ТЕОРІЯ РИЗИКІВ

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Шифр і назва спеціальності	123 Комп'ютерна інженерія	**Інститут**	Навчально-науковий інститут комп'ютерних наук та інформаційних технологій
Назва програми	Сучасне програмування, мобільні пристрої та комп'ютерні ігри	**Кафедра**	Комп'ютерна інженерія та програмування
Тип програми	Освітньо-наукова	**Мова навчання**	українська

Викладач

Коломійцев Олексій Володимирович, oleksii.kolomiitsev@khpi.edu.ua

Доктор технічних наук, професор, заслужений винахідник України, професор кафедри «КІП» НТУ «ХПІ», автор понад 1300 наукових та науково-методичних праць. Провідний лектор з дисциплін: «Основи безпеки програм та даних», «Теорія ризиків».

Загальна інформація про навчальну дисципліну

Анотація	В дисципліні розглядаються основи теорії ризиків та дослідження системи захисту інформації (даних) у комп'ютерних мережах. Розгляд даних питань забезпечує максимальну спроможність як користувачів, так і комп'ютерних мереж працювати в складному кіберсередовищі, мінімізуючи ризик атаки.
Цілі навчальної дисципліни	Забезпечити теоретичну та практичну підготовку майбутніх фахівців з основних методів, способів, принципів виявлення, аналізу і оцінки ризиків; дати знання про особливості управління ризиками; отримати практичні навички реалізації системи управління ризиками
Формат	Лекції, практичні заняття, самостійна робота, консультації. Підсумковий контроль – екзамен.
Семестр	Третій

Результати навчання:

РН3. Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.

РН11. Приймати ефективні рішення з питань розроблення, впровадження та експлуатації комп'ютерних систем і мереж, аналізувати альтернативи, оцінювати ризики та імовірні наслідки рішень.

Теми, що розглядаються:

Тема 1. Сутність, види та класифікація ризиків

Тема 2. Сутність управління ризиками

Тема 3. Методи оцінки ризиків

Тема 4. Основні загрози використання комп'ютерних мереж для користувачів. Організаційно-технічні заходи щодо технічного захисту інформації

Тема 5. Засоби і методи виявлення та блокування технічних каналів витоку акустичної інформації. Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами

Тема 6. Мережеві пристрої зв'язку. Інфраструктура забезпечення мережевої безпеки

Тема 7. Створення комплексної системи захисту інформаційного простору України від загроз кібертероризму

Тема 8. Стратегія кібербезпеки України (2021 – 2025 роки)

ФОРМА ТА МЕТОДИ НАВЧАННЯ

На лекційних заняттях викладання матеріалу здійснюється в усній формі із записом основних положень лекції у конспект. Для демонстрації презентацій застосовується медіапроектор та комп'ютер.

Призначення практичних занять полягає в поглибленні опрацювання теоретичного матеріалу. При підготовці до практичних занять студентам рекомендується ознайомитися з тематикою заняття, прочитати конспект лекцій на задану тему, ознайомитися з рекомендованою літературою. Практичні заняття розвивають у студентів навички самостійної роботи з вирішення конкретних завдань.

Самостійна робота здійснюється з метою засвоєння та відпрацювання навчального матеріалу, формування у студентів самостійності, здатності до підготовки до майбутніх занять та контролів. Самостійна робота забезпечується підручниками, навчально-методичними посібниками, конспектами лекцій та методичними вказівками. Умовно самостійну роботу можна розділити на базову, яка забезпечує підготовку студента до аудиторних занять та контрольних заходів, та додаткову, яка спрямована на закріплення знань та розвиток аналітичних навичок. Раціональне планування та організація самостійної роботи є важливою умовою її ефективності.

Студенти мають можливість навчатися та розробляти реальні проєкти, взявши участь у програмі «Інноваційний кампус» НТУ «ХПІ». Додаткові знання студенти отримують у рамках неформальної освіти, завдяки організаціям, що забезпечують надання освітніх послуг, такі як NixSolution, GlobalLogic, EPAM та ін.

МЕТОДИ КОНТРОЛЮ

Поточний контроль реалізується у формі опитування, виконання завдань на практичних заняттях, проведення контрольних робіт тощо. Контроль складової робочої програми, яка освоюється під час самостійної роботи студента, проводиться шляхом перевірки конспектів та виконання завдань на практичних заняттях. Семестровий контроль проводиться у формі екзамену відповідно до навчального плану в обсязі навчального матеріалу, визначеного навчальною програмою та у терміни, встановлені навчальним планом. Семестровий контроль може проводитися в усній формі по екзаменаційних білетах або в письмовій формі за контрольними завданнями, а також шляхом тестування з використанням технічних засобів. Можливе поєднання різних форм контролю. Форма проведення семестрового контролю зазначається у робочій програмі навчальної дисципліни. Результати поточного контролю (поточна успішність) можуть враховуватись як допоміжна інформація для виставлення оцінки з даної дисципліни.

Студент вважається допущеним до семестрового екзамену з навчальної дисципліни за умови повного відпрацювання усіх занять та індивідуальних завдань, передбачених навчальною програмою з дисципліни.

Знання та компетенції, які студенти отримають на зовнішніх курсах компаній (GlobalLogic, EPAM та ін.) а також завдяки участі у програмі «Інноваційний кампус» НТУ «ХПІ», можуть бути частково зараховані у вигляді балів за практичні роботи.

РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ, ТА ШКАЛА ОЦІНЮВАННЯ ЗНАНЬ ТА УМІНЬ (НАЦІОНАЛЬНА ТА ECTS)

Таблиця 1 – Розподіл балів для оцінювання успішності студента для заліку

Практичні роботи	Контрольні роботи	Екзамен	Сума
60	20	20	100

Критерії та система оцінювання знань та вмінь студентів.

Згідно основних положень ЄКТС, під системою оцінювання слід розуміти сукупність методів (письмові, усні і практичні тести, екзамени, проекти, тощо), що використовуються при оцінюванні досягнень особами, що навчаються, очікуваних результатів навчання.

Успішне оцінювання результатів навчання є передумовою присвоєння кредитів особі, що навчається. Тому твердження про результати вивчення компонентів програм завжди повинні супроводжуватися зрозумілими та відповідними критеріями оцінювання для присвоєння кредитів. Це дає можливість стверджувати, чи отримала особа, що навчається, необхідні знання, розуміння, компетенції.

Критерії оцінювання – це описи того, що як очікується, має зробити особа, яка навчається, щоб продемонструвати досягнення результату навчання.

Основними концептуальними положеннями системи оцінювання знань та вмінь студентів є:

1. Підвищення якості підготовки і конкурентоспроможності фахівців за рахунок стимулювання самостійної та систематичної роботи студентів

протягом навчального семестру, встановлення постійного зворотного зв'язку викладачів з кожним студентом та своєчасного коригування його навчальної діяльності.

2. Підвищення об'єктивності оцінювання знань студентів відбувається за рахунок контролю протягом семестру із використанням 100-бальної шкали (табл. 2). Оцінки обов'язково переводять у національну шкалу (з виставленням державної семестрової оцінки «відмінно», «добре», «задовільно» чи «незадовільно») та у шкалу ECTS (A, B, C, D, E, FX, F).

Таблиця 2 – Шкала оцінювання знань та умінь: національна та ECTS

Рейтингова оцінка, бали	**Оцінка ECTS та її визначення**	**Національна оцінка**	**Критерії оцінювання**	
			позитивні	**негативні**
1	2	3	4	5
90-100	A	Відмінно	**- глибоке знання** навчального матеріалу модуля, що містяться в **основних і додаткових літературних джерелах;** **- вміння аналізувати** явища, які вивчаються, в їхньому взаємозв'язку і розвитку; **- вміння** проводити **теоретичні розрахунки**; **- відповіді** на запитання **чіткі**, **лаконічні, логічно послідовні;** **- вміння вирішувати складні практичні задачі.**	- відповіді на запитання можуть містити **незначні неточності**
82-89	B	Добре	**- глибокий рівень знань** в обсязі **обов'язкового матеріалу**, що передбачений модулем; - вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**; - вміння вирішувати **складні практичні задачі.**	- відповіді на запитання містять **певні неточності**
75-81	C	Добре	- м**іцні знання** матеріалу, що вивчається, та його **практичного застосування;** - вміння давати **аргументовані відповіді** на запитання і проводити **теоретичні розрахунки**; - вміння вирішувати **практичні задачі.**	- невміння використовувати теоретичні знання для вирішення **складних практичних задач**

1	2	3	4	5
64-74	D	Задовільно	- знання **основних фундаментальних положень** матеріалу, що вивчається, та їх **практичного застосування**; - вміння вирішувати прості **практичні задачі**.	- невміння давати **аргументовані відповіді** на запитання; - невміння **аналізувати** викладений матеріал і **виконувати розрахунки;** - невміння вирішувати **складні практичні задачі.**
60-63	E	Задовільно	- знання **основних фундаментальних положень** матеріалу модуля, - вміння вирішувати найпростіші **практичні задачі**.	- незнання **окремих (непринципових) питань** з матеріалу модуля; - невміння **послідовно і аргументовано** висловлювати думку; - невміння застосовувати теоретичні положення при розв'язанні **практичних задач**
35-59	FX (потрібне додаткове вивчення)	Незадо-вільно	**- додаткове вивчення** матеріалу модуля може бути виконане **в терміни, що передбачені навчальним планом**.	- незнання **основних фундаментальних положень** навчального матеріалу модуля; **- істотні помилки** у відповідях на запитання; - невміння розв'язувати **прості практичні задачі**
1-34	F (потрібне повторне вивчення)	Незадо-вільно	–	- повна **відсутність знань** значної частини навчального матеріалу модуля; **- істотні помилки** у відповідях на запитання; - незнання основних фундаментальних положень; - невміння орієнтуватися під час розв'язання **простих практичних задач**

НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчально-методичний комплекс дисципліни «Теорія ризиків» знаходиться на сервері та сайті кафедри. Він вміщує: силабус, навчальний посібник, методичні вказівки до виконання практичних робіт та ін.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова література

1	Машина Н.І. Ризик і методи його вимірювання. Навчальний посібник. – К.: ЦНЛ, 2003. – 188 с.
2	Гуменюк В.Я. Управління ризиками. Навчальний посібник. / В.Я. Гуменюк, Г.Ю. Міщук, О.О. Олійник – Рівне: НУВГП, 2009, – 156 с.
3	Гур'єв В.І. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека» / В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова – Ніжин: ФОП Лук'янченко В.В. ТПК «Орхідея», 2018. – 166 с.
4	Бурячок В.Л. Інформаційна та кібербезпека: Соціотехнічний аспект. Підручник /В.Л. Бурячок, В.Б. Толубко, В.О. Хорощко, С.В. Толюпа – Львів: «Магнолія 2006», 2018. – 320 с.
5	Когут Ю.І. Кібербезпека та ризики цифрової трансформації компаній. / Ю.І. Когут. – Навчальні та Практичні посібники, Новинки видавництв України, видавництво Сідкон, 2021. – 372 с.

Допоміжна література

6	Кузьминова Н.В. Курс лекций по дисциплине «Управление рисками». / Н.В. Кузьминова, Н.В. Моргунова, Н.М. Филимонова; Владим. гос. ун-т. – Владимир: Изд-во Владим. гос. ун-та, 2007. – 76 с.
7	Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Підручник /В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко – К.: ТОВ «СТК ГРУП Україна», 2015. – 449 с.
8	Гиносян К.А. Основы управления рисками организациями. Учебное пособие. / К.А. Гиносян. – Ереван: Изд-во РАО, 2018. – 153 с.
9	Березуцький В.В. Небезпечні виробничі ризики та надійність: навчальний посібник для студентів за напрямком підготовки 6.170202 «Цивільна безпека» / В.В. Березуцький, М.І. Адаменко. – Харків: НТУ «ХПІ», 2016. – 385 с.

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

1. Ризик (інформаційна безпека). [Електронний ресурс]. – Режими доступу: https://uk.wikipedia.org/wiki/Ризик_(інформаційна_безпека).

2. Теорія ризику. Поняття про ризик. Джерела та чинники. [Електронний ресурс]. – Режими доступу: https://studfile.net/preview/5394673/.

3. Стратегія кібербезпеки України. (2021 – 2025 роки). Безпечний кіберпростір – запорука успішного розвитку України. (Проект). [Електронний ресурс]. – Режими доступу: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf.

4. ДСТУ IEC/ISO 31010:2013 – Управління ризиками – методи оцінки ризику. [Електронний ресурс]. – Режими доступу: https://khoda.gov.ua/image/catalog/files/dstu%2031010.pdf.

Інформаційні ресурси в Інтернеті з конкретних питань простіше усього шукати за допомогою пошукової системи Google, задавши відповідні ключові слова.

Структурно-логічна схема вивчення навчальної дисципліни

Вивчення цієї дисципліни безпосередньо спирається на:	На результати вивчення цієї дисципліни безпосередньо спираються:
Контроль та діагностика комп'ютерних систем	

Провідний лектор: проф. каф. «КІП»

професор Олексій КОЛОМІЙЦЕВ _____

(посада, звання, ПІБ) (підпис)