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

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г. Глазунова
"___" _____ 2023 р.

НАВЧАЛЬНО-МЕТОДИЧНИЙ КОМПЛЕКС

з дисципліни

«РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

для підготовки бакалаврів за спеціальністю 125 «Кібербезпека»

КИЇВ-2023

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

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г. Глазунова
"__" _____ 2023 р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем, мереж та кібербезпеки
Протокол №10 від "17" травня 2023 р.
Завідувач кафедри
(доц. Касаткін Д.Ю.)

РОЗГЛЯНУТО
Гарант ОП
«Кібербезпека»
_____
Гарант ОП
_____ (проф. Лахно В.А.)

«РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Спеціальність	125 - Кібербезпека
Освітня програма	Кібербезпека
Факультет	інформаційних технологій
Розробник:	Сагун А.В., к.т.н., доцент

Київ – 2023

Опис навчальної дисципліни

«МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ»

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	Бакалавр	
Галузь знань	12 – Інформаційні технології	
Спеціальність	125 – Кібербезпека	
Освітня програма	Кібербезпека	
Характеристика навчальної дисципліни		
Вид	обов'язкова	
Загальна кількість годин	120	
Кількість кредитів ECTS	4	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
Форма контролю	екзамен	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	2	
Семестр	4	
Лекційні заняття, год.	30	
Практичні, семінарські заняття	30	
Лабораторні заняття, год.	-	
Самостійна робота, год.	60	
Індивідуальні завдання	-	
Кількість тижневих аудиторних годин для денної форми навчання	4 (15 тижнів)	

1. Мета, завдання та компетентності навчальної дисципліни

Мета: формування комплексу знань щодо основ теорії ризиків інформаційної безпеки, набуття студентом теоретичних знань та практичних навичок щодо ідентифікація та управління ризиками інформаційної безпеки в інформаційно-телекомунікаційних (автоматизованих) системах в межах встановленої політики безпеки.

Завдання навчальної дисципліни: визначення та керування ризиками, пов'язаними з використанням інформаційних систем, які підтримують місію та бізнес-функції організації.

В результаті вивчення навчальної дисципліни студент повинен:

знати:

- основні поняття, терміни і означення загальної теорії ризиків
- основи управління ризиками, методи управління ризиками. Міжнародні стандарти по управлінню ризиками
- ризик – орієнтований підхід забезпечення кібербезпеки
- експертні методи оцінки ризиків. Метод Делфі
- систему управляння ризиками в загальні концепції Політики інформаційної безпеки підприємства
- Вимоги до оцінки і обробки ризиків інформаційної безпеки з урахуванням потреб організації, стандарту ISO/IEC 27001:2013 та оцінки ризиків з використанням рекомендацій ДСТУ ISO/IEC 27005.

вміти:

- проводити класифікацію та оцінку ризиків, вимірювання ризиків ІБ (ISO/IEC 27001:2013).
- здійснювати якісний аналіз експертної оцінки ризиків з використанням методу Делфі.
- застосовувати ризик – орієнтований підхід забезпечення кібербезпеки підприємств і організацій.
- використовувати рекомендації та вимоги Міжнародного стандарту по управлінню ризиками (ISO/IEC 27001:2013).
- користуватися програмними продуктами для аналізу ризиків інформаційної безпеки: CRAMM, RiskWatch.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 8. Здатність до абстрактного і системного мислення, аналізу та синтезу.

Спеціальні (фахові, предметні) компетентності (СК):

СК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

В результаті вивчення навчальної дисципліни студент набуде певні програмні результати (РН), а саме:

ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

ПРН 13. Аналізувати проекти інформаційно - телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних;

ПРН 19. Застосовувати теорії, методи та засоби захисту для забезпечення безпеки інформації в інформаційно - телекомунікаційних системах.

ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;

ПРН 29. 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;

ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно - телекомунікаційних систем;

ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно - телекомунікаційних систем;

ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно - телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;

ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.

В контексті зазначених вище компетентностей та програмних результатів навчання задачі викладання дисципліни визначають необхідний комплекс знань і вмінь, що отримують студенти під час вивчення дисципліни.

Навчальна програма розрахована на студентів, які навчаються за освітньою програмою підготовки бакалавра за спеціальністю «Кібербезпека».

Програма побудована за вимогами кредитно-модульної системи організації навчального процесу у закладах вищої освіти і використанням академічної системи оцінювання досягнень студентів та шкали оцінок Європейської кредитно-трансферної системи (ECTS).

Робоча навчальна програма з курсу є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма дисципліни розроблена на підставі наступних документів:

- освітня програма підготовки бакалаврів за спеціальністю 125 «Кібербезпека»;
- навчальний план підготовки бакалаврів за спеціальністю 125 «Кібербезпека».
- освітньо-професійної програми «Кібербезпека» першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека».

Навчальна програма характеризує шляхи перетворення інформації, що одержується студентом впродовж вивчання курсу, і відбиває зміст курсу, розподілення його на розділи та їх обсяги, дані про форми вивчення та контролю знань.

Теоретичною базою для вивчення курсу «Ризики інформаційної безпеки» є курси «Інформаційна безпека держави», «Теорія ймовірностей, імовірнісні процеси і математична статистика» ОПП першого (бакалаврського) рівня вищої освіти .

2. Програма та структура навчальної дисципліни

– повного терміну денної (заочної) форми навчання;

Назви змістових модулів і тем	Кількість годин												
	денна форма							Заочна форма					
	тиж-ні	всього	у тому числі					всього	у тому числі				
			л	п	лр	інд	с.р.		л	п	лр	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13	14
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	12	4	4			4						
Тема 3. Основи управління ризиками. Методи управління ризиками. Міжнародні стандарти по управлінню ризиками (ISO/IEC 27001:2013)	3	14	2	4			8						
Тема 4. Ризик – орієнтований підхід забезпечення кібербезпеки та його задачі. Стратегії обробки ризиків. Вимоги до оцінки і обробки ризиків	4	6	2	4			-						

інформаційної безпеки з урахуванням потреб організації, стандарт ISO/IEC 27001:2013.													
Тема 5. Оцінка та моделювання ризикованих ситуацій. Калібрування шкали оцінки ризиків з використанням рекомендацій ДСТУ ISO/IEC 27005.	5	16	4	4			8						
Разом за змістовим модулем 1		**52**	**14**	**16**			**22**						
Змістовий модуль 2. Ризики в політиках інформаційної безпеки підприємств. Експертні методи оцінки та обробка ризиків													
Тема 7. Експертні методи оцінки ризиків. Метод Делфі. Якісний аналіз ризиків з використанням методу Делфі. Метод бальної оцінки ризиків.	7	14	2	6			6						
Тема 8. Система управляння ризиками в загальні концепції Політики інформаційної безпеки підприємства.	8	10	2	-			8						
Тема 9. Моделі аналізу ризиків інформаційної безпеки. Моделі ALE, SLE. Програмні продукти для аналізу ризиків інформаційної безпеки: CRAMM, RiskWatch.	10	16	4	4			8						
Тема 10. План реагування на ризики: реалізація заходів з реагування на ризики; оцінка ефективності реалізованих заходів.	12	16	4	4			8						
Тема 11. Ризики та керування ризиками у комплексних системах безпеки діяльності банківських та фінансово-кредитних установ.	14	12	4	-			8						
Разом за змістовим модулем 2		**68**	**16**	**14**			**38**						
Всього годин		**120**	**30**	**30**			**60**						

3. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

4. Теми семінарських занять

№ з/п	Назва теми	Кількість годин

	Не передбачено робочим навчальним планом	

5. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Аналіз та ідентифікація ризикованих активів	4
2	Оцінка та моделювання ризикованих ситуацій	4
3	Калібровка шкали оцінки ризиків з використанням рекомендацій ДСТУ ISO/IEC 27005»	4
4	Складання розділу «Управління ризиками інформаційної безпеки» Політики інформаційної безпеки підприємства	4
5	Якісний аналіз ризиків з використанням методів експертної оцінки	6
6	Моделі ALE, SLE	4
7	Програмні продукти для аналізу ризиків інформаційної безпеки: CRAMM, RiskWatch.	4
	Разом за семестр	**30**
	Разом	**30**

Курсове проектування - Не передбачено робочим навчальним планом.

6. САМОСТІЙНА РОБОТА СТУДЕНТІВ

Самостійна робота студентів передбачає:

– систематичне відвідання усіх видів аудиторних занять і ведення конспекту лекцій;

– систематичне вивчення лекційного матеріалу і навчальної літератури, що рекомендуються;

– сумлінну підготовку до лабораторних занять;

– вчасне і якісне оформлення звітів про лабораторні роботи.

–

6.1Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Сучасні методи і засоби контролю ризиків на підприємствах і в організаціях	8
2	ПО для аналізу ризиків. Фази аналізу ризиків	10
3	Методи обробки ризиків: планування протидії ризикам	8
4	Методи оцінки ризиків ІБ: OCTAVE Allegro, MEHARY, Magerit	10
5	Принципи роботи та застосування стандарту NIST Special Publication 800-30 Revision 1 для оцінки ризиків	8
6	Види втрат з результатами реалізації ризиків	6
7	Залишкові ризики, методи обробки залишкових ризиків	10

7. Контрольні питання, комплекти тестів для визначення рівня засвоєння знань студентами

7.1. Питання для перевірки знань студентів:

1. Основні поняття, терміни і означення загальної теорії ризиків.

2. Класифікація та оцінки ризиків, вимірювання ризиків ІБ (ISO/IEC 27001:2013)

3. Основи управління ризиками. Теорія управління ризиками

4. Методи управління ризиками: прийняття, передача, ігнорування.

5. Міжнародні стандарти по управлінню ризиками.

6. Ризик – орієнтований підхід забезпечення кібербезпеки.

7. Оцінка та моделювання ризикованих ситуацій.

8. Калібровка шкали оцінки ризиків з використанням рекоменацій ДСТУ ISO/IEC 27005.

9. Експертні методи оцінки ризиків.

10. Метод Дельфі. Якісний аналіз ризиків з використанням методу Дельфі.

11. Експертні методи оцінки ризиків. Метод бальної оцінки ризиків. Розрахунок коефіцієнту конкордації.

12. Методи управління ризиками. Міжнародні стандарти по управлінню ризиками (ISO/IEC 27001:2013)

13. Система управляння ризиками в загальні концепції Політики інформаційної безпеки підприємства.

14. Моделі аналізу ризиків інформаційної безпеки. Моделі ALE, SLE.

15. Програмні продукти для аналізу ризиків інформаційної безпеки: CRAMM, RiskWatch.

16. План реагування на ризики: реалізація заходів з реагування на ризики; оцінка ефективності реалізованих заходів.

17. Стандарт методів загального оцінювання ризиків ДСТУ IEC/ISO 31010:2013/

18. Ризики та керування ризиками у комплексних системах безпеки діяльності банківських та фінансово-кредитних установ.

19. Зв'язок між вразливостями та ризиками для інформації в теорії ризиків ІБ.

20. Складання Політик безпеки в розділі «управління ризиками» для підприємств та установ.

7.2. Приклади тестових питань з дисципліни:

Теоретичні (максимальна оцінка від 5 до 10 балів за відповідь на кожне запитання)
1. Поняття залишкового ризику. Механізми обробки залишкового ризику (10 балів)
2. Що являє собою ризик з точки зору інформаційної безпеки (5 балів)
Тестові завдання (В системі дистанційної освіти elearn) https://elearn.nubip.edu.ua/course/view.php?id=4163
1. Студент відповідає на 15 випадково відібраних питань з 40 існуючих в системі elearn (15 балів)

8. Методи навчання

Виконання лабораторних робіт з використанням ПЗ Excel, Google G-Suite, ПЗ CRAMM, виконання індивідуальних навчально-дослідних завдань.

9. Форми контролю

Систематичний контроль за самостійною роботою студентів і якістю засвоєння ними поточного навчального матеріалу:

– на лабораторних роботах шляхом перевірки підготовки до виконання роботи;

– роботу над індивідуальними завданнями до лабораторних робіт;

– вивчення літератури, що рекомендувалася, та конспекту лекцій;

– оформлення звітів про виконання лабораторним роботам.

Поточний контроль знань студентів проводиться:

– на лабораторних роботах оцінюється підготовка до роботи, обсяг її виконання, результати захисту звіту;

– на лекційних заняттях виконується вибіркове опитування студентів;

– шляхом проведення модульних контролів знань студентів та виставлення рейтингових оцінок знань студентів по усім видам занять.

10. Розподіл балів, які отримують студенти

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл. 1 «ПОЛОЖЕННЯ про екзамени та заліки у НУБіП України» (наказ про уведення в дію від «26» квітня 2023 р. протокол № 10):

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзамен	**Залік**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

Для визначення рейтингу студента із засвоєння дисципліни $R_{дис}$ (до 100 балів) одержаний рейтинг з атестації $R_{АТ}$ (до 30 балів) додається до рейтингу студента з навчальної роботи $R_{НР}$ (до 70 балів): $R_{дис}=R_{НР}+R_{АТ}$.

11. Методичне забезпечення

1. Конспект лекцій з курсу "Ризики інформаційної безпеки". - Київ, НУБіП, 2021 (https://elearn.nubip.edu.ua/course/view.php?id=4163)

12. Рекомендована література

Основна

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.

Додаткова

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

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

3. Endorf C. F. Measuring ROI on security / Carl F. Endorf // Information security management handbook / Edited by Harold F. Tipton and Micki Krauze. – 6th edition. – Boca Raton: Auerbach Publications, 2017. – Part 1, Section 1.1, Ch. 12.

4. 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.

Інформаційні ресурси

1. https://elearn.nubip.edu.ua/course/view.php?id=4163
2. www.securityfocus.com.
3. www.sysinternals.com.
4. http://zakon1.rada.gov.ua