



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ



Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мережні інформаційні технології

Освітньо-професійна програма «Комп'ютерна інженерія»

першого рівня вищої освіти

за спеціальністю 123 Комп'ютерна інженерія

галузі знань 12 Інформаційні технології

кваліфікація Бакалавр з комп'ютерної інженерії

Розглянуто на засіданні кафедри
Протокол №13 від 31 березня 2022 р.

КРОПИВНИЦЬКИЙ – 2022

ЗМІСТ

1. Загальна інформація
2. Анотація до дисципліни
3. Мета і завдання дисципліни
4. Формат дисципліни
5. Результати навчання
6. Обсяг дисципліни
7. Пререквізити
8. Технічне і програмне забезпечення / обладнання
9. Політика дисципліни
10. Навчально-методична карта дисципліни
11. Система оцінювання та вимоги
12. Рекомендована література й джерела

1. Загальна інформація

Назва дисципліни	Мережні інформаційні технології
Рік викладання	2022-2023 календарний рік
Викладач	Лектор – Коваленко Анна Степанівна , кандидат технічних наук, доцент, http://kbpz.kntu.kr.ua/kovalenko-anna/ https://scholar.google.com.ua/citations?user=jEfDXi0AAAAJ&hl=ru https://www.scopus.com/authid/detail.uri?authorId=57219410986 Асистент – Марченко Костянтин Миколайович , кандидат технічних наук, доцент, http://kbpz.kntu.kr.ua/marchenko-konstantin/ https://scholar.google.ru/citations?hl=ru&pli=1&user=fiezdsAAAAJ https://orcid.org/0000-0001-6269-5379
Контактний телефон	службовий: (0522)390-449 – робочі дні з 8 ³⁰ до 14 ²⁰ Мобільні телефони / Viber / Telegram надано у описі курсу «Мережні інформаційні технології» на сервері дистанційної освіти ЦНТУ. –URL: http://moodle.kntu.kr.ua/course/view.php?id=1669
E-mail:	У описі курсу «Мережні інформаційні технології» на сервері дистанційної освіти ЦНТУ. – URL: http://moodle.kntu.kr.ua/course/view.php?id=1669
Консультації	<i>очні</i> – відповідно до затвердженого графіку консультацій; <i>онлайн</i> – е-листування, у месенджері (Telegram), вебінари на платформах Zoom, Discord

2. Анотація дисципліни

Навчальний курс «Мережні інформаційні технології» призначений для набуття теоретичних знань та практичних навичок ідентифікування, класифікування та опису рівня безпеки мережних комерційних чи наукових проєктів. Отримання навичок пошуку та використанню мережного спеціалізованого системного інструментарію для вирішення проблем програмно-технічних систем з зазначенням можливих обмежень обраних технологій.

3. Мета і завдання дисципліни

Метою викладання навчальної дисципліни «Мережні інформаційні технології» є забезпечення здобувачів вищої освіти комплексом знань, умінь та навичок, необхідних для застосування в професійній діяльності у сфері ідентифікування, класифікування та опису роботи програмно-технічних засобів.

Основними **завданнями** вивчення навчальної дисципліни є формування наступних компетенцій бакалавра з комп'ютерної інженерії:

Завданням вивчення дисципліни є формування компетентностей (Z– загальних, P – фахових):

- **Z7** Вміння виявляти, ставити та вирішувати проблеми.
- **P12** Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних та кіберфізичних систем, мереж та їхніх компонентів шляхом використання аналітичних методів і методів моделювання
- **P13** Здатність вирішувати проблеми у галузі комп'ютерних та інформаційних технологій, визначати обмеження цих технологій.

4. Формат дисципліни

Для денної форми навчання:

Викладання курсу передбачає для засвоєння дисципліни традиційні лекційні заняття із застосуванням мультимедійних презентацій, у поєднанні з лабораторними заняттями.

Формат очний (*Face to face*)

Для заочної форми навчання:

Під час сесії формат очний (*Face to face*), у міжсесійний період – дистанційний (*online*).

5. Результати навчання

У результаті вивчення навчальної дисципліни студент буде забезпечити наступні програмні результати:

Знати:

- N2. Мати навички проведення експериментів, збирання даних та моделювання в комп'ютерних системах.
- N5. Мати знання основ економіки та управління

Вміти:

- N7. Вміти розв'язувати задачі аналізу та синтезу засобів, характерних для спеціальності.
- N16. Вміти оцінювати отримані результати та аргументовано захищати прийняті рішення.

Набути навичок автономії і відповідальності:

- N19. Здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати у межах компетенції рішення.

6. Обсяг дисципліни

Ознака дисципліни, вид заняття	Кількість годин
Рекомендації щодо семестру вивчення	5 семестр
Спеціальність	123 «Комп'ютерна інженерія»
Кількість кредитів / годин	6/180
Кількість змістових модулів	2
Нормативна / вибіркова	вибіркова
лекції	28
лабораторні	28
самостійна робота	94
Вид підсумкового контролю : екзамен	40

7. Пререквізити

Враховуючи послідовність накопичення знань і набуття вмінь, для опанування навчальної дисципліни необхідні знання й вміння, здобуті під час вивчення навчальних дисциплін «Основи комп'ютерних технологій», «Комп'ютерні мережі», «Web-програмування».

8. Технічне і програмне забезпечення / обладнання

Лекційні заняття проводяться в аудиторіях обладнаних мультимедійним проектором. Лабораторні роботи виконуються у аудиторіях кафедри кібербезпеки та програмного забезпечення, обладнаних відповідним апаратним та програмним забезпеченням (ауд 501, 507, 508, 517), з відкритою бездротовою мережею Wi-Fi, вільним доступом до Інтернету. Оскільки при вивченні дисципліни використовуються інформаційні технології навчання, система дистанційної освіти Moodle, студенту необхідно мати комп'ютерну техніку (з виходом у Internet) та оргтехніку для комунікації з викладачами, виконання тестових завдань в системі дистанційної освіти.

9. Політика дисципліни

Академічна доброчесність:

Очікується, що студенти будуть дотримуватися принципів академічної доброчесності, усвідомлювати наслідки її порушення. Детальніше за посиланням URL : <http://www.kntu.kr.ua/doc/dobro.pdf>

Відвідування занять

Є важливою складовою навчання. Очікується, що всі студенти відвідають лекції і лабораторні заняття курсу. Пропущені заняття повинні бути відпрацьовані не пізніше, ніж за тиждень до залікової сесії.

Поведінка на заняттях

Недопустимість: запізньєнь на заняття, списування та плагіат, несвоєчасне виконання поставленого завдання.

При організації освітнього процесу в Центральноукраїнському національному технічному університеті студенти, викладачі та адміністрація діють відповідно до:

- Положення про організацію освітнього процесу;
- Положення про організацію вивчення навчальних дисциплін вільного вибору;
- Положення про рубіжний контроль успішності і сесійну атестацію студентів ЦНТУ;
- Кодексу академічної доброчесності ЦНТУ.

10. Навчально-методична карта дисципліни

Тиждень, дата, академічні години	Тема, основні питання (розкривають зміст і є орієнтирами для підготовки до модульного і підсумкового контролю)	Форма діяльності (заняття) /формат	Матеріали	Література, інформаційні ресурси	Завдання, години	Вага оцінки	Термін виконання
Змістовний модуль 1. Робота з операційними системи.							
Тиж.1 (за розкладом) (2 год.)	Тема лекції 1. Захист рівня операційної системи. Частина 1. Основи термінології. Підвищення безпеки системи.	Лекція / <i>Face to face</i>	Презентація	5-12, 15-19, 22	Самостійно опрацювати теоретичний матеріал теми 1. (3 год.)	2 бали	Самостійна робота 1 тижня
Тиж.1 (за розкладом) (2 год.)	Тема ЛР 1. Розробка поштового клієнта. Частина 1. Створення технічного завдання. Розробка мережного програмного забезпечення.	Лабораторна робота / <i>Face to face</i>	Методичні рекомендації	1-5, 13-14, 20-21, 22-31	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 1. (3 год.)	2 бали	Самостійна робота 1 тижня
Тиж.2 (за розкладом) (2 год.)	Тема лекції 2. Захист рівня операційної системи. Частина 2. Особливості підвищення безпеки Windows	Лекція / <i>Face to face</i>	Презентація	5-12, 15-19, 22	Самостійно опрацювати теоретичний матеріал теми 2. (3 год.)	2 бали	Самостійна робота 2 тижня
Тиж.2 (за розкладом) (2 год.)	Тема ЛР 1. Розробка поштового клієнта. Частина 2. Формування пакету тестових даних, презентування роботи розробленої системи, оформлення звіту.	Лабораторна робота / <i>Face to face</i>	Методичні рекомендації	1-5, 13-14, 20-21, 22-31	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 1. (3 год.)	2 бали	Самостійна робота 2 тижня

Тиж.3 (за розкладом) (2 год.)	Тема лекції 3. Міжмережні екрани. Частина 1. Основи архітектури мереж. Приклади роботи з пакетами даних TCP/IP	Лекція / <i>Face to face</i>	Презентація	5-12, 15-19, 22	Самостійно опрацювати теоретичний матеріал теми 3. (3 год.)	2 бали	Самостійна робота 3 тижня
Тиж.3 (за розкладом) (2 год.)	Тема ЛР 2. Розробка сканера TCP/UDP. Частина 1. Створення технічного завдання. Розробка мережного програмного забезпечення.	Лабораторна робота / <i>Face to face</i>	Методичні рекомендації	1-5, 13-14, 20-21, 22-31	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 2. (3 год.)	2 бали	Самостійна робота 3 тижня
Тиж.4 (за розкладом) (2 год.)	Тема лекції 4. Міжмережні екрани. Частина 2. Міжмережний екран з відкритими вихідними текстами на платформі Linux.	Лекція / <i>Face to face</i>	Презентація	5-12, 15-19, 22	Самостійно опрацювати теоретичний матеріал теми 4. (3 год.)	2 бали	Самостійна робота 4 тижня
Тиж.4 (за розкладом) (2 год.)	Тема ЛР 2. Розробка сканера TCP/UDP. Частина 2. Формування пакету тестових даних, презентування роботи розробленої системи, оформлення звіту.	Лабораторна робота / <i>Face to face</i>	Методичні рекомендації	1-5, 13-14, 20-21, 22-31	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 2. (3 год.)	2 бали	Самостійна робота 4 тижня
Тиж.5 (за розкладом) (2 год.)	Тема лекції 5. Сканери портів. Частина 1. Internet Assigned Numbers Authority (IANA). Огляд найпоширеніших протоколів.	Лекція / <i>Face to face</i>	Презентація	5-12, 15-19, 22	Самостійно опрацювати теоретичний матеріал теми 5. (3 год.)	2 бали	Самостійна робота 5 тижня

Тиж.5 (за розкладом) (2 год.)	Тема ЛР 3. Розробка сканера безпеки. Частина 1. Створення технічного завдання. Розробка мережного програмного забезпечення.	Лабораторна робота / <i>Face to face</i>	Методичні рекомендації	1-5, 13-14, 20-21, 22-31	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 3. (4 год.)	2 бали	Самостійна робота 5 тижня
Тиж.6 (за розкладом) (2 год.)	Тема лекції 6. Сканери портів. Частина 2. Огляд сканерів портів.	Лекція / <i>Face to face</i>	Презентація	5-12, 15-19, 22	Самостійно опрацювати теоретичний матеріал теми 6. (4 год.)	2 бали	Самостійна робота 6 тижня
Тиж.6 (за розкладом) (2 год.)	Тема ЛР 3. Розробка сканера безпеки. Частина 2. Формування пакету тестових даних, презентування роботи розробленої системи, оформлення звіту.	Лабораторна робота / <i>Face to face</i>	Методичні рекомендації	1-5, 13-14, 20-21, 22-31	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 3. (4 год.)	2 бали	Самостійна робота 6 тижня
Тиж.7 (за розкладом) (2 год.)	Тема лекції 7. Сканери вразливостей. Частина 1. Теорія виявлення загроз в безпеці систем.	Лекція / <i>Face to face</i>	Презентація	5-12, 15-19, 22	Самостійно опрацювати теоретичний матеріал теми 7. (4 год.)	3 бали	Самостійна робота 7 тижня
Тиж.7 (за розкладом) (2 год.)	Тема ЛР 4. Розробка програмного забезпечення що реєструє дії користувача (KEYLOGGER). Частина 1. Створення технічного завдання. Розробка мережного програмного забезпечення.	Лабораторна робота / <i>Face to face</i>	Методичні рекомендації	1-5, 13-14, 20-21, 22-31	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 4. (4 год.)	3 бали	Самостійна робота 7 тижня
Максимальна кількість балів за змістовим модулем 1						30 балів	

Змістовний модуль 2. Сканери підсистем.

Тиж.8 (за розкладом) (2 год.)	Тема лекції 8. Сканери вразливостей. Частина 2. Огляд сканерів вразливостей.	Лекція / <i>Face to face</i>	Презентація	5-12, 15-19, 22	Самостійно опрацювати теоретичний матеріал теми 8. (3 год.)	2 бали	Самостійна робота 8 тижня
Тиж.8 (за розкладом) (2 год.)	Тема ЛР 4. Розробка програмного забезпечення що реєструє дії користувача (KEYLOGGER). Частина 2. Формування пакету тестових даних, презентування роботи розробленої системи, оформлення звіту.	Лабораторна робота / <i>Face to face</i>	Методичні рекомендації	1-5, 13-14, 20-21, 22-31	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 4. (3 год.)	2 бали	Самостійна робота 8 тижня
Тиж.9 (за розкладом) (2 год.)	Тема лекції 9. Мережні аналізатори. Частина 1. Теорія та особливості застосування мережних аналізаторів.	Лекція / <i>Face to face</i>	Презентація	5-12, 15-19, 22	Самостійно опрацювати теоретичний матеріал теми 9. (3 год.)	2 бали	Самостійна робота 9 тижня
Тиж.9 (за розкладом) (2 год.)	Тема ЛР 5. Вивчення механізму аналізу перехоплених пакетів протоколу ТСР/ІР. Частина 1. Створення технічного завдання. Розробка мережного програмного забезпечення.	Лабораторна робота / <i>Face to face</i>	Методичні рекомендації	1-5, 13-14, 20-21, 22-31	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 5. (3 год.)	2 бали	Самостійна робота 9 тижня
Тиж.10 (за розкладом) (2 год.)	Тема лекції 10. Мережні аналізатори. Частина 2. Огляд мережних аналізаторів.	Лекція / <i>Face to face</i>	Презентація	5-12, 15-19, 22	Самостійно опрацювати теоретичний матеріал теми 10. (3 год.)	2 бали	Самостійна робота 10 тижня

Тиж.10 (за розкладом) (2 год.)	Тема ЛР 5. Вивчення механізму аналізу перехоплених пакетів протоколу TCP/IP. Частина 2. Формування пакету тестових даних, презентування роботи розробленої системи, оформлення звіту.	Лабораторна робота / <i>Face to face</i>	Методичні рекомендації	1-5, 13-14, 20-21, 22-31	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 5. (3 год.)	2 бали	Самостійна робота 10 тижня
Тиж.11 (за розкладом) (2 год.)	Тема лекції 11. Системи виявлення вторгнень. Частина 1. Теорія та приклади сигнатур мережеских систем виявлення вторгнень.	Лекція / <i>Face to face</i>	Презентація	5-12, 15-19, 22	Самостійно опрацювати теоретичний матеріал теми 11. (3 год.)	2 бали	Самостійна робота 11 тижня
Тиж.11 (за розкладом) (2 год.)	Тема ЛР 6. Вивчення механізму розподілених атак типу «відмова в обслуговуванні» (DoS/DDoS). Частина 1. Створення технічного завдання. Розробка мережного програмного забезпечення.	Лабораторна робота / <i>Face to face</i>	Методичні рекомендації	1-5, 13-14, 20-21, 22-31	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 6. (3 год.)	2 бали	Самостійна робота 11 тижня
Тиж.12 (за розкладом) (2 год.)	Тема лекції 12. Системи виявлення вторгнень. Частина 2. Огляд систем виявлення вторгнень.	Лекція / <i>Face to face</i>	Презентація	5-12, 15-19, 22	Самостійно опрацювати теоретичний матеріал теми 12. (3 год.)	2 бали	Самостійна робота до 12 тижня

Тиж.12 (за розкладом) (2 год.)	Тема ЛР 6. Вивчення механізму розподілених атак типу «відмова в обслуговуванні» (DoS/DDoS). Частина 2. Формування пакету тестових даних, презентування роботи розробленої системи, оформлення звіту.	Лабораторна робота / <i>Face to face</i>	Методичні рекомендації	1-5, 13-14, 20-21, 22-31	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 6. (4 год.)	2 бали	Самостійна робота до 12 тижня
Тиж.13 (за розкладом) (2 год.)	Тема лекції 13. Засоби аналізу та керування. Частина 1. Основи використання системних, мережних та прикладних утиліт.	Лекція / <i>Face to face</i>	Презентація	5-12, 15-19, 22	Самостійно опрацювати теоретичний матеріал теми 13. (4 год.)	2 бали	Самостійна робота 13 тижня
Тиж.13 (за розкладом) (2 год.)	Тема ЛР 7. Вивчення механізму фішинг запитів. Частина 1. Створення технічного завдання. Розробка мережного програмного забезпечення.	Лабораторна робота / <i>Face to face</i>	Методичні рекомендації	1-5, 13-14, 20-21, 22-31	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 7. (4 год.)	2 бали	Самостійна робота 13 тижня
Тиж.14 (за розкладом) (2 год.)	Тема лекції 14. Засоби аналізу та керування. Частина 2. Програми моніторингу, конфігурації та аналізу системи.	Лекція / <i>Face to face</i>	Презентація	5-12, 15-19, 22	Самостійно опрацювати теоретичний матеріал теми 14. (4 год.)	3 бали	Самостійна робота 14 тижня

Тиж.14 (за розкладом) (2 год.)	Тема ЛР 7. Вивчення механізму фішинг запитів. Частина 2. Формування пакету тестових даних, презентування роботи розробленої системи, оформлення звіту.	Лабораторна робота / <i>Face to face</i>	Методичні рекомендації	1-5, 13-14, 20-21, 22-31	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 7. (4 год.)	3 бали	Самостійна робота 14 тижня
Максимальна кількість балів за змістовим модулем 2						30 балів	
Максимальна кількість балів за екзамен						40 балів	

11. Система оцінювання та вимоги

Види контролю: поточний, підсумковий.

Методи контролю: спостереження за навчальною діяльністю, усне опитування, письмовий контроль, тестовий контроль.

Форма підсумкового контролю: екзамен.

Контроль знань і умінь (поточний і підсумковий) з дисципліни «Мережні інформаційні технології» здійснюється згідно з кредитною трансферно-накопичувальною системою організації навчального процесу. Рейтинг студента із засвоєння дисципліни визначається за 100-бальною шкалою. Він складається з рейтингу навчальної роботи (засвоєння теоретичного матеріалу під час аудиторних занять та самостійної роботи, виконання лабораторних завдань), для оцінювання якої призначається 60 балів, та екзамену, максимальна оцінка за який складає 40 балів.

Розподіл балів, які отримують студенти при вивченні дисципліни «Мережні інформаційні технології»

Поточний контроль та самостійна робота														Екз.	Сума
Змістовий модуль 1. Робота з операційними системами.															
Л1	ЛР1	Л2	ЛР1	Л3	ЛР2	Л4	ЛР2	Л5	ЛР3	Л6	ЛР3	Л7	ЛР4		
2	2	2	2	2	2	2	2	2	2	2	2	3	3		
30															
Змістовий модуль 2. Сканери підсистем.															
Л8	ЛР4	Л9	ЛР5	Л10	ЛР5	Л11	ЛР6	Л12	ЛР6	Л13	ЛР7	Л14	ЛР7		
2	2	2	2	2	2	2	2	2	2	2	2	3	3		
30														40	100

Примітка: Т1, Т2,...,Т7 – тема, Л – теоретичні (лекційні) заняття, ЛР – лабораторні заняття

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою
		залік
90-100	A	зараховано
82-89	B	
74-81	C	
64-73	D	
60-63	E	
35-59	FX	не зараховано з можливістю повторного складання
1-34	F	не зараховано з обов'язковим повторним вивченням дисципліни

Критерії оцінювання знань і вмінь здобувачів визначені Положенням про організацію освітнього процесу в ЦНТУ (стор. 32-33).

12. Рекомендована література й джерела

Базова

1. Коваленко А.С., Коваленко А.В., Смирнов А.А., Смирнов С.А. Технология тестирования DOM XSS уязвимости. Scientific & practical cyber security journal (SPCSJ) Volume 1. Issue 1. P. 38-45 **Georgia**. Tbilisi. Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667. Режим доступу: <https://journal.scsa.ge/wp-content/uploads/2018/12/8-dom-xss-testing-technology-vulnerabilities.pdf> (**Закордонне фахове видання**)
2. A. Kovalenko, O. Kovalenko, O. Smirnov, S. Smirnov, V. Vialkova. The mathematical model of the testing technology for DOM XSS vulnerabilities. Scientific & practical cyber security journal (SPCSJ) Vol 2 Issue 1, 22-28 pp. [Електронний Журнал]. Georgia. Tbilisi: SCSA – 2018. Режим доступу: <https://journal.scsa.ge/ru/papers/the-mathematical-model-of-the-testing-technology-for-dom-xss-vulnerabilities-3/> (**Закордонне фахове видання**)
3. Коваленко А.С., Смірнова Т.В., Буравченко К.О., Щербань А.В., Багдасарян Е.К., «Проектування та оптимізація структурованих кабельних систем для автоматизації виробничих процесів підприємства» Сучасні інформаційні системи. 2022. Т. 6, № 1. С. 129-133. Режим доступу: <http://ais.khpi.edu.ua/article/view/254256/251522> (**Фахове видання. Категорія «Б»**)
4. Смірнова Т.В., Янков М.О., Грудік В.В., Горбов В.О., Коваленко А.С. «Планування радіопокриття та моделювання поширення радіосигналів мобільних мереж 5G для автоматизації виробничих процесів». Електронне моделювання, № 3, т. 44. С. 113-122. 2022. Режим доступу: <https://www.emodel.org.ua/uk/archive-ukr/2022/44-3-u/c-113-122> (**Фахове видання. Категорія «Б»**)
5. Коваленко А.С., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Смірнов О.А., Смірнов С.А., Основи безпеки в комп'ютерних мережах, **Навчальний посібник** – Кропивницький: вид. Лисенко В.Ф. 2018. – 177 с.
6. Vinit Jain. Wireshark Fundamentals. Apress Media. 2022. 267 с.
7. Derek Fisher. Application Security Program Handbook. Manning Publications. 2021. 155 с.
8. Alyssa Miller. Cybersecurity Career Guide. Manning Publications. 2022. 368 с.
9. Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, Andrew Martin. CyBOK The Cyber Security Body of Knowledge. The National Cyber Security Centre. 2019. 854 с.
10. Matt Walker. Certified Ethical Hacker Practice Exams. McGraw Hill. 2022. 352 с.
11. Samir Kumar Rakshit. Ethical Hacker's Penetration Testing Guide. BPB Online. 2022. 509 с.
12. Josh Armitage. Cloud Native Security Cookbook. O'Reilly Media. 2022. 516 с.

Допоміжна

13. Nishant Bhajaria. Data Privacy. Manning. 2022. 805 с.
14. Joshua S. Ponelat, Lukas L. Rosenstock. Designing APIs with Swagger and OpenAPI. Manning Publications. 2022. 426 с.
15. Loren Kohnfelder. Designing Secure Software. No Starch Press. 2022. 332 с.
16. Corey J. Ball. Hacking APIs. No Starch Press. 2022. 353 с.
17. Kevin Beaver. Hacking for Dummies. John Wiley & Sons. 2022. 419 с.
18. Cameron Wyatt PH.D. Kali Linux Tutorial. Independently published. 2021. 60 с.
19. Vijay Kumar Velu. Mastering Kali Linux for Advanced Penetration Testing. Packt Publishing Ltd. 2022. 573 с.

Методичне забезпечення

20. Коваленко А.С., Коваленко О.В., Марченко К.М. «Мережні інформаційні технології». Методичні вказівки до виконання лабораторних робіт для студентів денної форми навчання галузі 12 Інформаційні технології. – Кропивницький: ЦНТУ – 2022. – 60 с.
21. Коваленко А.С., Коваленко О.В., Марченко К.М. «Мережні інформаційні технології». Методичні вказівки до виконання контрольних робіт для студентів заочної форми навчання галузі 12 Інформаційні технології. – Кропивницький: ЦНТУ – 2022. – 60 с.

Інформаційні ресурси

22. Курс «Мережні інформаційні технології» на сервері дистанційної освіти ЦНТУ. – URL: <http://moodle.kntu.kr.ua/course/view.php?id=1669>
23. Онлайн-курси UDEMY. – URL: <https://www.udemy.com/> – платформа онлайн-курсів різних ІТ тематик.
24. Онлайн-курси Prometheus. – URL: <https://prometheus.org.ua/> – українська платформа безкоштовних онлайн-курсів
25. Онлайн-курси Coursera. – URL: <https://www.coursera.org> – платформа онлайн-курсів різних ІТ тематик.
26. <https://habr.com> – колективний блог з новинами та аналітичними статтями про інформаційні технології та програмування.
27. <http://stackoverflow.com/> – система питань і відповідей для професійних програмістів та новачків у програмуванні.
28. <https://dou.ua/> – український веб-сайт з елементами колективного блогу, створений для розповсюдження новин, аналітичних статей та свіжої інформації пов'язаної із інформаційними технологіями.
29. <https://www.google.com/> – основна пошукова платформа.
30. <https://www.youtube.com> – Відеохостинг, що надає користувачам послуги зберігання, доставки та показу відео. На платформі розміщено багато курсів ІТ спрямованості.
31. <https://biblprog.org.ua/ua/programming/> – каталог безкоштовних середовищ розроблення ПЗ.