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

Кафедра обчислювальної техніки

ЗАХИСТ ІНФОРМАЦІЇ У КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*123 Комп'ютерна інженерія*
Освітня програма	*Комп'ютерна інженерія*
Статус дисципліни	*Обов'язкова (нормативна) компонента ОП, циклу професійної підготовки*
Форма навчання	*очна (денна) / заочна*
Рік підготовки, семестр	*4 курс, весняний*
Обсяг дисципліни	*4,5 кредитів /135 год. Денна форма: лекцій 36 годин, лаб. роб. 18 год., СРС 81 год. Заочна форма: лекцій 8 год., лаб. роб. 8 год., СРС 119 год.*
Семестровий контроль/ контрольні заходи	*Екзамен*
Розклад занять	*http://rozklad.kpi.ua/, http://roz.kpi.ua/*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор, лабораторні: *доктор технічних наук, професор Писарчук Олексій Олександрович, ziks582@gmail.com.*
Розміщення курсу	*https://drive.google.com/drive/u/0/folders/1ZXSjg9uhGO4GmMAvH5vwEk1kVyaRGZ6d* *https://classroom.google.com/c/NTI1NDE1NDgyMjQw?cjc=kd2w3cg*

Програма навчальної дисципліни

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

Дисципліна «Захист інформації в комп'ютерних системах та мережах» *призначена для набуття студентами здатності забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах і мережах з метою реалізації встановленої політики інформаційної безпеки. Це досягається вивченням теоретичних основ побудови і практики застосування методів та засобів захисту інформації в комп'ютерних системах з метою запобігання несанкціонованому доступи, витоку, руйнації, знищення і модифікації інформації різної категорії шляхом реалізації політики і створення комплексних корпоративних систем захисту інформації.*

Метою вивчення курсу *є: набуття студентами здатності забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах і мережах з метою реалізації встановленої політики інформаційної* безпеки.

Мета курсу досягається реалізацією часткових завдань і напрямків:

1. Вивчення основних положень законодавчої база в сфері захисту інформації в комп'ютерних системах: національні законодавчі акти і стандарти у сфері захисту інформації: категорії, основні положення, порядок і сфера застосування; законодавчі акти та стандарти інших держав у сфері захисту інформації – 1 лекція;

2. Визначення складу, організаційних, технічних та програмно-апаратних засобів

комплексної системи захисту корпоративної інформації: інформація як об'єкт захисту; категорії інформації, як об'єкту захисту; канали витоку корпоративної інформації; загрози інформації в комп'ютерних системах; модель порушника; методи, методології, засоби, заходи і технології комплексного захисту корпоративної інформації (організаційні заходи, технічний захист інформації, протидія технічним засобам моніторингу) – 2 лекції, 1 лабораторна робота (2 год.);

3. Комп'ютерні віруси та вірусологія: класифікація вірусів; алгоритми функціонування вірусів; технології та засоби створення і розповсюдження комп'ютерних вірусів; конструктори вірусів; антивірусне програмне забезпечення та сутність його побудови і застосування; методи та технології захисту комп'ютерних систем від вірусів – 2 лекції, 1 лабораторна робота;

4. Кібернетичні загрози комп'ютерним системам та протидія їм: кібернетична та (і) комп'ютерна атака, поняття, класифікація, модель, зміст етапів; методи і технології організації та реалізації кібернетичних атак; методології, методи і технології протидії кібернетичним атакам; и, метод програмне забезпечення та сутність його побудови і застосування; методи та технології захисту комп'ютерних систем від вірусів – 2 лекції, 1 лабораторна робота;

5. Криптографічний захист інформації в комп'ютерних системах: загальні відомості про класичну криптологію, криптографію та криптографічний аналіз; традиційні історичні шифри; алгоритми блочного шифрування; принципи побудови сучасних симетричних криптографічних шифрів та систем; асиметричні криптографічні системи шифрування (сутність та математичні основи; алгоритми та криптографічні системи; технології реалізації та уразливість) – 9 лекцій, 4 лабораторна робота;

6. Методи, методології, технології і засоби аутентифікації та ідентифікації, як елемент захисту інформації в комп'ютерних системах: методи і технології ідентифікації користувачів; електронний цифровий підпис, центри сертифікації електронних ключів – 2 лекції, 1 лабораторна робота.

***По завершенню курсу студент матиме експертизу** у базових складових, методологій і технологій захисту інформації в комп'ютерних системах та мережах, що виявляється у здатності використовувати та здійснювати профільну діяльність, керуючись та використовуючи:*

Основні положень законодавчої база в сфері захисту інформації в комп'ютерних системах: національні законодавчі акти і стандарти у сфері захисту інформації: категорії, основні положення, порядок і сфера застосування; законодавчі акти та стандарти інших держав у сфері захисту інформації.

Склад організаційних, технічних та програмно-апаратних засобів комплексної системи захисту корпоративної інформації: інформація як об'єкт захисту; категорії інформації, як об'єкту захисту; канали витоку корпоративної інформації; загрози інформації в комп'ютерних системах; модель порушника; методи, методології, засоби, заходи і технології комплексного захисту корпоративної інформації (організаційні заходи, технічний захист інформації, протидія технічним засобам моніторингу;

Принципи побудови, дії та захисту від комп'ютерних вірусів та основи вірусології: класифікація вірусів; алгоритми функціонування вірусів; технології та засоби створення і розповсюдження комп'ютерних вірусів; конструктори вірусів; антивірусне програмне забезпечення та сутність його побудови і застосування; методи та технології захисту комп'ютерних систем від вірусів;

Методи, етапи способи та засоби здійснення кібернетичних атак на комп'ютерні системи, методи, засоби і технології протидії їм: кібернетична та (і) комп'ютерна атака, поняття, класифікація, модель, зміст етапів; методи і технології організації та реалізації кібернетичних атак; методології, методи і технології протидії кібернетичним атакам; и, метод програмне забезпечення та сутність його побудови і застосування; методи та технології захисту комп'ютерних систем від вірусів;

Методи, математичні моделі, алгоритми і технології криптографічного захисту інформації в комп'ютерних системах: загальні відомості про класичну криптологію, криптографію та криптографічний аналіз; традиційні історичні шифри; алгоритми блочного шифрування; принципи побудови сучасних симетричних криптографічних шифрів та систем; асиметричні криптографічні системи шифрування (сутність та математичні основи; алгоритми та криптографічні системи; технології реалізації та уразливість);

Методи, методології, технології і засоби аутентифікації та ідентифікації, як елемент захисту інформації в комп'ютерних системах: методи і технології ідентифікації користувачів; електронний цифровий підпис, центри сертифікації електронних ключів.

Практична частина курсу орієнтована на вміння:

Застосовувати положення законодавчої база в сфері захисту інформації в комп'ютерних системах;

Розробляти, створювати і впроваджувати комплексні системи захисту корпоративної інформації;

Виявляти і протидіяти комп'ютерним вірусам;

Оцінювати уразливість, виявляти ознаки підготовки та здійснення кібернетичних атак, проектувати створювати та впроваджувати заходи і засоби протидії кібернетичним загрозам;

Здійснювати криптографічний захист інформації в комп'ютерних системах;

Впроваджувати дієві механізми аутентифікації та ідентифікації в комп'ютерних системах.

Успішне опанування дисципліни «Захист інформації в комп'ютерних системах та мережах» потребує від студента: *базових знань з комп'ютерних мереж та систем, фізики процесів, що протікають в радіоелектронних компонентах, базових знань з дискретної математики, систем числення, множин, матричних обчислень. Це досягається вивченням навчальних дисциплін: Комп'ютерні мережі, Комп'ютерні системи, Архітектура комп'ютерів. Частина 1,2,3, Комп'ютерна схемотехніка, Комп'ютерна логіка. Частина 1,2, Комп'ютерна електроніка, Вища математика. Частина 1,2,3, Аналітична геометрія та лінійна алгебра, Програмування Частина 1,2, Дискретна математика, Фізика, Теорія електричних кіл та сигналів, Теорія ймовірності та математична статистика, Структури даних та алгоритми,*

Навчальна «Захист інформації в комп'ютерних системах та мережах» дисципліна забезпечує наступні програмні результати навчання освітньо-професійної програми 123 Комп'ютерна інженерія, Комп'ютерні системи та мережі:

ЗК2 Здатність вчитися і оволодівати сучасними знаннями;

ЗК8 Здатність працювати в команді;

ФК1 Здатність застосовувати законодавчу та нормативно правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії;

ФК4 Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки;

ФК6 Здатність проектувати, впроваджувати та обслуговувати комп'ютерні системи та мережі різного виду та призначення;

ФК7 Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп'ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності;

ФК8 Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп'ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.;

ФК9 Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи;

ФК13 Здатність вирішувати проблеми у галузі комп'ютерних та інформаційних технологій, визначати обмеження цих технологій;

ФК16 Здатність проектувати, розробляти, впроваджувати та обслуговувати програмно-апаратне забезпечення для високопродуктивних паралельних та розподілених комп'ютерні систем та їх складових на сучасній елементній базі, зокрема, з використанням ПЛІС і систем автоматизованого проектування;

ФК17 Здатність проектувати, впроваджувати, адмініструвати та обслуговувати глобальні та локальні інтелектуальні програмно-конфігуровні комп'ютерні мережі;

ФК19 Здатність організації обчислювальних процесів в високопродуктивних комп'ютерних системах з різною структурною організацією на основівикористання новітніх технологій планування і диспетчеризації та сучасних операційних систем;

ПРН3 Знати новітні технології в галузі комп'ютерної інженерії;

ПРН6 Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей;

ПРН9 Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності;

ПРН10 Вміти розробляти програмне забезпечення для вбудованих і розподілених застосувань, мобільних і гібридних систем, розраховувати, експлуатувати, типове для спеціальності обладнання;

ПРН20 Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.

***Компетенції, отримані в результаті опанування курсу використаються** для реалізації практичних питань із захисту інформації в процесі професійної діяльності, а також у реалізації завдань курсового проектування, розробки кваліфікаційних робіт тощо.*

***Курс включає** 4,5 кредитів /135 год. Денна форма: лекцій 36 годин, лаб. роб. 18 год., СРС 81 год. Заочна форма: лекцій 8 год., лаб. роб. 8 год., СРС 119 год.*

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

Пререквізити:

***Успішне опанування дисципліни «Захист інформації в комп'ютерних системах та мережах» потребує від студента:** базових знань з комп'ютерних мереж та систем, фізики процесів, що протікають в радіоелектронних компонентах, базових знань з дискретної математики, систем числення, множин, матричних обчислень. Це досягається вивченням навчальних дисциплін: Комп'ютерні мережі, Комп'ютерні системи, Архітектура комп'ютерів. Частина 1,2,3, Комп'ютерна схемотехніка, Комп'ютерна логіка. Частина 1,2, Комп'ютерна електроніка, Вища математика. Частина 1,2,3, Аналітична геометрія та лінійна алгебра, Програмування Частина 1,2, Дискретна математика, Фізика, Теорія електричних кіл та сигналів, Теорія ймовірності та математична статистика, Структури даних та алгоритми,*

Постреквізити:

Дисципліна відноситься до обов'язкової (нормативної) компоненти ОП, циклу професійної підготовки, та спрямовано на реалізацію переліку результатів навчання: ЗК2, ЗК8,ФК1, ФК4, ФК6, ФК7, ФК8, ФК9, ФК13, ФК16, ФК17, ФК19, ПРН3, ПРН6, ПРН9, ПРН10, ПРН20.

***Компетенції, отримані в результаті опанування курсу використаються** для реалізації практичних питань із захисту інформації в процесі професійної діяльності, а також у реалізації завдань курсового проектування, розробки кваліфікаційних робіт тощо.*

3. Зміст навчальної дисципліни

Розділ 1. Основні відомості про захист інформації в комп'ютерних системах.

Тема 1. *Основні положення законодавчої база в сфері захисту інформації в комп'ютерних системах.*

Розділ 2. Організаційні, технічні та програмно-апаратні засоби комплексної системи захисту корпоративної інформації.

Тема 2. *Комплексна система захисту корпоративної інформації. Об'єкт захисту та загрози.*

Тема 3 *Комплексна система захисту корпоративної інформації. Склад та структура.*

Розділ 3. Комп'ютерні віруси та вірусологія.

Тема 4. *Загальні відомості про комп'ютерні віруси.*

Тема 5. *Технології захисту комп'ютерних систем від комп'ютерних вірусів.*

Розділ 4. Кібернетичні загрози комп'ютерним системам та протидія їм.

Тема 6. *Методи і засоби реалізації кібернетичних атак.*

Тема 7. *Методи і засоби протидії кібернетичним атакам.*

Розділ 5. Криптографічний захист інформації в комп'ютерних системах.

Розділ 5.1. Загальні відомості про криптографію та криптологію.

Тема 8. *Загальні відомості про класичну криптологію, криптографію та криптографічний аналіз.*

Тема 9. *Традиційні історичні шифри. Математичні та алгоритмічні основи.*

Тема 10. *Традиційні історичні шифри. Технології реалізації та уразливість.*

Розділ 5.2. Методи, моделі, алгоритми та системи блочного шифрування.

Тема 11. *Алгоритми блочного шифрування. Математичні та алгоритмічні основи.*

Тема 12. *Алгоритми блочного шифрування. Технології реалізації та уразливість.*

Розділ 5.3. Методи, моделі, алгоритми та системи симетричного шифрування.

Тема 13. *Симетричні шифри та системи. Математичні та алгоритмічні основи.*

Тема 14. Симетричні шифри та системи. Технології реалізації та уразливість.

Розділ 5.5. Методи, моделі, алгоритми та системи асиметричного шифрування.

Тема 15. *Асиметричні шифри та системи. Математичні та алгоритмічні основи.*

Тема 16. *Асиметричні шифри та системи. Технології реалізації та уразливість.*

Розділ 6. Методи, методології, технології і засоби аутентифікації та ідентифікації.

Тема 17. *Методи і технології ідентифікації користувачів в розподіленнях комп'ютерних системах.*

Тема 18. *Електронний цифровий підпис, методи та засоби.*

4. Навчальні матеріали та ресурси

4.1. Базова література:

1. Навчально-методичний комплекс з дисципліни: «Захист інформації в комп'ютерних системах та мережах»

[https://drive.google.com/drive/u/0/folders/ 1ZXSjg9uhGO4GmMAvH5vwEk1kVyaRGZ6d].

2. Електронний курс на освітній платформі Sikorsky «Захист інформації в комп'ютерних системах та мережах»: https://classroom.google.com/c/NTI1NDE1NDgyMjQw?cjc=kd2w3cg.

3. Писарчук О.О. Основи захисту інформації: навчальний посібник / О.О. Писарчук, Ю. Г. Даник, С. Г. Вдовенко та ін (Рекомендовано МОН України). – Житомир: ЖВІ ДУТ, 2015. – 226 с.: іл.

4. Корченко О. Г. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К.: ДУТ, 2014. – 448 с. https://er.nau.edu.ua/handle/NAU/32583.

5. Хорошко В.А. Методи й засоби захисту інформації / ВА Хорошко, АА Чекатков - К.: ЮНІОР, 2003.

6. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с. https://nni1.naiau.kiev.ua/files/KIT/posibnuk%20tzi.pdf.

7. Журановський Н.Ф. Теорія інформації та кодування. Підручник. – К.: Професіонал, 2001.

8. https://shron1.chtyvo.org.ua/Zhurakovskyi_Yurii/Teoria_informatsii_ta_koduvannia.pdf?PHPSESSID=4067ajtadnmghsicnaqvg4g4u2.

9. Навчально-методичний комплекс з дисципліни: Захист інформації в комп'ютерних системах https://drive.google.com/drive/u/0/folders/1ZXSjg9uhGO4GmMAvH5vwEk1kVyaRGZ6d

10. Електронний курс на освітній платформі Sikorsky «Захист інформації у комп'ютерних системах», 2022: https://classroom.google.com/c/NTI1NDE1NDgyMjQw?cjc=kd2w3cg

11. Нормативні документи з питань технічного захисту інформаціїhttps://cip.gov.ua/ua/news/perelik-dokumentiv-sistemi-tekhnichnogo-zakhistu-informaciyi-nd-tzi.

4.2. Додаткова література:

1. Антонюк А.Ф. Основи захисту інформації в автоматизованих системах. Навчальний посібник. - К.: Академія, 2003.

2. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

3. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. – К.: Вид. Національної академії внут. справ, 2012. – 104 с.

4. Кузнецов О.О. Захист інформації в інформаційних системах. / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. - Харків: Вид. ХНЕУ, 2011.– 510.

5. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

6. Остапов С.Е. Технології захисту інформації: навч. посіб. / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – Х.: ХНЕУ, 2013. – 476 с.

7. Дронюк І. М. Технології захисту інформації на матеріальних носіях Монографія. Львів : Видавництво Львівської політехніки, 2017. 200 с

8. Kryptographie in C und C++ / MichaelWelschenbach ; translated by David Kramer.2nd American ed., rev. and enl.

9. Тарнавський, Ю. А. Технології захисту інформації [Електронний ресурс] : підручник для студентів спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський ; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с

10. Вітер С.А. Захист облікової інформації та кібербезпека підприємства / С.А. Вітер, І.І. Світлишин // Економіка і суспільство: електронне фахове видання. – 2017. – № 11. – С. 497–502.

11. Ляхович Г.І. Захист облікової інформації в умовах аутсорсингу із використанням інформаційно-комп'ютерних технологій / Г.І. Ляхович // Бізнес Інформ. – 2017. – № 12. – С. 408–412.

12. Шпак В.А. Організація захисту облікової інформації / В.А. Шпак // Бухгалтерський облік, аналіз та аудит: проблеми теорії, методології, організації. – 2015. – № 2. – С. 181–187.

Хорошко В. О. Математичні моделі інформаційно-комунікаційних систем і мереж щодо захисту інформації на основі теорії варіаційно-градієнтних методів / В. О. Хорошко, Т. В. Майсак, Н. Б. Дахно // Моделювання та інформаційні системи в економіці. - 2015. - № 91. - С. 246-255.

4.3. Інформаційні ресурси:

https://drive.google.com/drive/u/0/folders/1ZXSjg9uhGO4GmMAvH5vwEk1kVyaRGZ6d
https://classroom.google.com/c/NTI1NDE1NDgyMjQw?cjc=kd2w3cg
https://www.virustotal.com/gui/
https://itc.ua/articles/antivirusy_onlajn_34274/
https://www.antivirusguide.com/
https://cissm.umd.edu/cissm-cyber-events-database
https://data.world/datasets/cybersecurity
https://owasp.org/
https://www.mitre.org/focus-areas/cybersecurity

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Навчальна дисципліна «Захист інформації в комп'ютерних системах та мережах» включає *,5 кредитів /135 год. Денна форма: лекцій 36 годин, лаб. роб. 18 год., СРС 81 год. Заочна форма: лекцій 8 год., лаб. роб. 8 год., СРС 119 год.*

За дисципліною передбачено проведення таких видів аудиторних занять: лекційних заняття; лабораторні роботи; модульна контрольна робота; залік.

Лекційні заняття розкривають теоретичні основи захисту інформації в комп'ютерних системах та мережах основних галузей, їх практичне застосування у створенні комплексної системи захисту інформації та організації і реалізації безпечного розподіленого інформаційного обміну в комп'ютерних системах та мережах.

Практична частина курсу (лабораторні роботи) орієнтована на реалізацію процесу проектування комплексної системи захисту інформації, її складових та розробки криптоалгоритмів.

Розділ 1. Основні відомості про захист інформації в комп'ютерних системах.

Тема 1. *Основні положення законодавчої база в сфері захисту інформації в комп'ютерних системах:*

зміст та задачі дисципліни;

національні законодавчі акти і стандарти у сфері захисту інформації: категорії, основні положення, порядок і сфера застосування;

законодавчі акти та стандарти інших держав у сфері захисту інформації.

Розділ 2. Організаційні, технічні та програмно-апаратні засоби комплексної системи захисту корпоративної інформації.

Тема 2. *Комплексна система захисту корпоративної інформації. Об'єкт захисту та загрози:*

інформація як об'єкт захисту;

категорії інформації, як об'єкту захисту;

канали витоку корпоративної інформації;

загрози інформації в комп'ютерних системах;

Тема 3 *Комплексна система захисту корпоративної інформації. Склад та структура:*

модель порушника;

методи, методології, засоби, заходи і технології комплексного захисту корпоративної інформації (організаційні заходи, технічний захист інформації, протидія технічним засобам моніторингу).

Розділ 3. Комп'ютерні віруси та вірусологія.

Тема 4. *Загальні відомості про комп'ютерні віруси:*

класифікація вірусів;

алгоритми функціонування вірусів;

технології та засоби створення і розповсюдження комп'ютерних вірусів.

Тема 5. *Технології захисту комп'ютерних систем від комп'ютерних вірусів:*

конструктори вірусів;

антивірусне програмне забезпечення та сутність його побудови і застосування;

методи та технології захисту комп'ютерних систем від вірусів.

Розділ 4. Кібернетичні загрози комп'ютерним системам та протидія їм.

Тема 6. *Методи і засоби реалізації кібернетичних атак:*

кібернетична та (і) комп'ютерна атака, поняття, класифікація, модель, зміст етапів;

методи і технології організації та реалізації кібернетичних атак.

Тема 7. *Методи і засоби протидії кібернетичним атакам:*

методології, методи і технології протидії кібернетичним атакам (методи, програмне забезпечення та сутність його побудови і застосування);

методи та технології захисту комп'ютерних систем від вірусів.

Розділ 5. Криптографічний захист інформації в комп'ютерних системах.

Розділ 5.1. Загальні відомості про криптографію та криптологію.

Тема 8. *Загальні відомості про класичну криптологію, криптографію та криптографічний аналіз:*

Загальні відомості про шифрування, кодування, криптографію і криптологію;

Задачі дешифрування;

Технології та системи криптографічного захисту інформації.

Тема 9. *Традиційні історичні шифри. Математичні та алгоритмічні основи:*

Загальні відомості та галузі застосування.

Шифрування на основі одно та багато алфавітних підстановок: шифри Цезаря та «скитала»;

Шифр Віжинера та квадрати Уітстона.

Біграмні шифри.

Потокові шифри з необмеженою довжиною ключа.

Шифрування «гамуванням».

Тема 10. *Традиційні історичні шифри. Технології реалізації та уразливість:*

Реалізація традиційних історичних шифрів з використанням засобів Python;

Приклади реалізації традиційних шифрів в Python;

Уразливість традиційних історичних шифрів.

Розділ 5.2. Методи, моделі, алгоритми та системи блочного шифрування.

Тема 11. *Алгоритми блочного шифрування. Математичні та алгоритмічні основи:*

Сутність та математичні основи методів блочного шифрування.;

Тема 12. *Алгоритми блочного шифрування. Технології реалізації та уразливість:*

Технології блочного шифрування в Python, уразливість.

Розділ 5.3. Методи, моделі, алгоритми та системи симетричного шифрування.

Тема 13. *Симетричні шифри та системи. Математичні та алгоритмічні основи:*

Шифрування на основі чередування перестановок та підстановок;

Стандарт шифрування Data Encryption Standard. (DES).

Тема 14. Симетричні шифри та системи. Технології реалізації та уразливість:

Блок управління ключами в DES. Алгоритм 3-DES та чотири режими реалізації криптографічного захисту на основі DES.

Технології асиметричного шифрування в Python, уразливість.

Розділ 5.5. Методи, моделі, алгоритми та системи асиметричного шифрування.

Тема 15. *Асиметричні шифри та системи. Математичні та алгоритмічні основи:*

Криптографія по Діффі і Хелману. Незворотні функції в шифруванні. Три схеми та задачі криптозахисту.

Система RSA. Модулярна арифметика. Алгоритм швидкого дискретного потенціювання. Процесор – акселератор RSA;

Технології асиметричного шифрування в Python, уразливість.

Тема 16. *Асиметричні шифри та системи. Технології реалізації та уразливість:*

Проблема генерації великих простих чисел (ВПЧ). Тест Рабіна та мала теорема Ферма. Перевірки на простоту.

Схеми та алгоритми розрахунків ключів для системи RSA. Класичний та розширений алгоритми Евкліда.

Технології асиметричного шифрування в Python, уразливість.

Розділ 6. Методи, методології, технології і засоби аутентифікації та ідентифікації.

Тема 17. *Методи і технології ідентифікації користувачів в розподіленнях комп'ютерних системах:*

методи аутентифікація та ідентифікація суб'єктів на основі симетричних систем шифрування. Поняття майстер ключа та змінного ключа;

технології аутентифікація та ідентифікація в Python.

Тема 18. *Електронний цифровий підпис, методи та засоби:*

встановлення цілісності повідомлень на основі симетричних та асиметричних систем шифрування. Поняття сигнатури повідомлення та цифрового підпису;

аутентифікація та ідентифікація суб'єктів в протоколах відкритих замовлень. Поняття електронних чеку та квитанції;

багаторівнева організація формування та використання ключів шифрування. Функції майстер-ключа, системного, клієнтського, торгово-касового та сесійного ключів.

Цикл лабораторних робіт з дисципліни «Захист інформації в комп'ютерних системах та мережах» спрямовано на набуття практичних навичок реалізації та дослідження особливостей і ефективності складових комплексної системи захисту корпоративної інформації як у вигляді окремих елементів, так і в синергетичному поєднанні в єдину систему.

Цикл лабораторних робіт побудовано на принципах нарощування функціональності комплексної системи захисту корпоративної інформації. Це реалізується в декількох аспектах:

евристичний синтез комплексної системи захисту корпоративної інформації;

дослідження особливостей комп'ютерних вірусів та створення системи протидії;

дослідження особливостей кібернетичного впливу на комп'ютерні системи та створення системи протидії;

розробка криптографічних систем захисту інформації та дослідження їх уразливості.

Питання вірусології та кібернетичної безпеки відпрацьовуються на реальному шкідливому програмному забезпеченні з використанням технологій віртуальних обчислювальних систем.

Питання розробки криптографічних систем захисту інформації та дослідження їх уразливості реалізується з використанням можливостей мови програмування високого рівня – Python.

Тематика лабораторних робіт:

Лабораторна робота №1. *(2 год.) Дослідження процесів створення комплексної системи захисту корпоративної інформації:*

Розробка проекту КСЗІ для конкретного об'єкту інформаційної діяльності – комп'ютерної системи (встановлення категорії інформації, що захищається; дослідження каналів витоку, модель загроз; модель порушника; комплекс організаційних та технічних заходів і засобів захисту інформації; структура КСЗІ; дослідження ефективності КСЗІ).

Лабораторна робота №2. *(2 год.) Дослідження процесів захисту інформації від комп'ютерних вірусів:*

Створення ізольованого віртуального середовища досліджень; генерація вірусів та дослідження їх сигнатур; дослідження ефективності детектування сигнатур вірусів різними програмними засобами; створення системи захисту інформації від комп'ютерних вірусів та дослідження її ефективності.

Лабораторна робота №3. *(2 год.) Дослідження процесів захисту інформації від кібернетичних атак:*

Створення ізольованого віртуального середовища досліджень; дослідження уразливості оточення до кібернетичних впливів; створення системи захисту інформації від кібернетичних впливів та дослідження її ефективності.

Лабораторна робота №4. *(2 год.) Дослідження технологій традиційного шифрування та їх уразливості:*

Розробка скрипта в Python, що реалізує технології традиційного шифрування за заданим алгоритмом та дослідження їх уразливості.

Лабораторна робота №5. *(2 год.) Дослідження технологій блочного шифрування та їх уразливості:*

Розробка скрипта в Python, що реалізує технології блочного шифрування за заданим алгоритмом та дослідження їх уразливості.

Лабораторна робота №6. *(2 год.) Дослідження технологій симетричного шифрування та їх уразливості:*

Розробка скрипта в Python, що реалізує технології симетричного шифрування за заданим алгоритмом та дослідження їх уразливості.

Лабораторна робота №7. *(2 год.) Дослідження технологій асиметричного шифрування та їх уразливості:*

Розробка скрипта в Python, що реалізує технології асиметричного шифрування за заданим алгоритмом та дослідження їх уразливості.

Лабораторна робота №8. *(2 год.) Дослідження технологій аутентифікації та ідентифікації в розподілених комп'ютерних системах:*

Розробка скрипта в Python, що реалізує технології електронного цифрового підпису та дослідження ефективності процесів аутентифікації та ідентифікації в розподілених комп'ютерних системах.

Модульна контрольна робота *(2 год).*

6. Самостійна робота здобувача вищої освіти денної форми навчання

Денна форма навчання, бюджет часу: лекцій 36 годин, лаб. роб. 18 год., СРС 81 год

Види самостійної роботи (66 годин):

самостійне опрацювання матеріалів лекційних занять (1 година х 17 лекцій = 17 годин);

підготовка та оброблення проведення розрахунків за первинними даними, отриманими на лабораторних заняттях, виконання лабораторних робіт, розв'язок задач надання на перевірку (рекомендовано 2 години х 9 лабораторних робіт = 18 годин);

виконання модульної контрольної роботи (МКР = 4 години);

підготовка до заліку (8 години);

налаштування віртуального середовища для виконання лабораторних робіт (3 години);

опрацювання тем на самостійну роботу (16 годин).

Теми на самостійне опрацювання (денна форма навчання).

Розділ 1. Основні відомості про захист інформації в комп'ютерних системах.

Тема 1. *Основні положення законодавчої база в сфері захисту інформації в комп'ютерних системах:*

законодавчі акти та стандарти інших держав у сфері захисту інформації.

Розділ 2. Організаційні, технічні та програмно-апаратні засоби комплексної системи захисту корпоративної інформації.

Тема 2. *Комплексна система захисту корпоративної інформації. Об'єкт захисту та загрози:*

загрози інформації в комп'ютерних системах;

Тема 3 *Комплексна система захисту корпоративної інформації. Склад та структура:*

технічний захист інформації, протидія технічним засобам моніторингу).

Розділ 3. Комп'ютерні віруси та вірусологія.

Тема 4. *Загальні відомості про комп'ютерні віруси:*

технології та засоби створення і розповсюдження комп'ютерних вірусів.

Тема 5. *Технології захисту комп'ютерних систем від комп'ютерних вірусів:*

методи та технології захисту комп'ютерних систем від вірусів.

Розділ 4. Кібернетичні загрози комп'ютерним системам та протидія їм.

Тема 6. *Методи і засоби реалізації кібернетичних атак:*

методи і технології організації та реалізації кібернетичних атак.

Тема 7. *Методи і засоби протидії кібернетичним атакам:*

методи та технології захисту комп'ютерних систем від вірусів.

Розділ 5. Криптографічний захист інформації в комп'ютерних системах.

Розділ 5.1. Загальні відомості про криптографію та криптологію.

Тема 8. *Загальні відомості про класичну криптологію, криптографію та криптографічний аналіз:*

Технології та системи криптографічного захисту інформації.

Тема 9. *Традиційні історичні шифри. Математичні та алгоритмічні основи: Біграмні шифри. Потокові шифри з необмеженою довжиною ключа.*

Тема 10. *Традиційні історичні шифри. Технології реалізації та уразливість: Приклади реалізації традиційних шифрів в Python;*

Розділ 5.2. Методи, моделі, алгоритми та системи блочного шифрування.

Тема 12. *Алгоритми блочного шифрування. Технології реалізації та уразливість: Технології блочного шифрування в Python, уразливість.*

Розділ 5.3. Методи, моделі, алгоритми та системи симетричного шифрування.

Тема 13. *Симетричні шифри та системи. Математичні та алгоритмічні основи: Стандарт шифрування Data Encryption Standard. (DES).*

Тема 14. Симетричні шифри та системи. Технології реалізації та уразливість: *Технології асиметричного шифрування в Python, уразливість.*

Розділ 5.5. Методи, моделі, алгоритми та системи асиметричного шифрування.

Тема 15. *Асиметричні шифри та системи. Математичні та алгоритмічні основи: Технології асиметричного шифрування в Python, уразливість.*

Тема 16. *Асиметричні шифри та системи. Технології реалізації та уразливість: Технології асиметричного шифрування в Python, уразливість.*

Розділ 6. Методи, методології, технології і засоби аутентифікації та ідентифікації.

Тема 17. *Методи і технології ідентифікації користувачів в розподіленнях комп'ютерних системах:*

технології аутентифікація та ідентифікація в Python.

Тема 18. *Електронний цифровий підпис, методи та засоби:*

багаторівнева організація формування та використання ключів шифрування. Функції майстер-ключа, системного, клієнтського, торгово-касового та сесійного ключів.

7. Методика викладання дисципліни на заочній формі навчання

Заочна форма бюджет часу: лекцій 8 год., лаб. роб. 8 год., СРС 119 год.

Теми на аудиторне опрацювання:

Розділ 1. Основні відомості про захист інформації в комп'ютерних системах.

Тема 1. *Основні положення законодавчої база в сфері захисту інформації в комп'ютерних системах:*

зміст та задачі дисципліни;

національні законодавчі акти і стандарти у сфері захисту інформації: категорії, основні положення, порядок і сфера застосування;

законодавчі акти та стандарти інших держав у сфері захисту інформації.

Розділ 2. Організаційні, технічні та програмно-апаратні засоби комплексної системи захисту корпоративної інформації.

Тема 2. *Комплексна система захисту корпоративної інформації. Об'єкт захисту та загрози:*

інформація як об'єкт захисту;

категорії інформації, як об'єкту захисту;

канали витоку корпоративної інформації;

загрози інформації в комп'ютерних системах;

Розділ 3. Комп'ютерні віруси та вірусологія.

Тема 4. *Загальні відомості про комп'ютерні віруси:*

класифікація вірусів;

алгоритми функціонування вірусів;

технології та засоби створення і розповсюдження комп'ютерних вірусів.

Розділ 5. Криптографічний захист інформації в комп'ютерних системах.

Розділ 5.1. Загальні відомості про криптографію та криптологію.

Тема 8. *Загальні відомості про класичну криптологію, криптографію та криптографічний аналіз:*

Загальні відомості про шифрування, кодування, криптографію і криптологію;

Задачі дешифрування;

Технології та системи криптографічного захисту інформації.

Лабораторна робота №1. *(2 год.) Дослідження процесів створення комплексної системи захисту корпоративної інформації:*

Розробка проекту КСЗІ для конкретного об'єкту інформаційної діяльності – комп'ютерної системи (встановлення категорії інформації, що захищається; дослідження каналів витоку, модель загроз; модель порушника; комплекс організаційних та технічних заходів і засобів захисту інформації; структура КСЗІ; дослідження ефективності КСЗІ).

Лабораторна робота №2. *(2 год.) Дослідження процесів захисту інформації від комп'ютерних вірусів:*

Створення ізольованого віртуального середовища досліджень; генерація вірусів та дослідження їх сигнатур; дослідження ефективності детектування сигнатур вірусів різними програмними засобами; створення системи захисту інформації від комп'ютерних вірусів та дослідження її ефективності.

Лабораторна робота №3. *(2 год.) Дослідження процесів захисту інформації від кібернетичних атак:*

Створення ізольованого віртуального середовища досліджень; дослідження уразливості оточення до кібернетичних впливів; створення системи захисту інформації від кібернетичних впливів та дослідження її ефективності.

Лабораторна робота №4. *(2 год.) Дослідження технологій традиційного шифрування та їх уразливості:*

Розробка скрипта в Python, що реалізує технології традиційного шифрування за заданим алгоритмом та дослідження їх уразливості.

Види самостійної роботи (104 годин):

самостійне опрацювання матеріалів лекційних занять (1 година х 17 лекцій = 17 годин);

підготовка та оброблення проведення розрахунків за первинними даними, отриманими на лабораторних заняттях, виконання лабораторних робіт, розв'язок задач надання на перевірку (рекомендовано 2 години х 9 лабораторних робіт = 18 годин);

виконання модульної контрольної роботи (МКР = 4 години);

підготовка до заліку (8 години);

налаштування віртуального середовища для виконання лабораторних робіт (3 години);

опрацювання тем на самостійну роботу (504 годин).

Теми на аудиторне опрацювання:

Розділ 1. Основні відомості про захист інформації в комп'ютерних системах.

Розділ 2. Організаційні, технічні та програмно-апаратні засоби комплексної системи захисту корпоративної інформації.

Тема 3 *Комплексна система захисту корпоративної інформації. Склад та структура:*

модель порушника;

методи, методології, засоби, заходи і технології комплексного захисту корпоративної інформації (організаційні заходи, технічний захист інформації, протидія технічним засобам моніторингу).

Розділ 3. Комп'ютерні віруси та вірусологія.

Тема 5. *Технології захисту комп'ютерних систем від комп'ютерних вірусів:*

конструктори вірусів;

антивірусне програмне забезпечення та сутність його побудови і застосування;

методи та технології захисту комп'ютерних систем від вірусів.

Розділ 4. Кібернетичні загрози комп'ютерним системам та протидія їм.

Тема 6. *Методи і засоби реалізації кібернетичних атак:*

кібернетична та (і) комп'ютерна атака, поняття, класифікація, модель, зміст етапів;

методи і технології організації та реалізації кібернетичних атак.

Тема 7. *Методи і засоби протидії кібернетичним атакам:*

методології, методи і технології протидії кібернетичним атакам (методи, програмне забезпечення та сутність його побудови і застосування);

методи та технології захисту комп'ютерних систем від вірусів.

Розділ 5. Криптографічний захист інформації в комп'ютерних системах.

Розділ 5.1. Загальні відомості про криптографію та криптологію.

Тема 9. *Традиційні історичні шифри. Математичні та алгоритмічні основи:*

Загальні відомості та галузі застосування.

Шифрування на основі одно та багато алфавітних підстановок: шифри Цезаря та «скитала»;

Шифр Віжинера та квадрати Уітстона.

Біграмні шифри.

Потокові шифри з необмеженою довжиною ключа.

Шифрування «гамуванням».

Тема 10. *Традиційні історичні шифри. Технології реалізації та уразливість:*

Реалізація традиційних історичних шифрів з використанням засобів Python;

Приклади реалізації традиційних шифрів в Python;

Уразливість традиційних історичних шифрів.

Розділ 5.2. Методи, моделі, алгоритми та системи блочного шифрування.

Тема 11. *Алгоритми блочного шифрування. Математичні та алгоритмічні основи:*

Сутність та математичні основи методів блочного шифрування.;

Тема 12. *Алгоритми блочного шифрування. Технології реалізації та уразливість:*

Технології блочного шифрування в Python, уразливість.

Розділ 5.3. Методи, моделі, алгоритми та системи симетричного шифрування.

Тема 13. *Симетричні шифри та системи. Математичні та алгоритмічні основи:*

Шифрування на основі чередування перестановок та підстановок;

Стандарт шифрування Data Encryption Standard. (DES).

Тема 14. Симетричні шифри та системи. Технології реалізації та уразливість:

Блок управління ключами в DES. Алгоритм 3-DES та чотири режими реалізації криптографічного захисту на основі DES.

Технології асиметричного шифрування в Python, уразливість.

Розділ 5.5. Методи, моделі, алгоритми та системи асиметричного шифрування.

Тема 15. *Асиметричні шифри та системи. Математичні та алгоритмічні основи:*

Криптографія по Діффі і Хелману. Незворотні функції в шифруванні. Три схеми та задачі криптозахисту.

Система RSA. Модулярна арифметика. Алгоритм швидкого дискретного потенціювання. Процесор – акселератор RSA;

Технології асиметричного шифрування в Python, уразливість.

Тема 16. *Асиметричні шифри та системи. Технології реалізації та уразливість:*

Проблема генерації великих простих чисел (ВПЧ). Тест Рабіна та мала теорема Ферма. Перевірки на простоту.

Схеми та алгоритми розрахунків ключів для системи RSA. Класичний та розширений алгоритми Евкліда.

Технології асиметричного шифрування в Python, уразливість.

Розділ 6. Методи, методології, технології і засоби аутентифікації та ідентифікації.

Тема 17. *Методи і технології ідентифікації користувачів в розподіленнях комп'ютерних системах:*

методи аутентифікація та ідентифікація суб'єктів на основі симетричних систем

шифрування. Поняття майстер ключа та змінного ключа;

технології аутентифікація та ідентифікація в Python.

***Тема 18.** Електронний цифровий підпис, методи та засоби:*

встановлення цілісності повідомлень на основі симетричних та асиметричних систем шифрування. Поняття сигнатури повідомлення та цифрового підпису;

аутентифікація та ідентифікація суб'єктів в протоколах відкритих замовлень. Поняття електронних чеку та квитанції;

багаторівнева організація формування та використання ключів шифрування. Функції майстер-ключа, системного, клієнтського, торгово-касового та сесійного ключів.

***Лабораторна робота №5.** (2 год.) Дослідження технологій блочного шифрування та їх уразливості:*

Розробка скрипта в Python, що реалізує технології блочного шифрування за заданим алгоритмом та дослідження їх уразливості.

***Лабораторна робота №6.** (2 год.) Дослідження технологій симетричного шифрування та їх уразливості:*

Розробка скрипта в Python, що реалізує технології симетричного шифрування за заданим алгоритмом та дослідження їх уразливості.

***Лабораторна робота №7.** (2 год.) Дослідження технологій асиметричного шифрування та їх уразливості:*

Розробка скрипта в Python, що реалізує технології асиметричного шифрування за заданим алгоритмом та дослідження їх уразливості.

***Лабораторна робота №8.** (2 год.) Дослідження технологій аутентифікації та ідентифікації в розподілених комп'ютерних системах:*

Розробка скрипта в Python, що реалізує технології електронного цифрового підпису та дослідження ефективності процесів аутентифікації та ідентифікації в розподілених комп'ютерних системах.

***Модульна контрольна робота** (2 год).*

Політика та контроль

8. Політика навчальної дисципліни (освітнього компонента)

Для виконання лабораторних робіт та модульних контрольних робіт встановлюються дедлайни.

Виконання лабораторних робіт поза встановлених термінів супроводжуються штрафними балами, які вираховуються із оцінки за протокол (п. 2.9. ПОЛОЖЕННЯ про систему оцінювання результатів навчання). МКР не приймається поза встановлені терміни.

Штрафні бали виставляються за: невчасну здачу лабораторної роботи. Кількість штрафних балів не більше 10 (9 лабораторних робіт + МКР). Штрафні бали та жорсткі дедлайни не запроваджуються у період військового стану.

Заохочувальні бали виставляються за: R&D результати виконання лабораторних робіт; активну участь на лекціях; виконання поточних домашніх завдань, ведення конспекту, підготовка повідомлення з презентацією по одній із тем СРС дисципліни тощо. Кількість заохочуваних балів не більше 10.

Виконанню кожної лабораторної роботи передує виконання індивідуального завдання і оформлення його у вигляді протоколу. Студент, який прийшов на заняття без оформленого протоколу до лабораторної роботи не допускається. Першим етапом студент захищає результати отримані під час виконання індивідуального завдання до лабораторної роботи, на другому етапі – захищає теорію шляхом усного опитування або тестування (за необхідності). Захист лабораторних робіт може бути проведено за результатами аналізу повноти і якості виконання протоколу. Бали отримані за виконання лабораторної роботи, за теоретичною частиною та за протокол входять в оцінку за лабораторну роботу.

Перездача лабораторної роботи у разі її позитивної оцінки з метою підвищення оцінки – не передбачено.

Виконання лабораторних робіт є обов'язковими для допуску до семестрового контролю. Умовою допуску до семестрового контролю є зарахування всіх лабораторних робіт та стартовий рейтинг не менше 60 балів.

Модульна контрольна робота пишеться на лекційному занятті без застосування допоміжних засобів (мобільні телефони, планшети та ін.); результат в електронному вигляді надаються викладачеві.

Модульна контрольна робота не переписується за умови негативної оцінки. Негативна оцінка за МКР прирівнюється до 0 балів, в цьому випадку МКР не зараховується.

Оцінка, яку студент може отримати за виконання кожної лабораторної роботи та за модульну контрольну роботу наведені в таблиці 1 оцінювання семестрових робіт, розділ 8 силабусу.

Таким чином мінімальна оцінка, яку повинен отримати студент для допуску до семестрового контролю дорівнює 60 балів, максимальна – 100 балів за виконання всіх поточних робіт за семестр.

Здобувачі, які виконали всі умови допуску до заліку (виконали всі лабораторні роботи) та мають рейтингову оцінку менше 60 балів, а також ти здобувачі, хто бажає підвищити свою рейтингову оцінку, на останньому за розкладом занятті мають можливість пройти семестровий контроль у вигляді залікової контрольної роботи.

У разі виконання залікової контрольної роботи рейтингова оцінка визначається як сума балів за залікову контрольну роботу та балів за індивідуальні семестрові завдання.

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

Для навчальної дисципліни «Захист інформації в комп'ютерних системах та мережах», як прикладної дисципліни, що спрямована на отримання комплексного ґрунтовного теоретичного базису та потужних практичних навичок забезпечення захисту інформації, що обробляється в комп'ютерних та кіберфізичних системах і мережах з метою реалізації встановленої політики інформаційної безпеки застосовується РСО-1 (п. 2.1. ПОЛОЖЕННЯ про систему оцінювання результатів навчання в КПІ ім. Ігоря Сікорського, https://osvita.kpi.ua/sites/default/files/downloads/Pologennia_RSO_2022.pdf).

Семестровий рейтинг студента розраховується, виходячи із 100-бальної шкали. Рейтинг складається з балів, що студент отримав за виконання 9 лабораторних робіт РЛ та однієї модульної контрольної роботи РМКР.

Завдання лабораторних робіт розділені за рівнями складності. Високий рівень складності передбачає отримання максимум 9 балів, середній рівень – 7 балів.

Максимальна кількість балів за лабораторні роботи (РЛ) за високим рівнем складає 81 бал, за середнім рівнем - 63 балів.

Розподіл балів за виконання лабораторних робіт.

1.1. Якість / повнота оформлення протоколу з лабораторної роботи – 1 бал.

1.2. Своєчасний захист роботи – 1 бал.

1.3. Повнота аналізу отриманих результатів – 1 бал.

1.4. Якість та повнота виконання технічних умов завдання, функціональність розробленої технічної продукції (програмного скрипта) -4 бали.

1.5. Рівень теоретичної підготовки – 2 бали.

**** Для умов дистанційного навчання бали за теоретичну підготовленість (п.1.4) можуть нараховуватись за результатами аналізу вмісту протоколу з лабораторної роботи.*

**** Для умов військового стану – своєчасність захисту лабораторної роботи (п.1.2) – не застосовується а додається до п.1.4.*

Максимальна кількість балів за МКР - РМКР = 9.

Розподіл балів за виконання МКР.

2.1. Якість / повнота оформлення звіту з МКР – 1 бал;

2.2. Повнота розкриття суті та оригінальність відповіді на теоретичні питання – 1,5 балів за кожне питання – загалом – 3 бали;

2.3. Повнота, оригінальність та якість виконання практичного питання – 5 бали.

Максимальна кількість балів за залікову роботу складає R3 = 10 балів.

3.1. Якість / повнота оформлення звіту із залікової роботи – 1 бал;

3.2. Повнота розкриття суті та оригінальність відповіді на теоретичні питання – 2 балів за кожне питання – загалом – 4 бали;

3.3. Повнота, оригінальність та якість виконання практичного питання – 5 бали.

*У разі **значних запозичень / порушення вимог доброчесності** в звітному протоколі з лабораторної роботи - робота може бути не зарахована, або повернення на переопрацювання. За таких умов МКР та залікова робота – не зараховуються.*

***Календарна атестація студентів** (на 8 та 14 тижнях семестрів) з дисципліни проводиться за значенням поточного рейтингу студента на час атестації. Якщо значення цього рейтингу не менше 50 % від максимально можливого на час атестації, студент вважається атестованим. В іншому випадку в атестаційній відомості виставляється «неатестовано».*

Таким чином, порядок визначення загального рейтингу пояснюється Таб.1 та визначається за виразом

$$R = RЛ + RМКР + R3.$$

Таблиця 1

Загальний рейтинг за дисципліною

Звітність	*Лр1*	*Лр2*	*Лр3*	*Лр4*	*Лр5*	*Лр6*	*Лр7*	*Лр8*	*Лр9*	*МК*	*СУМА*	*Залік*	*Сумма+залік*
Високий рівень	*9*	*9*	*9*	*9*	*9*	*9*	*9*	*9*	*9*	*9*	*90*	*10*	*100*
Середній рівень	*7*	*7*	*7*	*7*	*7*	*7*	*7*	*7*	*7*	*9*	*72*	*10*	*82*

Максимальна кількість балів за семестр не перевищує RC = 100.

З урахуванням одержаної суми балів кінцева оцінка визначається за Табл.2.

Таблиця 2

Визначення семестрової оцінки

Кількість балів	***Оцінка***
100-95	*Відмінно*
94-85	*Дуже добре*
84-75	*Добре*
74-65	*Задовільно*
64-60	*Достатньо*
Менше 60	*Незадовільно*
Не виконані умови допуску	*Не допущено*

10. Визнання результатів неформальної освіти

Визнання результатів неформальної освіти здійснюється у відповідності до Положення про визнання в КПІ ім. Ігоря Сікорського результатів навчання, набутих у неформальній / інформальній освіті, див. за посиланням:

https://osvita.kpi.ua/sites/default/files/downloads/%D0%9D%D0%B5%D1%84%D0%BE%D1%80%D0%BC_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC.pdf

За даним курсом можуть бути визнати результати навчання здобуті у неформальній / інформальній освіті в обсязі, що не перевищує 10% від загального обсягу навчального курсу (п.2.6 Положення).

У разі виконання рекомендованого викладачем онлайн курсу додаткова валідація результатів неформального навчання не потрібна. Поточний контроль з відповідної частини курсу оцінюється відповідно до рейтингової системи оцінювання результатів навчання та політики навчальної дисципліни. В такому форматі одним онлайн курсом можна замінити одну лабораторну роботу на вибір (8 балів) і не можна замінити МКР.

У разі зарахування сторонніх результатів неформальної освіти, визнання результатів проводиться на початку семестру, у якому передбачено опанування освітнього компонента, який може бути частково зарахований. Викладач проводить аналіз їх відповідності силабусу, проводить співбесіду із студентом. Студент має підготувати і захистити звіт з результатами опанованої частини курсу. В окремих випадках може бути зарахований весь курс, або більша частина курсу. Процедура відбувається згідно Положення з дозволу декана, валідацію результатів навчання проводить комісія.

Робочу програму навчальної дисципліни (силабус):

Складено професором кафедри обчислювальної техніки, доктором технічних наук, професором Писарчуком Олексієм Олександровичем.

Ухвалено кафедрою обчислювальної техніки (протокол № 10 від 25.05.2023).

Погоджено Методичною комісією факультету інформатики та обчислювальної техніки (протокол № 11 від 30.06.2023).