Міністерство освіти і науки України
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра *інформаційних технологій та програмної інженерії*

"**ЗАТВЕРДЖУЮ**"
Завідувач кафедри

Білоус Ірина Володимирівна
"_____" _____ 20__ р.

***РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ***

# ПРОГРАМНІ ЗАСОБИ МЕРЕЖЕВИХ ТЕХНОЛОГІЙ

# (ВБ22)

**Освітня програма «*Інженерія програмного забезпечення*»**

Рівень вищої освіти – *перший (бакалаврський)*

Спеціальність *121 – Інженерія програмного забезпечення*

Мова навчання: *українська*

Статус дисципліни: *вибіркова*

| Форма навчан. | Рік навч. | Сем. | Розподіл годин | | | | | Разом | За тиждень | | ІНДЗ | Контр. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Всього ауд. | Лек | Прак | Лаб. | СРС | | Ауд. | СРС | | |
| Денна | 4 | 8 | 50 | 30 | 0 | 20 | 100 | 150 | 5 | 10 | РГР | З |

Чернігів – 2021 рік

Робоча програма *Програмні засоби мережевих технологій*
(назва навчальної дисципліни)
для здобувачів вищої освіти галузі знань *12 – Інформаційні технології* спеціальності *121 – Інженерія програмного забезпечення*
Розробник робочої навчальної програми:
*викладач кафедри інформаційних технологій та програмної інженерії НУ «Чернігівська політехніка»* _____ *(І.А. Бурмака)*
(підпис) (прізвище та ініціали)

Робочу програму схвалено на засіданні кафедри *інформаційних технологій та програмної інженерії*

Протокол від "31" серпня *2021*року № _1

Завідувач кафедри *інформаційних технологій та програмної інженерії*

_____ (*Білоус І.В.*)
(підпис) (прізвище та ініціали)

## Abstract

**Network defending technology software (VB 22)**

**2021/2022 Sem.2**

**Course Description**

The purpose of discipline " Network defending technology software" is a theoretical and practical training in activities related to the construction of secure networked automated systems, as well as teaching the principles and methods of information security in computer networks.

The tasks of the course:

• study of typical security threats in computer networks; teaching and cryptographic software and hardware methods of information security in computer networks;

• acquisition of skills setup and operation of the means of ensuring security in computer networks;

• mastery of tools and methods to design and build a secure network of automated systems;

• mastery of tools and methods to detect and neutralize attempts to breach security in computer networks.

As the result of mastering the discipline a student should:

***Know:***

- tools and methods of storage and transmission of authentication information;
- mechanisms for implementing attacks in network TCP / IP;
- basic protocols to identify and authenticate subscribers;
- defense mechanisms and tools to ensure network security;
- tools and methods of prevention and intrusion detection.

***Learning outcomes:***

- formulate and configure security policy major operating systems, and local area computer networks built based on them;
- use secure protocols, firewalls, and intrusion detection tools to protect information networks;
- implement measures against violation of network security using various software and hardware protection.

## 1 Опис навчальної дисципліни

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><th>денна форма навчання</th></tr>
<tr><td rowspan="2">Кількість кредитів – 5</td><td>Галузь знань<br>12 «Інформаційні технології»</td><td rowspan="2">Вибіркова</td></tr>
<tr><td></td></tr>
<tr><td>Модулів – 5</td><td rowspan="5">Спеціальність:<br>121 «Інженерія програмного забезпечення»</td><td>Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 4</td><td>4-й</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 150</td><td>8-й</td></tr>
<tr><td rowspan="8">Освітньо-кваліфікаційний рівень:<br>бакалавр</td><td>Лекції</td></tr>
<tr><td rowspan="8">Тижневих годин: аудиторних – 5; самостійної роботи і індивідуальної студента – 10</td><td>30 год.</td></tr>
<tr><td>Лабораторні</td></tr>
<tr><td>20 год.</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>100 год.</td></tr>
<tr><td>Вид контролю:</td></tr>
<tr><td>Залік</td></tr>
</table>

**Примітка**.
Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить 50:100=1:2.

Передумовою для вивчення дисципліни є успішне засвоєння дисциплін "*Операційні системи*", "*Архітектура комп'ютерних мереж*", "*Програмно-апаратні засоби персональних комп'ютерів*" та здобуті такі результати навчання, як вміння складати програми мовою С, знання апаратних та програмних засобів комп'ютерних мереж.

Дисципліна може використовуватися під час підготовки випускної кваліфікаційної роботи бакалавра за відповідною темою.

## 2 Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни “*Програмні засоби мережевих технологій*” є закріплення та розвиток фахових компетентностей бакалавра в галузі знань *12 – Інформаційні технології* із застосування у організації та захисту комп’ютерних мереж. Зокрема, це:

– ЗК1. здатність до абстрактного мислення, аналізу та синтезу.

– ЗК2. здатність застосовувати знання у практичних ситуаціях.

– ЗК5. здатність вчитися і оволодівати сучасними знаннями.

– ЗК6. здатність до пошуку, оброблення та аналізу інформації з різних джерел.

– ЗК13. Здатність працювати в міжнародному контексті.

– ФК17. Здатність розробляти архітектури, модулі та компоненти програмних систем.

– ФК19. Здатність дотримуватися специфікацій, стандартів, правил і рекомендацій в професійній галузі при реалізації процесів життєвого циклу.

– ФК20. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки)

– ФК21. Володіння знаннями про інформаційні моделі даних, здатність створювати програмне забезпечення для зберігання, видобування та опрацювання даних.

– ФК24. Здатність накопичувати, обробляти та систематизувати професійні знання щодо створення і супроводження програмного забезпечення та визнання важливості навчання протягом всього життя.

– ФК27. Здатність обґрунтовано обирати та освоювати інструментарій з розробки та супроводження програмного забезпечення.

– ФК28. Здатність до алгоритмічного та логічного мислення.

## 3 Очікувані результати навчання з дисципліни

Навчальна дисципліна “*Програмні засоби мережевих технологій*” має допомогти сформувати наступні програмні результати навчання:

– ПР01. Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.

– ПР04. Знати і застосовувати професійні стандарти і інші нормативно-правові документи в галузі інженерії програмного забезпечення.

– ПР15.Мотивовано обирати мови програмування та технології розробки для розв'язання завдань створення і супроводження програмного забезпечення.

– ПР18. Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних.

– ПР21.Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних

програмних систем.

Після вивчення дисципліни студенти **повинні знати*:***

– механізми реалізації атак в мережах TCP/IP;

– основні протоколи ідентифікації і автентифікації абонентів мережі;

– захисні механізми та засоби забезпечення мережевої безпеки; засоби та методи запобігання та виявлення вторгнень;

– алгоритми та фреймворки для створення захищених мережевих додатків.

У результаті опанування навчальною дисципліною студенти **повинні вміти** :

– формулювати і налаштовувати політику безпеки основних операційних систем, а також локальних комп'ютерних мереж, побудованих на їх основі;

– застосовувати захищені протоколи, міжмережеві екрани і засоби виявлення вторгнень для захисту інформації в мережах;

– здійснювати заходи протидії порушенням мережевої безпеки з використанням різних програмних і апаратних засобів захисту;

– створювати захищені мережеві додатки;

– створювати мережні сервіси автентифікації, авторизації та обліку.

## 4 Критерії оцінювання результатів навчання

З тими студентами, які до проведення підсумкового семестрового контролю не встигли виконати всі обов’язкові види робіт та мають підсумкову оцінку менше 40 балів (за шкалою оцінювання), проводяться додаткові індивідуальні заняття, за результатами яких визначається, наскільки глибоко засвоєний матеріал, та чи необхідне повторне вивчення дисципліни.

Дисципліну можна вважати такою, що засвоєна, якщо студент:

***1) знає:***

– механізми реалізації атак в мережах TCP / IP;

– основні протоколи ідентифікації і автентифікації абонентів мережі;

– захисні механізми та засоби забезпечення мережевої безпеки;

– засоби та методи запобігання та виявлення вторгнень

– алгоритми та фреймворки для створення захищених мережевих додатків.

***2) вміє:***

– формулювати і налаштовувати політику безпеки основних операційних систем, а також локальних комп'ютерних мереж, побудованих на їх основі;

– застосовувати захищені протоколи, міжмережеві екрани і засоби виявлення вторгнень для захисту інформації в мережах;

– створювати захищені мережеві додатки;

– здійснювати заходи протидії порушенням мережевої безпеки з використанням різних програмних і апаратних засобів захисту.

## 5 Засоби діагностики результатів навчання

Для визначення рівню засвоєння навчального матеріалу застосовуються наступні методи контролю:

- поточне опитування на лекціях;

- оцінки за захист лабораторних робіт;
- модульний тестовий контроль;
- залік.

Для діагностики знань використовується модульно-рейтингова система зі 100-бальною шкалою оцінювання.

## 6. Програма навчальної дисципліни

**Змістовний модуль 1. Типові загрози мережевій безпеці**

**Тема № 1. Мережеві атаки**

Стадії проведення мережевої атаки. Класифікації мережевих загроз, вразливостей і атак. Атаки на реалізації мережевих протоколів, окремі вузли та служби. Основні механізми проведення мережевих атак на різних рівнях моделі ISO / OSI. Проблеми забезпечення конфіденційності, цілісності та доступності інформації на різних рівнях моделі ISO / OSI.

**Тема № 2. Методи перехоплення мережевих з'єднань в мережах TCP/IP**

Імперсонації наосліп. Десинхронізація TCP-з'єднань. Атаки, спрямовані на мережеву інфраструктуру.

**Тема №3. Приклади атак в мережах TCP/IP**

Технічні заходи захисту від мережевих атак. Примус до прискореної передачі. Атаки, спрямовані на відмову в обслуговуванні. Зміна конфігурації та стану хостів. Недоліки протоколів сімейства TCP / IP з точки зору забезпечення безпеки інформації.

**Змістовний модуль 2. Криптографічні методи захисту інформації в комп'ютерних мережах**

**Тема № 4. Криптографічні протоколи забезпечення безпеки**

Протоколи автентифікації на прикладному рівні. Протокол Kerberos. Протоколи автентифікації на транспортному рівні. Протокол SSL / TLS. Переваги і недоліки автентифікації на різних рівнях моделі ISO / OSI.

**Тема № 5. Захист віртуальних приватних мереж (VPN)**

Призначення, основні можливості, принципи функціонування та варіанти реалізації VPN. Організація тунелювання на різних рівнях моделі ISO / OSI. Переваги і недоліки застосування VPN. Протокол IPSEC. Протоколи AH і ESP. Особливості роботи протоколу IPSEC в тунельному і транспортному режимах. Протокол управління ключами ISAKMP / Oakley. Використання протоколу L2TP для організації віртуальних приватних мереж.

**Змістовний модуль 3. Захищені мережеві додатки**

**Тема № 6. Захищений обмін даними в мережевих додатках**

Автентифікація мережевих додатків. Захищені протоколи для швидкого та захищеного обміну даними.

**Тема № 7. Розробка захищених мережевих додатків**

Шифрування, забезпечення цілісності з використанням програмного інтерфейсу SSPI. Програмний інтерфейс openssl.

## 7 Структура навчальної дисципліни

| Назви змістових модулів і тем | | Кількість годин для денної/заочної форми навчання | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Всього | | У тому числі | | | | | | | |
| | | | | Лек. | | Пр. | | Лаб. | | С.р. | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| **Модуль 1. Типові загрози мережевій безпеці** | | | | | | | | | | | |
| 1 | Тема № 1. Мережеві атаки | 13 | | 3 | | | | | | 10 | |
| 2 | Тема № 2. Методи перехоплення мережевих з'єднань в мережах TCP/IP | 15 | | 3 | | | | 2 | | 10 | |
| 3 | Тема № 3. Приклади атак в мережах TCP/IP | 21 | | 4 | | | | 2 | | 15 | |
| | **Разом за змістовим модулем 1** | **49** | | **10** | | | | **4** | | **35** | |
| **Модуль 2. Криптографічні методи захисту інформації в комп'ютерних мережах** | | | | | | | | | | | |
| 4 | Тема № 4. Криптографічні протоколи забезпечення безпеки | 23 | | 3 | | | | 4 | | 16 | |
| 5 | Тема №5. Захист віртуальних приватних мереж (VPN) | 21 | | 3 | | | | 4 | | 14 | |
| | **Разом за змістовим модулем 2** | **44** | | **6** | | | | **8** | | **30** | |
| **Модуль 3. Захищені мережеві додатки** | | | | | | | | | | | |
| 6 | Тема № 6. Захищений обмін даними в мережевих додатках | 26 | | 7 | | | | 4 | | 15 | |
| 7 | Тема № 7. Розробка захищених мережевих додатків | 21 | | 7 | | | | 4 | | 20 | |
| | **Разом за змістовим модулем 3** | **47** | | **14** | | | | **8** | | **35** | |
| | **Усього годин за дисципліну** | **150** | | **30** | | | | **20** | | **100** | |

## 8 Теми лабораторних занять

| № з/п | Назва теми | Кількість годин (д/з) |
|---|---|---|
| 1 | Атаки в мережах TCP/IP | 4 |
| 2 | Дослідження криптографічних протоколів | 4 |
| 3 | Налаштування та захист VPN | 4 |
| 4 | Створення захищених мережевих додатків | 8 |
| **Разом** | | **20** |

## 9 Самостійна робота

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | Підготовка до лабораторних робіт | 35 |
| 2 | Підготовка до тестів | 10 |
| 3 | Засвоєння лекційного матеріалу | 35 |
| 4 | Виконання РГР | 20 |
| | Разом | 100 |

## 10 Індивідуальні завдання

Робочим планом передбачено виконання лабораторних робіт. Докладна інформація щодо змісту, варіантів завдань, порядку оформлення та захисту лабораторних робіт міститься в [14.1]. Також передбачено виконання індивідуальних завдань з дисципліни у вигляді розрахунково-графічної роботи (РГР). Конкретна мета РГР, залежно від варіанту завдання, полягає у розробці захищеного мережевого додатку, стійкого до основних сучасних мережевих атак. Виконання, оформлення та захист РГР здійснюється здобувачем вищої освіти в індивідуальному порядку відповідно до методичних рекомендацій.

Докладна інформація про РГР міститься в [14.2]. Форми контролю та оцінювання виконання РГР наведені в таблиці.

| Вид роботи | Форма контролю | Кількість балів | |
|---|---|---|---|
| Виконання індивідуального завдання відповідно до варіанта | 1. Відповідність умовам завдання | 0… | 2 |
| Пояснювальна записка | 1. Обґрунтованість рішень | 0… | 2 |
| | 2. Посилання на першоджерела | 0… | 2 |
| | 3. Відповідність оформлення вимогам | 0… | 2 |
| | 4. Своєчасність здачі | 0… | 2 |
| Захист РГР | Самостійність виконання (відповіді на запитання) | 0… | 10 |
| **Разом** | | **0…** | **20** |

## 11 Методи контролю

Оцінювання знань здобувачів здійснюється відповідно до «Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти Національного університету «Чернігівська політехніка».

Політика дотримання академічної доброчесності ґрунтується на «Кодексі академічної доброчесності Національного університету «Чернігівська політехніка»».

З дисципліни здобувач може набрати до 80% підсумкової оцінки за виконання всіх видів робіт, що виконуються протягом семестру і до 20% підсумкової оцінки – на диференційованому заліку.

Виконання та особистий захист усіх лабораторних робіт, зазначених у робочій навчальній програмі з дисципліни, є обов'язковим. Поточний контроль проводиться шляхом спілкування із здобувачами під час лекцій та консультацій та опитувань здобувачів під час захисту лабораторних робіт [14.1] та РГР [14.2].

Результати поточного контролю за відповідний модуль оприлюднюються викладачем на наступному аудиторному занятті. Бали, які набрані здобувачем під час модульних контролів, складають оцінку поточного контролю.

Диференційовані заліки складаються здобувачами відповідно до розкладу, який доводиться до викладачів і здобувачів не пізніше, ніж за тиждень до початку залікового тижня.

Семестровий контроль у вигляді *заліку* проводиться на останньому тижні навчального семестру (заліковий тиждень) з трьома запитаннями. Оцінка за результатами вивчення дисципліни формується шляхом додавання підсумкових результатів поточного контролю до залікової оцінки. Ті здобувачі, які не виконали всі обов'язкові види робіт та за результатами роботи в семестрі набрали менше 40 балів, мають пройти повторний курс вивчення дисципліни. Взаємозв'язок між набраними балами і оцінкою наведений у розділі 12.

Якщо відповідь повна і зміст відповіді здобувача повністю відповідає сутності поставлених запитань, можна отримати від 17 до 20 балів. В тому випадку, коли здобувач відповідає без грубих помилок, можна отримати від 12 до 16 балів. Якщо при відповіді здобувач допускає грубі помилки, і всі запитання вирішені менш, ніж на половину, можна отримати від 8 до 12 балів. За не відповідь хоча б на одне запитання, не можна отримати більше 8 балів.

Якщо здобувач виконав всі види робіт протягом семестру та набрав не менше 60 балів, то він, за бажанням, може залишити набрану кількість балів як підсумкову оцінку і не складати залік.

В випадку повторного складання заліку всі набрані протягом семестру бали анулюються, а повторний залік складається з трьома питаннями. Питання до заліку знаходяться у [16.1].

У випадку, якщо здобувач протягом семестру не виконав в повному обсязі передбачених робочою програмою всіх видів навчальної роботи, має невідпрацьовані лабораторні роботи або не набрав мінімально необхідну кількість балів (40), він не допускається до складання заліку під час залікового тижня, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань здобувачів вищої освіти Національного університету «Чернігівська політехніка».

Повторне складання заліку з метою підвищення позитивної оцінки не дозволяється.

## 12 Розподіл балів, які отримують студенти

Поточний контроль за модулями

| Модуль за тематичним планом дисципліни та форма контролю | Кількість балів |
|---|---|
| **Змістовий модуль 1. Типові загрози мережевій безпеці** | **0… 30** |
| 1 Повнота ведення конспектів занять | 0… 5 |
| 2 Відсутність пропусків занять | 0… 5 |
| 3 Результати захисту лабораторних робіт | 0… 20 |
| **Змістовий модуль 2. Криптографічні методи захисту інформації в комп'ютерних мережах** | **0… 30** |
| 1 Повнота ведення конспектів занять | 0… 5 |
| 2 Відсутність пропусків занять | 0… 5 |
| 3 Результати захисту лабораторних робіт | 0… 20 |
| **Змістовий модуль 3. Захищені мережеві додатки** | **0… 30** |
| 1 Повнота ведення конспектів занять | 0… 5 |
| 2 Відсутність пропусків занять | 0… 5 |
| 3 Результати захисту лабораторних робіт | 0… 20 |

Підсумковий модульний контроль

| Модуль за тематичним планом дисципліни та вид контролю | Кількість балів |
|---|---|
| **Змістовий модуль 1** | **0… 60** |
| 1 Тестова модульна контрольна робота | 0… 30 |
| 2 Результат поточного контролю | 0… 30 |
| **Змістовий модуль 2** | **0… 60** |
| 1 Тестова модульна контрольна робота | 0… 30 |
| 2 Результат поточного контролю | 0… 30 |
| **Змістовий модуль 3** | **0… 60** |
| 1 Тестова модульна контрольна робота | 0… 30 |
| 2 Результат поточного контролю | 0… 30 |
| **Зважена модульна оцінка** | **0… 60** |
| **Оцінка за РГР** | **0... 20** |
| **Семестрова оцінка поточного контролю** | **0... 80** |

**Шкала оцінювання: національна та ECTS**

| Сума балів за всі види навчальної діяльності | Оцінка ECTS | Оцінка за національною шкалою | |
|---|---|---|---|
| | | для екзамену, курсової роботи | для заліку |
| 90 – 100 | **A** | відмінно | зараховано |
| 82-89 | **B** | добре | |
| 75-81 | **C** | | |

| | | | |
|---|---|---|---|
| 66-74 | **D** | задовільно | |
| 60-65 | **E** | | |
| 0-59 | **FX** | незадовільно з можливістю повторного складання | не зараховано з можливістю повторного складання |

## 13 Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

Лекційний матеріал подається у вигляді презентацій за допомогою медіа-проектора або виведення на монітори робочих станцій. Під час лекцій аналізуються проблемні ситуації, організується зворотний зв'язок з аудиторією шляхом формулювання запитань і стислих відповідей з обох сторін.

Особливістю виконання лабораторних робіт є застосування спеціального обладнання та прикладного програмного забезпечення навчальної лабораторії кафедри ІТтаПІ.

## 14 Методичне забезпечення

1. Програмні засоби мережевих технологій. Методичні вказівки до виконання лабораторних робіт для студентів спеціальності 121 «Інженерія програмного забезпечення». – Чернігів: ЧНТУ, 2019. – 31 с. – Електронні данні. – Режим доступу: http://eln.stu.cn.ua/course/view.php?id=3427, обмежений. – Заголовок з екрану.
2. Програмні засоби мережевих технологій. Методичні вказівки до виконання розрахунково-графічної та самостійної роботи для студентів спеціальності 121 «Інженерія програмного забезпечення». – Чернігів: ЧНТУ – 2019. – 11 с. – Електронні данні. – Режим доступу: http://eln.stu.cn.ua/course/view.php?id=3427, обмежений. – Заголовок з екрану.

## 15 Рекомендована література

### Базова


1. БурячокВ.Л. Технології забезпечення безпекимережевої інфраструк-тури. [Підручник]/В.Л.Бурячок, А.О.Аносов, В.В.Семко, В.Ю.Со-колов, П.М.Складанний. –К.:КУБГ, 2019. –218с.
2. Захист інформації в комп'ютерних системах та мережах : навч. посібник / С. Г. Семенов [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : НТУ "ХПІ", 2014. – 251 с.
3. ДСТУ 3396.2-97 державний стандарт України.Захист інформації. Технічний захист інформації. Терміни та визначення. http://www.czo.gov.ua/index.php?page=docs&id=41
4. М. В. Грайворонський, О. М. Новіков ; за заг. ред. М.З.Згуровського. Безпека інформаційно-комунікаційних систем — К. : Видавнича група BHV, 2009. — 608 с. Є друкований і електронний варіанти в бібліотеці СумДУ

### Допоміжна

1. Прикладна криптологія:системи шифрування:підручник/ О.Г. Корченко, В.П. Сіденко, Ю.О. Дрейс.–К.:ДУТ,2014. –448с.:іл.
2. Організація комп'ютерних мереж [Електронний ресурс]: підручник: для студ.спеціальності 121 «Інженерія програмного забезпечення» та 122«Комп'ютерні науки»/ КПІ ім. Ігоря Сікорського; Ю.А. Тарнавський, І.М.Кузьменко. –Київ : КПІ ім. Ігоря Сікорського, 2018. –259с.
3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд-е 2-е, испр.: Пер с англ.–М.: "Вильямс", 2003.–1104 с.

## 16 Електронні інформаційні ресурси

1. Система дистанційного навчання НУ «Чернігівська політехніка». Курс: Програмні засоби мережевих технологій. – [Електронний ресурс]. – Режим доступу : https://eln.stu.cn.ua/course/view.php?id=3427
2. Cisco network academy. – [Електронний ресурс]. – Режим доступу : https://netacad.com
3. Mikrotik routers and wireless. – [Електронний ресурс]. – Режим доступу : https://mikrotik.com
4. RFC 2411 – IP Security Document Roadmap. – [Електронний ресурс]. – Режим доступу : https://tools.ietf.org/html/rfc2411
5. RFC 6071 – IP Security(IPSec). – [Електронний ресурс]. – Режим доступу : https://tools.ietf.org/html/rfc6071