ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж

ЗАТВЕРДЖУЮ
Декан ФПКТС
_____ Савенко О.С.
«31» 08 2020 р.

СИЛАБУС
Навчальна дисципліна: "Мережеві операційні системи"

Освітньо-професійна програма: «Кібербезпека»

Рівень вищої освіти: перший (бакалаврський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Андрощук Олександр Степанович
Профайл викладач(ів)	http://ksm.khnu.km.ua/sklad-kafedry/
E-mail викладача(ів)	asa_20_1968@ukr.net
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khnu.km.ua/course/view.php?id=5914
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us04web.zoom.us/j/6097696793 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2020-2021, семестр III (осінньо-зимовий)
Розклад	Лекції – середа, 3 пара, онлайн. Лабораторні роботи – четвер (чисельник), 1-2 пара, 1-113
Консультації	Очні: середа, 2 пара, 1-103; Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, у т.ч. ІРС			Залік	Іспит
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття						
Д	2	3	5	150	68	34	34	-	-	82	-	-	-	+

Анотація дисципліни

Дисципліна формує у студентів знання про сучасні операційні системи, забезпечення ідентифікації, аутентифікації та авторизації суб'єктів доступу в операційних системах, безпеці інформації в сучасних операційних системах, методи та засоби захисту інформації в сучасних операційних системах.

Дисципліна викладається для студентів денної форми навчання спеціальності «Кібербезпека». При викладанні дисципліни використовуються наступні форми (методи) навчання: пояснювально-ілюстративні, практичні, продуктивні, застосування інформаційно-комп'ютерних технологій (інструменти та утиліти ОС Windows та Linux Ubuntu).

Пререквізити: стандарти і політики кібербезпеки, англійська мова.

Кореквізити: програмні і програмно-апаратні засоби захисту інформаційних систем від несанкціонованого доступу

Мета і завдання дисципліни

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 6. Здатність відновлювати штатне, функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

результати навчання:

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.

РН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

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	**Призначення і функції операційних систем, як складові захисту інформації** Управління процесами. Управління пам'яттю. Управління файлами і зовнішніми пристроями. Захист даних і адміністрування. Інтерфейс прикладного програмування. Інтерфейс користувача	**ЛР №1** Дослідження операційних систем Windows та Linux. Налаштування, командний рядок, системні функції роботи з процесами та віртуальною пам'яттю	Опрацювання теоретичного матеріалу лекції №1. Підготовка до виконання ЛР №1.	4	[2] с. 16-22 [3] с. 42-90 [4] с. 19-88 [5] с. 6-54 [6] с. 63-75
2	**Функціональні компоненти мережевої операційних систем** Мережеві та розподілені операційні системи. Функціональні компоненти мережевої операційної системи. Мережеві служби і мережеві сервіси. Варіанти впровадження мережевих служб в операційних системах	-	Опрацювання теоретичного матеріалу лекції №2. Підготовка до захисту ЛР №1.	6	[7] с. 144-158 [13] с. 59-78
3	**Архітектури операційних систем** Огляд особливостей операційних систем для різних класів обчислювальних пристроїв. Архітектура операційних систем. Ядро і допоміжні модулі операційних систем	**ЛР №2** Дослідження та розробка алгоритмів антивірусного програмного забезпечення. Протидія вірусам в операційній системі Windows	Опрацювання теоретичного матеріалу лекції №3. Підготовка до виконання ЛР №2.	4	[1] с. 15-32 [2] с. 28-42 [14] с. 463-498
4	**Сутність проблеми захисту операційних систем** Сучасні вимоги, що висуваються до захищених операційних систем. Порушення політики інформаційної безпеки. Атаки на рівні операційної системи	-	Опрацювання теоретичного матеріалу лекції №4. Підготовка до захисту ЛР №2.	6	[6] с. 661-693 [14] с. 463-498

5	**Найпоширеніші загрози безпеці операційних систем** Несанкціонований доступ. Незаконне використання привілеїв. Атаки типу: "салямі", "приховані канали", "маскарад", "збір сміття" та "злам системи". Шкідливе програмне забезпечення	**ЛР №3** Розмежування прав доступу в операційній системі Windows, політики безпеки Windows	Опрацювання теоретичного матеріалу лекції №5. Підготовка до виконання ЛР №3.	4	[6] с. 728-754 [8] с. 47-56 [12] с. 12-31 [14] с. 463-498
6	**Комп'ютерні віруси, як загроза операційним системам** Джерела розповсюдження комп'ютерних вірусів. Класифікація комп'ютерних вірусів	-	Опрацювання теоретичного матеріалу лекції №6. Підготовка до захисту ЛР №3.	6	[6] с. 728-754 [14] с. 463-498
7	**Систематизація комп'ютерних вірусів** Файлові віруси. Завантажувальні віруси. Макро-віруси. Мережні віруси. Стелс-віруси. Поліморфні-віруси	**ЛР №4** Налаштування аудиту безпеки в операційній системі Windows, засоби резервування	Опрацювання теоретичного матеріалу лекції №7. Підготовка до виконання ЛР №4.	4	[6] с. 728-754 [8] с. 47-56 [12] с. 12-31 [14] с. 463-498
8	**Технології боротьби з вірусами в операційних системах** Ознаки інфікованої операційної системи. Пасивні та активні технології боротьби з комп'ютерними вірусами. Технології виявлення вірусів. Класифікація антивірусного програмного забезпечення	-	Опрацювання теоретичного матеріалу лекції №8. Підготовка до захисту ЛР №4.	6	[6] с. 728-754 [14] с. 463-498
9	**Сучасні технології ідентифікації користувачів операційних систем** Апаратні та програмні технології ідентифікації. Біометричні технології ідентифікації	**ЛР №5** Шифрування файлів в файловій системі NTFS	Опрацювання теоретичного матеріалу лекції №9. Підготовка до виконання ЛР №5.	4	[6] с. 693-706 [9] с. 239-298 [15] с. 115-151

10	**Організація безпеки операційної системи Windows** Компоненти системи захисту операційної системи Windows. Механізм захисту об'єктів операційної системи Windows. Ідентифікатор захисту. Маркери доступу. Дескриптори захисту. Права та привілеї (суперпривілеї) облікових записів. Типові права користувачів ОС Windows	-	Опрацювання теоретичного матеріалу лекції №10. Підготовка до захисту ЛР №5.	6	[6] с. 1042-1053 [15] с. 151-166
11	**Аудит безпеки операційної системи Windows** Категорії аудиту безпеки. Процес входу користувача в операційну систему. Політика обмеженого використання програм. Резервування в ОС Windows	**ЛР №6** Дослідження технології захисту цілісності даних RAID	Опрацювання теоретичного матеріалу лекції №11. Підготовка до виконання ЛР №6.	4	[6] с. 1042-1053 [9] с. 239-298 [13] с. 521-589
12	**Файлові системи операційної системи Windows (частина 1)** Файлова система NTFS. Технології захисту цілісності даних. RAID-масиви. Технологія гарячої фіксації. Механізм транзакцій. Безпека в NTFS. Стандартні та спеціальні дозволи для файлів і каталогів	-	Опрацювання теоретичного матеріалу лекції №12. Підготовка до захисту ЛР №6.	6	[6] с. 1029-1042 [13] с. 491-499
13	**Файлові системи операційної системи Windows (частина 2)** Архітектура файлової системи EFS. Технології шифрування EFS	**ЛР №7** Розмежування прав доступу в операційній системі Linux	Опрацювання теоретичного матеріалу лекції №13. Підготовка до виконання ЛР №7.	4	[6] с. 1029-1042 [10] с. 87-109 [13] с. 499-501

14	**Організація безпеки операційної системи Linux** Модель безпеки операційної системи Linux. Підсистема ідентифікації та аутентифікації. Підсистема розмежування доступу. Монітор безпеки. Розмежування прав доступу до файлів та каталогів. Стандартні та спеціальні дозволи	-	Опрацювання теоретичного матеріалу лекції №14. Підготовка до захисту ЛР №7.	6	[6] с. 804-876
15	**Технології підвищення рівня захищеності операційної системи Linux** Linux з покращеним рівнем безпеки (SELinux). Система мандатного контролю доступу AppArmor. Система забезпечення мандатного контролю доступу TOMOYO Linux. Резервування в ОС Linux	**ЛР №8** Дослідження безпеки мобільних операційних систем	Опрацювання теоретичного матеріалу лекції №15. Підготовка до виконання ЛР №8.	4	[6] с. 876-923 [16] с. 136-157, 451-458 [17] [18]
16	**Організація безпеки операційної системи Android** Архітектура операційної системи Android. Модель безпеки операційної системи Android. Підсистема ідентифікації та аутентифікації. Підсистема розмежування доступу. Стандартні та спеціальні дозволи	-	Опрацювання теоретичного матеріалу лекції №16. Підготовка до захисту ЛР №8.	6	[6] с. 876-923
17	**Організація безпеки операційної системи iOS** Архітектура операційної системи iOS. Модель безпеки операційної системи iOS. Характеристика функціонування компонентів Secure Enclave та TouchID	**Тестування**	Опрацювання теоретичного матеріалу лекції №17. Підготовка до тестування.	2	[6] с. 876-923 [19] [20]

*** лекції проводяться по 2 години щотижня;**
**** лабораторні проводяться по 4 години раз в два тижні.**

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, 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.

Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ https://www.khnu.km.ua/root/files/01/10/03/006.pdf.

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	Тестування	Семестровий контроль (іспит)
Тема	2-7	1-7	1-7
Ваговий коефіцієнт	0,4	0,2	0,4

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 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 через10 днів після проходження тестування.

Семестровий контроль (іспит). Підсумковий контрольний захід з дисципліни проводиться в формі іспиту. Екзаменаційний білет складається з двох теоретичних питань і задачі. Під час іспиту за наданими відповідями і рішеннями (розв'язками) виконується оцінювання рівня засвоєння студентом матеріалу дисципліни.

Оцінка за підсумковий контрольний захід проставляється викладачем в електронний журнал дисципліни в день здачі іспиту і враховується в автоматизованому режимі при визначенні підсумкової семестрової оцінки студента з дисципліни за інституційною шкалою і шкалою ЄКТС

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**	**Інституційна оцінка, критерії оцінювання**	
A	4,75–5,00	5	***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	***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. Означення операційної системи.
2. ОС як розширена машина. Інтерфейси операційної системи.
3. Ресурси. Завдання розподілу ресурсів.
4. Основні функції ОС.
5. Поняття архітектури ОС.
6. Механізми і політики.
7. Поняття ядра ОС.
8. Основні функції ядра.
9. Системне програмне забезпечення.
10. Режими виконання програмного коду.
11. Монолітна архітектура ОС, приклади.
12. Багатошарова архітектура ОС, приклади.
13. Мікроядрова архітектура ОС, приклади.
14. Об’єктна архітектура.
15. Архітектура ОС Novell Netware.
16. Архітектура ОС UNIX (Linux).
17. Архітектура ОС Windows.
18. Функціональні вимоги до сучасних ОС.
19. Ринкові вимоги до ОС.
20. Апаратна незалежність і здатність до перенесення.
21. Програмна сумісність.
22. Прикладні програмні середовища.
23. Розширюваність.
24. Поняття мультипрограмування
25. Критерії ефективності обчислювальної системи.
26. Управління процесами
27. Управління пам’яттю
28. Управління файлами і зовнішніми пристроями
29. Захист даних і адміністрування
30. Інтерфейс прикладного програмування
31. Інтерфейс користувача
32. Мережеві та розподілені операційні системи
33. Функціональні компоненти мережевої операційної системи
34. Мережеві служби і мережеві сервіси
35. Варіанти впровадження мережевих служб в операційних системах
36. Сучасні вимоги, що висуваються до захищених операційних систем
37. Порушення політики інформаційної безпеки
38. Атаки на рівні операційної системи
39. Несанкціонований доступ
40. Незаконне використання привілеїв
41. Атаки типу: "салямі", "приховані канали", "маскарад", "збір сміття" та "злам системи"
42. Шкідливе програмне забезпечення
43. Джерела розповсюдження комп’ютерних вірусів
44. Класифікація комп’ютерних вірусів
45. Файлові віруси
46. Завантажувальні віруси
47. Макро-віруси
48. Мережні віруси
49. Стелс-віруси
50. Поліморфні-віруси

51. Ознаки інфікованої операційної системи
52. Пасивні та активні технології боротьби з комп'ютерними вірусами
53. Технології виявлення вірусів
54. Класифікація антивірусного програмного забезпечення
55. Апаратні та програмні технології ідентифікації
56. Біометричні технології ідентифікації
57. Компоненти системи захисту операційної системи Windows
58. Механізм захисту об'єктів операційної системи Windows
59. Ідентифікатор захисту
60. Маркери доступу
61. Дескриптори захисту
62. Права та привілеї (суперпривілеї) облікових записів
63. Категорії аудиту безпеки
64. Процес входу користувача в операційну систему
65. Політика обмеженого використання програм
66. Резервування в ОС Windows
67. Файлова система NTFS
68. Технології захисту цілісності даних
69. RAID-масиви.
70. Технологія гарячої фіксації
71. Механізм транзакцій
72. Безпека в NTFS
73. Стандартні та спеціальні дозволи для файлів і каталогів
74. Архітектура файлової системи EFS
75. Технології шифрування EFS
76. Модель безпеки операційної системи Linux
77. Підсистема ідентифікації та аутентифікації
78. Підсистема розмежування доступу
79. Монітор безпеки
80. Розмежування прав доступу до файлів та каталогів
81. Стандартні та спеціальні дозволи
82. Linux з покращеним рівнем безпеки (SELinux)
83. Система мандатного контролю доступу AppArmor
84. Система забезпечення мандатного контролю доступу TOMOYO Linux
85. Резервування в ОС Linux
86. Архітектура операційної системи Android
87. Модель безпеки операційної системи Android
88. Підсистема ідентифікації та аутентифікації
89. Підсистема розмежування доступу
90. Стандартні та спеціальні дозволи
91. Архітектура операційної системи iOS
92. Модель безпеки операційної системи iOS
93. Характеристика функціонування компонентів Secure Enclave та TouchID

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни “Мережеві операційні системи” повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, розміщеною в електронному варіанті в модульному середовищі.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

№	Назва	Режим доступу
1.	Операційні системи: навчальний посібник/ І. М. Федотова-Півень, І. В. Миронець, О. Б. Півень, С. В. Сисоєнко, Т. В. Миронюк; [за ред. В. М. Рудницького]. – Харків: ТОВ «ДІСА ПЛЮС», 2019. – 216 с.	https://er.chdtu.edu.ua/bitstream/ChSTU/1041/1/ОПЕРАЦІЙНІ%20СИСТЕМИ_навч.пос..pdf
2.	Операційні системи: консп. лекц. / укл. А.Г. Микитишин, І.В. Чихіра. - Тернопіль : ТНТУ імені Івана Пулюя, 2016. - 107 с.	http://elartu.tntu.edu.ua/handle/123456789/18304
3.	Операційні системи: навч. посібник / Б. І. Погребняк, М. В. Булаєнко. – Харків: ХНУМГ ім. О. М. Бекетова, 2018. – 104 с.	http://eprints.kname.edu.ua/51761/1/2017%20печ.%2050Н%20ОС_УП_КН_ua.doc.pdf
4.	Операційні системи. Лабораторний практикум: навчальний посібник / В.Г. Зайцев, І.П. Дробязко. – Київ: КПІ ім. І. Сікорського, 2018. – 88 с.	https://ela.kpi.ua/handle/123456789/25434
5.	Операційна система Windows: навчальний посібник [Електронний ресурс]/ Н.А. Рибачок. – Київ: КПІ ім. І. Сікорського, 2018.	https://ela.kpi.ua/handle/123456789/27211
6.	Современные операционные системы. 4-е изд./ Э. Таненбаум, Х. Бос. – СПб.: Питер, 2015. – 1120 с.	http://www.dut.edu.ua/uploads/l_1381_22728986.pdf
7.	Організація комп’ютерних мереж: підручник/ Ю.А. Тарнавський, І.М. Кузьменко. – Київ: КПІ ім. І. Сікорського, 2018. – 259 с.	https://ela.kpi.ua/bitstream/123456789/25156/1/Tarnavsky_Kuzmenko_Org_Komp_merej.pdf
8.	Адміністрування комп’ютерних мереж та операційних систем [Електронний ресурс]/ В.В. Поліщук В.В. – Ужгород: 2019.	https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/24567/1/Методичне%20видання%20адміністрування%20КМ%20і%20ОС.pdf
9.	Операційні системи: лабораторний практикум/ Д.Ю. Голубничий, А.В. Холодкова, О.В. Шматко, М.М. Козуля. – Харків: НТУ «ХПІ», 2019. – 336 с.	https://core.ac.uk/display/228315502?recSetID=
10.	Практичне програмування для ОС Linux: навчально-методичний посібник / Ю.М. Єфремов, М.Ф. Єфремов. – Житомир: ЖДТУ, 2018. – 112 с.	https://learn.ztu.edu.ua/pluginfile.php/45155/mod_resource/content/1/Програмування%20для%20Linux.pdf
11.	Самоучитель Microsoft Windows 10/ Д.Н. Колесниченко. – СПб.: БХВ-Петербург, 2016. – 352 с.	https://www.twirpx.com/file/3256330/
12.	Адміністрування операційних систем [Електронний ресурс]/ Л.О.Левченко, В.А.Глива. – Київ: КПІ ім. І. Сікорського, 2018.	https://core.ac.uk/reader/323536765
13.	Основи операційних систем. Навчальний посібник/ В.С. Авраменко, А.С. Авраменко. – Черкаси: ЧНУ ім. Богдана Хмельницького, 2018. – 524 с.	http://eprints.cdu.edu.ua/1480/1/osnovu.pdf
14.	Інформаційна безпека: навчальний посібник/ Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В.	https://drive.google.com/file/d/1Zqzz0pxqtm8KfmDnUvqYRWDYi0o6qsR_/view?usp=sharing

	Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.	
15.	Комплексна безпека інформаційних мережевих систем. Навчальний посібник/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. – Львів, «Магнолія 2006», 2016. – 256 с.	http://elartu.tntu.edu.ua/handle/123456789/18299
16.	Linux. От новичка к профессионалу. 6-е изд., перераб. и доп./ Д.Н. Колисниченко. – СПб.: БХВ-Петербург, 2018. – 672 с.	https://codernet.ru/books/linux/linux_ot_novichka_k_professionalu_6-e_izdanie/
17.	Linux Security Module Usage. TOMOYO [Електронний ресурс]	https://www.kernel.org/doc/html/v4.15/admin-guide/LSM/tomoyo.html
18.	Включение и Отключение SELinux [Електронний ресурс]	https://docs.fedoraproject.org/ru-RU/Fedora/13/html/Security-Enhanced_Linux/sect-Security-Enhanced_Linux-Working_with_SELinux-Enabling_and_Disabling_SELinux.html
19.	Безопасность платформы Apple [Електронний ресурс]	https://support.apple.com/ru-ru/guide/security/welcome/web
20.	IOS Security [Електронний ресурс]	https://developer.apple.com/documentation/security

Додаткова

21.	Unix and Linux system administration handbook. Fifth edition/ E. Nemeth, G. Snyder, T. R. Hein, B. Whaley, D. Mackin. – Pearson Education, Inc, 2018. – 1179 p.	https://mog.dog/files/SP2019/2017%20Nemeth%20Evi%20etal%20-%20UNIX%20and%20Linux%20System%20Administration%20Handbook%5B5thED%5D_Rell.pdf
22.	Unix and Linux System Administration and Shell Programming. – PR NTR KMT, 2014. – 328 p.	https://www.pdfdrive.com/unix-and-linux-system-administration-and-shell-programming-d1246846.html
23.	The Practice of System and Network Administration. Volume 1. Third Edition/ Th. A. Limoncelli, Ch. J. Hogan, S. R. Chalup. – Virtual.NET Inc., Lumeta Corporation, 2017. – 1426 p.	https://www.pdfdrive.com/the-practice-of-system-and-network-administration-volume-1-devops-and-other-best-practices-for-enterprise-it-d157098292.html
24.	Linux Command Line. A Beginner's Guide/ Ray Yao. – Ray Yao, USA, 2014. – 90 p.	https://www.pdfdrive.com/linux-linux-command-line-cover-all-essential-linux-commands-a-complete-introduction-to-linux-operating-system-linux-kernel-for-beginners-learn-linux-in-easy-steps-fast-a-beginners-guide-d200442383.html
25.	Mastering Windows Server 2019. Second Edition/ J. Krause. – Packt Publishing Ltd, 2019. – 1010 p.	https://el.newoutlook.it/download/book/Mastering-Windows-Server-2019-Second-Edition.pdf
26.	Сучасні мережеві технології: Навчально-методичний посібник [Електронний ресурс]/ О.А. Рижов, А.І. Андросов, Н.А. Іванькова. – Запоріжжя: [ЗДМУ], 2018.	http://dspace.zsmu.edu.ua/bitstream/123456789/9659/1/сучасні%20мереж_техн_метод.pdf
27.	Самоучитель системного администратора. 4-е изд./ А. М. Кенин, Д. Н. Колисниченко. – СПб.: БХВ-Петербург, 2016. – 528 с.	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwizrO_3nozuAhXvlYsKHRs9Ct4QFjADegQIDBAC&url=https%3A%2F%2Fpjc.

		mobi%2Fuploads%2Fs%2Fg%2Fr%2Fp%2Fgrpdcm75blut%2Ffile%2FgPbQdB5F.pdf&usg=AOvVaw1bLa4g1rhzPkYVBS19b4nW
28.	Посібник адміністратора. – Seiko Epson Corporation, 2019. – 131 с.	https://download4.epson.biz/sec_pubs/wf-7710_series/admg/uk/manual.pdf?pageid=&tab=&LGW=&CNW=&OSV=&EXE=&VER=
29.	Основи інформаційної та кібернетичної безпеки. Навчальний посібник/ В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К., 2018. – 320 с.	http://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf
30.	Аналіз можливостей управління мережею Інтернет у сучасних умовах / О.С. Андрощук, В. В. Пилипчук, О. В. Буяло// Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки. – Хмельницький : Видавництво НАДПСУ, 2017. – № 1(71). – С. 271-284.	http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=znpnapv_vtn_2017_1_22
31.	Аналіз зовнішніх механізмів управління мережею Інтернет/ О. С. Андрощук, В. В. Пилипчук, О. В. Буяло // Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки. – Хмельницький: Видавництво НАДПСУ, 2016. – № 4(70). – С. 175-184.	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiu3L6upa_uAhXQ-ioKHVPiANMQFjAAegQIAxAC&url=http%3A%2F%2Firbis-nbuv.gov.ua%2Fcgi-bin%2Firbis_nbuv%2Fcgiirbis_64.exe%3FC21COM%3D2%26I21DBN%3DUJRN%26P21DBN%3DUJRN%26IMAGE_FILE_DOWNLOAD%3D1%26Image_file_name%3DPDF%2Fznpnapv_vtn_2016_4_17.pdf&usg=AOvVaw0SJL2tsl2Uc8NQw-NlYAaP
32.	Метод багатофакторної автентифікації на основі модифікованих крипто-кодових систем Нідеррайтера–Мак-Еліса. / С. П. Євсеев, В. М. Федорченко, О. С. Андрощук // Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки. – Хмельницький : Видавництво НАДПСУ, 2017. – № 3(73). – С. 275–288	http://nbuv.gov.ua/UJRN/znpnapv_vtn_2017_3_24

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання (розміщені усі необхідні матеріали з дисципліни, в тому числі завдання для поточного та семестрового контролю знань). Доступ до ресурсу: https://msn.khnu.km.ua.
2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.

Розробник	_____ Підпис	д.т.н., професор Вчений ступінь, звання	О.С. Андрощук Ініціали, прізвище викладача
Погоджено			
Гарант освітньої програми	_____ Підпис	к.т.н., доцент Вчений ступінь, звання	В.М. Чешун Ініціали, прізвище
Зав. кафедри кібербезпеки та комп'ютерних систем і мереж	_____ Підпис	к.т.н., доцент Вчений ступінь, звання	Ю.П. Кльоц Ініціали, прізвище