ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету IT
Підпис Олег САВЕНКО
Ім'я, ПРІЗВИЩЕ
«27» 08 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Операційні системи та технології їх захисту

Галузь знань	12 – Інформаційні технології
Спеціальність	125 – Кібербезпека та захист інформації
Рівень вищої освіти	Перший бакалаврський
Освітньо-професійна програма	Кібербезпека та захист інформації
Обсяг дисципліни	5 кредитів ЄКТС
Шифр дисципліни	ОПП.02
Мова навчання	Українська
Статус дисципліни	Обов'язкова, дисципліна професійної підготовки
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Очна (денна)	1	2	5	150	72	36	36			78			+	

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека та захист інформації» першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації»

Робоча програма складена _____ канд. техн. наук, доц. Юрій КЛЬОЦ

_____ Наталія ПЕТЛЯК
Підпис(и) автора(ів) Ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 31.08.2023 № 1 Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2023

ОПЕРАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ ЇХ ЗАХИСТУ

Тип дисципліни	Обов'язкова
Освітній рівень	Перший (бакалаврський)
Мова викладання	Українська
Семестр	Другий
Кількість встановлених кредитів ЄКТС	5
Форми навчання, для яких викладається дисципліна	Очна денна

Студент, який успішно завершив вивчення дисципліни, повинен: *використовувати* програмні та програмно-апаратні комплекси захисту інформаційних ресурсів в операційних системах, *забезпечувати* функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в операційних системах; *використовувати* інформаційно-комунікаційні технології, сучасні методи і моделі інформаційної безпеки та/або кібербезпеки, теорії та методи захисту для забезпечення операційних систем; *реалізовувати* заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в операційних системах за рахунок вирішення задач управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів згідно встановленої політики інформаційної і/або кібербезпеки; *вирішувати* задачі управління процесами відновлення штатного функціонування операційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження з використанням процедур резервування згідно встановленої політики безпеки.

Зміст навчальної дисципліни: Призначення і функції ОС, як складові захисту інформації. Управління процесами. Управління пам'яттю. Управління файлами і зовнішніми пристроями. Захист даних і адміністрування. Інтерфейс прикладного програмування. Інтерфейс користувача. Мережеві та розподілені ОС. Функціональні компоненти мережевої ОС. Мережеві служби і мережеві сервіси. Варіанти впровадження мережевих служб в ОС. Огляд особливостей ОС для різних класів обчислювальних пристроїв. Архітектура ОС. Ядро і допоміжні модулі ОС. Сучасні вимоги, що висуваються до захищених операційних систем. Порушення політики інформаційної безпеки ОС. Несанкціонований доступ. Незаконне використання привілеїв. Атаки типу: "салямі", "приховані канали", "маскарад", "збір сміття" та "злам системи". Шкідливе програмне забезпечення. Джерела розповсюдження комп'ютерних вірусів. Класифікація та систематизація комп'ютерних вірусів. Технології боротьби з вірусами в операційних системах. Апаратні та програмні технології ідентифікації. Біометричні технології ідентифікації. Реалізація безпеки в операційній системі Windows. Аудит безпеки операційної системи Windows. Файлові системи операційної системи Windows. Реалізація безпеки в операційній системі Linux. Технології підвищення рівня захищеності операційної системи Linux. Організація безпеки операційної системи Android. Організація безпеки операційної системи iOS.

Пререквізити: алгоритмізація та програмування, основи інформаційної безпеки.

Кореквізити: безпека вебресурсів, захист інформації в інформаційно-комунікаційних системах

Запланована навчальна діяльність: лекцій 36 год, лабораторних робіт 36 год., самостійної роботи 78 год., разом 150 год.

Методи навчання: пояснювально-ілюстративні, практичні, продуктивні, застосування інформаційно-комп'ютерних технологій (інструменти та утиліти ОС Windows та Linux Ubuntu).

Форми оцінювання результатів навчання: усне опитування, письмова контрольна робота, захист лабораторних робіт, тестування, підсумковий контрольний захід (семестровий контроль).

Вид семестрового контролю: залік.

Навчальні ресурси

1. Авраменко В.С., Авраменко А.С. Основи операційних систем: навч. посіб. Черкаси: ЧНУ ім. Богдана Хмельницького, 2018. 524 с.
2. Інформаційна безпека: навч. посіб. / Ю. Я. Бобало та ін.; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. Львів: Видавництво Львівської політехніки, 2019. 580 с.
3. Жаровський Р.О. Захист інформації у комп'ютерних системах: консп.лекц. Тернопіль: ТНТУ імені Івана Пулюя, 2019. 268с.
4. Операційна ситема Linux: принципи роботи з файловою системою: навч.посіб. / Черевик В.М., Танцюра Л.І., Коротков С.С., Сосновий В.О. Київ: ДУТ, 2021. 147 с.
5. Операційні системи: навч. посіб. / Федотова-Півень І. М., Миронець І. В., Півень О. Б., Сисоєнко С. В., Миронюк Т. В.; за ред. В. М. Рудницького. Харків: ТОВ «ДІСА ПЛЮС», 2019. 216 с.

Викладач: Петляк Н.С.

ВСТУП

Дисципліна “Операційні системи та технології їх захисту” - складова професійної підготовки бакалаврів зі спеціальності «Кібербезпека та захист інформації».

Метою дисципліни є забезпечити здатність студентів визначати загрози безпеці інформації в сучасних операційних системах, обґрунтовано обирати і грамотно налаштовувати засоби захисту в сучасних операційних системах.

Предметом дисципліни є основні методи та алгоритми захисту інформації в сучасних операційних системах, методи та засоби управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в операційних системах.

Завдання дисципліни. Забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до Стандарту вищої освіти та освітньо-професійної програми підготовки бакалаврів зі спеціальності „Кібербезпека”:

компетентності:

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

результати навчання:

РН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

РН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

РН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

РН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки.

РН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

Студент, який успішно завершив вивчення дисципліни, повинен: *використовувати* програмні та програмно-апаратні комплекси захисту інформаційних ресурсів в операційних системах, *забезпечувати* функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в операційних системах; *використовувати* інформаційно-комунікаційні технології, сучасні методи і моделі інформаційної безпеки та/або кібербезпеки, теорії та методи захисту для забезпечення операційних систем; *реалізовувати* заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в операційних системах за рахунок вирішення задач управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів згідно встановленої політики інформаційної і/або кібербезпеки; *вирішувати* задачі управління процесами відновлення штатного функціонування операційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження з використанням процедур резервування згідно встановленої політики безпеки.

СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин відведених на:		
	лекції	лабораторні роботи	самостійну роботу
Тема 1. Призначення, функції та архітектури операційних систем	12	8	16
Тема 2. Інформаційна безпека операційних систем	6	8	18
Тема 3. Реалізація безпеки в операційній системі Windows	8	12	20
Тема 4. Реалізація безпеки в операційній системі Linux	6	8	12
Тема 5. Реалізація безпеки в мобільних операційних системах	4	0	12
Разом:	**36**	**36**	**78**

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
Тема 1. Призначення, функції та архітектури операційних систем		
1	**Поняття операційної системи** 1. Призначення та функції 2. Класифікація сучасних операційних систем 3. Архітектурні особливості будови сучасних операційних систем 4. Операційні системи Windows, Unix і Linux - архітектура та порівняльний аналіз Літ.: [1] с.59-78 [5] с.8-35,123-144 [7] с.5-12, 21-26, [9] с.7-17 [10] с.13-28	2
2	**Файлові системи операційних систем** 1. Файлові системи FAT, NTFS 2. Архітектура файлової системи EFS 3. Файлові системи exFAT, Ext4, BtrFS, ReiserFS, XFS, JFS 4. RAID-масиви Літ.: [1] с.474-506 [5] с.105-121[7] с.29-33 [9] с.186-219 [10] с.35-59	2
3	**Технології віртуалізації** 1. Віртуалізація операційних систем 2. Віртуалізація програмного забезпечення 3. Віртуалізація інфраструктури 4. Віртуалізація віддалених робочих столів 5. Віртуалізація систем зберігання даних 6. Віртуалізація мережі Літ.: [10] с.85-90, [30] с.27-52	2
4	**Процеси в операційних системах** 1. Основні відомості про процеси. 2. Управління процесами 3. Взаємодія процесів Літ.:[1] с.67-69, [5] с.36-70, [12] с.31-38	2
5	**Потоки в операційних системах** 1. Основні операції з потоками 2. Способи реалізації 3. Стани потоків Літ.: [5] с. 73-78, [12] с.78-82	2
6	**Керування пам'яттю в операційних системах** 1. Функції операційної системи по керуванню пам’яттю 2. Технології розподілу пам’яті 3. Віртуальна пам’ять Літ.: [5] с.84-104, [12] с. 112-140	2
Тема 2. Інформаційна безпека операційних систем		
7	**Сутність проблеми захисту операційних систем** 1. Вимоги, що висуваються до захищених операційних систем 2. Поняття та призначення політики інформаційної безпеки 3. Порушення політики інформаційної безпеки 4. Атаки на рівні операційної системи Літ.: [2] с.11-39 [3] с.5-60 [6] с.23-60 [22] с.593-602	2
8	**Технології боротьби з вірусами в операційних системах** 1. Ознаки інфікованої операційної системи 2. Технології виявлення вірусів 3. Класифікація антивірусного програмного забезпечення Літ.: [2] с.463-499 [3] с.240-256 [6] с.71-87	2

9	**Сучасні технології ідентифікації користувачів операційних систем** 1. Парольна технологія ідентифікації 2. Апаратна технологія ідентифікації 3. Біометрична технологія ідентифікації 4. Багатофакторна ідентифікація Літ.: [2] с.272-278 [3] с.94-114 [6] с.53-60	2
Тема 3. Реалізація безпеки в операційній системі Windows		
10	**Організація безпеки операційної системи Windows** 1. Компоненти системи захисту операційної системи Windows 2. Механізм захисту об'єктів операційної системи Windows 3. Аудит безпеки операційної системи Windows Літ.: [22] с.966-975 Літ.: [3] с.256-268 [21] с.383-407	2
11	**Конфігурація та моніторинг операційної системи Windows** 1. Запуск від імені адміністратора, локальні користувачі та домени 2. CLI і PowerShell 3. Інструмент керування Windows, диспетчер завдань і монітор ресурсів 4. Доступ до мережевих ресурсів, порти і служби Windows 5. Windows Server Літ.: [8][14]	2
12	**Політики безпеки операційної системи Windows (частина 1)** 1. Політики облікових записів 2. Локальні політики 3. Монітор брандмауера для програми Windows Defender 4. Політика диспетчера списку мереж Літ.: [8] [11] [26]	2
13	**Політики безпеки операційної системи Windows: (частина 2)** 1. Політика відкритого ключа 2. Політика управління додатками 3. Політика IP-безпеки на «Локальний комп'ютер» 4. Конфігурація розширеної політики аудиту Літ.: [11] [15]	2
Тема 4. Реалізація безпеки в операційній системі Linux		
14	**Організація безпеки операційної системи Linux** 1. Модель безпеки операційної системи Linux 2. Підсистема ідентифікації та аутентифікації 3. Підсистема розмежування доступу 4. Монітор безпеки Літ.: [4] с.75-84 [10] с.31-33,90-102 [22] с. 798-802 [8] [16]	2
15	**Технології підвищення рівня захищеності операційної системи Linux** 1. Linux з покращеним рівнем безпеки (SELinux) 2. Система мандатного контролю доступу AppArmor 3. Система забезпечення мандатного контролю доступу TOMOYO Linux 4. Резервування в ОС Linux Літ.: [1] с.31-34 [13] с. 96-118	2
16	**Робота на хості Linux** 1. Порти і служби 2. Процеси 3. Зловмисне програмне забезпечення на хості Linux 4. Перевірка руткіта Літ.: [8] [1] с.167-197	2
Тема 5. Реалізація безпеки в мобільних операційних системах		
17	**Організація безпеки операційної системи Android** 1. Модель безпеки операційної системи Android 2. Ідентифікації та аутентифікації	2

	3. Розмежування доступу 4. Стандартні та спеціальні дозволи Літ.: [1] с.50-52 [5] с.30-36 [22] с.838-844	
18	**Організація безпеки операційної системи iOS** 1. Архітектура операційної системи iOS 2. Модель безпеки операційної системи iOS 3. Характеристика функціонування компонентів Secure Enclave та TouchID Літ.: [1] с.50-56 [7] с. 54-58	2
	Разом за семестр:	**36**

Перелік лабораторних робіт

№ п/п	Теми лабораторних робіт	Кількість годин
1	Дослідження операційних систем Windows та Linux. Налаштування, командний рядок, системні функції роботи з процесами та віртуальною пам'яттю. Літ.: [1] с. 128-150, [9] с. 25-30	4
2	Робота з Bat файлами Літ.: [2] с. 80-90, [7] с. 10-12, [10] с. 20-25	4
3	Знайомство та базові операції з Power Shell Літ.: [7] с. 20-30, [9] с. 35-40	4
4	Командалети PowerShell для адміністрування ОС Windows Літ.: [7] с. 17-28, [9] с. 34-45	4
5	Редактор vi в ОС Ubuntu Літ.: [5] с.67-70, [4] с. 35-50	4
6	Дослідження технології захисту цілісності даних Raid Літ.: [15] с. 50-70	4
7	Розмежування прав доступу в UNIX та Windows. Права доступу до файлів і керування ними. Літ.: [4] с. 53-71, [6] с. 112-128, [3] с. 112-120, [32] [33]	4
8	Налаштування аудиту в UNIX та Windows Літ.: [3] с. 152-180, [13], [34]	4
9	Підсумкове заняття. Тестування.	4
	Разом за семестр:	**36**

Зміст самостійної (індивідуальної) роботи

Об'єм самостійної роботи з дисципліни "Операційні системи та технології їх захисту" становить 78 годин. Він включає опрацювання теоретичного матеріалу (лекційного, методичних вказівок та літературних джерел), підготовку до тестування, виконання практичних завдань, підготовку до виконання та захисту лабораторних робіт. Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час, в тому числі із застосуванням технологій інтерактивного та дистанційного навчання.

Номер тижня	Теми самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу лекції №1. Підготовка до виконання лабораторної роботи №1.	4
2	Опрацювання теоретичного матеріалу лекції №2. Підготовка до виконання лабораторної роботи №1.	4
3	Опрацювання теоретичного матеріалу лекції №3. Підготовка до виконання лабораторної роботи №2. Підготовка до захисту лабораторної роботи №1.	4
4	Опрацювання теоретичного матеріалу лекції №4. Підготовка до виконання лабораторної роботи №2. Підготовка до захисту лабораторної роботи №1.	4
5	Опрацювання теоретичного матеріалу лекції №5. Підготовка до виконання лабораторної роботи №3. Підготовка до захисту лабораторної роботи №2.	5
6	Опрацювання теоретичного матеріалу лекції №6. Підготовка до виконання лабораторної роботи №3. Підготовка до захисту лабораторної роботи №2. Підготовка до контрольної роботи №1.	5
7	Опрацювання теоретичного матеріалу лекції №7. Підготовка до виконання лабораторної роботи №4. Підготовка до захисту лабораторної роботи №3.	4
8	Опрацювання теоретичного матеріалу лекції №8. Підготовка до виконання лабораторної роботи №4. Підготовка до захисту лабораторної роботи №3.	4
9	Опрацювання теоретичного матеріалу лекції №9. Підготовка до виконання лабораторної роботи №5. Підготовка до захисту лабораторної роботи №4. Підготовка до контрольної роботи №2.	4
10	Опрацювання теоретичного матеріалу лекції №10. Підготовка до виконання лабораторної роботи №5. Підготовка до захисту лабораторної роботи №4.	4
11	Опрацювання теоретичного матеріалу лекції №11. Підготовка до виконання лабораторної роботи №6. Підготовка до захисту лабораторної роботи №5.	4
12	Опрацювання теоретичного матеріалу лекції №12. Підготовка до виконання лабораторної роботи №6. Підготовка до захисту лабораторної роботи №5.	4
13	Опрацювання теоретичного матеріалу лекції №13. Підготовка до виконання лабораторної роботи №7. Підготовка до захисту лабораторної роботи №6. Підготовка до контрольної роботи №3.	4
14	Опрацювання теоретичного матеріалу лекції №14. Підготовка до виконання лабораторної роботи №7. Підготовка до захисту лабораторної роботи №6.	4
15	Опрацювання теоретичного матеріалу лекції №15. Підготовка до виконання лабораторної роботи №8. Підготовка до захисту лабораторної роботи №7.	4
16	Опрацювання теоретичного матеріалу лекції №16. Підготовка до виконання лабораторної роботи №8. Підготовка до захисту лабораторної роботи №7. Підготовка до контрольної роботи №4.	4
17	Опрацювання теоретичного матеріалу лекції №17. Підготовка до захисту лабораторної роботи №8. Підготовка до тестування.	6
18	Опрацювання теоретичного матеріалу лекції №18. Підготовка до захисту	6

	лабораторної роботи №8. Підготовка до тестування.	
	Разом за семестр:	**78**

ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться пояснювально-ілюстративними методами з супроводом презентаційних матеріалів, лабораторні заняття проводяться практичними, продуктивними методами, з використанням інформаційно-комп'ютерних технологій (інструменти та утиліти ОС Windows та Linux Ubuntu, емулятори ОС мобільних пристроїв, тощо) і мають за мету – набуття студентами практичних навичок визначення загроз безпеці інформації в сучасних операційних системах, налаштування засобів захисту в сучасних операційних системах.

Застосовувані при викладанні дисципліни методи навчання сприяють розвитку у студентів навичок soft skills: прилюдні захисти лабораторних робіт з обґрунтуванням прийнятих рішень щодо вибору методів рішення завдань в діалозі з викладачем і групою сприяють формуванню і удосконаленню вмінь публічних виступів, емпатичного слухання, відстоювання власної точки зору, самоаналізу і самокритики; адаптованість, вміння користуватися інтернет-ресурсами та іншими джерелами інформації, синтезувати та критично осмислювати інформацію з різних джерел передбачені специфікою дисципліни; обмежений час на виконання лабораторних робіт, контрольних завдань, чітко визначені і надані в силабусі терміни проходження контрольних точок і відпрацювання заборгованостей сприяють розвитку пунктуальності, здатності до самоорганізації та управління часом (тайм-менеджменту).

При вивченні дисципліни можуть бути зараховані результати навчання, здобуті у неформальній освіті. Визнання результатів навчання, здобутих у неформальній освіті, реалізується згідно з чинним законодавством і регулюється Положеннях про порядок визнання та перезарахування результатів навчання здобувачів вищої освіти у ХНУ https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-poryadok-vyznannya-ta-perezarahuvannya-rezultativ-navchannya.pdf

МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни.

При цьому використовуються такі методи поточного контролю:

- усне опитування;
- захист лабораторних робіт;
- тестування.

Семестровий контроль проводиться у формі заліку. При виведенні підсумкової семестрової оцінки враховуються результати поточного контролю (залік за рейтингом формується автоматично за результатами поточного контролю).

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів за ваговими коефіцієнтами

	Аудиторна робота	**Самостійна робота**		**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Тестовий контроль	Контрольна робота	Залік за рейтингом
Тема	1-5	1-5	1-4	
Ваговий коефіцієнт	0,4	0,4	0,2	

Оцінювання лабораторних робіт. Оцінка, яка виставляється за лабораторне заняття, складається з таких елементів: усне опитування студентів перед допуском до виконання лабораторної роботи; знання теоретичного матеріалу з теми; якість оформлення звіту; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної роботи.

Термін захисту звіту з лабораторної роботи вважається своєчасним, якщо студент захистив її в день виконання або на наступному після виконання роботи занятті. Пропущене лабораторне заняття студент зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку за лабораторне заняття викладач оголошує одразу після захисту звіту з лабораторної роботи і проставляє в електронний журнал дисципліни.

Оцінювання контрольної роботи. Контрольна робота складається з теоретичного питання та практичного завдання. Оцінювання здійснюється за чотирибальною шкалою. Оцінку «відмінно» отримує студент який дав повну письмову відповідь на теоретичне питання та правильно виконав поставлене практичне завдання. Оцінку «добре» отримує студент, який допустив дві-три несуттєві помилки при відповіді на теоретичне питання та правильно виконав поставлене практичне завдання. Оцінку «задовільно» отримує студент, який дав лише часткову відповідь на теоретичне питання або допустив суттєві помилки при виконанні практичного завдання. Оцінку «незадовільно» отримує студент, який не зміг виконати практичне завдання або не дав відповіді на теоретичне питання. Оцінку за контрольну роботу викладач проставляє в електронний журнал дисципліни не пізніше ніж через десять днів після проведення контрольного заходу.

Оцінювання тестових завдань. Тематичний тест для кожного студента складається з двадцяти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 20.

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту

Сума балів за тестове завдання	1–10	11–14	15–17	18–20
Оцінка за 4-ри бальною шкалою	2	3	4	5

На тестування відводиться 20 хвилин (для закритої форми тестів – по одній хвилині на кожне завдання). Правильні відповіді студент записує у талоні відповідей. При цьому усі графи для відповідей мають бути заповнені цифрами, що відповідають правильним, на погляд студента, відповідям. Через 20 хвилин студенти здають викладачу завдання з талонами відповідей.

Тестування студент може також пройти і в онлайн-режимі в модульному середовищі для навчання MOODLE.

Оцінку за тестування викладач проставляє в електронний журнал дисципліни не пізніше ніж через 10 днів після проходження тестування.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями оцінювання знань.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	**Узагальнений критерій**
Відмінно	Студент глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає, логічний виклад відповіді державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві–три несуттєві помилки.
Задовільно	Студент виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, допускає неточності і суттєві помилки у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно	Студент виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка "незадовільно" виставляється студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка «задовільно».

Студент, який у встановлені терміни не виконав індивідуальний план поточної роботи з дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

Залік вважається зданим при отриманні студентом за зведеними результатами поточного контролю підсумкової оцінки з дисципліни від 3,00 до 5,00 балів. При цьому за вітчизняною шкалою ставиться оцінка за двобальною шкалою, а за шкалою ECTS – оцінка, що відповідає набраній студентом кількості балів.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Інституційна інтервальна шкала балів**	**Інституційна оцінка, критерії оцінювання**		
A	4,75–5,00	5	Зараховано	***Відмінно*** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4		***Добре*** – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4		***Добре*** – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3		***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24	3		***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	Незараховано	***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2		***Незадовільно*** – необхідна серйозна подальша робота і повторне вивчення дисципліни

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ
ЗДОБУТИХ СТУДЕНТАМИ РЕЗУЛЬТАТІВ НАВЧАННЯ

1. Призначення та функції.
2. Класифікація сучасних операційних систем.
3. Тенденції в розвитку ОС.
4. Технології проектування.
5. Основні поняття концепції операційної системи.
6. Архітектурні особливості будови сучасних операційних систем.
7. Операційні системи Windows, Unix і Linux - архітектура та порівняльний аналіз.
8. Складові частини ядра.
9. Підходи до проектування ядра.
10. Багаторівневі системи.
11. Змішані системи.
12. Файлова система FAT.
13. Файлова система NTFS.
14. Архітектура файлової системи EFS.
15. Файлові системи exFAT, Ext4, BtrFS, ReiserFS, XFS, JFS.
16. Технології віртуалізації
17. Процеси
18. Потоки
19. Керування пам’яттю
20. RAID-масиви
21. Вимоги, що висуваються до захищених операційних систем.
22. Поняття та призначення політики інформаційної безпеки.
23. Порушення політики інформаційної безпеки.
24. Атаки на рівні операційної системи.
25. Несанкціонований доступ.
26. Незаконне використання привілеїв.
27. Атаки типу: "салямі", "приховані канали", "маскарад", "збір сміття" та "злам системи".
28. Шкідливе програмне забезпечення.
29. Ознаки інфікованої операційної системи.
30. Технології виявлення вірусів.
31. Класифікація антивірусного програмного забезпечення.
32. Парольна технологія ідентифікації.
33. Апаратна технологія ідентифікації.
34. Біометрична технологія ідентифікації.
35. Багатофакторна ідентифікація.
36. Компоненти системи захисту ОС Windows.
37. Механізм захисту об’єктів ОС Windows.
38. Ідентифікатор захисту.
39. Маркери доступу.
40. Дескриптори захисту.
41. Права та привілеї (суперпривілеї) облікових записів.
42. Типові права користувачів ОС Windows.
43. Категорії аудиту безпеки.
44. Процес входу користувача в операційну систему.
45. Політика обмеженого використання програм.
46. Резервування в ОС Windows
47. Запуск від імені адміністратора, локальні користувачі та домени.
48. CLI і PowerShell.
49. Інструмент керування Windows, диспетчер завдань і монітор ресурсів.
50. Доступ до мережевих ресурсів.
51. Windows Server.

52. Політики облікових записів.
53. Локальні політики.
54. Монітор брандмауера для програми Windows Defender.
55. Політика диспетчера списку мереж.
56. Політика відкритого ключа.
57. Політика управління додатками.
58. Політика IP-безпеки на «Локальний комп'ютер».
59. Конфігурація розширеної політики аудиту.
60. Модель безпеки операційної системи Linux.
61. Підсистема ідентифікації та аутентифікації.
62. Підсистема розмежування доступу.
63. Монітор безпеки.
64. Linux з покращеним рівнем безпеки (SELinux).
65. Система мандатного контролю доступу AppArmor.
66. Система забезпечення мандатного контролю доступу TOMOYO Linux.
67. Резервування в ОС Linux.
68. Процеси та форки.
69. Зловмисне програмне забезпечення на хості Linux.
70. Перевірка руткіта.
71. Модель безпеки ОС Android.
72. Ідентифікації та аутентифікації.
73. Розмежування доступу.
74. Стандартні та спеціальні дозволи.
75. Архітектура операційної системи iOS.
76. Модель безпеки операційної системи iOS.
77. Характеристика функціонування компонентів Secure Enclave та TouchID.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни “Операційні системи та технології їх захисту” повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, розміщеною в електронному варіанті в модульному середовищі.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Авраменко В.С., Авраменко А.С. Основи операційних систем: навч. посіб. Черкаси: ЧНУ ім. Богдана Хмельницького, 2018. 524 с.
2. Інформаційна безпека: навч. посіб. / Ю. Я. Бобало та ін.; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. Львів: Видавництво Львівської політехніки, 2019. 580 с.
3. Жаровський Р.О. Захист інформації у комп’ютерних системах: консп.лекц. Тернопіль: ТНТУ імені Івана Пулюя, 2019. 268с.
4. Операційна ситема Linux: принципи роботи з файловою системою: навч.посіб. / Черевик В.М., Танцюра Л.І., Коротков С.С., Сосновий В.О. Київ: ДУТ, 2021. 147 с.
5. Операційні системи: навч. посіб. / Федотова-Півень І. М., Миронець І. В., Півень О. Б., Сисоєнко С. В., Миронюк Т. В.; за ред. В. М. Рудницького. Харків: ТОВ «ДІСА ПЛЮС», 2019. 216 с.
6. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки: навч. посіб. Дніпро: Дніпроп. держ.ун-т внутріш. справ, 2020. 128 с.
7. Гаркуша І.М. Операційні системи: конспект лекцій. Дніпро: НТУ «ДП», 2020. 73 с.
8. CyberOps Associate. URL: https://contenthub.netacad.com/cyberops (дата звернення: 30.08.2023)
9. Зайцев В.Г., Дробязко І.П. Операційні системи. Лабораторний практикум: навч.посіб. Київ: КПІ ім. І. Сікорського, 2018. 88 с.
10. Погребняк Б. І., Булаєнко М. В. Операційні системи: навч. посіб. Харків: ХНУМГ ім. О. М. Бекетова, 2018. 104 с.

Додаткова

11. Configure security policy settings. URL: https://docs.microsoft.com/uk-ua/windows/security/threat-protection/security-policy-settings/how-to-configure-security-policy-settings (дата звернення: 30.08.2023)
12. Зайцев В. Г., Дробязко І. П.. Операційні системи: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2019. 240 с.
13. Горбань Г. В., Кандиба І. О. Операційна система Linux : навч. посіб. Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2019. 276 с.
14. Security configuration guidance support. URL: https://support.microsoft.com/en-us/topic/security-configuration-guidance-support-ea9aef24-347f-15fa-b94f-36f967907f2f (дата звернення 29.08.2023)
15. Advanced security audit policies. URL: https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings (дата звернення 15.08.2023)
16. Путівник по Linux. Адміністрування системи. URL: https://cutt.ly/4CyDqCT (дата звернення 5.08.2023)
17. NTFS overview. URL: https://docs.microsoft.com/en-us/windows-server/storage/file-server/ntfs-overview (дата звернення 20.08.2023)
18. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посіб. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 144 с.
19. Security auditing. URL: https://docs.microsoft.com/uk-ua/windows/security/threat-protection/auditing/security-auditing-overview (дата звернення 25.08.2023)
20. Linux Essentials. URL: https://learning.lpi.org/pdfstore/LPI-Learning-Material-010-160-uk.pdf (дата звернення: 20.07.2023)
21. Менеджмент інформаційної безпеки : навч. посіб. / О.Г. Корченкота ін. Ніжин: ФОП

Лук'яненко В.В. ТПК «Орхідея», 2019. 408 с
22. Tanenbaum A., Bos H.. Modern operating systems. Fourth edition. Amsterdam: Vrije Universiteit, The Netherlands, 2016. 1137 pages
23. Security policy settings. URL: https://docs.microsoft.com/uk-ua/windows/security/threat-protection/security-policy-settings/security-policy-settings (дата звернення: 15.08.2023)
24. Мосіюк О. О., Федорчук А. Л. Операційні системи та системне програмування: навч.-метод. посіб. Житомир: Вид-во ЖДУ ім. Івана Франка, 2022. 76 с.
25. RAID-масиви. URL: https://stud.com.ua/97217/informatika/raid_masivi (дата звернення: 15.08.2023)
26. Help protect my PC with Microsoft Defender Offline. URL: https://support.microsoft.com/en-us/windows/help-protect-my-pc-with-microsoft-defender-offline-9306d528-64bf-4668-5b80-ff533f183d6c (дата звернення: 12.08.2023)
27. Тарарака В.Д.. Архітектура комп'ютерних систем: навч. посіб. - Житомир: ЖДТУ, 2018. 383 с.
28. M. Helmke, A. Hudson, P. Hudson. Ubuntu, Indiana, 2019. 756 с.
29. A. Miroshnikov. Windows® Security Monitoring: Scenarios and Patterns. Canada: John Wiley & Sons, 2018. 614 pages
30. Костюченко А.О., Горошко Ю.В. Віртуалізація операційних систем: навчально-методичний посібник. Ч.: ФОП Баликіна С.М., 2021. 56 с.
31. Жихаревич В.В. Операційні системи: лабораторний практикум. – Чернівці: ЧНУ, „Рута, 2018. – 248 с.
32. Anna Ilyenko, Sergiy Ilyenkko, Tatiana Kulish, Перспективні методи захисту операційної системи Windows. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/162/156
33. Булатецький Віталій Вікторович, Булатецька Леся Віталіївна, Гришанович Тетяна Олександрівна АНАЛІЗ ФАЙЛОВИХ ОБ'ЄКТІВ ОПЕРАЦІЙНОЇ СИСТЕМИ WINDOWS 10 ДЛЯ ОЧИЩЕННЯ Й ОПТИМІЗАЦІЇ ПРОСТОРУ СИСТЕМНОГО РОЗДІЛУ URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/336/279

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання. URL: https://msn.khmnu.edu.ua/ .
2. Електронна бібліотека університету. URL: http://library.khmnu.edu.ua/ .