

Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Кафедра безпеки інформації та телекомунікацій

«ЗАТВЕРДЖЕНО»
на засіданні кафедри БІТ

(протокол № 9 від 23.04.2019 р.)

завідувач кафедри
Корнієнко В.І. _____

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Теорія ризиків»

Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Освітній рівень.....	бакалавр
Освітньо-професійна програма	Кібербезпека
Спеціалізація	
Статус	вибіркова
Загальний обсяг	4 кредити ЄКТС (120 годин)
Форма підсумкового контролю	екзамен
Термін викладання	5-й семестр
Мова викладання	українська

Викладачі: ст. в. Тимофєєв Д.С.

Пролонговано: на 20__/20__ н.р. _____ (_____) «__» 20__ р.
(підпис, ПІБ, дата)

на 20__/20__ н.р. _____ (_____) «__» 20__ р.
(підпис, ПІБ, дата)

Дніпро
НТУ «ДП»
2019

Робоча програма навчальної дисципліни «Теорія ризиків» для бакалаврів спеціальності 125 «Кібербезпека» / Нац. техн. ун-т. «Дніпровська політехніка», каф. безпеки інформації та телекомунікацій – Д. : НТУ «ДП», 2019. – 13 с.

Розробник – Тимофєєв Д.С.

Робоча програма регламентує:

- мету дисципліни;
- дисциплінарні результати навчання, сформовані на основі трансформації очікуваних результатів навчання освітньої програми;
- базові дисципліни;
- обсяг і розподіл за формами організації освітнього процесу та видами навчальних занять;
- програму дисципліни (тематичний план за видами навчальних занять);
- алгоритм оцінювання рівня досягнення дисциплінарних результатів навчання (шкали, засоби, процедури та критерії оцінювання);
- інструменти, обладнання та програмне забезпечення;
- рекомендовані джерела інформації.

Робоча програма призначена для реалізації компетентнісного підходу під час планування освітнього процесу, викладання дисципліни, підготовки студентів до контрольних заходів, контролю провадження освітньої діяльності, внутрішнього та зовнішнього контролю забезпечення якості вищої освіти, акредитації освітніх програм у межах спеціальності.

Робоча програма буде в пригоді для формування змісту підвищення кваліфікації науково-педагогічних працівників кафедр університету.

Погоджено рішенням методичної комісії спеціальності 125 «Кібербезпека» (протокол № 9 від 23.04.2019 р.).

ЗМІСТ

1 МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ	4
2 ОЧІКУВАНІ ДИСЦИПЛІНАРНІ РЕЗУЛЬТАТИ НАВЧАННЯ.....	4
3 БАЗОВІ ДИСЦИПЛІНИ	4
4 ОБСЯГ І РОЗПОДІЛ ЗА ФОРМАМИ ОРГАНІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ ТА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ	5
5 ПРОГРАМА ДИСЦИПЛІНИ ЗА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ.....	5
6 ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ	7
6.1 Шкали	7
6.2 Засоби та процедури.....	7
6.3 Критерії.....	9
7 ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ	12
8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ.....	12

1 МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

В освітньо-професійній програмі Національного технічного університету «Дніпровська політехніка» спеціальності 125 «Кібербезпека» здійснено розподіл програмних результатів навчання (ПРН) за організаційними формами освітнього процесу. Зокрема, до дисципліни В1.1 «Теорія ризиків» віднесено такі результати навчання:

ВР1.5	Забезпечувати функціонування системи управління інформаційною та\або кібербезпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісного і якісного оцінки.
ВР2.4	Аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в ІТС;

Мета дисципліни – формування компетентностей щодо застосування ризик-орієнтованого підходу до управління інформаційною та кібербезпекою.

Реалізація мети вимагає трансформації програмних результатів навчання в дисциплінарні та адекватний відбір змісту навчальної дисципліни за цим критерієм.

2 ОЧІКУВАНІ ДИСЦИПЛІНАРНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Шифр ПРН	Дисциплінарні результати навчання (ДРН)	
	шифр ДРН	зміст
ВР1.5	ВР1.5-В1.1	Забезпечувати функціонування системи управління інформаційною та\або кібербезпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісного і якісного оцінки.
ВР2.4	ВР2.4-В1.1	Аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в ІТС;

3 БАЗОВІ ДИСЦИПЛІНИ

Назва дисципліни	Здобуті результати навчання
Ф3 Вступ до фаху	Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
Ф14 Основи забезпечення безпеки інформації	Готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки;
Б3 Теорія ймовірностей та математична статистика	Здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; Застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем;

4 ОБСЯГ І РОЗПОДІЛ ЗА ФОРМАМИ ОРГАНІЗАЦІЇ ОСВІТНЬОГО ПРОЦЕСУ ТА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ

Вид навчальних занять	Обсяг, години	Розподіл за формами навчання, години					
		денна		вечірня		заочна	
		аудиторні заняття	самостійна робота	аудиторні заняття	самостійна робота	аудиторні заняття	самостійна робота
лекційні	70	24	46	14	56	10	60
практичні	50	22	28	12	38	8	42
лабораторні	-	-	-	-	-	-	-
семінари	-	-	-	-	-	-	-
РАЗОМ	120	46	74	26	94	18	102

5 ПРОГРАМА ДИСЦИПЛІНИ ЗА ВИДАМИ НАВЧАЛЬНИХ ЗАНЯТЬ

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, години
	ЛЕКЦІЇ	70
BP1.5-B1.1	<p>Розвиток загальної теорії ризиків в історичному аспекті. Фактори, що зумовлюють підвищення ролі теорії ризиків в сучасному світі.</p> <p>Об'єкти дослідження загальної теорії ризиків. Концепції ризику. Основні визначення. Ризик. Ризик інформаційної безпеки. Загроза. Уразливість. Актив. Аналіз, оцінка та оцінювання ризику. Управління ризиком. Властивості, що визначають поняття і прояв ризику.</p> <p>Поняття невизначеності. Класифікація невизначеностей. Класифікація ризиків. Концепції аналізу ризику (за сферами прояву). Методи аналізу ризику в рамках технократичної концепції.</p> <p>Основні національні та міжнародні стандарти в сфері аналізу, оцінки та управління ризиками.</p> <p>Основні міжнародні стандарти в сфері управління ризиками інформаційної безпеки.</p>	30
BP2.4-B1.1	<p>Система управління інформаційними ризиками. Структура. Процесна модель управління ризиками.</p> <p>Процес управління ризиками інформаційної безпеки відповідно до ISO 27005.</p> <p>Процес управління ризиками інформаційної безпеки відповідно до ISO 27005. Характеристика етапу «Встановлення контексту».</p> <p>Процес управління ризиками інформаційної безпеки відповідно до ISO 27005. Характеристика етапу «Встановлення контексту».</p> <p>Область застосування і кордони.</p> <p>Оцінка ризиків інформаційної безпеки. Основні методики.</p> <p>Аналіз ризиків інформаційної безпеки відповідно до ISO 27005.</p> <p>Етап ідентифікації ризиків.</p> <p>Ідентифікація активів.</p> <p>Ідентифікація загроз.</p> <p>Ідентифікація контролів.</p> <p>Ідентифікація вразливостей.</p>	40

Шифри ДРН	Види та тематика навчальних занять	Обсяг складових, години
	Ідентифікація наслідків. Оцінка ризиків інформаційної безпеки відповідно до ISO 27005. Методології. Оцінка ймовірності. Оцінка наслідків. Обробка ризиків інформаційної безпеки відповідно до ISO 27005. Комунікації ризику інформаційної безпеки відповідно до ISO 27005. Моніторинг та перегляд ризику інформаційної безпеки відповідно до ISO 27005.	
	ПРАКТИЧНІ ЗАНЯТТЯ	50
BP1.5-B1.1 BP2.4-B1.1	Програмне моделювання процесу управління ризиками інформаційної безпеки	10
	Оцінка ризиків невідповідності вимогам ДСТУ ISO/IEC 27001	10
	Оцінка ризиків із застосуванням моделювання інформаційних потоків	10
	Оцінка ризиків із застосуванням моделювання загроз та вразливостей	10
	Оцінка ризиків із застосуванням методики FAIR	10
	РАЗОМ	120

6 ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Сертифікація досягнень студентів здійснюється за допомогою прозорих процедур, що ґрунтуються на об'єктивних критеріях відповідно до «Положення про оцінювання результатів навчання здобувачів вищої освіти».

Досягнутий рівень компетентностей відносно очікуваних, що ідентифікований під час контрольних заходів, відображає реальний результат навчання студента за дисципліною.

6.1 Шкали

Оцінювання навчальних досягнень студентів НТУ «ДП» здійснюється за рейтинговою (100-бальною) та інституційною шкалами. Остання необхідна (за офіційною відсутністю національної шкали) для конвертації (переведення) оцінок мобільних студентів.

Шкали оцінювання навчальних досягнень студентів НТУ «ДП»

Рейтингова	Інституційна
90...100	відмінно / Excellent
74...89	добре / Good
60...73	задовільно / Satisfactory
0...59	незадовільно / Fail

Кредити навчальної дисципліни зараховується, якщо студент отримав підсумкову оцінку не менше 60-ти балів. Нижча оцінка вважається академічною заборгованістю, що підлягає ліквідації.

6.2 Засоби та процедури

Зміст засобів діагностики спрямовано на контроль рівня сформованості знань, умінь, комунікації, автономності та відповідальності студента за вимогами НРК до 7-го кваліфікаційного рівня під час демонстрації регламентованих робочою програмою результатів навчання.

Студент на контрольних заходах має виконувати завдання, орієнтовані виключно на демонстрацію дисциплінарних результатів навчання (розділ 2).

Засоби діагностики, що надаються студентам на контрольних заходах у вигляді завдань для поточного та підсумкового контролю, формуються шляхом конкретизації вихідних даних та способу демонстрації дисциплінарних результатів навчання.

Засоби діагностики (контрольні завдання) для поточного та підсумкового контролю дисципліни затверджуються кафедрою.

Види засобів діагностики та процедур оцінювання для поточного та підсумкового контролю дисципліни подано нижче.

Засоби діагностики та процедури оцінювання

ПОТОЧНИЙ КОНТРОЛЬ			ПІДСУМКОВИЙ КОНТРОЛЬ	
навчальне заняття	засоби діагностики	процедури	засоби діагностики	процедури
лекції	контрольні завдання за кожною темою	виконання завдання під час лекцій	комплексна контрольна робота (ККР)	визначення середньозваженого результату поточних контролів; виконання ККР під час екзамену за бажанням студента
практичні	контрольні завдання за кожною темою	виконання завдань під час практичних занять		
	або індивідуальне завдання	виконання завдань під час самостійної роботи		

Під час поточного контролю лекційні заняття оцінюються шляхом визначення якості виконання контрольних конкретизованих завдань. Практичні заняття оцінюються якістю виконання контрольного або індивідуального завдання.

Якщо зміст певного виду занять підпорядковано декільком дескрипторам, то інтегральне значення оцінки може визначатися з урахуванням вагових коефіцієнтів, що встановлюються викладачем.

За наявності рівня результатів поточних контролів з усіх видів навчальних занять не менше 60 балів, підсумковий контроль здійснюється без участі студента шляхом визначення середньозваженого значення поточних оцінок.

Незалежно від результатів поточного контролю кожен студент під час екзамену має право виконувати ККР, яка містить завдання, що охоплюють ключові дисциплінарні результати навчання.

Кількість конкретизованих завдань ККР повинна відповідати відведеному часу на виконання. Кількість варіантів ККР має забезпечити індивідуалізацію завдання.

Значення оцінки за виконання ККР визначається середньою оцінкою складових (конкретизованих завдань) і є остаточним.

Інтегральне значення оцінки виконання ККР може визначатися з урахуванням вагових коефіцієнтів, що встановлюється кафедрою для кожного дескриптора НРК.

6.3 Критерії

Реальні результати навчання студента ідентифікуються та вимірюються відносно очікуваних під час контрольних заходів за допомогою критеріїв, що описують дії студента для демонстрації досягнення результатів навчання.

Для оцінювання виконання контрольних завдань під час поточного контролю лекційних і практичних занять в якості критерія використовується коефіцієнт засвоєння, що автоматично адаптує показник оцінки до рейтингової шкали:

$$O_i = 100 a/m,$$

де a – число правильних відповідей або виконаних суттєвих операцій відповідно до еталону рішення; m – загальна кількість запитань або суттєвих операцій еталону.

Індивідуальні завдання та комплексні контрольні роботи оцінюються експертно за допомогою критеріїв, що характеризують співвідношення вимог до рівня компетентностей і показників оцінки за рейтинговою шкалою.

Зміст критеріїв спирається на компетентності характеристики, визначені НРК для бакалаврського рівня вищої освіти (подано нижче).

Загальні критерії досягнення результатів навчання для 7-го кваліфікаційного рівня за НРК

Інтегральна компетентність – здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у певній галузі професійної діяльності або у процесі навчання, що передбачає застосування певних теорій та методів відповідної науки і характеризується комплексністю та невизначеністю умов.

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
Знання		
♦ концептуальні знання, набуті у процесі навчання та професійної	- Відповідь відмінна – правильна, обґрунтована, осмислена. Характеризує наявність: - концептуальних знань; - високого ступеню володіння станом питання; - критичного осмислення основних теорій, принципів,	95-100

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
діяльності, включаючи певні знання сучасних досягнень; ♦ критичне осмислення основних теорій, принципів, методів і понять у навчанні та професійній діяльності	методів і понять у навчанні та професійній діяльності	
	Відповідь містить негрубі помилки або описки	90-94
	Відповідь правильна, але має певні неточності	85-89
	Відповідь правильна, але має певні неточності й недостатньо обґрунтована	80-84
	Відповідь правильна, але має певні неточності, недостатньо обґрунтована та осмислена	74-79
	Відповідь фрагментарна	70-73
	Відповідь демонструє нечіткі уявлення студента про об'єкт вивчення	65-69
	Рівень знань мінімально задовільний	60-64
	Рівень знань незадовільний	<60
Уміння		
♦ розв'язання складних непередбачуваних задач і проблем у спеціалізованих сферах професійної діяльності та/або навчання, що передбачає збирання та інтерпретацію інформації (даних), вибір методів та інструментальних засобів, застосування інноваційних підходів	- Відповідь характеризує уміння: - виявляти проблеми; - формулювати гіпотези; - розв'язувати проблеми; - обирати адекватні методи та інструментальні засоби; - збирати та логічно й зрозуміло інтерпретувати інформацію; - використовувати інноваційні підходи до розв'язання завдання	95-100
	Відповідь характеризує уміння застосовувати знання в практичній діяльності з не грубими помилками	90-94
	Відповідь характеризує уміння застосовувати знання в практичній діяльності, але має певні неточності при реалізації однієї вимоги	85-89
	Відповідь характеризує уміння застосовувати знання в практичній діяльності, але має певні неточності при реалізації двох вимог	80-84
	Відповідь характеризує уміння застосовувати знання в практичній діяльності, але має певні неточності при реалізації трьох вимог	74-79
	Відповідь характеризує уміння застосовувати знання в практичній діяльності, але має певні неточності при реалізації чотирьох вимог	70-73
	Відповідь характеризує уміння застосовувати знання в практичній діяльності при виконанні завдань за зразком	65-69
	Відповідь характеризує уміння застосовувати знання при виконанні завдань за зразком, але з неточностями	60-64
	Рівень умінь незадовільний	<60
Комунікація		
♦ донесення до фахівців і нефахівців інформації, ідей, проблем, рішень та власного досвіду в	- Вільне володіння проблематикою галузі. Зрозумілість відповіді (доповіді). Мова: - правильна; - - чиста; - - ясна;	95-100

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
галузі професійної діяльності; ♦ здатність ефективно формувати комунікаційну стратегію	<ul style="list-style-type: none"> - - точна; - - логічна; - - виразна; - - лаконічна. Комунікаційна стратегія: <ul style="list-style-type: none"> - послідовний і несуперечливий розвиток думки; - наявність логічних власних суджень; - доречна аргументації та її відповідність відстоюваним положенням; - правильна структура відповіді (доповіді); - правильність відповідей на запитання; - доречна техніка відповідей на запитання; - здатність робити висновки та формулювати пропозиції 	
	Достатнє володіння проблематикою галузі з незначними хибами. Достатня зрозумілість відповіді (доповіді) з незначними хибами. Доречна комунікаційна стратегія з незначними хибами	90-94
	Добре володіння проблематикою галузі. Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано три вимоги)	85-89
	Добре володіння проблематикою галузі. Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано чотири вимоги)	80-84
	Добре володіння проблематикою галузі. Добра зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано п'ять вимог)	74-79
	Задовільне володіння проблематикою галузі. Задовільна зрозумілість відповіді (доповіді) та доречна комунікаційна стратегія (сумарно не реалізовано сім вимог)	70-73
	Часткове володіння проблематикою галузі. Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано дев'ять вимог)	65-69
	Фрагментарне володіння проблематикою галузі. Задовільна зрозумілість відповіді (доповіді) та комунікаційна стратегія з хибами (сумарно не реалізовано 10 вимог)	60-64
	Рівень комунікації незадовільний	<60
Автономність та відповідальність		
♦ управління комплексними діями або проектами, відповідальність за прийняття рішень у непередбачуваних	<ul style="list-style-type: none"> - Відмінне володіння компетенціями менеджменту особистості, орієнтованих на: 1) управління комплексними проектами, що передбачає: - дослідницький характер навчальної діяльності, позначена вмінням самостійно оцінювати різноманітні 	95-100

Дескриптори НРК	Вимоги до знань, умінь, комунікації, автономності та відповідальності	Показник оцінки
умовах; ♦ відповідальність за професійний розвиток окремих осіб та/або груп осіб ♦ здатність до подальшого навчання з високим рівнем автономності	життєві ситуації, явища, факти, виявляти і відстоювати особисту позицію; - здатність до роботи в команді; - контроль власних дій; 2) відповідальність за прийняття рішень в непередбачуваних умовах, що включає: - обґрунтування власних рішень положеннями нормативної бази галузевого та державного рівнів; - самостійність під час виконання поставлених завдань; - ініціативу в обговоренні проблем; - відповідальність за взаємовідносини; 3) відповідальність за професійний розвиток окремих осіб та/або груп осіб, що передбачає: - використання професійно-орієнтовних навичок; - використання доказів із самостійною і правильною аргументацією; - володіння всіма видами навчальної діяльності; 4) здатність до подальшого навчання з високим рівнем автономності, що передбачає: - ступінь володіння фундаментальними знаннями; - самостійність оцінних суджень; - високий рівень сформованості загальнонавчальних умінь і навичок; - самостійний пошук та аналіз джерел інформації	
	Упевнене володіння компетенціями менеджменту особистості (не реалізовано дві вимоги)	90-94
	Добре володіння компетенціями менеджменту особистості (не реалізовано три вимоги)	85-89
	Добре володіння компетенціями менеджменту особистості (не реалізовано чотири вимоги)	80-84
	Добре володіння компетенціями менеджменту особистості (не реалізовано шість вимог)	74-79
	Задовільне володіння компетенціями менеджменту особистості (не реалізовано сім вимог)	70-73
	Задовільне володіння компетенціями менеджменту особистості (не реалізовано вісім вимог)	65-69
	Рівень автономності та відповідальності фрагментарний	60-64
	Рівень автономності та відповідальності незадовільний	<60

7 ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Технічні засоби навчання.

Дистанційна платформа Moodle.

8 РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Василенко О. А. Математично-статистичні методи аналізу у прикладних дослідженнях: навч. посіб. / О. А. Василенко, І. А. Сенча. – Одеса: ОНАЗ ім. О. С. Попова, 2011. – 166 с.
2. ДСТУ ISO/IEC 27005:2015 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT)
3. ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 4. Вибір засобів захисту (ISO/IEC TR 13335-4:2000, IDT)
4. ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 1. Концепції й моделі безпеки ІТ (ISO/IEC TR 13335-1:1996, IDT)
5. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 2. Керування та планування безпеки ІТ (ISO/IEC TR 13335-2:1997, IDT): ДСТУ ISO/IEC TR 13335-2:2003. — Вид. офіц. — Вперше введ. 2004-10-01. — К. : Держспоживстандарт України, 2005. — IV. — 16 с. (Національний стандарт України).
6. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 3. Методи керування захистом ІТ (ISO/IEC TR 13335-3:1998, IDT): ДСТУ ISO/IEC TR 13335-3:2003. — Вид. офіц. — Вперше введ. 2004-10-01. — К. : Держспоживстандарт України, 2005. — IV. — 16 с. (Національний стандарт України).
5. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України [Текст]: лист департаменту інформатизації Національного банку України банкам України від 03 березня 2011 р. № 24-112/365. – К.: НБУ, 2011.
6. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та керівні вказівки (ISO 31000:2018, IDT) (Національний стандарт України).
7. ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT) (Національний стандарт України).
8. ДСТУ ISO Guide 73:2013 Керування ризиком. Словник термінів (ISO Guide 73:2009, IDT)
9. Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой Управление рисками информационной безопасности. Учебное пособие для вузов. - 2-е изд., испр. - М.: Горячая линия-Телеком, 2014. -130 с.: ил. - Серия «Вопросы управления информационной безопасностью. Выпуск 1».
10. Тимофеев Д.С. Методичні рекомендації до самостійної роботи студентів з дисципліни «Теорія ризиків»/ Д.С. Тимофеев [та ін.]; Нац. гірн. ун-т, каф. безпеки інформації та телекомунікацій. – Д. : НГУ, 2016. – 60 с.

11. Астахов А.М. Искусство управления информационными рисками. – М. : ДМК Пресс, 2010. – 312с.
12. Вишняков Я.Д. Общая теория рисков : учеб. пособие для студ. высш. учеб. заведений / Я.Д.Вишняков, Н.Н.Радаев. — 2-е изд., испр. —М. : Издательский центр «Академия», 2008. — 368 с.
13. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99.–К.: ДСТСЗІ СБ України, 1999. - 26 с.

Навчальне видання

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Теорія ризиків» для бакалаврів
спеціальності 125 «Кібербезпека»

Розробник: Дмитро Сергійович Тимофєєв