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

Кафедра системного проектування

РИЗИК-ОРІЄНТОВАНА ІНФОРМАЦІЙНА БЕЗПЕКА РОЗПОДІЛЕНИХ КОМП'ЮТЕРНИХ СИСТЕМ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	***Другий (магістерський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*122 Комп'ютерні науки*
Освітня програма	*Комп'ютерні науки*
Статус дисципліни	*Нормативна*
Форма навчання	*очна(денна)/дистанційна/змішана*
Рік підготовки, семестр	*2 курс, осінній семестр*
Обсяг дисципліни	*4 кредити, 120 годин, 36 годин – лекції, 18 годин – лабораторні роботи, 66 - СРС*
Семестровий контроль/ контрольні заходи	*Іспит, МКР, РГР*
Розклад занять	*Середа, 12:20-13:55 (лекції), 14:15 -15:50 (лабораторні роботи)*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *доктор технічних наук, професор Мухін Вадим Євгенійович, v_mukhin@i.ua, (067)5087684* Лабораторні: *доктор технічних наук, професор Мухін Вадим Євгенійович, v_mukhin@i.ua, (067)5087684*
Розміщення курсу	*https://drive.google.com/drive/folders/1dM8e3GwE39UAuuOGW2muubMbSQFQ9TSB*

Програма навчальної дисципліни

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

1.1. Опис навчальної дисципліни

Навчальна дисципліна “Ризик-орієнтована інформаційна безпека розподілених комп’ютерних систем” призначена для вивчення методів та засобів управління та мінімізації ризиків порушення інформаційної безпеки, сучасних стандартів та засобів в галузі управління ризиками інформаційної безпеки шифрування для побудови комплексних систем захисту комп’ютерних систем та мереж. Навчальна дисципліна призначена для вивчення методів аналізу та прогнозування ризиків інформаційної безпеки та прийомів настроювання реакції програмно-технічних засобів захисту операційних систем з урахуванням виявлених ризиків для створення високо захищених розподілених комп’ютерних систем.

1.2. Мета и завдання навчальної дисципліни

Метою навчальної дисципліни є формування у студентів компетентностей.

ЗДАТНІСТЬ:

- аналізу завдань та нормативно-правової бази в галузі аналізу та прогнозування ризиків порушення інформаційної безпеки в комп’ютерних системах, прийомів настроювання реакції відповідного програмно-технічного забезпечення для захисту інформаційних ресурсів систем;
- застосування стандартних засобів та алгоритмів оцінки ризиків інформаційної безпеки для підвищення захисту особливо важливої інформації;
- застосування моделей встановлення довіри суб’єктів до розподілених комп'ютерних систем;
- застосування методів та засобів мінімізації ризиків захищеності інформаційних систем на основі концепції управління ризиками захищеності інформаційних систем;
- аналізу принципів формування політики безпеки розподілених комп'ютерних систем для захисту інформації обмеженого доступу в мережах підтримки інформаційних та Web-технологій.

1.3. Результати вивчення навчальної дисципліни

Після засвоєння навчальної дисципліни студенти мають оволодіти такими компетентностями:

Загальні компетентності (ЗК):

ЗК 1 – Здатність до абстрактного мислення, аналізу та синтезу.

ЗК 2 – Здатність застосовувати знання у практичних ситуаціях.

ЗК 5 – Здатність вчитися й оволодівати сучасними знаннями.

Фахові компетентності спеціальності (ФК):

ФК 1 – Усвідомлення теоретичних засад комп'ютерних наук.

ФК 19 – Здатність до професійного володіння інструментальними середовищами моніторингу та захисту інформації, розробки проектних рішень з захисту даних в розподілених та інших програмних системах.

Внаслідок вивчення курсу студент повинен бути здатний продемонструвати такі ***програмні результати навчання ОНП:***

ПРН1 – Мати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп'ютерних наук і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у сфері комп'ютерних наук та на межі галузей знань.

ПРН2 – Мати спеціалізовані уміння/навички розв'язання проблем комп'ютерних наук, необхідні- для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур.

ПРН9 – Розробляти алгоритмічне та програмне забезпечення для аналізу даних (включно з великими).

ПРН11 – Створювати нові алгоритми розв'язування задач у сфері комп'ютерних наук, оцінювати їх ефективність та обмеження на їх застосування.

ПРН13 – Оцінювати та забезпечувати якість інформаційних та комп'ютерних систем різного призначення.

ПРН14 – Тестувати програмне забезпечення.

ПРН18 – Збирати, формалізувати, систематизувати і аналізувати потреби та вимоги до інформаційної або комп'ютерної системи, що розробляється, експлуатується чи супроводжується.

ПРН19 – Аналізувати сучасний стан і світові тенденції розвитку комп'ютерних наук та інформаційних технологій.

ПРН28 – Аналізувати та застосовувати протоколи мережевого захисту інформації, розраховувати та реалізовувати політики захисту інформації на програмному та технічному рівнях, розуміти правові засади, на яких базується організація захисту інформації в Україні.

В результаті вивчення курсу студент повинен бути здатний продемонструвати такі:

ЗНАННЯ:

- основні концепції створення гарантованих систем захисту інформації;
- принципів побудови методів управління ризиками безпеки EBIOS, MEHARI, OCTAVE, CRAMM, CORAS;
- існуючих механізмів реалізації моделей захисту, які впроваджуються в різних операційних системах на основі аналізу ризиків інформаційної безпеки;
- стандартів в галузі управління ризиками інформаційної безпеки комп'ютерних систем;
- механізмів управління ризиками інформаційної безпеки на основі засобів RA Software Tool та RiskWatch;
- принципів побудови інфраструктур безпеки PKC GridLab, PROGRESS, ALiCe,

NextGrid, XenoTrust;

- вимог до стандартів щодо класифікації та критеріїв захищеності комп'ютерних систем від несанкціонованого доступу до інформації в контексті ризик-орієнтованого підходу до забезпечення їх захищеності.

УМІННЯ:

- виконати етапи проектування та модифікації підсистем захисту інформації від несанкціонованого доступу на основі аналізу ризиків інформаційної безпеки;
- врахувати вимоги стандартів в галузі управління ризиками інформаційної безпеки комп'ютерних систем в процесі реалізації комплексної системи захисту інформації;
- виконати аналітичні оцінки ризиків порушення захищеності розподілених комп'ютерних систем з використанням методик аналізу та оцінок ризиків безпеки;
- виконати розробку елементів політики безпеки розподілених комп'ютерних систем;
- виконати налагодження програмних комплексів для аналізу ризиків порушення інформаційної безпеки, організувати їх розміщення та виконання на робочий станції та в комп'ютерній мережі.

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

Міждисциплінарні зв'язки: Навчальна дисципліна відноситься до циклу професійної підготовки. Дисципліні передують наступні курси: „Основи сервіс-орієнтованих обчислень і архітектур", „Методи та технології обчислювального інтелекту", "Методи дослідження складних систем та процесів", "Обробка надвеликих масивів даних".

Дисципліною забезпечуються наступні компоненти: Науково-дослідна практика

3. Зміст навчальної дисципліни

Розділ 1. Принципи забезпечення інформаційної безпеки

Тема 1.1. Проблеми забезпечення інформаційної безпеки.

Тема 1.2. Класифікація методів забезпечення безпеки інформаційних систем.

Тема 1.3. Базова модель забезпечення безпеки розподілених комп'ютерних систем.

Тема 1.4. Моделі для встановлення довіри до розподілених комп'ютерних систем.

Тема 1.5. Інфраструктури безпеки PKC GridLab, PROGRESS, ALiCe, NextGrid, XenoTrust.

Тема 1.6. Сучасні стандарти та керівні документи в галузі забезпечення інформаційної безпеки.

Розділ 2. Загальна концепція, аналіз та прогнозування ризиків для різних об'єктів

Тема 2.1. Загальна концепція, аналіз та прогнозування ризиків для різних об'єктів

Тема 2.2. Класифікація ризиків.

Тема 2.3. Основні підходи та методи аналізу ризиків.

Тема 2.4. Методи аналізу ризиків.

Тема 2.5. Методи оцінки ризиків.

Тема 2.6. Стандарти у сфері управління ризиками.

Розділ 3. Методи та засоби аналізу та управління ризиком безпеки інформаційних систем

Тема 3.1. Методи та засоби аналізу та управління ризиками захищеності інформаційних систем.

Тема 3.2. Методи керування ризиками захищеності.

Тема 3.3. Засоби управління ризиками безпеки.

Тема 3.4. Порівняльна оцінка методів та засобів аналізу та управління ризиками захищеності.

Розділ 4. Політика безпеки та формування довіри до розподілених комп'ютерних систем

Тема 4.1. Політика безпеки та формування довіри у розподілених комп'ютерних системах.

Тема 4.2. Основні елементи політики безпеки

4. Навчальні матеріали та ресурси

4.1. Базова література

1. Архипов О. Є., Муратов О. Є., Бровко В. Д. Основи теорії ризиків : навч. посіб / О. Є. Архипов, О. Є. Муратов, В. Д. Бровко. – Київ : НА СБ України, 2019. – 267 с.

2. Основи теорії надійності технічних систем / Павлюк О. М. , Медиковський М.О., Лиса Н.К., Ізонін І.В. – Львів, Львівська політехніка, 2021. – 208 с

3. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT)

4. Замула О. А., В. І. Черниш. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О. А. Замула, В. І. Черниш // Системи обробки інформації: збірних наукових праць. – Харків : ХУ ПС, 2014. – Вип. 2(92). – с. 53–56.

5. Antonucci D. The Cyber Risk Handbook / Domenic Antonucci. – New Jersey: John Wiley & Sons, 2017. – 433 с.

6. Барибін О. І. Стандартизація та сертифікація в галузі інформаційної безпеки : навч. посіб. / О. І. Барибін. – Вінниця : ДонНУ імені Василя Стуса, 2018. – 238 с.

7. Бурячок В. Л., Хорошко В. О. Технологія прийняття рішень у складних соціотехнічних системах : монографія / В. Л. Бурячок, В. О. Хорошко. – Київ : ДУІКТ, 2012. – 344 с.

8. Економічний ризик: методи оцінки та управління : 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.

9. Henry K. Risk management and analysis / K. Henry // Information Security Management Handbook / Edited by H. F. Tipton, M. Krauze. – 6th edition. – Boca Raton : Auerbach Publications, 2017. – Part 1, Section 1.4, Ch. 28. – 329 p.

10. Логінова Н. І. правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с.

4.2. Допоміжна література

1. ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT)
2. 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.
3. Antonucci D. The Cyber Risk Handbook / Domenic Antonucci. – New Jersey: John Wiley & Sons, 2017. – 433 c.
4. Arnold V.I. Catastrophe Theory, 3rd ed. Berlin: Springer-Verlag, 1992.
5. Endorf C. F. Measuring ROI on security / Carl F. Endorf // Information security management handbook / Edited by H. F. Tipton, M. Krauze. – 6th edition. – Boca Raton : Auerbach Publications, 2017. – Part 1, Section 1.1, Ch. 12. – P. 133–137.
6. Gilmore Robert. Catastrophe Theory of Scientists and Engineers. New York: Dover, 1993.
7. ISO/IEC 13335:2000 «Information technology. Guidelines for the management of IT Security. Part 4: Selection of safeguards».
8. ISO/IEC 13335-1:2004 «Information technology. Security techniques. Management of information and communications technology security».
9. ISO/IEC 13335-3:1998 «Information technology. Guidelines for the management of IT Security. Part 3: Techniques for the management of IT Security».
10. ISO/IEC 15408-1:2009 «The Common Criteria for Information Technology
11. ISO/IEC 27001:2005 «Information technology. Security techniques. Information security management systems. Requirements».
12. ISO/IEC 27002:2005 «Information technology. Security techniques. Code of practice for information security management».
13. ISO/IEC Guide 73:2009 «Risk management. Vocabulary. Guidelines for use in standards»
14. Хорошев В. Базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах. Сб. Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні, вып.3, 2001. с. 86-90.
15. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-05 [Електронний ресурс] / Нормативна база Держспецзв'язку // 2015
Режим доступу:http://www.dstszi.gov.ua/dstszi/control/uk/ publish/article?art id=46074
16. Стратегія національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015) 7. Закон України "Про національну безпеку (2018)
17. Стратегія кібербезпеки України" (Введено в дію Указом Президента України від 15 березня 2016 року №96/2016)
18. НД ТЗІ 1.6-004-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.
19. Information Security Handbook for Network Beginners. National Center of Incident Readiness and Strategy for Cybersecurity (NISC), 2011.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

5.1. Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань *(перелік дидактичних засобів, завдання на СРС із посиланням на літературу)*	Кільк. ауд.год.
1	**Проблеми забезпечення інформаційної безпеки.** Загальні вимоги до безпеки розподілених комп'ютерних систем. Основні напрямки загроз та канали витоку інформації. Цілі, суб'єкти та схеми активних та пасивних вторгнень. Інтеграція засобів захисту з існуючими системами та технологіями. Взаємодія засобів захисту з різними програмними платформами та середовищами: J2EE, .NET, Linux-сервера. Основні напрямки загроз та канали витоку інформації. Цілі, суб'єкти та схеми активних та пасивних вторгнень. [1, с.56- 88; 6, с. 63-84]	**2**
2	**Класифікація методів забезпечення безпеки інформаційних систем.** Архітектурні, інфраструктурні, управлінські, адаптивні методи безпеки розподілених комп'ютерних мереж. Засоби аналізу захищеності. Засоби виявлення атак. Засоби адаптації. Засоби координації [1, с. 110 -121 6, с. 76 -91 7, с. 54 - 61]	**2**
3	**Базова модель забезпечення безпеки розподілених комп'ютерних систем.** Загальні принципи побудови моделі безпеки РКС Модель безпеки РКС Захист протоколів передачі даних Засоби передачі даних РКС Аутентифікація та передача/відображення сертифікатів безпеки. [6, с. 203 -210]	**2**
4	**Моделі для встановлення довіри до розподілених комп'ютерних систем.** Моделі довіри на основі центрів сертифікації із схемами з відкритим ключем моделі суворої ієрархії Центрів Сертифікації Модель розподіленої довіри. Модель довіри на основі середовища PGP. Моделі довіри на основі репутаційних механізмів [1, с. 182 -193 4, с. 250 - 262]	**2**
5	**Інфраструктури безпеки РКС GridLab, PROGRESS, ALiCe, NextGrid, XenoTrust.** Особливості реалізації ряду інфраструктур безпеки РКС, що застосовуються Основні характеристики сучасних засобів забезпечення безпеки розподілених комп'ютерних систем. Переваги та недоліки інфраструктур безпеки РКС [8, с. 221 - 249]	**2**
6	**Сучасні стандарти та керівні документи в галузі забезпечення інформаційної безпеки.** Законодавча та нормативна база в галузі інформаційної безпеки в Україні. Стандарт ISO/IEC 13335: "Посібник з управління інформаційною безпекою". Стандарт ISO/IEC 15408: “Загальні критерії оцінки безпеки інформаційних технологій” Серія стандартів ISO/IEC 2700x [2, с. 15 -23 5, с. 120 - 145 8, с. 115 - 126]	**2**

7	**Загальна концепція, аналіз та прогнозування ризиків для різних об'єктів.** Сучасні концепції ризиків. Об'єкти дослідження теорії ризиків. Джерела небезпеки та невизначеності у природі, технічних системах, суспільстві, економіці та політиці. Об'єкти ризику чи безпеки: суб'єкти забезпечення безпеки. Альтернативна концепція ризику як невизначеності [1, с. 37 -52 6, с. 53 -77]	**2**
8	**Класифікація ризиків.** Природні, техногенні, соціальні, економічні, політичні ризики. Класифікація ризиків по об'єкту впливу негативних факторів Ризик-утворюючі фактори [1, с. 140- 162 2, с. 15 -25 6, с. 220 - 242]	**2**
9	**Основні підходи та методи аналізу ризиків.** Базові концепції аналізу ризиків. Методичний апарат аналізу ризику Види та завдання аналізу ризиків Ідентифікація ризику Якісна та кількісна оцінка ризиків. Прогнозування ризиків. Візуалізація ризиків. [1, с. 140-162 7, с. 144 - 168]	**2**
10	**Методи аналізу ризиків.** Методичний апарат аналізу ризиків. Феноменологічний метод. Детерміністський метод. Експертний метод. Статистичні, ймовірнісно-статистичні, теоретико-імовірнісні, евристичні методики аналізу ризиків. [1, с. 140 -162, 7 с. 144- 168]	**2**
11	**Методи оцінки ризиків.** Теоретико-імовірнісний, ймовірно-статистичний, статистичний, експертний методи ймовірнісної оцінки показників ризиків. Основні методи прогнозування ризиків Методи прогнозування наслідків небезпечних дій агентів вторгнень оцінки та прогнозування небезпечних дій агентів вторгнень [1, с. 169 - 183 6, с. 270 - 295]	**2**
12	**Стандарти у сфері управління ризиками.** Стандарт ISO/IEC Guide 73 Стандарт управління ризиками AS/NZS 4360. Процес управління ризиками відповідно до стандарту AS/NZS 4360. Стандарт ISO/IEC 27005: Управління ризиками захищеності. Процес управління ризиками захищеності відповідно до стандарту ISO/IEC 27005 [2, с. 26 -33 3, с. 53 -56 5, с. 171 - 193]	**2**
13	**Методи та засоби аналізу та управління ризиками захищеності інформаційних систем.** Концепція управління ризиками захищеності інформаційних систем. Загальна схема процесу управління ризиками захищеності інформаційних систем Аналіз середовища та ідентифікація ресурсів системи : Аналіз ризиків захищеності. Запобігання (мінімізація) ризику. Формування вимог до інформаційної безпеки. [1, с. 205 -217 6, с.279 - 302]	**2**
14	**Методи керування ризиками захищеності.** Методи управління ризиками безпеки EBIOS, MEHARI, OCTAVE, CRAMM, CORAS. Програмні засоби управління ризиками COBRA та RiskWatch. Переваги та недоліки методів управління ризиками захищеності та програмних	**2**

	засобів управління ризиками. [6, с.279-302 7, с. 155 -179]	
15	**Засоби управління ризиками безпеки.** Програмний засіб для аналізу та управління ризиками COBRA Програмний засіб RA Software Tool. Модулі RA Software Tool. Комплексна система аналізу та управління ризиками RiskWatch. [1, с. 188 - 211 6, с. 294 - 312]	**2**
16	**Порівняльна оцінка методів та засобів аналізу та управління ризиками захищеності.** Переваги та недоліки методів та засобів управління ризиками захищеності. Підвищення ефективності процесу мінімізації ризиків. [6, с. 313 - 325]	**2**
17	**Політика безпеки та формування довіри у розподілених комп'ютерних системах.** Принципи формування політики безпеки розподілених комп'ютерних систем. Дві основні функції політики безпеки. Три основні розділи політики безпеки. Життєвий цикл політики безпеки [6, с. 320 – 335 8, с. 234 - 255]	**2**
18	**Основні елементи політики безпеки.** Призначення рівнів допуску суб'єктів до об'єктів РКС Управління доступом суб'єктів до об'єктів РКС Безпека використання об'єктів. Надання захищеного каналу зв'язку Аналіз дій суб'єктів Рейтинговий механізм встановлення довіри у розподілених комп'ютерних системах Реалізація засобів захисту РКС, які підтримують механізм формування довіри [6, с. 320- 335 8, с. 234 - 255]	**2**

5.2. Лабораторні роботи

Метою проведення циклу лабораторних робіт є придбання студентами необхідних практичних навиків дослідження методів та засобів аналізу ризиків інформаційної безпеки та формування комплексної системи захисту інформації від несанкціонованого доступу, розробки та налагодження компонентів інтерфейсу адміністратора безпеки для дослідження механізмів зниження ризиків для безпечної обробки даних в автоматизованих комп'ютерних системах.

Лабораторна робота включає:

- постановку вхідної задачі,
- теоретичні відомості з методів та засобів рішення задачі,
- аналіз математичного та алгоритмічного забезпечення,
- аналіз засобів дослідження,
- інтерпретація результатів та висновки,
- результати виконання модельних експериментів
- інтерпретація результатів моделювання та висновки.

№ з/п	Назва лабораторної роботи	Кількість ауд. годин
1	Дослідження механізму управління ризиками інформаційної безпеки на основі засобу EBIOS	2
2	Дослідження механізму управління ризиками інформаційної безпеки на основі засобу MEHARI	2

3	Дослідження механізму управління ризиками інформаційної безпеки на основі засобу OCTAVE	2
4	Дослідження механізму управління ризиками інформаційної безпеки на основі засобу CRAMM	2
5	Дослідження механізму управління ризиками інформаційної безпеки на основі засобу CORAS	2
6	Дослідження механізму управління ризиками інформаційної безпеки на основі засобу COBRA	2
7	Дослідження механізму управління ризиками інформаційної безпеки на основі засобу RA Software Tool	2
8	Дослідження механізму управління ризиками інформаційної безпеки на основі засобу RiskWatch	4

6. Самостійна робота здобувача вищої освіти

№ з/п	Назви тем і питань, що виноситься на самостійне опрацювання та посилання на навчальну літературу	Кількість годин СРС
1	Провести порівняльний аналіз параметрів каналів витоку інформації [1, с.56- 88; 6, с. 63-84]	4
2	Дослідити структури сучасних засобів виявлення атак [1, с. 110 -121 6, с. 76 -91 7, с. 54 - 61]	4
3	Дослідити структури моделей Белла і Ла-Падули. [6, с. 203 -210]	4
4	Особливості реалізації центрів сертифікації із схемами з відкритим ключем [1, с. 182 -193 4, с. 250 - 262]	4
5	Провести аналіз параметрів засобів забезпечення безпеки розподілених комп'ютерних систем GridLab, PROGRESS, ALiCe, NextGrid, XenoTrust. [8, с. 221 - 249]	4
6	Провести аналіз стандарту ISO/IEC 15408: “Загальні критерії оцінки безпеки інформаційних технологій” [2, с. 15 -23 5, с. 120 - 145 8, с. 115 - 126]	4
7	Дослідити альтернативні концепції ризику на основі аналізу сукупності ймовірнісних та невизначених факторів [1, с. 37 -52 6, с. 53 -77]	4
8	Дослідити та класифікувати ризик-утворюючі фактори [1, с. 140- 162 2, с. 15 -25 6, с. 220 - 242]	4
9	Провести аналіз механізмів прогнозування ризиків, а також засобів принципів ризиків [1, с. 140-162 7, с. 144 - 168]	4
10	Виконати порівняльний аналіз статистичних та теоретико-імовірнісних методик аналізу ризиків. [1, с. 140 -162, 7 с. 144- 168]	4
11	Дослідити переваги та недоліки основних методів прогнозування ризиків [1, с. 169 - 183 6, с. 270 - 295]	2
12	Виконати аналіз процесів управління ризиками захищеності відповідно до стандарту ISO/IEC 27005. [2, с. 26 -33 3, с. 53 -56 5, с.	2

	171 - 193]	
13	Дослідити принципи формування вимог до інформаційної безпеки. [1, с. 205 -217 6, с.279 - 302]	2
14	Провести аналіз переваг та недоліки програмних засобів управління ризиками COBRA та RiskWatch. [6, с.279-302 7, с. 155 -179]	4
15	Провести аналіз особливостей реалізації комплексної системи аналізу та управління ризиками RiskWatch [1, с. 188 - 211 6, с. 294 - 312].	4
16	Провести аналіз підходів щодо підвищення ефективності процесу мінімізації ризиків. [6, с. 313 - 325]	4
17	Дослідити особливості формування життєвого циклу політики безпеки [6, с. 320 – 335 8, с. 234 - 255]	4
18	Дослідити особливості реалізації засобів захисту РКС, які підтримують механізм формування довіри [6, с. 320- 335 8, с. 234 - 255]	4

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Застосовуються наступні вимоги до здобувачів:

- відвідування занять, як лекцій, так і лабораторних є обов'язковим;
- враховується активність на лекціях;
- лабораторні роботи повинні бути захищені персонально і в чітко визначені терміни;
- застосовується політика щодо академічної доброчесності, всі лабораторні роботи повинні бути виконані персонально з можливою перевіркою на плагіат
- додатково можуть застосовуватись інші вимоги, що не суперечать законодавству України та нормативним документам Університету.

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

Поточний контроль: експрес-опитування, опитування за темою заняття, МКР та РГР.
Календарний контроль: проводиться двічі на семестр як моніторинг поточного стану виконання вимог Силабусу.
Семестровий контроль: Іспит
Умови допуску до семестрового контролю: зарахування усіх лабораторних робіт та семестровий рейтинг не менше ніж 30 балів.

Рейтинг студента з дисципліни складається з балів, що отримуються за наступне:

1. Дві відповіді при лекційному опитуванні змісту попередньої лекції.
2. Виконання 2-х контрольних робіт.
3. Виконання 1 розрахунково-графічної роботи (РГР)

Система рейтингових (вагових) балів та критерії оцінювання

1. Поточний контроль засвоєння лекційного матеріалу

Ваговий бал - 2. Максимальна кількість балів на всіх лекціях дорівнює 2 бали *9 = 18 балів.

2. Виконання контрольних робіт.

Ваговий бал – 21 (максимально можливий) за кожну.

Штрафні бали за:

- несвоєчасний захист лабораторної роботи без поважної причини - 2 бали.

Умови позитивної проміжної атестації

Календарна атестація студентів (на 8 та 14 тижнях семестру) проводиться викладачем за значенням поточного рейтингу студента на час атестації. Для отримання "зараховано" з першої проміжної атестації (8-ий тиждень) студент повинен мати не менше ніж 25 балів. Для отримання "зараховано" з другої проміжної атестації (14-ий тиждень) повинен мати не менше ніж 50 балів.

До іспиту допускаються студенти, у яких зараховані всі лабораторні роботи, а також значення R > 30 (30% від R).

Розрахунок шкали (R) рейтингу:

Сума вагових балів контрольних заходів протягом семестру складає:

R=18+42= 60 балів.

Атестація проводиться за поточним рейтингом студента. Якщо поточний рейтинг складає не менше 50% від максимально можливого на цей момент, студент вважається атестованим.

Всі студенти повинні з'явитись на залік незалежно від набраного рейтингу. Оцінку на іспиті студенти отримують згідно таблиці:

R	Оцінка ECTS	Оцінка традиційна
95...100	A	Відмінно
85..94	B	Дуже добре
75...84	C	Добре
65...74	D	Задовільно
60...64	E	Достатньо
R < 60	FX	Незадовільно
R < 30	F	Недопущений

Якщо студент отримав за рейтингом R< 30 балів (менш ніж 30% від R) і по початку іспиту виконав необхідну додаткову роботу (підвищив свій рейтинг), то він допускається до заліку.

Ваговий бал за Іспит R складає **40 балів** і одержується за наступне:

1. Відповідь на 2 теоретичні питання оцінюються максимально в 20 балів по 10 балів за кожну вірну відповідь.

2. Відповідь на 2 практичних питання оцінюється максимально в 20 бали по 10 балів за кожну вірну відповідь.

Таким чином, сумарний бал є сумою R початковий та R за іспит.

9. Додаткова інформація з дисципліни (освітнього компонента)

Перелік основних питань, які виносяться на семестровий контроль:

1. Проблеми захисту інформації та периметр відповідальності механізмів захисту у комп'ютерних системах та мережах.
2. Загальні вимоги до системи безпеки розподілених комп'ютерних систем
3. Основні напрямки загроз та каналів витоку інформації в комп'ютерних системах та мережах.
4. Класифікація методів забезпечення безпеки розподілених комп'ютерних систем
5. Загальні принципи побудови моделі безпеки розподілених комп'ютерних систем
6. Структура моделі безпеки розподілених комп'ютерних систем
7. Моделі довіри на основі центрів сертифікації зі схемами з відкритим ключем
8. Ієрархічна модель на основі політики безпеки.
9. Модель розподіленої довіри.
10. Моделі довіри на основі репутаційних механізмів
11. Основні характеристики сучасних засобів забезпечення безпеки розподілених комп'ютерних систем
12. Основні стандарти та керівні документи в галузі інформаційної безпеки
13. Законодавча та нормативна база в галузі інформаційної безпеки в Україні
14. Сучасні концепції ризику
15. Об'єкти дослідження в теорії ризиків
16. Класифікація ризиків
17. Ризик-утворюючі фактори
18. Базові концепції аналізу ризиків
19. Методичний апарат аналізу ризику
20. Види та завдання аналізу ризиків
21. Методичний апарат аналізу ризиків
22. Методи оцінки ризиків
23. Прогнозування можливості виникнення небезпечних подій
24. Основні методи прогнозування ризиків
25. Методи прогнозування наслідків небезпечних дій агентів вторгнень
26. Стандарти в галузі управління ризиками захищеності інформаційних систем
27. Процес управління ризиками захищеності відповідно до стандарту ISO/IEC 27005
28. Концепція управління ризиками захищеності інформаційних систем
29. Загальна схема процесу управління ризиками захищеності інформаційних систем
30. Методи управління ризиками захищеності
31. Структура модулів методу MEHARI
32. Етапи методу OCTAVE
33. Основні складові методу CRAMM
34. Програмний засіб для аналізу та управління ризиками COBRA
35. Програмний засіб RA Software Tool
36. Порівняльна оцінка основних параметрів методів та засобів аналізу та управління ризиками захищеності
37. Принципи формування політики безпеки розподілених комп'ютерних систем
38. Базові елементи політики безпеки

39. Призначення рівнів допуску суб'єктів до об'єктів розподілених комп'ютерних систем
40. Основні засади формування довіри між вузлами розподілених комп'ютерних систем
41. Схема формування рейтингу (рівня довіри) вузлів розподілених комп'ютерних систем
42. Реалізація засобів захисту розподілених комп'ютерних систем , які підтримують механізм формування довіри
43. Структура засобів захисту розподілених комп'ютерних систем, що реалізуються на основі формування рейтингу вузлів

Робочу програму навчальної дисципліни (силабус):

Складено завідуючим кафедри системного проектування, доктором технічних наук, професором **Мухіним Вадимом Євгенійовичем**

Ухвалено кафедрою системного проектування (протокол № 13 від 17 червня 2024 р.)

Погоджено Методичною комісією ІПСА (протокол № 10 від 24 червня 2024 р.)

Погоджено науково-методичною комісією КПІ ім. Ігоря Сікорського зі спеціальності 122 (протокол № 11 від 28 червня 2024 р.)