Київський університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«05» 09 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ТЕОРІЯ РИЗИКІВ»

для студентів

спеціальності	125 Кібербезпека
освітнього рівня	першого (бакалаврського)
освітньої програми	125.00.01 Безпека інформаційних і комунікаційних систем

2022 – 2023 навчальний рік

Розробник:
Шевченко Світлана, кандидат педагогічних, доцент.

Викладач:
Шевченко Світлана, кандидат педагогічних, доцент.

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

Протокол від « 01 » вересня 2022 року № 12

Завідувач кафедри _____ Павло Складанний
(підпис)

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 «Безпека інформаційних і комунікаційних систем» першого (бакалаврського) рівня)

01. 09. 2022 р.

Керівник освітньої програми _____ Артем Платоненко
(підпис)

Робочу програму перевірено
01.09. 2022 р.
Заступник директора/декана _____ Євген Іваніченко
(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	5/150	
Курс	3	
Семестр	5	
Кількість змістових модулів з розподілом:	5	
Обсяг кредитів	5	
Обсяг годин, в тому числі:	150	
Аудиторні	70 год.	
Модульний контроль	10 год.	
Семестровий контроль		
Самостійна робота	70 год.	
Форма семестрового контролю	залік	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма дисципліни «Теорія ризиків» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки імені професора Володимира Бурячка на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчального плану спеціальності 125 Кібербезпека, освітньої програми 125.00.01.

Програма визначає обсяги знань, якими повинен опанувати здобувач першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Теорія ризиків» та необхідне методичне забезпечення, складові та технологію оцінювання навчальних досягнень студентів.

Метою вивчення навчальної дисципліни «Теорія ризиків» є формування системи знань та умінь з аналізу та оцінки ризиків для ефективного управління ними у різних сферах практичної діяльності, зокрема у кіберсистемах.

Основними **завданнями** вивчення дисципліни є формування у студентів аналітично-дослідницьких компетентностей, які необхідні сучасному фахівцю інформаційної та кібербезпеки, а саме: здатність до аналізу (ідентифікації, оцінки і прогнозу) ризику для побудови адекватних моделей із забезпеченням вірної інтерпретації отриманих результатів; здатність здійснювати кількісну та якісну оцінку ризику для прийняття рішень щодо зниження ризику і обґрунтування превентивних заходів для зменшення ймовірності негативних подій; здатність ефективно вибирати засоби для обробки даних у системах інформаційної та кібербезпеки у відповідності з поставленим завданням, аналізувати результати розрахунків, обґрунтовувати одержані результати та набуття **наступних фахових компетентностей**:

КФ-9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студент повинен
знати:

1) основні поняття і закони теорії ризиків для їх використання в сучасних кіберсистемах;
2) принципи побудови алгоритмів оцінки ризиків у кібербезпеці, основних стандартів оцінки ризиків та їх використання в задачах захисту інформації;
3) математичний апарат для визначення оцінки ризиків у професійній діяльності;

уміти:

1) аналізувати (ідентифікувати, оцінювати і прогнозувати) ризики в системах кібербезпеки для побудови адекватних моделей із забезпеченням вірної інтерпретації отриманих результатів;
2) застосовувати алгоритми та основні стандарти оцінки ризиків у кібербезпеці з метою ефективного управління ними;
3) використовувати математичний апарат та програмні засоби, які реалізують основні алгоритми оцінки ризиків для вирішення типових задач захисту інформації

та досягти наступних **програмних результатів навчання**:

ПРз-9. Забезпечувати 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, здійснення процедур їх кількісної і якісної оцінки.

ПРз-12. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) та SMART-системах; аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в IT та SMART-системах; аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назви змістових модулів і тем	Кількість годин					
	денна форма					
	Усього	у тому числі				
		л.	пр.	с	м.к.	с.р.
Змістовий модуль 1. Сутність та основні поняття ризикології						
Тема 1. Ризик та його ключові характеристики	9	2	2	2		3
Тема 2. Класифікація ризиків	9	2	2	2		3
Модульний контроль 1.	2				2	
Разом за змістовим модулем 1	**20**	**4**	**4**	**4**	**2**	**6**
Змістовий модуль 2. Основи ризик-менеджменту						
Тема 3. Аналіз ризиків та методи їх оцінювання	16	2	4	4		6
Тема 4. Методи управління ризиком	12	2	2	2		6
Модульний контроль 2.	2				2	
Разом за змістовим модулем 2	**30**	**4**	**6**	**6**	**2**	**12**

Змістовий модуль 3. Інформаційні ризики та їх особливості						
Тема 5. Ризики ІБ: суть, складові, нормативне забезпечення.	**12**	**2**	**2**	**2**		**6**
Тема 6. Теоретичні основи ризик-менеджменту в ІБ	**12**	**2**	**2**	**2**		**6**
Модульний контроль 3.	2				2	
Разом за змістовим модулем 3	**26**	**4**	**4**	**4**	**2**	**12**
Змістовий модуль 4. Сучасні підходи до аналізу та оцінювання ризиків ІБ						
Тема 7. Методи, засоби, інструментарій аналізу та оцінювання ризиків ІБ	34	2	6	6		20
Модульний контроль 4.	2				2	
Разом за змістовим модулем 4	**36**	**2**	**6**	**6**	**2**	**20**
Змістовий модуль 5. Управління ризиками інформаційної безпеки						
Тема 8. Методи обробки ризиків ІБ.	14	2	2	2		8
Тема 9. Методи реалізації рішень на основі аналізу та оцінки ризику	22	2	4	4		12
Модульний контроль 5.	2				2	
Разом за змістовим модулем 5	**38**	**4**	**6**	**6**	**2**	**20**
Усього годин	**150**	**18**	**26**	**26**	**10**	**70**

5. Програма навчальної дисципліни

<u>Змістовий модуль 1.</u> Сутність та основні поняття ризикології.

Тема 1. Ризик та його ключові характеристики.

Предмет теорії ризикології. Основні поняття теорії ризикології. Поняття невизначеності та ризику. Фактори виникнення ризику та його функції. Об'єкт, суб'єкт і джерела ризику.

Тема 2. Класифікація ризиків.

Підходи до класифікації ризиків. Критерії класифікації ризиків і види ризиків.

<u>Змістовий модуль 2.</u> Основи ризик-менеджменту

Тема 3. Аналіз ризиків та методи їх оцінювання.

Загальні принципу аналізу ризику. Основні підходи до виявлення ризику. 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).

Тема 4. Основи ризик-менеджменту.

Концепції ризик-менеджменту. Механізм управління ризиком. Блок-схема процесу управління ризиком, основні етапи управління ризиком та їх характеристика. Методи управління ризиками. Прийоми зниження ризику в управлінні ризиками. Моделі ризиків: модель «небезпека-ризик», модель «невизначеність-ризик», модель «можливості-ризик/шанс».

<u>Змістовий модуль 3.</u> Інформаційні ризики та їх особливості

Тема 5. Ризики ІБ: суть, складові, нормативне забезпечення.

Поняття ризику ІБ, його сутність. Поняття, що включаються в ризик ІБ. Нормативне забезпечення аналізу та оцінювання ризиків. Міжнародні стандарти забезпечення аналізу та оцінювання ризиків.

Тема 6. Теоретичні основи ризик-менеджменту в ІБ.

Блок-схема процесу управління ризиком ІБ, основні етапи управління ризиком та їх характеристики.

Змістовий модуль 4. Сучасні підходи до аналізу та оцінювання ризиків ІБ

Тема 7. Методи, засоби, інструментарій аналізу та оцінювання ризиків ІБ.

Аналітичні методи. Стохастичні методи. Теоретико-множинні методи. Логіко-ймовірнісні методи. Лінгвістичний підхід: теорія нечітких множин. Теоретико-графові методи.

Спеціалізовані програмні методи, засоби, інструментарій якісного та кількісного аналізу та оцінювання ризиків ІБ: ISAMM, EBIOS, Octave, IT-Grundschutz, CRAMM, Magerit, Cobra, RiskWatch та інші.

Змістовий модуль 5. Управління ризиками інформаційної безпеки

Тема 8. Методи обробки ризиків ІБ.

Прийоми зниження ризику ІБ. Передача ризику ІБ. Прийняття ризику ІБ. Страхування ризиків ІБ. Моніторинг показників ризиків ІБ.

Тема 9. Методи реалізації рішень на основі аналізу та оцінки ризику.

Управління ризиком у кібербезпеці за умов невизначеності середовища. Управління ризиком у кібербезпеці за умов конфлікту. Управління ризиком у кібербезпеці за умов нечіткої інформації. Прогнозування в задачах управління ризиком у кібербезпеці.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип поопераційної звітності, обов'язковості модульних контролів, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100. Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних заняттях, за виконання домашніх завдань, за модульну контрольну та самостійну індивідуальну роботу. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда.
- *Методи письмового контролю:* модульне письмове тестування, домашні завдання.
- *Комп'ютерного контролю:* тестові програми.
- *Методи самоконтролю:* самостійне оцінювання своїх знань з дисципліни, отриманих результатів за домашні завдання, постановка питань.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, на семінарах, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і домашніх завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і домашніх завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- постановка питань;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання

здійснюється відповідно до навчально-методичної карти дисципліни (п. 7), де зазначено види контролю і кількість балів за видами.

6.1 Система оцінювання навчальних досягнень студентів

Розрахунок рейтингових балів за видами поточного (модульного) контролю

№ з/п	Вид діяльності студента	Макс. кількість балів за одиницю	Модуль 1		Модуль 2		Модуль 3		Модуль 4		Модуль 5	
			Кільк. одиниць до розрахунку	Макс. кількість балів за вид	Кільк. одиниць до розрахунку	Макс. кількість балів за вид	Кільк. одиниць до розрахунку	Макс. кількість балів за вид	Кільк. одиниць до розрахунку	Макс. кількість балів за вид	Кільк. одиниць до розрахунку	Макс. кількість балів за вид
1	Відвідування лекцій	1	2	2	2	2	2	2	1	1	2	2
2	Відвідування практичних занять	1	2	2	3	3	2	2	3	3	3	3
3	Відвідування семінарів	1	2	2	3	3	2	2	3	3	3	3
4	Виконання завдань для самостійної роботи	5	1	5	1	5	1	5	1	5	1	5
5	Робота на практичних заняттях	10	2	20	3	30	2	20	3	30	3	30
6	Робота на семінарах	10	2	20	3	30	2	20	3	30	3	30
7	Виконання модульної контрольної роботи	25	1	25	1	25	1	25	1	25	1	25
	Макс. кількість балів за видами поточного контролю (МВ) (∑=445)	-	-	**76**	-	**98**	-	**76**		**97**		**98**

Методика розрахунків модульної і семестрової оцінок студента

№ з/п	Оцінка студента	Макс. оцінка	Модуль1	Модуль 2	Модуль 3	Модуль4	Модуль5
1	Максимальна підсумкова семестрова модульна оцінка (МС)	**60**	-	-	-		
2	Максимальні підсумкові оцінки за змістовими модулями (ММ)		**10**	**13**	**11**	**13**	**13**
3	Фактична кількість балів, отриманих студентом за видами поточного контролю *(приклад)* (ФБ)		*70*	*90*	*65*	*92*	*95*
4	Підсумкові фактичні оцінки студента за змістовими модулями М = ФБ*ММ/ МВ *(приклад)*		9	12	9	12	13
5	Підсумкова семестрова модульна оцінка студента $С = М_1+М_2+М_3 +М_4$ *(приклад)*		**55**				
6	Екзаменаційна рейтингова оцінка студентів, (Е) *(приклад)*	**40**	**40**				
7	Підсумкова семестрова рейтингова оцінка студента Р = С + Е *(приклад)*		**95/ А**				

6.2. Завдання для самостійної роботи та критерії її оцінювання

№ з/п	**Назва теми**	**Кількість годин**	**Бали**

Змістовий модуль 1. Сутність та основні поняття ризикології		**6**	**5**
1	Привести приклади різних видів ризиків щодо певного виду комерційної діяльності.	6	5
Змістовий модуль 2. Основи ризик-менеджменту		**12**	**5**
2	Для даного підприємства ідентифікувати ризики, здійснити якісний та кількісний аналіз ризиків та прийняти управлінське рішення щодо їх зниження.	5	5
Змістовий модуль 3. Інформаційні ризики та їх особливості		**12**	**5**
3	Здійснити порівняльний аналіз інформаційного ризику з іншими видами ризиків	12	5
Змістовий модуль 4. Сучасні підходи до аналізу та оцінювання ризиків ІБ		**20**	**5**
4	Виявлення повної множини загроз безпеки інформаційним ресурсам, які підлягають захисту. Проведення оцінки уразливості та ризиків для інформаційних ресурсів, що підлягають захисту, при виявленій множині загроз.	20	5
Змістовий модуль 5. Управління ризиками інформаційної безпеки		**20**	**5**
5	Можливості комп'ютерного моделювання та використання спеціалізованого програмного забезпечення для оцінки ризиків у кібербезпеці з метою управління ними	20	5
	Разом	**70**	**25**

6.3. Форми проведення модульного контролю та критерії оцінювання

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних заняттях, на семінарах, за виконання домашніх завдань, за модульну контрольну роботу. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу модуля. Форма проведення – автоматизований тестовий контроль. Модульна контрольна робота оцінюється у 25 балів.

Сума балів	Значення оцінки
22-25	студент виявив повне знання програмного матеріалу, успішно виконує передбачені програмою завдання, засвоїв основну літературу рекомендовану програмою, виявив систематичний характер знань з дисциплін і здатний до самостійного доповнення
13-21	студент 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	студент, 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 – залік на основі поточних оцінок.

6.5. Шкала відповідності оцінок

Контроль успішності студентів з урахуванням поточного оцінювання здійснюється відповідно до навчально-методичної карти дисципліни (п. 7), де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у європейську (ECTS) шкалу подано нижче у таблицях.

Шкала оцінювання ECTS

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

7. Навчально-методична картка дисципліни

Разом: 150 год., із них: лекції – 18 год., практичні заняття – 26 год., семінари – 26 год, модульний контроль – 10 год., самостійна робота – 70 год.

Модулі (назви, бали)	**1. Сутність та основні поняття ризикології**	**2. Основи ризик-менеджменту (98 балів)**	**3. Інформаційні ризики та їх особливості**	**4. Сучасні підходи до аналізу та оцінювання**	**5. Управління ризиками інформаційно**

	(76 балів)				**(76 балів)**		**ризиків ІБ (97 балів)**			**ї безпеки (98 балів)**	
Теми	1	2	3	4	5	6	7			8	9
Лекції (теми, бали)	1. Ризик та його ключові характеристики (1 бал)	2. Класифікація ризиків (1 бал)	3. Аналіз ризиків та методи їх оцінювання (1 бал)	4. Основи ризик-менеджменту (1 бал)	5. Ризики ІБ: суть, складові, нормативне забезпечення	6. Теоретичні основи ризик-менеджменту в ІБ (1 бал)	7.Методи, засоби, інструментарій аналізу та оцінювання ризиків ІБ (1 бал)			8. Методи обробки ризиків ІБ (1 бал)	9. Методи реалізації рішень на основі аналізу та оцінки ризику (1 бал)
Практичні заняття (теми, бали)	1.Структурні характеристики ризику (11 балів)	2. Побудова дерева рішень в контексті теорії корисності (11 балів)	3-4. Якісний та кількісний аналіз ризику (22 бали)	5. Основи ризик-менеджменту (11 балів)	6. Нормативне забезпечення у сфері ризиків ІБ (11 балів)	7. Теоретичні основи ризик-менеджменту в ІБ (11 бал)	8. SWOT-аналіз ризиків ІБ (11 балів)	9. Кількісний аналіз ризику ІБ (11 бали)	10. Метод експертних оцінок (11 балів)	11. Методи обробки ризиків ІБ (11 балів)	12-13. Методи реалізації рішень на основі аналізу та оцінки ризику (22 бали)
Семінарські заняття (теми, бали)	1.Структурні характеристики ризику (11 балів)	2. Теорії корисності (11 балів)	3-4. Якісний та кількісний аналіз ризику (22 бали)	5. Моделі ризиків (11 балів)	6. Ризики ІБ: суть, складові (11 балів)	7. Теоретичні основи ризик-менеджменту в ІБ (11 бал)	8. Методи аналізу та оцінювання ризику ІБ (11 бали)	9. Засоби аналізу та оцінювання ризику ІБ (11 бали)	10. Інструментарій аналізу та оцінювання ризику ІБ (11 балів)	11. Методи обробки ризиків ІБ (11 балів)	12-13. Методи реалізації рішень на основі аналізу та оцінки ризику (22 бали)
Самостійна робота	Самостійна робота (5 балів)		Самостійна робота (5 балів)		Самостійна робота (5 балів)		Самостійна робота (5 балів)			Самостійна робота (5 балів)	
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)		Модульна контрольна робота 2 (25 балів)		Модульна контрольна робота 3 (25 балів)		Модульна контрольна робота 4 (25 балів)			Модульна контрольна робота 5 (25 балів)	
Рейтингова оцінка	100 балів										

(бали)	

8. Рекомендовані джерела

Основна (базова)

1. Архипов О.Є., Муратов О.Є., Бровко В.Д. Основи теорії ризиків: навчальний посібник – К.: НА СБ України, 2019. – 267 с.
2. Архипов О. Є. Вступ до теорії ризиків: інформаційні ризики : моногр. / О. Є. Архипов. – К.: Нац. акад. СБУ, 2015. – 248 с.
3. Бурячок В.Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна і кібербезпека: соціотехнічний аспект: Підручник. – К.: ДУТ, 2015. – 288 с.
4. Інформаційна безпека держави [Текст]: навч. посіб. / В. М. Рудницький. С. О. Гнатюк, Н. В. Лада, Р. В. Бреус ; Черкаський державний технологічний університет. - Харків : [ДІСА ПЛЮС], 2018. - 359 с.

Додаткова

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. Antonucci D. The Cyber Risk Handbook / Domenic Antonucci. – New Jersey: John Wiley & Sons, 2017. – 433 c.
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. – P. 133-137.
4. Henry K. Risk management and analysis / Kevin Henry // Information Security Management Handbook / Edited by Harold F. Tipton, Micki Krauze. – 6th edition. – Boca Raton : Auerbach Publications, 2017. – Part 1, Section 1.4, Ch. 28. – P. 321-329.
5. ISO/IEC 27001:2005 «Information technology. Security techniques. Information security management systems. Requirements».
6. ISO/IEC 13335-3:1998 «Information technology. Guidelines for the management of IT Security. Part 3: Techniques for the management of IT Security».
7. ISO/IEC 13335:2000 «Information technology. Guidelines for the management of IT Security. Part 4: Selection of safeguards».
8. ISO/IEC 27002:2005 «Information technology. Security techniques. Code of practice for information security management».
9. ISO/IEC Guide 73:2009 «Risk management. Vocabulary. Guidelines for use in standards».
10. ISO/IEC 13335-1:2004 «Information technology. Security techniques. Management of information and communications technology security».
11. ISO/TR 13569:2005 «Financial services - Information security guidelines».
12. ISO/IEC TR 18044:2004 «Information technology. Security techniques. Information security incident management».
13. ISO/IEC 15408-1:2009 «The Common Criteria for Information Technology Security Evaluation. 1: Introduction and general model».
14. ISO/IEC 15408-2:2008 «The Common Criteria for Information Technology Security Evaluation. Security functional components».
15. ISO/IEC 15408-3:2008 «The Common Criteria for Information Technology Security Evaluation. Security assurance components».

16. 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.
17. Rittinghouse J. W. Business continuity and disaster recovery for infosec managers / John W. Rittinghouse, James F. Ransome. – Oxford: Elsevier, 2015. – 408 p.
18. Spedding L. Business risk management handbook: a sustainable approach / Linda Spedding, Adam Rose. – Oxford: Elsevier, 2018. – 768 p.
19. Архипов О. Є. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації / О. Є. Архипов, А. В. Скиба // Захист інформації. – 2012. – Т. 15. – № 4. – С. 366– 375.
20. Архипов О. Є. Щодо методики ідентифікації та оцінювання активів системи інформаційних технологій / О. Є. Архипов // Захист інформації. – 2011. – № 1(50). – С. 42–47.
21. Барибін О. І. Стандартизація та сертифікація в галузі інформаційної безпеки : Навчальний посібник. Вінниця : ДонНУ імені Василя Стуса, 2018. 238 с.
22. Василевич Л.Ф. Юртин І.І. Прийняття рішень за умов конфлікту та невизначеності середовища. Навчальний посібник – К. : Київ. ун-т ім.. Б. Грінченка. 2013. – 128с.
23. Економічний ризик: методи оцінки та управління [Текст] : 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
24. 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). – С. 53-56.

Додаткові ресурси
1. http://ito.vspu.net/Prakt_IT/PIDSUMOK/2014-2015/rob/Klochenok/tzi.html