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

Кафедра системного програмування і спеціалізованих комп'ютерних систем

ТЕХНОЛОГІЯ ПРОЕКТУВАННЯ СПЕЦІАЛІЗОВАНИХ ОПЕРАЦІЙНИХ СИСТЕМ

Робоча програма дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Другий (магістерський)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*123 Комп'ютерна інженерія*
Освітня програма	*ОНП Системне програмування та спеціалізовані комп'ютерні системи*
Статус дисципліни	*Вибіркова*
Форма навчання	*очна(денна)*
Рік підготовки, семестр	*1 курс, весняний семестр*
Обсяг дисципліни	*4 кредити ECTS*
Семестровий контроль/ контрольні заходи	*1 семестр: МКР, залік, РГР*
Розклад занять	*rozklad.kpi.ua*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Лекції, лабораторні заняття: к.т.н., доц. Потапова К.Р., avatarkina-avatarochka@ukr.net*
Розміщення курсу	*Кампус КПІ ім. Ігоря Сікорського https://campus.kpi.ua*

Програма навчальної дисципліни

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

Предметом навчальної дисципліни *є процеси розробки та проектування спеціалізованих операційних систем.*

Метою навчальної дисципліни *є формування у студентів здатностей:*

- *володіння основними методами безпечного інформаційного менеджменту в спеціалізованих операційних системах;*
- *розробки апаратних і програмних засобів, що призначені для захисту інформації в спеціалізованих операційних системах;*
- *використання сучасних апаратних і програмних засобів захисту інформації в спеціалізованих операційних системах.*

Об'єктом навчальної дисципліни *є процес проектування спеціалізованих операційних систем.*

Згідно з вимогами освітньо-професійної програми студенти після засвоєння дисципліни «Технологія проектування спеціалізованих операційних систем» мають продемонструвати такі результати навчання:

знання:

- *особливостей захисту інформації в спеціалізованих операційних системах;*
- *перелік та особливості основних загроз інформації в спеціалізованих операційних системах;*

- *підходів до розробки політики спеціалізованих операційних систем;*
- *порядку формування комплексу засобів захисту інформації в спеціалізованих операційних системах;*
- *принципів управління доступом до захищених ресурсів спеціалізованих операційних системах;*
- *прийомів технічного захисту інформації в спеціалізованих операційних системах;*
- *криптографічних методів і засобів захисту інформації в спеціалізованих операційних системах.*

уміння:

- *використовувати теоретичні знання для алгоритмічного проектування систем захисту в спеціалізованих операційних системах;*
- *настроювати систему захисту інформації в спеціалізованих операційних системах;*
- *створювати програмне забезпечення для вирішення конкретних прикладних задач в області захисту інформації в спеціалізованих операційних системах.*

досвід:

- *реалізації основних механізмів захисту інформації в спеціалізованих операційних системах.*

Компетентності, формуванню яких сприяє дана дисципліна:

- *здатність до адаптації і дій в новій ситуації;*
- *здатність до абстрактного мислення, аналізу і синтезу;*
- *здатність проводити дослідження на відповідному рівні;*
- *здатність до пошуку, оброблення та аналізу інформації з різних джерел;*
- *здатність виявляти, ставити та вирішувати проблеми;*
- *здатність приймати обгрунтовані рішення;*
- *здатність до визначення технічних характеристик, конструктивних особливостей застосування і експлуатації програмних, програмно-технічних засобів, комп'ютерних систем та мереж різного призначення;*
- *здатність розробляти алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем та мереж, інтернет додатків, кіберфізичних систем з використанням сучасних методів і мов програмування, а також засобів і систем автоматизації проектування;*
- *здатність будувати та досліджувати моделі комп'ютерних систем та мереж.*

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

Дисципліні «Технологія проектування спеціалізованих операційних систем» передують дисципліни «Цифрові ЕОМ», «Архітектура обчислювальних машин», «Надійність, контроль, діагностика та експлуатація ЕОМ», «Проектування баз даних» та «Захист інформації в комп'ютерних системах».

Успішне оволодіння знаннями з даної дисципліни забезпечує вивчення надалі таких курсів, як «Наукова робота за темою магістерської дисертації» (ПО7).

3. Зміст навчальної дисципліни

РОЗДІЛ 1. МЕТОДОЛОГІЯ СТВОРЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ОПЕРАЦІЙНИХ СИСТЕМ.

Тема 1.1. Предмет, мета та завдання курсу. Особливості захисту інформації в операційних системах

Тема 1.2. Критерії оцінки захищеності інформації

Тема 1.3. Розробка технічного завдання на створення системи захисту інформації в операційній системі

Тема 1.4. Технологія створення системи захисту інформації в операційних системах

Тема 1.5. Забезпечення надійності системи захисту інформації в операційних системах

Тема 1.6. Оптимізація системи захисту інформації в операційних системах

Тема 1.7. Підходи до створення системи захисту інформації провідних виробників

РОЗДІЛ 2. ПРИНЦИПИ ПРОЕКТУВАННЯ ОСНОВНИХ КОМПОНЕНТІВ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ СПЕЦІАЛІЗОВАНИХ ОПЕРАЦІЙНИХ СИСТЕМ

Тема 2.1. Проектування системи ідентифікації та аутентифікації користувачів

Тема 2.2. Керування доступом до об'єктів операційної системи

Тема 2.3. Контроль коректності функціонування механізмів захисту

Тема 2.4. Криптографічні системи захисту інформації

Тема 2.5. Стеганографічні системи захисту інформації

Тема 2.6. Огляд та оцінка систем захисту сучасних спеціалізованих операційних систем

Тема 2.7. Використання засобів штучного інтелекту для захисту спеціалізованих операційних систем

4. Навчальні матеріали та ресурси

Базова література:

1. Операційні системи: [Електронний ресурс]: навч. посіб. для студ. спеціальності 123 «Комп'ютерна інженерія» / В. Г. Зайцев, І. П. Дробязко; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 3 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2019. – 240 с.

2. Богуш В.М. Моніторинг систем інформаційної безпеки: навч. посібник [для студ. вищ. навч. закл.] / В.М. Богуш, А. М. Кудін. – К. : ДУІКТ, 2010. – 414 с.

3. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

4. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

5. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

6. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

Допоміжна література:

1. Таненбаум Е. Сучасні операційні системи. 2-е видання. – : 2002. – 1040 с.

2. Silberschatz A., Galvin P.B. Operating System Concepts.5-th Edition. , Addison Wesley, 1998.

3. Лав, Роберт. Розробка ядра Linux, 2-е видання. – ТОВ «І.Д.Вільямс», 2006. – 448 с.

Електронні ресурси:

1. *http://dir.osrc.info/SpecializirovannyeOS*

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

5.1 Лекційні заняття

Матеріали для вивчення дисципліни розміщені в електронному вигляді (Кампус КПІ ім. Ігоря Сікорського https://campus.kpi.ua). Контент доступний студенту із будь-якого місця в мережі Інтернет.
Лекції по дисципліні проводяться із використанням сучасних мультимедійних презентаційних технологій.

№ з/п	Назва теми лекції та перелік основних питань
1	Предмет, мета та завдання курсу. Особливості захисту інформації в операційних системах.
2	Критерії оцінки захищеності інформації.
3	Розробка технічного завдання на створення системи захисту інформації в операційній системі.
4	Технологія створення системи захисту інформації в операційних системах.
5	Забезпечення надійності системи захисту інформації в операційних системах.
6	Оптимізація системи захисту інформації в операційних системах.
7	Підходи до створення системи захисту інформації провідних виробників.
8	Проектування системи ідентифікації та аутентифікації користувачів.
9	Керування доступом до об’єктів операційної системи. Моделі розподілу прав доступу.
10	Контроль коректності функціонування механізмів захисту.
11	Криптографічні системи захисту інформації.
12	Стеганографічні системи захисту інформації.
13	Огляд та оцінка систем захисту сучасних спеціалізованих операційних систем.
14	Використання засобів штучного інтелекту для захисту спеціалізованих операційних систем.
15	Мережеві операційні системи і загальні принципи управління комп'ютерними мережами
16	Сумісність і множинні прикладні середовища. Способи реалізації прикладних програмних середовищ
17	Способи реалізації прикладних програмних середовищ
18	Використання прикладних програмних середовищ для проектування програмних засобів оброблення інформаційно-технологічних процесів

5.2. Лабораторні роботи

№ з/п	Назва лабораторної роботи	Кількість ауд. годин
1	Розробка системи шифрування даних Завдання: розробити програмне забезпечення для системи асиметричного шифрування даних в спеціалізованій операційній системі	6
2	Розробка систем стеганографічного захисту інформації	6

	Завдання: розробити програмне забезпечення для стеганографічного захисту інформації спеціалізованої операційної системи	
3	*Розробка додаткових компонент систем захисту від мережевих атак* *Завдання: розробити програмне забезпечення для захисту від мережевих атак на ресурси спеціалізованої операційної системи*	*6*

В умовах змішаного навчання 2023-2024 навчального року різні види занять, у тому числі контрольні заходи, проводяться з використанням сервісу Zoom.

6. Самостійна робота студента

До самостійної роботи студента відноситься виконання індивідуальних завдань з тематики, яка виноситься на лабораторні роботи, а також опрацювання теоретичного матеріалу за наданими текстами лекцій та додатковою літературою, у тому числі за темами, які винесені на самостійне вивчення (згідно таблиці 1). Усі навчальні матеріали (презентації лекцій, практичних занять, методичні вказівки до виконання лабораторних робіт) розміщені в електронному вигляді в e-mail груп, а також в середовищі «Електронний кампус». Навчальний контент доступний із будь-якого місця в мережі Інтернет. На самостійну роботу студент має витрачати кількість годин, що співвимірна із кількістю годин, проведених ним на аудиторних заняттях.

Таблиця 1. Питання, які виносяться на самостійне опрацювання

№ з/п	*Назва теми, що виноситься на самостійне опрацювання*
1	*Закони України "Про інформацію" та "Про державну таємницю"* *Визначення та пояснення основних термінів, що стосуються захисту інформації*
2	*Методологія розрахунку критеріїв захищеності* *Застосування експертних даних для визначення номенклатури величин параметрів захищеності*
3	*Вимоги до оформлення технічної документації засобів захисту спеціалізованих операційних систем* *Поняття офіційної технічної документації в області захисту інформації. Класифікація вимог. Порядок оформлення та затвердження*
4	*Використання CASE-технологій при проектуванні системи захисту спеціалізованих операційних систем* *Застосування мови моделювання UML та розробка основних діаграм при проектуванні систем захисту інформації спеціалізованих операційних систем*
5	*Закони розподілу щільності ймовірності безвідмовної роботи* *Перелік та характеристика основних законів розподілу щільності ймовірності безвідмовної роботи. Типові закони розподілу для основних компонент захисту*
6	*Градієнтні методи пошуку оптимуму* *Перелік та характеристик основні градієнтних методів пошуку оптимуму. Недоліки та переваги. Передумови застосування*
7	*Характеристика комплексних систем захисту інформації вітчизняного виробництва*

	Основні характеристики комплексних систем захисту вітчизняного виробництва. Обмеження на застосування. Шляхи вдосконалення
8	*Методологія зберігання та захисту парольних даних* *Передумови необхідності захищеного збереження парольних даних. Використання хеш-кодів та хеш-функцій. Обмеження та вразливості*
9	*Характеристика функціональних можливостей мережевих екранів провідних виробників* *Перелік основних функціональних можливостей. Перелік мережевих екранів провідних виробників. Переваги та недоліки. Комплексність захисту*
10	*Математичне забезпечення систем контролю цілісності Основні математичні методи та алгоритми, що використовуються для забезпечення контролю цілісності. Недоліки та переваги. Обмеження. Приклади застосування*
11	*Вітчизняні та закордонні стандарти в галузі криптографічного захисту* *Стандарт криптографічного перетворення даних ГОСТ 28147-89. Криптоалгоритм AES-128*
12	*Методологія пошуку прихованих даних в відео файлах* *Методи пошуку прихованих даних в метаданих відеофійлів. Методи пошуку прихованих даних в інформативній частині відеофійлів*
13	*Оцінити відповідність захисту операційних систем мобільних телефонів вітчизняним нормативним вимогам* *Перелік вітчизняних нормативних документів. Формування вимог до захисту операційних систем мобільних телефонів. Оцінка відповідності*
14	*Використання методів теорії генетичних алгоритмів для вирішення задач захисту інформації* *Основні положення теорії генетичних алгоритмів. Передумови застосування для вирішення задач захисту. Недоліки та переваги. Приклади застосування*

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Студент має вивчати дисципліну протягом другого семестру, дотримуючись календарного плану виконання завдань лабораторних робіт, вивчення тем лекційного матеріалу, та виконання модульної контрольної роботи. Усі завдання студент має виконувати самостійно і вчасно.

Завдання з лабораторної роботи вважається виконаним, якщо студент захистив його у викладача (показав працездатність, відповів на усі питання. Несвоєчасним вважається виконання завдання із затримкою більше 1 тижня. За несвоєчасну здачу лабораторних робіт передбачені штрафні бали. Такі обмеження стимулюють студента організувати систематичне виконання завдань та не допускати значного накопичення незданих лабораторних робіт на кінець семестру.

Для перевірки як теоретичних знань, так і практичних навичок в семестрі передбачена модульна контрольна робота (МКР).

Оцінювання студентів здійснюється згідно рейтингової оцінки рівня підготовки студентів з дисципліни. Поточний стан успішності студенти можуть бачити в системі «Електронний кампус».

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

8.1 Поточний контроль

Поточний контроль результатів навчання передбачає виконання студентами лабораторних робіт, МКР та РГР.

Вагові бали кожного завдання лабораторної роботи залежать від його складності і варіюються у діапазоні від 0 до 5 балів відповідно до табл. 2.

Таблиця 2. Вагові бали та критерії оцінювання лабораторних робіт

2 семестр					
		алгоритм	*оптимальність складання програми*	*захист*	*звіт*
1	*Розробка системи шифрування даних* *Завдання: розробити програмне забезпечення для системи асиметричного шифрування даних в спеціалізованій операційній системі*	*5*	*5*	*5*	*5*
2	*Розробка систем стеганографічного захисту інформації* *Завдання: розробити програмне забезпечення для стеганографічного захисту інформації спеціалізованої операційної системи*	*5*	*5*	*5*	*5*
3	*Розробка додаткових компонент систем захисту від мережевих атак* *Завдання: розробити програмне забезпечення для захисту від мережевих атак на ресурси спеціалізованої операційної системи*	*5*	*5*	*5*	*5*
Разом за лабораторні роботи		*60 балів*			

Критерії оцінювання лабораторних робіт включають якість розробки алгоритму програми, безпомилковість її виконання, якість захисту розробленої програми та підготовки звіту щодо виконаної роботи (див. табл. 2).

За несвоєчасну здачу комп'ютерного практикуму передбачені штрафні бали (% зниження згідно до табл. 3).

Таблиця 3. Штрафи за затримку здачі індивідуальних завдань комп'ютерного практикуму

Термін затримки	*Величина від'ємного бала*
2 тижні	*1*
4 тижні	*2*
6 тижнів	*3*
>8 тижнів	*4*

МКР проводиться у вигляді тестів, питання в яких можуть бути як теоретичними, так і практичними.

Вагові бали за МКР наведено в табл.4.

Таблиця 4. Вагові бали за МКР

№ та тема контрольної роботи	*Ваговий бал*
2 семестр	
Контрольна робота. Використання методів теорії генетичних алгоритмів для вирішення задач захисту інформації	*10*
Разом	*10*

РГР передбачає виконання індивідуальних завдань згідно до встановлених варіантів. Метою РГР є поглиблення знань і напрацювання навичок роботи з методами побудови бортових навігаційних ЕОМ. Ваговий бал РГР – 10 балів.

МКР передбачає виконання індивідуальних завдань згідно до встановлених варіантів. Метою МКР є поглиблення знань роботи з методів побудови правил класифікації.

8.2 Календарний контроль

Проводиться двічі на семестр як моніторинг поточного стану виконання вимог робочої програми.

8.3 Семестровий контроль

Семестровий контроль результатів навчання проводиться у вигляді заліку.

Умови допуску до семестрового контролю (заліку):

- зарахування усіх лабораторних робіт,

- виконання і захист МКР

- виконання і захист РГР

– стартовий рейтинг rC ≥ 40 балів (не менше 50 % від RC).

Розмір шкали рейтингу R = 100 балів, розмір стартової шкали RC = 40 балів, розмір залікової шкали RZ = 20 балів.

Підсумкова оцінка формується за результатами оцінювання знань та навичок студента в семестрі та на заліку за формулою: R = RC + RZ.

Підсумкова оцінка переводиться до залікової оцінки згідно з таблицею:

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

Робочу програму навчальної дисципліни (силабус):

Складено к.т.н., доц. Потапова К.Р.

Ухвалено кафедрою СПСКС (протокол № 6 від 03.01.2024)

Погоджено Методичною комісією факультету ПМ (протокол № 6 від 26.01.2024)