робота 6. Автоматизована оцінка та управління ризиками	здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;	7
Лабораторна робота 7. Документування в системі управління ризиками	вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;	7
Модульна контрольна робота 2	Контроль засвоєння матеріалу	6
Всього за модулем 2		**36**
Навчальна робота		**(М1 + М2)/*0,7 ≤ 70**
Екзамен		**30**
Всього за курс		**(Навчальна робота + екзамен) ≤ 100**

8.2. Шкала оцінювання знань здобувача вищої освіти

Рейтинг здобувача вищої освіти, бали	Оцінка за національною системою (екзамени/заліки)
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

8.3. Політика оцінювання

Політика щодо дедлайнів та перескладання	Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (пропорційно інтервалів пропущеної дати складання). Перескладання модульних контрольних та тестів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний).
Політика щодо академічної доброчесності	Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів). Лабораторні роботи мають бути виконані виключна за індивідуальними завданнями варіантів.
Політика щодо відвідування	Відвідування занять є обов'язковим. За об'єктивних причин (хвороба, участь в заходах від кафедри або факультету, міжнародне стажування) навчання може відбуватись індивідуально (в он-лайн формі за погодженням із деканом факультету)

9. Навчально-методичне забезпечення:

Електронний навчальний курс навчальної дисципліни (на навчальному порталі НУБіП України eLearn - https://elearn.nubip.edu.ua/course/view.php?id=4163), що складається з:

- лекцій та їх презентації (в електронному вигляді);
- завдань для виконання лабораторних та самостійних завдань;
- модульних контрольних робіт;
- блоку підсумкового оцінювання знань.
- методичні матеріали щодо вивчення навчальної дисципліни для здобувачів вищої освіти денної та заочної форм здобуття вищої освіти;
- програма навчальної дисципліни.

10. Рекомендовані джерела інформації

1. Ю. Лісовська. Книга Кібербезпека. Ризики та заходи. – Вид-во «Кондор», 2019. – 272 с. ISBN 978-617-7729-49-4.
2. Гуменюк В. Я. Управління ризиками : навч. посіб. / В. Я. Гуменюк, Г. Ю. Міщук, О. О. Олійник. – Рівне : НУВГП. - 2009. 156 с.
3. Машина Н.І. Ризик і методи його вимірювання: Навчальний посібник. - К.: ЦНЛ, 2003. - 188 с.
4. Василевич Л.Ф. Юртин І.І. Прийняття рішень за умов конфлікту та невизначеності середовища. Навчальний посібник – К. : Київ. ун-т ім.. Б. Грінченка. 2013. 128 с.