

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій Кафедра кібербезпеки

ЗАТВЕРДЖУЮ

Декан ФІТ

Тетяна ГОВОРУЩЕНКО

«31» серпня 2024 р.

СИЛАБУС

Навчальна дисципліна: «Захист та моніторинг комп'ютерних мереж»

Освітньо-професійна програма: «Кібербезпека та захист інформації»

Рівень вищої освіти: другий (магістерський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Муляр Ігор Володимирович
Профайл викладач(ів)	https://kb.khmnu.edu.ua/mulyar-igor-volodymyrovych
E-mail викладача(ів)	mulariv@khmnu.edu.ua
Контактний телефон	+3 8 067 938-15-44
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/course/view.php?id=8036
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us04web.zoom.us/j/5011940672 * 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 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							
Од	-	-	8	240	90	36	54	-	-	150	-	-	+	-	

Анотація дисципліни

Дисципліна «Захист та моніторинг комп'ютерних мереж» – вибіркова складова професійної підготовки магістрів спеціальності “125 – Кібербезпека та захист інформації”

Анотація дисципліни

Дисципліна «Захист та моніторинг комп'ютерних мереж» – вибіркова складова професійної підготовки магістрів спеціальності “125 – Кібербезпека”.

Мета і завдання дисципліни

Метою викладання навчальної дисципліни є формування у майбутніх спеціалістів умінь та компетенцій, необхідних для розробки та проектування захищених комп'ютерних мереж, їх адміністрування та супроводу; надання глибоких та міцних знань з питань методології атак на комп'ютерні мережі, аналізу захищеності комп'ютерних мереж та управління їх безпекою.

Предметом дисципліни є міжмережні екрани та схеми їх підключення, протоколи безпеки та їх налаштування, побудова захищених комп'ютерних мереж, безпека віддаленого доступу, розробка політики міжмережної взаємодії, сканери виявлення вразливостей, моніторинг подій та інцидентів в мережах, аналіз загроз інформаційній безпеці в мережах, експертиза захищеності мереж.

Завданням дисципліни є забезпечити набуття наступних компетентностей та досягнення наступних програмних результатів навчання:

компетентності:

- Розуміти завдання захисту мережевого трафіку та контролю доступу з використанням існуючих протоколів та інструментів.
- Розуміти методологію атак на комп'ютерні мережі та застосовувати це розуміння на практиці.
- Застосовувати політики безпеки для певного об'єкта (підприємства), щоб запобігти несанкціонованому доступу до комп'ютерних мереж
- Використовувати інструменти та утиліти для адміністрування та обслуговування комп'ютерних мереж відповідно до існуючих політик безпеки.
- Використовувати сучасні інструменти, IDS та SIEM-системи для аудиту, моніторингу процесів та виявлення вторгнень у комп'ютерних мережах.

результати навчання:

- Знати основні поняття комп'ютерних мереж та їх компонентів
- Захищати мережевий трафік та здійснювати контроль доступу за допомогою існуючих протоколів та інструментів
- Розробляти та аналізувати архітектуру мережі, яка відповідає підвищеним вимогам безпеки
- Розробляти політику безпеки на основі моделей атак на певний об'єкт (підприємство)
- Аналізувати комп'ютерні мережі за допомогою інструментів для аудиту та моніторингу.

Студент, який успішно завершив вивчення дисципліни, повинен: *знати* основні поняття комп'ютерних мереж та їх компонентів; *захищати* мережевий трафік та *здійснювати* контроль доступу за допомогою існуючих протоколів та інструментів; *розробляти* та *аналізувати* архітектуру мережі, яка відповідає підвищеним вимогам безпеки; *розробляти* політику безпеки на основі моделей атак на певний об'єкт (підприємство); *аналізувати* комп'ютерні мережі за допомогою інструментів для аудиту та моніторингу.

Тематичний і календарний план вивчення дисципліни

№ тижня	Тема лекції*	Тема лаб. роботи **	Самостійна робота		
			Зміст	Год.	Література
1	Основи комп'ютерних мереж	ЛР1. Проектування комп'ютерної мережі підприємства	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР1	9	[1] с. 10-80 [2] с. 8-12 [3] с. 84-95 [12] с. 4-12, с. 40-53, с. 63-69
2	Поняття про мережні протоколи та служби. Мережні моделі	-	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР1	8	[3] с. 84-95
3	Основи функціонування протоколу TCP/IP	ЛР2. IP-адресація та IP-маршрутизація в комп'ютерних мережах. Адміністрування комп'ютерних мереж TCP/IP-утилітами, TCP/IP-сервісами та засобами доменних групових політик	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР2	9	[3] с. 9-43, с. 60-67 [4] с. 71-136 [12] с. 69-71
4	Інші мережні протоколи (частина 1)	-	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР2	8	[3] с. 60-67, с. 84-95
5	Інші мережні протоколи (частина 2)	ЛР3. Дослідження брандмауерів та міжмережних екранів, як засобів захисту мережі від атак	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР3	9	[1] с. 66-80, с. 185-200 [16] с. 10-60
6	Брандмауери та їх функції у задачах захисту мереж	-	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР3	8	[1] с. 66-78 [3] с. 60-67 [12] с. 40-53
7	Міжмережні екрани та міжмережна взаємодія	ЛР4. Налаштування та управління віддаленим доступом засобами ОС сімейства Windows	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР4	9	[1] с. 146-160 [5] с. 13-21 [6] с. 7-22, с. 129-180 [10] с. 7-36 [12] с. 53-62
8	Безпека віддаленого доступу	-	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР №4 Підготовка до тестування	8	[1] с. 66-78, с. 146-160 [12] с. 40-62
9	Архітектура захищених комп'ютерних мереж	ЛР5. Дослідження технологій злому комп'ютерних мереж, збирання технічної та чуттєвої інформації, аналіз мережного трафіку	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР5	9	[7] с.180-233 [10] с. 163-186, с. 198-221

10	Резервування та відновлення роботи мереж	-	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР5	8	[1] с. 146-160 [12] с. 53-62 [15] с. 36-55
11	Політика інформаційної безпеки мережі підприємства	ЛР6. Дослідження вразливостей комп'ютерних мереж, сканування мережних протоколів	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР6	9	[8] с. 30-44 [10] с. 120-148 [11] с. 7-42 [13] с. 16-22
12	Проблеми інформаційної безпеки мереж	-	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР6	8	[14] с. 14-30 [15] с. 36-55
13	Класифікація атак на комп'ютерні мережі	ЛР7. Моніторинг інцидентів та подій у комп'ютерних мережах	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР7	9	[14] с. 5-13 [17] с. 5-12, с. 19-36 [18] с. 49-81
14	Аналіз та моделювання загроз мережної безпеки	-	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР7	8	[9] [14] с. 14-30 [19] с. 32-73
15	Аналіз захищеності комп'ютерних мереж	ЛР8. Управління ризиками інформаційної безпеки мережі з використанням програмних засобів	Опрацювання теоретичного матеріалу, підготовка до виконання ЛР8	9	[14] с. 83-88 [18] с. 116-142, с. 168-177 [20], с. 67-75 [21] [22]
16	Технології виявлення атак в комп'ютерних мережах	-	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР8	8	[9] [14] с. 32-63 [19] с. 32-73
17	Аудит безпеки комп'ютерних мереж (частина 1)	Підсумкове заняття Тестування	Опрацювання теоретичного матеріалу. Підготовка до тестування	9	[14] с. 32-63 [18] с. 240-308, с. 465-473
18	Аудит безпеки комп'ютерних мереж (частина 2)	-	Опрацювання теоретичного матеріалу.	5	-

* лекції проводяться по 2 години щотижня;

** лабораторні проводяться по 6 годин 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 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. В 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 перезарахування результатів навчання та визначення академічної різниці 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	Тестування	Семестровий контроль (залік)
Тема	1-7	1-7	-
Ваговий коефіцієнт	0,8	0,2	0

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 п'ятдесяти тестових завдань, кожне з яких оцінюється одним балом. Максимальна сума балів, яку може набрати студент, складає 50.

Відповідність набраних балів за тестове завдання оцінці, що виставляється студенту

Сума балів за тестове завдання	1–25	26–38	39–47	48–50
Оцінка за 4-ри бальною шкалою	2	3	4	5

На тестування відводиться 50 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 50 хвилин студенти здають викладачу завдання з талонами відповідей.

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

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 оцінку «незадовільно» за певним видом робіт, то він має передати її в установленому порядку, але обов'язково до терміну наступного контролю.

Студент, який не набрав позитивний середньозважений бал за поточну роботу або не виконав індивідуальний план з дисципліни повністю, вважається невстигаючим.

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».

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. Задачі захисту комп'ютерних мереж
2. Фізичний захист мереж (кабельна система, системи електропостачання, захист від стихійних лих)
3. Огляд програмних та програмно-апаратних методів захисту мереж (захист від мережних вірусів, захист від несанкціонованого доступу)
4. Адміністративні заходи
5. Використання брандмауера у задачах захисту мереж
6. Види брандмауерів
7. Міжмережний екран як засіб від вторгнення з Internet
8. Функціональні вимоги та компоненти міжмережних екранів
9. Фільтруючі маршрутизатори
10. Види шлюзів
11. Основні схеми мережевого захисту на базі між мережних екранів
12. Управління ідентифікацією і доступом
13. Організація захищеного віддаленого доступу
14. Моделі управління доступом (мандатні, дискреційні, рольові)
15. Управління доступом за схемою одноразового входу з авторизацією Single Sign - On (SSO)
16. Протокол Kerberos
17. Інфраструктура управління відкритими ключами PKI (Public Key Infrastructure)
18. Мережні протоколи та служби
19. Завдання та цілі адміністрування мереж
20. Моделі міжмережної взаємодії (модель OSI, модель TCP/IP)
21. Адресація вузлів в IP-мережах
22. Публічні і приватні IP-адреси
23. Відображення IP-адрес на фізичні адреси
24. Розбиття мереж на підмережі за допомогою маски підмережі
25. Введення в IP-маршрутизацію
26. Утиліти діагностування TCP/IP та DNS
27. Простір імен, домени і зони
28. Алгоритми роботи ітеративних і рекурсивних запитів DNS
29. Налаштування вузлів для виконання динамічної реєстрації на сервері DNS
30. Архітектура захищених комп'ютерних мереж
31. Параметри (сервіси, метрики, рівні) безпеки мереж
32. Протидія прослуховуванню трафіку
33. Сегментація мережі
34. Резервування мережного обладнання та каналів зв'язку
35. Системи архівування та дублювання інформації в мережах
36. Відновлення функціонування комп'ютерних мереж після здійснення кібератак, збоїв та відмов різних класів та походження
37. Проектування та монтаж захищених комп'ютерних мереж: загальні вимоги та вихідні дані проекту
38. Проектування та монтаж захищених комп'ютерних мереж: проектна документація на створення мережі.
39. Проектування та монтаж захищених комп'ютерних мереж: вибір архітектури та структури мережі.
40. Структура політики безпеки підприємства
41. Класифікація складових мережі з точки зору інформаційної безпеки
42. Матриця управління доступом та розподіл інформаційних потоків і ролей
43. Проблеми інформаційної безпеки мереж
44. Прояви загроз мережній безпеці
45. Стратегії зломщиків та порушників

46. Огляд основних інструментів злому
47. Класифікація атак на комп'ютерні мережі
48. Загрози, їх джерела та вразливості проводових та безпроводових мереж
50. Узагальнений підхід щодо побудови моделей загроз в комп'ютерних мережах
51. Концепція адаптивного управління безпекою
52. Технологія аналізу захищеності
53. Засоби аналізу захищеності мереж, мережних протоколів і сервісів (сканери уразливостей, сніфери, системи SIEM)
54. Технології виявлення атак в комп'ютерних мережах
55. Методи аналізу мережної інформації
56. Класифікація систем виявлення атак IDS (Intrusion Detection System)
57. Компоненти і архітектура IDS
58. Методи реагування на атаки, ведення журналів реєстрації
59. Завдання управління системою мережної безпеки
60. Архітектура управління засобами мережної безпеки
61. Функціонування системи управління засобами мережної безпеки
62. Аудит безпеки комп'ютерних мереж
63. Ризик-менеджмент у комп'ютерних мережах

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни «Захист та моніторинг комп'ютерних мереж» повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Технології забезпечення безпеки мережевої інфраструктури/ В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
2. Організація комп'ютерних мереж: підручник/ Ю.А. Тарнавський, І.М. Кузьменко. – Київ: КПІ ім. І. Сікорського, 2018. – 259 с.
3. Адміністрування комп'ютерних мереж та операційних систем [Електронний ресурс]/ В.В. Поліщук. – Ужгород: 2019. – режим доступу: <https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/24567/1/Методичне%20видання%20адміністрування%20КМ%20i%20ОС.pdf>
4. Інформаційна безпека в комп'ютерних мережах: навч. посіб./ О.А. Смірнов, О.К. Коноплицька-Слободенюк, С.А. Смірнов, К.О. Буравченко, Т.В. Смірнова, Л.І. Поліщук. – Кропивницький: Видавець Лисенко В.Ф., 2020. – 295 с. http://dspace.kntu.kr.ua/jspui/bitstream/123456789/9799/1/Inform_bezp_komp_mer.pdf
5. Проектування та монтаж локальних комп'ютерних мереж/ І. М. Журавська. – Миколаїв: Видавництво ЧДУ ім. Петра Могили, 2016. – 396 с.
6. Комп'ютерні мережі: навч. посіб./ Б.Ю. Жураковський, І.О. Зенів. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 213 с. https://ela.kpi.ua/bitstream/123456789/36689/1/Zhurakovkyi_Zeniv_Kompiuterni_merezhi_lab.pdf
7. Технології та протоколи інфокомунікаційних мереж. Частина 1[Електронний ресурс]/ О.Л. Недашківський. – Київ, 2017. – режим доступу: http://www.dut.edu.ua/uploads/1_1799_76743031.pdf
8. Моделювання систем захисту інформації/ А.О. Антонюк. - Ірпінь: Національний університет ДПС України, 2015. - 273 с.
9. . . . : . . . / . . . , - . . . : , 2017. - 464 .— ISBN 978-966-483-521-7
10. Комплексна безпека інформаційних мережевих систем. Навчальний посібник/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. – Львів, «Магнолія 2006», 2016. – 256 с
11. Комп'ютерні мережі та Інтернет. Навчальний посібник/ В.М. Франчук. – К.: НПУ імені М.П. Драгоманова, 2015 р. – 141 с.
12. Інформаційна безпека: навчальний посібник/ Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарев, С. С. Войтусік, А. Я. Горпенюк, О. А. Немкова, 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. Горбатого. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.
13. Інформаційна безпека держави: методичні вказівки до виконання лабораторних робіт/ уклад. О.А. Смірнов, О.К. Коноплицька-Слободенюк, В.Д. Хох, С.А. Смірнов/ – Кропивницький: ЦНТУ – 2017. – 90 с.
14. Захист інформації в комп'ютерних системах та мережах: навч. посіб./ С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Х.: НТУ «ХПІ», 2014.– 251 с. http://www.dgma.donetsk.ua/docs/kafedry/avp/metod/ БКМ%20Пос_бник.pdf
15. Технології захисту інформації: навчальний посібник/ С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. <http://kist.ntu.edu.ua/textPhD/tzi.pdf>
16. Апаратно-програмні засоби захисту інформації у корпораціях: навчально-методичний посібник [Електронний ресурс]/ В.Г. Крижановський, С.П. Сергієнко. – Вінниця : ДонНУ імені Василя Стуса, 2019. – режим доступу:

<https://r.donnu.edu.ua/bitstream/123456789/111/1/Методичка%20Засоби%20захисту%20інформації%20у%20корпораціях.pdf>

17. IBM QRadar. Installation Guide [Електронний ресурс]. – IBM Corp., 2019. – режим доступу: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.3/com.ibm.qradar.doc/b_siem_inst.pdf
18. Аудит та управління інцидентами інформаційної безпеки: навчальний посібник/ О.Г. Корченко, С.О. Гнатюк С.О, С.В. Казмірчук та ін. – К.: Центр навч.-наук. та наук.-пр. видавч. НА СБ України, 2014. – 190 с.

Додаткова

16. 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.
17. Operating System Concepts Essentials. Second Edition/ A. Silberschatz, P. B. Galvin, G. Gagne. – John Wiley & Sons, Inc, 2014. – 760 p.
18. Unix and Linux System Administration and Shell Programming. – PR NTR KMT, 2014. – 328 p.
19. 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.
20. Linux Command Line. A Beginner's Guide/ Ray Yao. – Ray Yao, USA, 2014. – 90 p.
21. Mastering Windows Server 2019. Second Edition/ J. Krause. – Packt Publishing Ltd, 2019. – 1010 p.
22. Network Security Assessment. Third edition/ Ch. McNab. – O'Reilly Media, Inc., 2017. – 546 p.
23. Wireless Networks [Електронний ресурс]/ J. Salazar. – Czech Technical University of Prague, 2017. – режим доступу: <http://standardsoui.ieee.org/oui/oui.txt>
24. Architecture Modeling and Analysis of Security in Android Systems/ B. Schmerl et al. – Software Architecture. – 2016. – P. 274-290.
25. Методи забезпечення гарантоздатності і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів: Монографія./ В.Л. Бурячок, В.Ю. Соколов. – Київ : КУБГ, 2019. - 164 с.
26. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення/ Бурячок В. Л. та ін. /Наукові записки Українського науково-дослідного інституту зв'язку. - 2016. – №3. – С. 48-61.
27. <https://doi.org/10.1007/978-966-552-254-1> / 0 ВHV, 2018. — 624 . — ISBN 978-966-552-254-1.
28. Комп'ютерні мережі. Книга 1/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів, «Магнолія 2006», 2013. – 256 с.
29. Комп'ютерні мережі. Книга 2/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів, «Магнолія 2006», 2014. – 312 с.
30. Основи інформаційної та кібернетичної безпеки. Навчальний посібник/ В. Л. Бурячок, Р. В. Киричок, П. М. Складанний – К., 2018. – 320 с.
31. Безпека безпроводових і мобільних мереж: Навчальний посібник/ В. Ю. Соколов, В. Л. Бурячок, М. М. Тадждіні / ред. перекл. О. П. Райтер. – 2 вид., доп. – К.: КУБГ, 2019. – 130 с.

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/plage_lib.php.