



# Теорія ризиків

## Робоча програма навчальної дисципліни (Силабус)

### Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Перший (освітньо- професійний)</i>
Галузь знань	<i>11 Математика та статистика</i>
Спеціальність	<i>113 "Прикладна математика"</i>
Освітня програма	<i>Математичні методи криптографічного захисту інформації</i>
Статус дисципліни	<i>Вибіркова</i>
Форма навчання	<i>очна(денна)</i>
Рік підготовки, семестр	<i>4 курс, 7 семестр</i>
Обсяг дисципліни	<i>120 годин (4 кредити ECTS) (18 год. лекцій, 18 год. практичних, Самостійна робота студентів: 84 год)</i>
Семестровий контроль/ контрольні заходи	<i>Залік/модульна контрольна робота</i>
Розклад занять	<i><a href="http://rozklad.kpi.ua/">http://rozklad.kpi.ua/</a></i>
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>Лектор: доктор технічних наук, професор, Даник Юрій Григорович, e-mail: Danyk_1@ukr.net</i> <i>Практичні: к.ф.-м.н., професор, Півень Олег Борисович, e-mail: pivolegbor@gmail.com</i>
Розміщення курсу	<i>Посилання на дистанційний ресурс <a href="https://do.ipk.kpi.ua/course/view.php?id=3245">https://do.ipk.kpi.ua/course/view.php?id=3245</a></i>

### Програма навчальної дисципліни

#### 1. Опис навчальної дисципліни, її мета, предмет вивчення 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-галузових: в економіці, екології, політиці, науці, техніці, медицині, військовій галузі, підприємстві, 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 „ризики”, 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<sup>1</sup> навчання згідно стандарту бакалаврів 113 "Прикладна математика":**

**Загальні компетентності:**

Здатність застосовувати знання у практичних ситуаціях.

K3 2. Знання та розуміння предметної області, термінології та головних визначень в сфері інформаційної безпеки та захисту інформації та розуміння професії.

K3 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

K3 5. Здатність до пошуку, оброблення та аналізу інформації.

K3 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

K3 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій.

**Фахові компетентності:**

ФК 3. Здатність обирати та застосовувати математичні методи для розв'язання прикладних задач, моделювання, аналізу, проектування, керування, прогнозування, прийняття рішень.

ФК 6. 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.

---

<sup>1</sup> Для нормативних дисциплін зазначається згідно матриці відповідності програмних компетентностей та результатів навчання в освітній програмі.

ФК 9. Здатність до проведення математичного і комп'ютерного моделювання, аналізу та обробки даних, обчислювального експерименту, розв'язання формалізованих задач за допомогою спеціалізованих програмних засобів..

ФК 11. Здатність до організації роботи колективу виконавців, приймання доцільних та економічно обґрунтованих організаційних та управлінських рішень, забезпечення безпечних умов праці.

ФК 12. Здатність до пошуку, систематичного вивчення та аналізу науково-технічної інформації, вітчизняного й закордонного досвіду, пов'язаного із застосуванням математичних методів для дослідження різноманітних процесів, явищ та систем.

### **Результати навчання:**

ПРН 2 Володіти основними положеннями та методами математичного, комплексного та функціонального аналізу, лінійної алгебри та теорії чисел, аналітичної геометрії, теорії диференціальних рівнянь, зокрема рівнянь у частинних похідних, теорії ймовірностей, математичної статистики та випадкових процесів, чисельними методами;

ПРН 8 Поєднувати методи математичного та комп'ютерного моделювання з неформальними процедурами експертного аналізу для пошуку оптимальних рішень;

ПРН 10 Володіти методиками вибору раціональних методів та алгоритмів розв'язання математичних задач оптимізації, дослідження операцій, оптимального керування і прийняття рішень, аналізу даних;

ПРН 11 Вміти застосовувати сучасні технології програмування та розроблення програмного забезпечення, програмної реалізації чисельних і символічних алгоритмів;

ПРН 16 Демонструвати навички взаємодії з іншими людьми, вміння працювати в команді.

ПРН 24 Знати та вміти використовувати основні засоби захисту та оборони держави, співвітчизників, матеріальних цінностей та територіальної цілісності держави, зокрема, у разі військових дій та надзвичайних ситуацій;

## **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 курсу «Теорія ймовірностей та математична статистика», (які викладаються на бакалавраті спеціальності 113 "Прикладна математика") та ін. 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**

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

**РОЗДІЛ 3. Управління ризиками**

**РОЗДІЛ 4. Аналіз та управління ризиками в різних сферах**

**РОЗДІЛ 5. Нормативно-правове забезпечення управління ризиками**

#### 4. Навчальні матеріали та ресурси

##### Базова література.

1. Архипов О. Є. Вступ до теорії ризиків: інформаційні ризики : моногр. / О. Є. Архипов. – К. : Нац. акад. СБУ, 2015. – 248 с.
2. 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.
3. 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.
4. Калініченко З.Д. Ризик-менеджмент: навчальний посібник / Дніпро: ДДУВС, 2021. 224 с.
5. Посохов І. М., Управління ризиками у підприємстві: навчальний посібник \ І. М. Посохов. – Харків : НТУ «ХПІ», 2015. – 220 с.
6. Стешенко О. Д. Ризикологія: Навч. посібник. – Харків: УкрДУЗТ, 2019. – 180 с.
7. Шклярук С. Г. Управління фінансовими ризиками: навч. посіб. / С. Г. Шклярук. — Київ : ДП «Вид. дім «Персонал», 2019. — 494 с.
8. 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. Є. 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 ВНУ.-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. Костина Н.В. Основные этапы развития теории риска [http://tdf.pskgu.ru/projects/pgu/storage/wt/wt142/wt142\\_19.pdf](http://tdf.pskgu.ru/projects/pgu/storage/wt/wt142/wt142_19.pdf)
9. 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.
10. Прилипко А. Новые стандарты серии ISO 31000 – Риск-менеджмент [Електронний ресурс] / А. Прилипко // Тренінговий портал України. – 2010. – Режим доступу : <http://trn.work.ua/articles/1750/>.
11. Технічні ризики. Теорія та практикум: [Електронний ресурс]: навч. посібник для студ. / О. М. Терент'єв, С. В. Зайченко, А. Й. Клецов, Н. А. Шевчук / КПІ ім. Ігоря Сікорського. - Електронні тестові дані ( 1 файл: 5207 КБ). Київ: КПІ ім. Ігоря Сікорського, 2020. - 168 с.
12. 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](http://gjia.georgetown.edu)
13. 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>
14. Grant P. ISO 31000:2009 – Setting a New Standard for Risk Management / Grant P. // *Risk Analysis*. – 2010. – Vol. 30. – № 6. – P. 881–886.; Grant P. ISO 31000:2018 – Risk management – Guidelines. Revision 1, 2018, <https://www.iso.org/ru/standard/65694.html>.
  15. Standards Australia. AS/NZS ISO 31000:2009. Risk management – Principles and guidelines [Електронний ресурс] / Standards Australia. – 2009. – Режим доступу : <http://sherq.org/31000.pdf>. ; Standards Australia. AS/NZS ISO 31000:2018. Risk management – Guidelines. <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en>
  16. AS/NZS 4360:2004 (In the form of AS/NZS ISO 31000:2009 – Principles and Guidelines on Implementation). [http://mkidn.gov.pl/media/docs/pol\\_obronna/20150309\\_3-NZ-AUST-2004.pdf](http://mkidn.gov.pl/media/docs/pol_obronna/20150309_3-NZ-AUST-2004.pdf).
  17. International standard ISO/IEC 27000. Retrieved from <https://ostec.blog/wp-content/uploads/2015/07/ISO-IEC-27000.pdf>.
  18. ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT).; ISO/IEC 31010:2019 – Risk management – Risk assessment techniques. <https://www.iso.org/ru/standard/72140.html>.
  19. BS 31100:2021 - BS 31100:2021 Risk management. Code of practice and guidance for the implementation of BS ISO 31000:2018 (Release 3.0), <https://standardsdevelopment.bsigroup.com/projects/2020-03218>.
  20. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. <https://www.iso.org/ru/standard/27001>
  21. ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection – Guidance on managing information security risks (Release 4.0). <https://www.iso.org/standard/80585.html>.
  22. ISO/IEC/IEEE 16085:2020 – Systems and software engineering – Life cycle processes – Risk management (Second edition). <https://www.iso.org/standard/72140.html>.
  23. ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management. Retrieved from <https://www.iso.org/standard/39612.html>.
  24. International standard ISO/IEC 27001. Retrieved from [http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/adeaf3e5\\_cc55\\_4222\\_8767\\_f26bcaec3f70/ISO\\_IEC\\_27001.pdf](http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/adeaf3e5_cc55_4222_8767_f26bcaec3f70/ISO_IEC_27001.pdf).
  25. NIST Special Publication 800-30 Revision 1 – Risk Management Guide for Information Technology Systems – Recommendations of the National Institute of Standards. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>.
  26. Information Security Management. Part 2. Specification for Information Security Management systems. British Standard BS 7799, Part 2. 2000.; BSI BS 7799-3-2017 Information security management systems Part 3: Guidelines for information security risk management, <https://knowledge.bsigroup.com/products/information-security-management-systems-guidelines-for-information-security-risk-management-1>.
  27. ISO/IEC 42001:2023 - Artificial Intelligence Management Systems. <https://www.iso.org/standard/42001>.
  28. NIST Cybersecurity Framework 2.0. 2024, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

## Навчальний контент

### 5. Методика опанування навчальної дисципліни (освітнього компонента)

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 GoogleMeet та відповідні слайди лекцій, а також матеріали дистанційного курсу, викладені на платформі Сікорський.

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

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.*

Механізми виникнення та розвинення ризиків. Невизначеність та її особливості. Структура ризиків. Моделі (концепції) ризиків

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

*Завдання на СРС:*

- 1. Вивчити матеріали лекції. Ознайомитись з рекомендованою літературою.*
- 2. Проблеми оцінювання ризиків в моделі «невизначеність-ризик». [1]. Вивчити матеріали лекції.*
- 3. Ознайомитись з рекомендованою літературою.*

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

Небезпеки, загрози та вразливості об'єктів ризику, види, характеристики, класифікація.

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

*Завдання на СРС:*

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

Аналіз ризиків: концепції аналізу, види та задачі, методи аналізу.

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

*Завдання на СРС:*

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

Методи та особливості оцінювання ризиків.

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

*Завдання на СРС:*

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

Прогнозування ризиків і втрат від їх реалізації.

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

*Завдання на СРС:*

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

Особливості експертного аналізу і оцінювання ризиків

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

*Завдання на СРС:*

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

### **РОЗДІЛ 3. Управління ризиками**

Організація управління ризиками, процес управління ризиками.

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

*Завдання на СРС:*

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

Особливості прийняття рішень про управління окремими специфічними видами ризиків.

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

*Завдання на СРС:*

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

Психологічні аспекти прийняття рішень в умовах ризику. Комунікація ризику.

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

*Завдання на СРС:*

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

### **РОЗДІЛ 4. Аналіз та управління ризиками в різних сферах**

Особливості підприємницьких та економічних ризиків.

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

*Завдання на СРС:*

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

Індивідуальні ризики: оцінювання ризиків передчасної смерті, прийнятність індивідуального ризику, регулювання індивідуального ризику

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

*Завдання на СРС:*

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

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:*

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

### **РОЗДІЛ 5. Нормативно-правове забезпечення управління ризиками**

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

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

*Завдання на СРС:*

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

Національне нормативне забезпечення управління ризиками.

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

*Завдання на СРС:*

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

### **Тема 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 здобувача**

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

№ з/п	Вид самостійної роботи	Кількість годин СРС
1.	Підготовка до лекційних занять	18
2.	Підготовка до практичних занять	52
2.	Підготовка до МКР	8
3.	Підготовка до заліку	6
	<b>Загалом</b>	<b>84</b>

## Політика та контроль

### 7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять не оцінюється, але рекомендується. Під час контрольних заходів студенти повинні дотримуватись політики академічної доброчесності, згідно Кодексу Честі НТУУ «КПІ ім. Ігоря Сікорського».

#### Академічна доброчесність

Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: <https://kpi.ua/code>.

#### Норми етичної поведінки

Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: <https://kpi.ua/code>.

#### Процедура оскарження результатів контрольних заходів

Студенти мають можливість підняти будь-яке питання, яке стосується процедури проведення та/або оцінювання контрольних заходів, та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами. Студенти мають право оскаржити результати контрольних заходів, але обов'язково аргументовано, пояснивши, з яким критерієм не погоджуються відповідно до оціночного листа та/або зауважень.

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

**Поточний контроль:** виконання практичних занять, МКР.

*Практичні заняття сформовані таким чином, що їх завдання сприяють засвоєнню матеріалу за темами дисципліни та формуванню практичних навичок.*

Заохочувальні бали надаються як загальна сума за курс за всіма видами занять – максимальна кількість балів за одне заняття – 1 бал.

Заохочувальні бали	
Критерій	Додається до семестрового рейтингу

Активність на більшості лекційних та практичних занять	+10 балів
--	-----------

**Календарний контроль:** проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу, 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.

### **Семестровий контроль - залік**

*Залік, проставляється за результатами роботи здобувача в семестрі та здачі контрольних заходів та здачі всіх практичних робіт. Бал формується як сума балів модульної контрольної та практичних занять. Якщо здобувач виконав усі поточні контрольні заходи і має рейтинг більший за 60 балів ( $RD \geq 60$ ), студент отримує оцінку відповідно до свого рейтингу.*

### **Пропущені контрольні заходи**

*Результат модульної контрольної роботи для студента(-ки), який не з'явився на контрольний захід, є нульовим. У такому разі, студент(-ка) має можливість написати модульну контрольну роботу, але максимальний бал за неї буде дорівнювати 50% від максимальної кількості балів за МКР. Повторне написання модульної контрольної роботи не допускається.*

*Здобувачі, які виконали всі умови отримання позитивної оцінки, але набрали менше 60 балів, виконують залікову контрольну роботу, яка оцінюється максимально в 24 бали. Попередні бали, отримані за МКР скасовуються. Студенти, що набрали 60 і вище балів, які бажають підвищити свою підсумкову оцінку, на заліковому тижні проходять семестровий контроль у вигляді залікового тесту з можливою максимальною кількістю 24 бали, при цьому результат попередньої МКР скасовується.*

### **Рейтингова система оцінювання:**

№ з/п	Контрольний захід	Макс. бал	Ваговий коеф.	Кіл-ть	Всього
1.	МКР (тест)	24	1	1	24
2.	Практичні заняття	8,12	8*8+1*12	9	76
	Всього				100

На захист студентами кожної виконаної практичної роботи відводиться 2 тижні. Відлік цих 2 тижнів починається з дати проведення за розкладом практичного заняття. У випадку здачі практичної роботи без поважних причин після вказаних 2 тижнів знімаються бали в межах діючих в НТУУ КПІ норм до рівня "задовільно".

### **Таблиця переведення рейтингових балів до оцінок за університетською шкалою:**

Рейтингові бали, RD	Оцінка за університетською шкалою
$95 \leq RD \leq 100$	Відмінно
$85 \leq RD \leq 94$	Дуже добре
$75 \leq RD \leq 84$	Добре
$65 \leq RD \leq 74$	Задовільно
$60 \leq RD \leq 64$	Достатньо

RD < 60	Незадовільно
Невиконання умов допуску	Не допущено

### **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 №8/2025 від 25.06.2025)

Погоджено Методичною комісією НН ФТІ (протокол № 6 від 30.06.2025)