ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра кібербезпеки

ЗАТВЕРДЖУЮ
Декан ФІТ
_____ Тетяна ГОВОРУЩЕНКО
«31» серпня 2024 р.

СИЛАБУС

Навчальна дисципліна: "*Операційні системи та технології їх захисту*"

Освітньо-професійна програма: «Кібербезпека та захист інформації»

Рівень вищої освіти: перший (бакалаврський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Петляк Наталія Сергіївна
Профайл викладач(ів)	https://kb.khmnu.edu.ua/petlyak-nataliya-sergiyivna/
E-mail викладача(ів)	npetlyak@khmnu.edu.ua
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/course/view.php?id=8126
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us02web.zoom.us/j/88595100831 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2024-2025, семестр II (зимово-весняний)
Консультації	Очні: згідно графіку консультацій Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

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			+	

Анотація дисципліни

Дисципліна викладається для студентів очної денної форми навчання спеціальності «Кібербезпека та захист інформації». При викладанні дисципліни використовуються наступні форми (методи) навчання: словесні та наочні (лекції); практичні та застосування інформаційно-комп'ютерних технологій (лабораторні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

Пререквізити: алгоритмізація та програмування, основи інформаційної безпеки.

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

Мета і завдання дисципліни

Метою викладання навчальної 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.

Завданням дисципліни є забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до Стандарту вищої освіти та освітньо-професійної програми підготовки бакалаврів зі спеціальності „Кібербезпека та захист інформації”:

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.

Тематичний і календарний план вивчення дисципліни

№ тижня	Тема лекції*	Тема лаб. роботи **	Самостійна роботи		
			Зміст	Год.	Література
1	**Тема 1. Призначення, функції та архітектури операційних систем** Поняття операційної системи	**ЛР1.** Дослідження операційних систем Windows та Linux. Налаштування, командний рядок, системні функції роботи з процесами та віртуальною пам'яттю	Опрацювання теоретичного матеріалу лекції №1.	4	[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	**Тема 1. Призначення, функції та архітектури операційних систем** Файлові системи операційних систем	**ЛР1.** Підгрупа 2	Опрацювання теоретичного матеріалу лекції №2. Підготовка до виконання лабораторної роботи №1	4	[1] с.474-506 [5] с.105-121 [7] с.29-33 [9] с.186-219 [10] с.35-59 [1] с. 128-150 [9] с. 25-30
3	**Тема 1. Призначення, функції та архітектури операційних систем** Технології віртуалізації	**ЛР2.** Робота з Bat файлами	Опрацювання теоретичного матеріалу лекції №3. Опрацювання теоретичного матеріалу лекції №2.	4	[10] с.85-90 [30] с.27-52
4	**Тема 1. Призначення, функції та архітектури операційних систем** Процеси в операційних системах	**ЛР2.** Підгрупа 2	Опрацювання теоретичного матеріалу лекції №4. Підготовка до захисту лабораторної роботи №1. Підготовка до виконання лабораторної роботи №2.	4	[1] с.67-69 [5] с.36-70 [12] с.31-38 [2] с. 80-90 [7] с. 10-12 [10] с. 20-25
5	**Тема 1. Призначення, функції та архітектури операційних систем** Потоки в операційних системах	**ЛР3.** Знайомство та базові операції з Power Shell	Опрацювання теоретичного матеріалу лекції №5. Опрацювання теоретичного матеріалу лекції №3.	5	[5] с. 73-78 [12] с.78-82
6	**Тема 1. Призначення, функції та архітектури операційних систем** Керування пам'яттю в операційних системах	**ЛР3.** Підгрупа 2	Опрацювання теоретичного матеріалу лекції №6. Підготовка до захисту лабораторної роботи №2. Підготовка до виконання лабораторної роботи №3.	5	[5] с.84-104 [12] с. 112-140 [7] с. 20-30 [9] с. 35-40
7	**Тема 2. Інформаційна безпека операційних систем** Сутність проблеми захисту операційних систем	**ЛР4.** Командалети PowerShell для адміністрування ОС Windows	Опрацювання теоретичного матеріалу лекції №7. Опрацювання теоретичного матеріалу лекції №4.	4	[2] с.11-39 [3] с.5-60 [6] с.23-60 [22] с.593-602

8	**Тема 2. Інформаційна безпека операційних систем** Технології боротьби з вірусами в операційних системах	**ЛР4.** Підгрупа 2	Опрацювання теоретичного матеріалу лекції №8. Підготовка до захисту лабораторної роботи №3. Підготовка до виконання лабораторної роботи №4.	4	[2] с.463-499 [3] с.240-256 [6] с.71-87 [7] с. 17-28 [9] с. 34-45
9	**Тема 2. Інформаційна безпека операційних систем** Сучасні технології ідентифікації користувачів операційних систем	**ЛР5.** Редактор vi в ОС Ubuntu	Опрацювання теоретичного матеріалу лекції №9. Опрацювання теоретичного матеріалу лекції №5.	4	[2] с.272-278 [3] с.94-114 [6] с.53-60
10	**Тема 3. Реалізація безпеки в операційній системі Windows** Організація безпеки операційної системи Windows	**ЛР5.** Підгрупа 2	Опрацювання теоретичного матеріалу лекції №10. Підготовка до захисту лабораторної роботи №4. Підготовка до виконання лабораторної роботи №5.	4	[22] с.966-975 [3] с.256-268 [21] с.383-407 [5] с.67-70 [4] с. 35-50
11	**Тема 3. Реалізація безпеки в операційній системі Windows** Конфігурація та моніторинг операційної системи Windows	**ЛР6.** Дослідження технології захисту цілісності даних Raid	Опрацювання теоретичного матеріалу лекції №11. Опрацювання теоретичного матеріалу лекції №6.	4	[8] [14]
12	**Тема 3. Реалізація безпеки в операційній системі Windows** Політики безпеки операційної системи Windows: (частина 1)	**ЛР6.** Підгрупа 2	Опрацювання теоретичного матеріалу лекції №12. Підготовка до захисту лабораторної роботи №5. Підготовка до виконання лабораторної роботи №6.	4	[8] [11] [26] [15] с. 50-70
13	**Тема 3. Реалізація безпеки в операційній системі Windows** Політики безпеки операційної системи Windows: (частина 2)	**ЛР7.** Розмежування прав доступу в UNIX та Windows. Права доступу до файлів і керування ними.	Опрацювання теоретичного матеріалу лекції №13. Опрацювання теоретичного матеріалу лекції №7.	4	[11] [15]

14	**Тема 4. Реалізація безпеки в операційній системі Linux** Організація безпеки операційної системи Linux	**ЛР7.** Підгрупа 2	Опрацювання теоретичного матеріалу лекції №14. Підготовка до захисту лабораторної роботи №6. Підготовка до виконання лабораторної роботи №7.	4	[4] с.75-84 [10] с.31-33,90-102 [22] с. 798-802 [8] [16] [4] с. 53-71 [6] с. 112-128 [3] с. 112-120 [32] [33]
15	**Тема 4. Реалізація безпеки в операційній системі Linux** Технології підвищення рівня захищеності операційної системи Linux	**ЛР8.** Налаштування аудиту в UNIX та Windows	Опрацювання теоретичного матеріалу лекції №15. Опрацювання теоретичного матеріалу лекції №8.	4	[1] с.31-34 [13] с. 96-118
16	**Тема 4. Реалізація безпеки в операційній системі Linux** Робота на хості Linux	**ЛР8.** Підгрупа 2	Опрацювання теоретичного матеріалу лекції №16. Підготовка до захисту лабораторної роботи №7. Підготовка до виконання лабораторної роботи №8.	4	[8] [1] с.167-197 [3] с. 152-180 [13] [34]
17	**Тема 5. Реалізація безпеки в мобільних операційних системах** Організація безпеки операційної системи Android	-	Опрацювання теоретичного матеріалу лекції №17. Опрацювання теоретичного матеріалу лекції №9.	6	[1] с.50-52 [5] с.30-36 [22] с.838-844
18	**Тема 5. Реалізація безпеки в мобільних операційних системах** Організація безпеки операційної системи iOS	-	Опрацювання теоретичного матеріалу лекції №18.	6	[1] с.50-56 [7] с. 54-58

ПОЛІТИКА ДИСЦИПЛІНИ

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції і лабораторні заняття згідно з розкладом, не запізнюватися на заняття, вчасно виконувати та здавати лабораторні роботи. Термін виконання лабораторної роботи вважається своєчасним, якщо студент здав/захистив її на поточному або наступному за ним занятті. За несвоєчасний захист лабораторної роботи з набраної студентом суми балів вираховується один бал. Пропущене з поважної причини лабораторне заняття студент повинен відпрацювати у встановлений викладачем термін.

Виконуючи усі навчальні завдання з дисципліни, студент має дотримуватися політики доброчесності. У разі наявності плагіату він отримує незадовільну оцінку і має виконати завдання за новою темою.

Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок визнання та перезарахування результатів навчання здобувачів вищої освіти у ХНУ.

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	**Контрольні заходи**		**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Тестовий контроль	Контрольна робота	Залік за рейтингом
Тема	1-4	1-4	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	0-11	12-14	15–18	19-20

Оцінка за 4-ри бальною шкалою	2	3	4	5

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.

Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав підсумковий контрольний захід (іспит), вважається невстигаючим.

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**	**Вітчизняна оцінка, критерії**	
A	4,75–5,00	зараховано	***Відмінно*** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74		***Добре*** – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24		***Добре*** – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74		***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
E	3,00–3,24		***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	незараховано	***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99		***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 повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі MOODLE.

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://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php