МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерної інженерії та інноваційних технологій

«ЗАТВЕРДЖУЮ»

Ректор Міжнародного гуманітарного університету д.ю.н., професор

_____ Костянтин ГРОМОВЕНКО

«29» серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОПЕРАЦІЙНІ СИСТЕМИ

Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Назва освітньої програми	Кібербезпека
Рівень вищої освіти	перший (бакалаврський) рівень

Одеса - 2025 рік

Робоча програма затверджена на засіданні кафедри комп'ютерної інженерії та інноваційних технологій протокол № 1 від 28 серпня 2025 року.

Розробники і викладачі	**Контактний тел.**	**E-mail**
доцент кафедри комп'ютерної інженерії та інноваційних технологій, кандидат технічних наук, доцент, **Педяш Володимир Віталійович**	+38067-37 87 003	vpedyash@gmail.com

Завідувач кафедри
комп'ютерної інженерії та
інноваційних технологій,
к.т.н., доцент _____ Лариса ЙОНА

Гарант освітньої програми,
к.т.н., доцент _____ Лариса ЙОНА

Узгоджено
Начальник навчального відділу _____ Лілія САЄНКО

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</th><th colspan="2">Характеристика навчальної дисципліни</th></tr>
<tr><th>денна форма навчання</th><th>заочна форма навчання</th></tr>
<tr><td rowspan="2">Кількість кредитів – 4

Загальна кількість годин – 120</td><td>Галузь –
12 Інформаційні технології</td><td colspan="2">обов’язкова</td></tr>
<tr><td rowspan="9">Спеціальність –
125 Кібербезпека та захист інформації</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">2-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>4-й</td><td>4-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="8">Мова навчання – українська</td><td rowspan="8">Рівень вищої освіти – перший (бакалаврський) рівень</td><td>26 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>14 год.</td><td>2 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>12 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>68 год.</td><td>110 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>Екзамен</td><td>Екзамен</td></tr>
</table>

Операційні системи – це фундаментальна дисципліна, що вивчає принципи організації, архітектури та функціонування сучасних операційних систем, які є основою функціонування інформаційно-комунікаційних систем (ІКС). Курс охоплює універсальні концепції, які реалізовано в різних класах ОС – настільних, серверних, мобільних та вбудованих, незалежно від конкретної платформи (Linux, Windows, macOS тощо). Особлива увага приділяється механізмам, що забезпечують безпеку, надійність і ефективне управління ресурсами в сучасних IT-середовищах.

Знання, отримані в рамках цієї дисципліни, є критично важливими для майбутніх фахівців з кібербезпеки, оскільки безпека операційних систем визначає базовий рівень захищеності всієї інформаційної інфраструктури. Розуміння архітектури процесів, управління пам’яттю, файлових систем, механізмів контролю доступу, віртуалізації та автоматизації дозволяє ефективно виявляти вразливості, застосовувати засоби захисту, забезпечувати неперервність бізнес-процесів та відновлювати функціонування ІКС після інцидентів.

Метою дисципліни є формування у студентів системного розуміння внутрішньої структури та поведінки операційних систем, а також розвиток практичних навичок аналізу та управління ОС з урахуванням вимог кібербезпеки. Курс спрямований на досягнення програмних результатів навчання та компетентностей, передбачених стандартом вищої освіти зі спеціальності «Кібербезпека та захист інформації». Він також узгоджений із темами розділу 2.3 програми єдиного державного кваліфікаційного іспиту (ЄДКІ), що стосуються архітектури, процесів, пам’яті, файлових систем та захисних механізмів операційних систем.

ПРЕРЕКВІЗИТИ. Передумовами є знання архітектури комп'ютерів («Комп'ютерна схемотехніка та архітектура комп'ютерів», ОК 15), навички програмування («Основи програмування», ОК 8) та знання з організації мереж («Комп'ютерні мережі», ОК 13).

ПОСТРЕКВІЗИТИ. Знання операційних систем є необхідними для вивчення «Безпеки програм та даних» (ОК 16), «Основ Web-безпеки» (ОК 22), «Web-технологій» (ОК 14), «Комплексних систем захисту інформації» (ОК 24), «Управління інформаційною та кібербезпекою» (ОК 30), «Основ цифрової криміналістики» (ОК 26) та «Етичного хакінгу та тестування на проникнення» (ОК 18).

2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ ТА ДОСЯГНЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ

У процесі реалізації програми дисципліни «Операційні системи» формуються наступні компетентності із передбачених освітньою програмою:

Інтегральна компетентність

ІК. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації.

Загальні компетентності (ЗК)

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності

Спеціальні (фахові, предметні) компетентності

СК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

СК 11. Здатність здійснювати проєктування, адміністрування та керування інформаційно-комунікаційними системами, забезпечуючи їхню надійність, безпеку та ефективність функціонування.

Навчальна дисципліна «Операційні системи» забезпечує досягнення програмних результатів навчання (РН), передбачених освітньою програмою:

РН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

РН 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.

РН 14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

РН 22. Вміти застосовувати методи та інструменти проєктування й адміністрування мереж і систем, виконувати налаштування, моніторинг та підтримку їхньої працездатності з урахуванням вимог інформаційної безпеки.

Заплановані результати навчання за навчальною дисципліною

Знання:

1. На понятійному рівні — основні категорії, принципи та архітектурні підходи до побудови сучасних операційних систем, у тому числі класифікацію ОС за призначенням (настільні, серверні, вбудовані, мобільні), моделі багатозадачності, багатокористувацькості та ізоляції.

2. Структуру та функціонування ключових підсистем операційних систем: управління

процесами та потоками, керування пам’яттю, організацію файлових систем, механізми безпеки та контролю доступу.

3. Принципи віртуалізації, контейнеризації та управління IT-середовищами, включаючи типи гіпервізорів, рівні абстракції та сучасні практики забезпечення надійності й масштабованості.

Уміння:

4. Аналізувати внутрішню структуру операційних систем, ідентифікувати компоненти та взаємозв’язки між підсистемами (процеси, пам’ять, файлові системи, безпека).

5. Застосовувати знання для оцінки рівня захищеності операційної системи на основі аналізу прав доступу, моделей автентифікації, журналізації та ізоляції процесів.

6. Обґрунтовано вибирати архітектурні рішення та механізми управління ресурсами залежно від типу завдання (серверне середовище, вбудовані системи, персональні комп’ютери).

7. Оцінювати вразливості, пов’язані з неправильним управлінням пам’яттю, небезпечними правами доступу до файлів, нестабільністю процесів або помилковою конфігурацією безпеки.

Навички:

8. Ефективно використовувати універсальні механізми ОС (незалежно від платформи) для вирішення практичних завдань у сфері кібербезпеки: моніторинг процесів, аналіз прав доступу, налаштування файлових систем, резервування даних, автоматизація завдань.

9. Виконувати діагностику та відновлення функціонування систем після збоїв або реалізації загроз, використовуючи засоби резервування, LVM, відновлення файлових систем та аналіз журналів подій.

10. Працювати у віртуальних середовищах з дотриманням принципів безпеки, ізоляції та керування конфігураціями, що відповідає вимогам сучасних практик кібербезпеки та стандартів.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Архітектура та класифікація сучасних операційних систем

Принципи побудови операційних систем: монолітна, мікроядерна, гібридна та модульна архітектури. Класифікація ОС за призначенням: настільні, серверні, вбудовані, мобільні. Роль операційної системи як посередника між апаратними компонентами та прикладним програмним забезпеченням. Моделі виконання завдань: багатозадачність, багатокористувацькість, реального часу. Вплив архітектурних рішень на безпеку, надійність і масштабованість інформаційно-комунікаційних систем (ІКС).

Тема 2. Механізми управління процесами та потоками виконання

Модель процесу: стан, перехід між станами, контекст, ідентифікатори. Потоки виконання як легковагові процеси. Принципи планування завдань: алгоритми, квантування часу, пріоритети. Синхронізація процесів: умови гонитви, взаємне виключення, семафори, монітори. Вплив нестабільної роботи процесів на безпеку ІКС.

Тема 3. Управління пам’яттю та механізми захисту

Організація пам’яті: фізична, віртуальна, стрічка обміну. Механізми адресації: сегментація, сторінкування. Принципи роботи системи управління пам’яттю: виділення, звільнення, ізоляція. Проблеми безпеки: витікання пам’яті, використання після звільнення (use-after-free), переповнення буфера. Захист через DEP, ASLR, SMAP.

Тема 4. Файлові системи та організація зберігання даних

Базові концепції: структури метаданих, inode/еквіваленти, журналювання, журнали транзакцій. Порівняння файлових систем: FAT32, NTFS, ext4, APFS, ZFS. Захист цілісності даних, механізми відновлення після збоїв. Роль файлових систем у реалізації політик резервного копіювання та аудиту.

Тема 5. Механізми безпеки та контролю доступу в операційних системах

Моделі безпеки: дискреційна (DAC), обов’язкова (MAC), рольова (RBAC). Принцип найменших привілеїв. Механізми автентифікації та авторизації: облікові записи, паролі, токени, PAM, Active Directory, LDAP. Контроль доступу на рівні файлів, процесів, мережі. Аудит та журналізація подій.

Тема 6. Управління конфігурацією та автоматизація системних завдань

Роль скриптів, сценаріїв та систем автоматизації у підтримці стабільності ОС. Принципи

конфігураційного управління: ідемпотентність, версіонування, транзакційність змін. Механізми планування завдань (cron, Windows Task Scheduler). Інтеграція з політиками безпеки: автоматичне оновлення, сканування на вразливості, звітування.

Тема 7. Віртуалізація, контейнеризація та управління сучасними ІТ-середовищами

Принципи віртуалізації: типи гіпервізорів (Type 1/Type 2), апаратна підтримка. Контейнеризація як альтернатива повній віртуалізації. Безпека віртуальних середовищ: ізоляція, побічні канали, ескалація привілеїв. Роль віртуальних систем у тестуванні, моделюванні загроз, резервному копіюванні.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин									
	денна форма					Заочна форма				
	усього	у тому числі				усього	у тому числі			
		лекц.	лаб.	практ.	сам. роб.		лекц.	лаб.	прак.	сам. роб.
Тема 1. Архітектура та класифікація сучасних операційних систем	12	2		2	8	17	2			15
Тема 2. Механізми управління процесами та потоками виконання	18	4	2	2	10	15				15
Тема 3. Управління пам’яттю та механізми захисту	18	4	2	2	10	17		2		15
Тема 4. Файлові системи та організація зберігання даних	18	4	2	2	10	17			2	15
Тема 5. Механізми безпеки та контролю доступу в операційних системах	18	4	2	2	10	17	2			15
Тема 6. Управління конфігурацією та автоматизація системних завдань	18	4	2	2	10	17		2		15
Тема 7. Віртуалізація, контейнеризація та управління сучасними ІТ-середовищами	18	4	2	2	10	20				20
Усього годин	**120**	**26**	**12**	**14**	**68**	**120**	**4**	**4**	**2**	**110**
ПІДСУМКОВИЙ КОНТРОЛЬ – ЕКЗАМЕН										

5. ПИТАННЯ ДО ПРАКТИЧНИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1. Архітектура та класифікація сучасних операційних систем.** 1. Основні функції, що виконує операційна система у сучасних інформаційно-комунікаційних системах. 2. Відмінності між монолітною, мікроядерною та гібридною архітектурами операційних систем. 3. Класифікація операційних систем за призначенням (настільні, серверні, вбудовані, мобільні) та їхні особливості. 4. Принципи багатозадачності, багатокористувацькості та ізоляції процесів у сучасних операційних системах. 5. Роль віртуалізації у розумінні архітектури операційної системи та її вплив на організацію ІТ-інфраструктури. 6. Складові компоненти ядра операційної системи та їх взаємодія з прикладним програмним забезпеченням	2	

2	**Тема 2. Механізми управління процесами та потоками виконання.** 1. Поняття процесу та потоку виконання в операційній системі та їх основні атрибути. 2. Стани процесу під час життєвого циклу та механізми переходу між станами. 3. Алгоритми планування завдань у операційних системах та їх вплив на продуктивність системи. 4. Проблема умов гонитви та механізми її уникнення через синхронізацію процесів. 5. Ізоляція процесів у сучасних операційних системах та наслідки її порушення. 6. Механізми взаємного виключення та передачі даних між процесами	2	
3	**Тема 3. Управління пам'яттю та механізми захисту.** 1. Рівні організації пам'яті в операційних системах (фізична, віртуальна, swap). 2. Механізми сторінкування та сегментації та їх роль у ефективному використанні пам'яті. 3. Принципи роботи системи віртуальної пам'яті та алгоритми її реалізації. 4. Загрози безпеки, пов'язані з помилками управління пам'яттю (buffer overflow, use-after-free). 5. Сучасні механізми захисту пам'яті (DEP, ASLR, SMAP) у операційних системах. 6. Контроль доступу процесів до адресного простору та системної пам'яті	2	
4	**Тема 4. Файлові системи та організація зберігання даних.** 1. Концепція файлової системи та її роль у логічній організації даних на фізичному носії. 2. Типи файлових систем у сучасних операційних системах (ext4, NTFS, APFS, ZFS) та їх відмінності. 3. Принцип журналювання файлової системи та його значення для цілісності та відновлення даних. 4. Структура метаданих файлової системи (атрибути, права, власник, час модифікації). 5. Механізми розширення дискового простору (LVM, динамічні томи, RAID) у різних операційних системах. 6. Надійність, швидкодія та безпека роботи з великими обсягами даних у сучасних операційних системах	2	2
5	**Тема 5. Механізми безпеки та контролю доступу в операційних системах.** 1. Моделі контролю доступу в операційних системах (DAC, MAC, RBAC) та їх порівняльна характеристика. 2. Принцип найменших привілеїв та його реалізація на рівні операційної системи. 3. Різниця між ідентифікацією, автентифікацією та авторизацією користувачів у сучасних ОС. 4. Організація управління обліковими записами та групами користувачів у операційних системах. 5. Система аудиту подій та журналізації дій користувачів і процесів у сучасних операційних системах. 6. Налаштування політик безпеки на рівні операційної системи для захисту від несанкціонованого доступу	2	
6	**Тема 6. Управління конфігурацією та автоматизація системних завдань.** 1. Засоби, що надає операційна система для автоматизації повторюваних системних завдань. 2. Концепція скриптів та їх інтеграція з командним інтерфейсом операційної системи.	2	

	3. Механізми планування завдань у різних операційних системах (cron, Task Scheduler тощо). 4. Використання скриптів для моніторингу, резервного копіювання та відновлення системи. 5. Принципи безпечної роботи зі скриптами (валідація вхідних даних, права виконання, логування). 6. Роль автоматизації у підтримці політик кібербезпеки та забезпеченні неперервності бізнес-процесів		
7	**Тема 7. Віртуалізація, контейнеризація та управління сучасними ІТ-середовищами.** 1. Принципи віртуалізації та її типи (повна, паравіртуалізація, апаратно-прискорена) у сучасних операційних системах. 2. Відмінності між гіпервізорами Type 1 і Type 2 та їх вплив на продуктивність і безпеку. 3. Призначення снепшотів (snapshot) віртуальних машин та їх використання для тестування та відновлення. 4. Відмінність контейнеризації від повної віртуалізації, її переваги та ризики. 5. Використання віртуальних середовищ для моделювання кіберзагроз та тестування систем захисту. 6. Механізми ізоляції, моніторингу та управління ресурсами віртуальних екземплярів у сучасних ІТ-середовищах	2	
	Всього	**14**	**2**

6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Операційні системи» включаються:

1. Знайомство з науковою та навчальною літературою відповідно зазначених у програмі тем.
2. Опрацювання лекційного матеріалу.
3. Підготовка до практичних занять.
4. Консультації з викладачем протягом семестру.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка та виконання індивідуальних завдань у вигляді есе, рефератів тощо.
7. Підготовка до підсумкового контролю.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1. Архітектура та класифікація сучасних операційних систем** Принципи побудови операційних систем: монолітна, мікроядерна, гібридна та модульна архітектури. Класифікація ОС за призначенням: настільні, серверні, вбудовані, мобільні. Роль операційної системи як посередника між апаратними компонентами та прикладним програмним забезпеченням. Моделі виконання завдань: багатозадачність, багатокористувацькість, реального часу. Вплив архітектурних рішень на безпеку, надійність і масштабованість інформаційно-комунікаційних систем (ІКС).	8	15
2	**Тема 2. Механізми управління процесами та потоками виконання** Модель процесу: стан, перехід між станами, контекст, ідентифікатори. Потоки виконання як легковагові процеси. Принципи планування завдань: алгоритми, квантування часу, пріоритети. Синхронізація процесів: умови гонитви, взаємне виключення, семафори, монітори. Вплив нестабільної роботи процесів на безпеку ІКС.	10	15

3	**Тема 3. Управління пам'яттю та механізми захисту** Організація пам'яті: фізична, віртуальна, стрічка обміну. Механізми адресації: сегментація, сторінкування. Принципи роботи системи управління пам'яттю: виділення, звільнення, ізоляція. Проблеми безпеки: витікання пам'яті, використання після звільнення (use-after-free), переповнення буфера. Захист через DEP, ASLR, SMAP.	10	15
4	**Тема 4. Файлові системи та організація зберігання даних** Базові концепції: структури метаданих, inode/еквіваленти, журналювання, журнали транзакцій. Порівняння файлових систем: FAT32, NTFS, ext4, APFS, ZFS. Захист цілісності даних, механізми відновлення після збоїв. Роль файлових систем у реалізації політик резервного копіювання та аудиту.	10	15
5	**Тема 5. Механізми безпеки та контролю доступу в операційних системах** Моделі безпеки: дискреційна (DAC), обов'язкова (MAC), рольова (RBAC). Принцип найменших привілеїв. Механізми автентифікації та авторизації: облікові записи, паролі, токени, PAM, Active Directory, LDAP. Контроль доступу на рівні файлів, процесів, мережі. Аудит та журналізація подій.	10	15
6	**Тема 6. Управління конфігурацією та автоматизація системних завдань** Роль скриптів, сценаріїв та систем автоматизації у підтримці стабільності ОС. Принципи конфігураційного управління: ідемпотентність, версіонування, транзакційність змін. Механізми планування завдань (cron, Windows Task Scheduler). Інтеграція з політиками безпеки: автоматичне оновлення, сканування на вразливості, звітування.	10	15
7	**Тема 7. Віртуалізація, контейнеризація та управління сучасними IT-середовищами** Принципи віртуалізації: типи гіпервізорів (Type 1/Type 2), апаратна підтримка. Контейнеризація як альтернатива повній віртуалізації. Безпека віртуальних середовищ: ізоляція, побічні канали, ескалація привілеїв. Роль віртуальних систем у тестуванні, моделюванні загроз, резервному копіюванні.	10	20
	Всього	**68**	**110**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю	**Складові оцінювання**	
	Для екзамену	**Для заліку**
поточний контроль, який здійснюється у ході: проведення практичних (лабораторних) занять, виконання самостійної роботи, індивідуальних завдань, дослідна робота здобувача тощо.	**50%**	**100%**
підсумковий контроль	**50%**	

Методи діагностики знань (контролю)	**фронтальне опитування; наукова доповідь, реферати, усне повідомлення, індивідуальне опитування; робота у групах; ділова гра, розв`язання ситуаційних завдань, кейсів, практичних завдань,, екзамен**

Питання до екзамену

1. Основні функції, що виконує операційна система у сучасних інформаційно-комунікаційних системах
2. Відмінності між монолітною, мікроядерною та гібридною архітектурами операційних систем
3. Класифікація операційних систем за призначенням (настільні, серверні, вбудовані, мобільні) та їхні особливості
4. Принципи багатозадачності, багатокористувацькості та ізоляції процесів у сучасних операційних системах
5. Роль віртуалізації у розумінні архітектури операційної системи та її вплив на організацію IT-інфраструктури
6. Складові компоненти ядра операційної системи та їх взаємодія з прикладним програмним забезпеченням
7. Поняття процесу та потоку виконання в операційній системі та їх основні атрибути
8. Стани процесу під час життєвого циклу та механізми переходу між станами
9. Алгоритми планування завдань у операційних системах та їх вплив на продуктивність системи
10. Проблема умов гонитви та механізми її уникнення через синхронізацію процесів
11. Ізоляція процесів у сучасних операційних системах та наслідки її порушення
12. Механізми взаємного виключення та передачі даних між процесами
13. Рівні організації пам’яті в операційних системах (фізична, віртуальна, swap)
14. Механізми сторінкування та сегментації та їх роль у ефективному використанні пам’яті
15. Принципи роботи системи віртуальної пам’яті та алгоритми її реалізації
16. Загрози безпеки, пов’язані з помилками управління пам’яттю (buffer overflow, use-after-free)
17. Сучасні механізми захисту пам’яті (DEP, ASLR, SMAP) у операційних системах
18. Контроль доступу процесів до адресного простору та системної пам’яті
19. Концепція файлової системи та її роль у логічній організації даних на фізичному носії
20. Типи файлових систем у сучасних операційних системах (ext4, NTFS, APFS, ZFS) та їх відмінності
21. Принцип журналювання файлової системи та його значення для цілісності та відновлення даних
22. Структура метаданих файлової системи (атрибути, права, власник, час модифікації)
23. Механізми розширення дискового простору (LVM, динамічні томи, RAID) у різних операційних системах
24. Надійність, швидкодія та безпека роботи з великими обсягами даних у сучасних операційних системах
25. Моделі контролю доступу в операційних системах (DAC, MAC, RBAC) та їх порівняльна характеристика
26. Принцип найменших привілеїв та його реалізація на рівні операційної системи
27. Різниця між ідентифікацією, автентифікацією та авторизацією користувачів у сучасних ОС
28. Організація управління обліковими записами та групами користувачів у операційних системах
29. Система аудиту подій та журналізації дій користувачів і процесів у сучасних операційних системах
30. Налаштування політик безпеки на рівні операційної системи для захисту від несанкціонованого доступу
31. Засоби, що надає операційна система для автоматизації повторюваних системних завдань
32. Концепція скриптів та їх інтеграція з командним інтерфейсом операційної системи
33. Механізми планування завдань у різних операційних системах (cron, Task Scheduler тощо)
34. Використання скриптів для моніторингу, резервного копіювання та відновлення системи
35. Принципи безпечної роботи зі скриптами (валідація вхідних даних, права виконання, логування)
36. Роль автоматизації у підтримці політик кібербезпеки та забезпеченні неперервності бізнес-

процесів
37. Принципи віртуалізації та її типи (повна, паравіртуалізація, апаратно-прискорена) у сучасних операційних системах
38. Відмінності між гіпервізорами Type 1 і Type 2 та їх вплив на продуктивність і безпеку
39. Призначення снепшотів (snapshot) віртуальних машин та їх використання для тестування та відновлення
40. Відмінність контейнеризації від повної віртуалізації, її переваги та ризики
41. Використання віртуальних середовищ для моделювання кіберзагроз та тестування систем захисту
42. Механізми ізоляції, моніторингу та управління ресурсами віртуальних екземплярів у сучасних ІТ-середовищах

8. ОЦІНЮВАННЯ ЗДОБУВАЧІВ ВИЩОЇ ТА ФАХОВОЇ ПЕРДВИЩОЇ ОСВІТИ ЗА НАВЧАЛЬНУ ДИСЦИПЛІНУ У МІЖНАРОДНОМУ ГУМАНІТАРНОМУ УНІВЕРСИТЕТІ

(*поточний контроль, підсумковий контроль, загальний результат оцінювання)*

ЕКЗАМЕН

Поточний контроль			
Види роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальний відсоток оцінювання**
Систематичність і активність роботи на практичних (лабораторних) заняттях			
1.1. Підготовка до практичних (лабораторних) занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних (лабораторних) занять	**30**
Виконання завдань для самостійного опрацювання			
1.2. Індивідуальне тестування, завдання, підготовка реферату (есе) за заданою тематикою	Відповідно до робочої програми та розкладу занять	Розгляд відповідного матеріалу під час аудиторних занять або ІКР[1], перевірка конспектів навчальних текстів тощо	**10**
Виконання індивідуальних завдань, дослідна робота здобувача			
1.3. Інші види індивідуальних завдань, в т.ч.підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	Відповідно до робочої програми та розкладу занять	Обговорення результатів проведеної роботи під час аудиторних занять, наукових конференцій та круглих столів.	**10**
Разом балів за поточний контроль			**50**
Підсумковий контроль екзамен			**50**
Загальний результат оцінювання			**100**

Поточний контроль знань здобувачів освіти при формі контролю **екзамен** (максимум 50 балів) оцінюється за шкалою *(«2», «3», «4», «5»)*, з обов'язковим переведенням балів за кожний вид роботи таким чином:

[1] Індивідуально-консультативна робота викладача зі здобувачами

- за підготовку до аудиторних занять (максимум 30 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості практичних (лабораторних) занять, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 6;
- за виконання завдань для самостійного опрацювання (тестування, завдання, підготовка реферату (есе) за заданою тематикою) (максимум 10 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості програмного матеріалу, що виноситься на самостійне вивчення, для переводу зазначених балів середньоарифметична оцінка множиться на коефіцієнт 2;
- за інші види індивідуальних завдань, в т.ч. підготовку наукових публікацій, участь у роботі круглих столів, конференцій тощо (максимум 10- балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості інших видів індивідуальних завдань, для переводу балів за пдготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 2.

КРИТЕРІЇ ОЦІНЮВАННЯ ЗА ПОТОЧНИЙ КОНТРОЛЬ

- «2»- виставляється за неправильну відповідь (письмову роботу), яка не відповідає змісту теми та свідчить про нерозуміння її основних положень;
- «3» -виставляється за відповідь (письмову роботу), яка відповідає змісту теми, але є неповною і неточною у визначенні понять, свідчить про неповне розуміння основних положень навчального матеріалу, свідчить про те, що знання студента мають фрагментарний, поверховий характер;
- «4» - оцінюється правильна і обґрунтована відповідь (письмова робота), з якої видно, що студент знає й розуміє теоретичний матеріал в обсязі навчальної теми, володіє необхідними навичками, не допускає суттєвих помилок.
- «5» - оцінюється повна, правильна, ґрунтовна відповідь (письмова робота) на запитання теми, що передбачає логічність і послідовність викладу матеріалу, володіння термінологією, показує вміння повно й глибоко використовувати теоретичні знання в практичній площині.

КРИТЕРІЇ ОЦІНЮВАННЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ ЗДОБУВАЧІВ ЗА ЕКЗАМЕН
(максимум 50 балів)

Рівень знань оцінюється:

- від 40 до 50 балів - студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки;
- 30 до 40 балів - студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді;
- 20 - 30 балів - студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки.
- 10 - 20 балів - володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих;
- 0 10 балів - володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки.

9. КРИТЕРІЇ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ
(для іспиту / заліку)

Рівень знань оцінюється:

- «відмінно» / «зараховано» А - від 90 до 100 балів. Студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та семінарських заняттях, під час

яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

- «добре» / «зараховано» B - від 82 до 89 балів. Студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та семінарських заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» C - від 74 до 81 балів. Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, реферату та активність у науково-дослідній роботі;
- «задовільно» / «зараховано» D - від 64 до 73 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, рефератів (есе);
- «задовільно» / «зараховано» E - від 60 до 63 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, має неповний конспект з завданнями до самостійної роботи.
- «незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів. Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.
- «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 0 до 34 балів. Студент не володіє навчальним матеріалом.

ТАБЛИЦЯ ВІДПОВІДНОСТІ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗА РІЗНИМИ ШКАЛАМИ

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	
74-81	C		
64-73	D	Задовільно	
60-63	E		
35-59	Fx	Незадовільно	Не зараховано
1-34	F		

10. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Матвєєва Н.О. Основи роботи та програмування в операційній системі Linux: навчальний посібник /Н.О. Матвєєва, В.С. Хандецький, О.В. Спірінцева – Д.: ЛІРА, 2018, −156 с.
2. Педяш В. В. Йона Л. Г., Мазур Г. Д.. Операційні системи : метод. реком. для практичних та лабораторних занять [Електронне видання] / Кафедра комп'ютерної інженерії та інноваційних технологій Міжнародного гуманітарного університету. — Одеса, 2025. — 121 с. — Режим доступу: https://hdl.handle.net/11300/32283

3. Харченко В. П., Знаковська Є. А., Бородін В. А. Операційні системи та системи програмування: навч. посіб /В. П. Харченко, Є. А. Знаковська, В. А. Бородін – К.: Вид-во Нац. авіац. ун-ту «НАУ-друк», 2012.– 360с.
4. Авраменко В. С., Авраменко А. С. Основи операційних систем. Навчальний посібник. – Черкаси: ЧНУ імені Богдана Хмельницького, 2018. – 524 с.
5. Погребняк Б. І. Операційні системи : навч. посібник / Б. І. Погребняк, М. В. Булаєнко ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2018. – 104 с.
6. 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.

Допоміжна

7. Silberschatz A., Galvin P. B., Gagne G. Operating System Concepts / A. Silberschatz, P. B. Galvin, G. Gagne. – 10th ed. – Hoboken, NJ : John Wiley & Sons, 2018. – 976 p.
8. Tanenbaum A. S., Bos H. Modern Operating Systems / A. S. Tanenbaum, H. Bos. – 4th ed. – Boston : Pearson Education, 2015. – 1136 p.
9. Stallings W. Operating Systems: Internals and Design Principles / W. Stallings. – 9th ed. – Boston : Pearson Education, 2018. – 864 p.
10. Arpaci-Dusseau R. H., Arpaci-Dusseau A. C. Operating Systems: Three Easy Pieces / R. H. Arpaci-Dusseau, A. C. Arpaci-Dusseau. – Madison, WI : Arpaci-Dusseau Books, 2018. – 720 p.

Інформаційні ресурси

11. Національна бібліотека України ім. В.І. Вернадського : веб-сайт. URL: http://www.nbuv.gov.ua.
12. Он-лайн бібліотека. URL: http://www.lib.com.ua
13. Dive into Systems. URL: https://diveintosystems.org/
14. Open Textbook Library. URL: https://open.umn.edu/opentextbooks
15. Directory of Open Access Books (DOAB). URL: https://www.doabooks.org/
16. LWN.net (Linux Weekly News). URL: https://lwn.net/