Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий фізико-технічний інститут
Кафедра інформаційної безпеки

ТЕОРІЯ РИЗИКІВ

Робоча програма навчальної дисципліни (Силабус)

1. Реквізити навчальної дисципліни

Рівень вищої освіти	***Перший (освітньо- професійний)***
Галузь знань	*11 Математика і статистика*
Спеціальність	*113 Прикладна математика*
Освітня програма	*Математичні методи криптографічного захисту інформації*
Статус дисципліни	*Вибіркова*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*4 курс, 7 семестр*
Обсяг дисципліни	*Загальна кількість: 120 годин / 4 кредити* *Лекційних занять: 18 годин* *Практичних занять: 18 годин* Самостійна робота студентів: *84* години
Семестровий контроль/ контрольні заходи	*Залік, модульна контрольна робота, поточний контроль*
Розклад занять	*http://rozklad.kpi.ua/*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *доктор технічних наук, професор, Даник Юрій Григорович, e-mail: Danyk_1@ukr.net* Практичні: *доктор технічних наук, професор, Даник Юрій Григорович,* *e-mail: Danyk_1@ukr.net*
Розміщення курсу	Посилання на дистанційний ресурс (Платформа “Сікорський”: курс Комплексні системи захисту інформації: проектування, впровадження, супровід https://do.ipo.kpi.ua/course/view.php?id=3245

2. Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Типовою ознакою сучасного суспільства є зростання кількості і різноманіття викликів, небезпек, і загроз пов’язаних з його всебічним розвитком і ризиків їх реалізації.

Поширеність та масовість виникнення ризиків в усіх сферах людської діяльності є стимулом пошуку способів їх пом’якшення або ж уникнення. Ризик – це також неминучий супутник будь-яких відкриттів, технологічних проривів, вдалих інноваційних та управлінських дій.

У загальному випадку ризики аналізуються та досліджуються з певних позицій, частіше за все з діяльнісно-галузевих: в економіці, екології, політиці, науці, техніці, медицині, військовій галузі, підприємництві, інформаційній діяльності, кібербезпеці тощо.

В цій ситуації на перший план виходить розгляд умов виникнення й розвинення ризикових ситуацій, механізмів та стадій формування ризику, знання типових моделей ризиків, які дозволяють формалізувати опис та дослідження ризиків незалежно від сфери їх існування, розгляду загальних аспектів яких присвячений цей курс.

Тому для ефективної підготовки майбутнім фахівцям спеціальності *113 "Прикладна математика"* необхідно володіти знаннями щодо теоретико-методичних та прикладних засад аналізу та управління ризиками (в тому числі і в сфері інформаційної та кібербезпеки) та їх практичного використання.

При вивченні дисципліни «Теорія ризиків» студенти одержують теоретичні знання про формування і розвиток теорії і практики аналізу та менеджменту ризиків, понятійного апарату та термінології, щодо ризикоутворюючих факторів, структури та моделей ризиків, практичні навички визначення та виконання завдань щодо своєчасних виявлення, оцінки і аналізу ризиків, в кожному конкретному випадку, вміння виконувати постановку задачі щодо управління ризиками, знання вимог міжнародних і вітчизняних стандартів в цій сфері, знання про математичні методи та засоби, які застосовуються для оцінки та аналізу ризиків і роблять управління ризиками більш ефективним. Набуті знання та вміння можуть бути використані студентами у майбутній професійній діяльності за фахом.

Об'єктом вивчення дисципліни є явище ризику в процесі повного циклу його існування - від моменту виникнення до моменту зникнення, ефективність процесів, умови функціонування систем і наслідки рішень оцінити, які на перспективу у вичерпній повноті та з необхідною точністю неможливо.

Предметом навчальної дисципліни є види і особливості ризиків, методи їх аналізу і управління ними.

Метою навчальної дисципліни є – дати уявлення про сутність і зміст поняття „ризик”, типи та моделі ризиків, їх класифікацію, визначальні властивості та шляхи формування, методи аналізу та прогнозування ризиків, а також головні принципи управління ризиками в різних сферах людської діяльності.

Програмні результати навчання:

Загальні компетентності:

ЗК 1 – Здатність учитися і оволодівати сучасними знаннями.

ЗК 2 – Здатність застосовувати знання у практичних ситуаціях.

ЗК 3 – Здатність генерувати нові ідеї (креативність).

ЗК 5 – Здатність проведення досліджень на відповідному рівні.

ЗК 6 – Здатність до абстрактного мислення, аналізу та синтезу.

ЗК 7 – Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

Фахові компетентності:

ФК1 – Здатність використовувати й адаптувати математичні теорії, методи та прийоми для доведення математичних тверджень і теорем.

ФК6 – Здатність розв’язувати професійні задачі за допомогою комп’ютерної техніки, комп’ютерних мереж та Інтернету, в середовищі сучасних операційних систем, з використанням стандартних офісних додатків.

ФК9 – Здатність до проведення математичного і комп’ютерного моделювання, аналізу та обробки даних, обчислювального експерименту, розв’язання формалізованих задач за допомогою спеціалізованих програмних засобів.

ФК13 – Здатність зрозуміти постановку завдання, сформульовану мовою певної предметної галузі, здійснювати пошук та збір необхідних вихідних даних.

ФК14 – Здатність сформулювати математичну постановку задачі, спираючись на постановку мовою предметної галузі, та обирати метод її розв’язання, що забезпечує потрібні точність і надійність результату.

Результати навчання:

РН1 – Демонструвати знання й розуміння основних концепцій, принципів, теорій прикладної математики і використовувати їх на практиці.

РН4 – Виконувати математичний опис, аналіз та синтез дискретних об’єктів та систем, використовуючи поняття й методи дискретної математики та теорії алгоритмів.

РН6 – Володіти основними методами розробки дискретних і неперервних математичних моделей об’єктів та процесів, аналітичного дослідження цих моделей на предмет існування та єдиності їх розв’язку.
РН10 – Володіти методиками вибору раціональних методів та алгоритмів розв’язання математичних задач оптимізації, дослідження операцій, оптимального керування і прийняття рішень, аналізу даних.
РН 13 – Використовувати в практичній роботі спеціалізовані програмні продукти та програмні системи комп’ютерної математики.
РН19 – Збирати та інтерпретувати відповідні дані й аналізувати складності в межах своєї спеціалізації для донесення суджень, які відбивають відповідні соціальні та етичні проблеми.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Дисципліна «Теорія ризиків» частково використовує знання та вміння, набуті у ході вивчення курсів «Теорія ймовірностей” та “Математична статистика» та поглиблює їх у напрямку управління ризиками.

Результати вивчення даної дисципліни можуть бути застосовані у професійній діяльності за фахом та для написання бакалаврської кваліфікаційної роботи.

3. Зміст навчальної дисципліни

РОЗДІЛ 1. Ризик: визначення та зміст в різних сферах діяльності, основні властивості та характеристики

Лекція 1.

Сутність ризику. Ризики в історичному аспекті та в сучасному світі. Основні характеристики ризиків.
Література: [1-8] , дод. література [9,13,14].
Завдання на СРС:
1. *Особливості розвитку теорії ризиків в різних сферах [9]*
2. *Вивчити матеріали лекції. Ознайомитись з рекомендованою літературою.*

Лекція 2.

Механізми виникнення та розвинення ризиків. Невизначеність та її особливості. Структура ризиків. Моделі (концепції) ризиків
Література: [1-8], дод. література [1-8].
Завдання на СРС:
1. *Вивчити матеріали лекції. Ознайомитись з рекомендованою літературою.*
2. *Проблеми оцінювання ризиків в моделі «невизначеність-ризик». [1]*

РОЗДІЛ 2. Ризикоутворюючі фактори, їх описові та кількісні характеристики. Методи аналізу та вимірювання ризиків

Лекція 3.

Небезпеки, загрози та вразливості об’єктів ризику, види, характеристики, класифікація. Аналіз ризиків: концепції аналізу, види та задачі, методи аналізу.
Література: [1,3, 6,8], дод. література [1-5,7,8].
Завдання на СРС:
1. *Вивчити матеріали лекції. Ознайомитись з рекомендованою літературою.*

Лекція 4.

Методи та особливості оцінювання ризиків. Прогнозування ризиків і втрат від їх реалізації.
Особливості експертного аналізу і оцінювання ризиків
Література: [1-8], дод. література [1-5,7,8].
Завдання на СРС:

1. *Вивчити матеріали лекції. Ознайомитись з рекомендованою літературою.*

РОЗДІЛ 3. Управління ризиками

Лекція 5.

Організація управління ризиками, процес управління ризиками.

Література: [1,3, 6,8], дод. література [6,26].

Завдання на СРС:

3. ***1.*** *Вивчити матеріали лекції. Ознайомитись з рекомендованою літературою.*

Лекція 6.

Особливості прийняття рішень про управління окремими специфічними видами ризиків. Психологічні аспекти прийняття рішень в умовах ризику. Комунікація ризику.

Література: [1,3, 6,8], дод. література [1-8,11,12,26].

Завдання на СРС:

4. ***1.*** *Вивчити матеріали лекції. Ознайомитись з рекомендованою літературою.*

РОЗДІЛ 4. Аналіз та управління ризиками в різних сферах

Лекція 7.

Особливості підприємницьких та економічних ризиків. Індивідуальні ризики: оцінювання ризиків передчасної смерті, прийнятність індивідуального ризику, регулювання індивідуального ризику

Література: [1-8], дод. література [1-8].

Завдання на СРС:

5. ***1.*** *Вивчити матеріали лекції. Ознайомитись з рекомендованою літературою.*

Лекція 8.

Інформаційні ризики. Методи оцінювання. Вартісно-мотиваційний підхід до аналізу інформаційних ризиків.

Література: [1,3, 6,8], дод. література [1-5,7,8].

Завдання на СРС:

6. ***1.*** *Вивчити матеріали лекції. Ознайомитись з рекомендованою літературою.*

РОЗДІЛ 5. Нормативно-правове забезпечення управління ризиками

Лекція 9.

Міжнародні стандарти з управління ризиками. Стандарти ISO про принципи аналізу та управління інформаційними ризиками. Національне нормативне забезпечення управління ризиками.

Література: [1,3, 6,8], дод. література [15-25].

Завдання на СРС:

7. ***1.*** *Вивчити матеріали лекції. Ознайомитись з рекомендованою літературою.*

№ КП	№ Розділу	№ Теми	Зміст практикуму	Кількість аудит. годин
1.	1	1.1	Загальний алгоритм комплексного оцінювання ризиків.	2
2.	1	1.2	Розрахунок та оцінка ризику і середнього ризику. Розрахунок та побудова профілю ризиків.	2
3.	1	1.2	Обґрунтування вибору моделей ризиків для типових ситуацій реалізації загроз	2
4.	2	2.1	Обробка результатів групової експертизи, оцінка рівнів компетентності експертів та якості добору групи експертів.	2
5.	2	2.2	Побудова моделі компетентності експерта, обробка результатів групової експертизи із залучення модельних оцінок компетентності експертів.	2
6	3	3.1, 3.2	Розробка положення про внутрішній контроль та управління ризиками	2
7.	4	4.1	Оцінка економічних ризиків вибору варіанту системи	2

			захисту інформації за умов відомих ймовірностей виникнення загроз та відповідних ним втрат.	
8.	4	4.2	Оцінювання ризиків загибелі людини від різних факторів і причин та індивідуальних ризиків загибелі та стати жертвою нещасного випадку жителя певного населеного пункту.	2
9	4	4.2	Розрахунок загального ризику можливої реалізації загрози інформаційним ресурсам, які належать до активів корпоративної інформаційної системи за умов відомої шкоди від порушення конфіденційності ресурсу.	2
	Всього			18

4. Навчальні матеріали та ресурси

Базова література.

8. *Боровик М. В. Ризик-менеджмент : конспект лекцій / М. В. Боровик ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2018. – 65 с.*
9. *Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега, видання друге, перероблене, доповнене – Одеса: ОНАЗ ім. О.С. Попова, 2020. – 327 с.*
10. *Калініченко З.Д. Ризик-менеджмент: навчальний посібник / Дніпро: ДДУВС, 2021. 224 с.*
11. *Посохов І. М., Управління ризиками у підприємництві: навчальний посібник \ І. М. Посохов. – Харків : НТУ «ХПІ», 2015. – 220 с.*
12. *Стешенко О. Д. Ризикологія: Навч. посібник. – Харків: УкрДУЗТ, 2019. – 180 с.*
13. *Шклярук С. Г. Управління фінансовими ризиками: навч. посіб. / С. Г. Шклярук. — Київ : ДП «Вид. дім «Персонал», 2019. — 494 с.*
14. *Roeser Sabine* Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk*, Springer Science & Business Media, 2012, 1187 p.*

Додаткова література.

1. *Архипов О. Є. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації / О. Е. Архипов, А. В. Скиба // Захист інформації. – 2012. – Т. 15. – № 4. – С. 366–375.*
2. *Грайворонський М.В., Новіков О.М. «Безпека інформаційно-комунікаційних систем»-К.: Видавнича група BHV.-2009.-608 с.*
3. *Даник Ю.Г., Грищук Р.В. Основи кібербезпеки: Монографія. – Житомир: ЖНАЕУ, 2016. – 636 с.;*
4. *Даник Ю.Г. Національна безпека: запобігання критичним ситуаціям:/ Ю.Г. Даник, Ю.І. Катков, М.Ф. Пічугін – К. : МО України, Житомир: Рута, 2006. – 388 с.*
5. *Дубровін В. І. Прийняття рішень у процесі управління ризиками проектів / В. І. Дубровін, В.М. Льовкін. – Запоріжжя : ЗНТУ, 2012. – 196 с.*
6. *Качинський А.Б. Безпека, загрози та ризик: наукові концепції та математичні методи.-К.: ІПНБ, НА СБУ.- 2004.-472 с.*
7. *Качинський А.Б. Безпека складних систем // А.Б. Качинський. – К.: ТОВ «Юстіон», 2017. – 494 с.*
8. *Лисенко І. А. Методичні вказівки до виконання лабораторних робіт з навчальної дисципліни "Теорія ризиків" [для студ. денної та заочної форми навч. освітнього ступеню "Бакалавр", за спеціальністю 125 Кібербезпека] Видання оновлене та доповнене / Уклад. І. А. Лисенко – Кропивницький: ЦНТУ, 2018.– 32 с.*
9. *Технічні ризики. Теорія та практикум: [Електронний ресурс]: навч. посібник для студ. / О.М. Терентьєв, С. В. Зайченко, А. Й. Клещов, Н. А. Шевчук / КПІ ім. Ігоря Сікорського. - Електронні тестові дані (1 файл: 5207 КБ). Київ: КПІ ім. Ігоря Сікорського, 2020. – 168 с.*
10. *Danyk Y., Maliarchuk T., Briggs Ch. Hitting Home: Cyber-Hybrid Warfare in Ukraine and Its Impact on the United States the Georgetown Journal of International Affairs (GJIA), 02.2020, gjia.georgetown.edu.*

11. *Danyk Y., Maliarchuk T., Greg Simons Hybrid war and cyber-attacks: creating legal and operational dilemmas, Global Change, Peace & Security, ISSN: 1478-1158 (Print) 1478-1166 (Online) Journal homepage: https://www.tandfonline.com/loi/cpar20, https://doi.org/10.1080/14781158. 2020.1732899*
12. BS 7799-3:2006. Information security management systems. Guidelines for information security risk management.
13. ISO/IEC 27005:2008. Information technology – Security techniques – Information security risk management.
14. ISO/IEC 16085:2006. Systems and software engineering – Life cycle processes – Risk management.
15. ISO/IEC 17799:2005 – Information technology – Security techniques – Code of practice for information security management.
16. ISO/IEC 27005:2008 – Information Technology – Security techniques – Information security risk management.
17. NIST Special Publication 800-30 – Risk Management Guide for Information Technology Systems – Recommendations of the National Institute of Standards.
18. Information Technology – Practice for Information Security Management. International Standard ISO/IEC 17799:2000(E).
19. Information Security Management. Part 2. Specification for Information Security Management systems. British Standard BS 7799, Part 2. 2000.

15. Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Методи навчання: пояснювально-демонстраційний метод, частково-пошуковий, репродуктивний метод.

В рамках дисципліни заплановано наступні види навчальних занять:

- ✔ лекції;
- ✔ практичні заняття;
- ✔ самостійна робота.

На лекціях розкриваються найбільш суттєві теоретичні питання, які дозволяють забезпечити студентам можливість глибокого самостійного вивчення всього програмного матеріалу. Теми та порядок самостійної роботи сформовано в логічній послідовності і повністю узгоджуються з метою дисципліни та здійснюються з використанням рекомендованої літератури та глобальної мережі Internet. На заняттях використовуються звичайна дошка, а також презентації лекцій з використанням мультимедіа-проектора. В дистанційному режимі використовуються засоби Google Meet та відповідні слайди лекцій, а також матеріали дистанційного курсу, викладені на платформі Сікорський.

Теми та порядок освоєння дисципліни «Теорія ризиків» наведений нижче.

Назви змістових модулів і тем	Кількість годин				
	Всього	у тому числі			
		Лекції	Лабораторні	Практичні	СРС
1	2	3	4	5	6
Розділ 1. **Ризик: визначення та зміст в різних сферах діяльності, основні властивості та характеристики**					
Тема 1. Сутність ризику. Ризики в історичному аспекті та в сучасному світі. Основні характеристики ризиків		2		2	6
Тема 2. Механізми виникнення та розвинення ризиків. Невизначеність та її особливості. Структура ризиків. Моделі (концепції) ризиків		2		4	6
Разом за розділом 1	22	4		6	12

Розділ 2. **Ризикоутворюючі фактори, їх описові та кількісні характеристики. Методи аналізу та вимірювання ризиків**					
Тема 1. Небезпеки, загрози та вразливості об'єктів ризику, види, характеристики, класифікація. Аналіз ризиків: концепції аналізу, види та задачі, методи аналізу.		2		2	12
Тема 2. Методи та особливості оцінювання ризиків. Прогнозування ризиків і втрат від їх реалізації. Особливості експертного аналізу і оцінювання ризиків		2		2	12
Разом за розділом 2	32	4		4	24
Розділ 3. **Управління ризиками**					
Тема 1. Організація управління ризиками, процес управління ризиками.		2			8
Тема 2. Особливості прийняття рішень про управління окремими специфічними видами ризиків. Психологічні аспекти прийняття рішень в умовах ризику. Комунікація ризику.		2		2	10
Разом за розділом 3	24	4		2	18
Розділ 4. **Аналіз та управління ризиками в різних сферах**					
Тема 1. Особливості підприємницьких та економічних ризиків. Індивідуальні ризики: оцінювання ризиків передчасної смерті, прийнятність індивідуального ризику, регулювання індивідуального ризику		2		4	6
Тема 2. Інформаційні ризики. Методи оцінювання. Вартістно-мотиваційний підхід до аналізу інформаційних ризиків.		2		2	6
Разом за розділом 4	22	4		6	12
Модульна контрольна робота	2				2
Розділ 5. **Нормативно-правове забезпечення управління ризиками**					
Тема 1. Міжнародні стандарти з управління ризиками. Стандарти ISO про принципи аналізу та управління інформаційними ризиками. Національне нормативне забезпечення управління ризиками.		2			14
Разом за розділом 5	16	2			14
Залік	2				2
Всього годин	120	18		18	84

Теми практичних занять

№ КП	Зміст практикуму	Кількість ауд. годин
1.	Загальний алгоритм комплексного оцінювання ризиків.	2
2.	Розрахунок та оцінка ризику і середнього ризику. Розрахунок та побудова профілю ризиків.	2
3.	Обґрунтування вибору моделей ризиків для типових ситуацій реалізації загроз	2
4.	Обробка результатів групової експертизи, оцінка рівнів компетентності експертів та якості добору групи експертів	2
5.	Побудова моделі компетентності експерта, обробка результатів групової експертизи із залучення модельних оцінок компетентності експертів.	2
6	Розробка положення про внутрішній контроль та управління ризиками	2
7.	Оцінка економічних ризиків вибору варіанту системи захисту інформації за умов відомих ймовірностей виникнення загроз та відповідних ним втрат.	2
8.	Оцінювання ризиків загибелі людини від різних факторів і причин та індивідуальних ризиків загибелі та стати жертвою нещасного випадку жителя певного населеного пункту.	2
9	Розрахунок загального ризику можливої реалізації загрози інформаційним ресурсам, які належать до активів корпоративної інформаційної системи за умов відомої шкоди від порушення конфіденційності ресурсу.	2
	Всього:	18

6. Самостійна робота студента

Самостійна робота здобувача складається з опанування питань лекційного матеріалу, завдань на СРС, підготовки до захисту комп'ютерних практикумів.

№ п/п	Вид самостійної роботи	Кількість годин СРС
	Підготовка до лекційних занять	20
	Підготовка до практичних занять	40
	Підготовка до МКР	24
	Всього	84

16. Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять не оцінюється, але рекомендується. Завдання практичних занять виконуються та захищаються у відповідності до встановлених дедлайнів на протязі семестру.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Поточний контроль: МКР.

Календарний контроль проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу. Календарний контроль базується на поточній рейтинговій оцінці. Умовою позитивної атестації є значення поточного рейтингу студента не менше 50% від максимально можливого на час атестації. Бал, необхідний для отримання позитивного календарного контролю доноситься до студентів викладачем не пізніше ніж за 2 тижні до початку календарного контролю.

Рейтингова система оцінювання:

№ з/п	Контрольний захід	Макс. бал	Ваговий коеф.	Кіл-ть	Всього
1.	МКР	5	5	1	50
2.	Колоквіум	5	1.8	8	50
	Всього				100

Залік та робота в семестрі

Залік проставляється по результатах роботи в семестрі. Рейтингова оцінка роботи за семестр складається з результатів за МКР та колоквіуму. Якщо здобувач виконав усі поточні контрольні заходи і має рейтинг більший за 60 балів (RD ≥ 60), студент отримує оцінку згідно зі своїм рейтингом.

Таблиця переведення рейтингових балів до оцінок за університетською шкалою:

Рейтингові бали, RD	Оцінка за університетською шкалою	Можливість отримання оцінки «автоматом»
95 ≤ RD ≤ 100	Відмінно	-
85 ≤ RD ≤ 94	Дуже добре	-
75 ≤ RD ≤ 84	Добре	-
65 ≤ RD ≤ 74	Задовільно	-
60 ≤ RD ≤ 64	Достатньо	-
RD < 60	Незадовільно	-

9. Додаткова інформація

Питання, що виносяться на МКР та залікову співбесіду (якщо вона проводиться) повністю відповідають тим, що перелічені в складі змісту дисципліни.

Робочу програму навчальної дисципліни (силабус):
Склав: проф. каф. Інформаційної безпеки Даник Юрій Григорович
Ухвалено кафедрою інформаційної безпеки (протокол №6/2022 від 22.06.2022)
Погоджено Методичною комісією факультету[1] (протокол № 6 від 30.06.2022)

[1] Методичною радою університету – для загальноуніверситетських дисциплін.