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

Системи захисту обчислювальних мереж

(ВБ21)

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	3

Чернігів – 2021 рік

Робоча програма _____*Системи захисту обчислювальних мереж*_____
(назва навчальної дисципліни)
для здобувачів вищої освіти галузі знань *12 – Інформаційні технології*
спеціальності *121 – Інженерія програмного забезпечення*
Розробник робочої навчальної програми:
доцент кафедри інформаційних технологій та програмної інженерії НУ «Чернігівська політехніка», д.т.н. _____ *(Ю.М. Лисецький)*
(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

Computer network protection systems (VB 21)
2021/2022 Sem. 2

Course Description

After mastering the discipline the students formed accurate system holistic understanding of the complex issues that arise and must be solved by the process of planning and using computer systems and networks. Main attention is paid to security issues.

In the discipline studies the networks protocols used for security connections, planning and development of network systems, security models of actual computer systems, some questions related to network protocols choice for new computer systems, implementation of transport protocols for real-time systems, protocols of authorization and authentication, network security tools.

Contents: computer networks, protocols, computer system, authentication, authorization, accounting, information types, security models, security politics, network security systems.

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
12 «Інформаційні технології»</td><td rowspan="2">Вибіркова</td></tr>
<tr><td></td></tr>
<tr><td>Модулів – 5</td><td rowspan="5">Спеціальність:
121 «Інженерія програмного забезпечення»</td><td>Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 3</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>Лекції</td></tr>
<tr><td rowspan="8">Тижневих годин: аудиторних – 5; самостійної роботи і індивідуальної студента – 10</td><td rowspan="8">Освітньо-кваліфікаційний рівень:
бакалавр</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

Передумови для вивчення дисципліни - *є дисципліна «Архітектура комп'ютерних мереж»*.

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

2 Мета та завдання навчальної дисципліни

Метою викладання дисципліни "*Системи захисту обчислювальних мереж*" є необхідність формування у здобувачів чіткої системи уявлень про цілісний комплекс проблем, що мають бути вирішені у процесі проектування та розробки комп'ютерних мереж і систем, які відповідають вимогам кваліфікаційної характеристики фахівця. 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.

– 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)

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

– ФК26. Здатність здійснювати процес інтеграції системи, застосовувати стандарти і процедури управління змінами для підтримки цілісності, загальної функціональності і надійності програмного забезпечення.

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

– ФК28. Здатність до алгоритмічного та логічного мислення.

– ФК29. Здатність до розробки і реалізації методів тестування та випробування програмних комплексів.

3 Очікувані результати навчання з дисципліни

Навчальна дисципліна " *Системи захисту обчислювальних мереж* " 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.

– ПР14.Застосовувати на практиці інструментальні програмні засоби1 доменного аналізу, проектування, тестування, візуалізації, вимірювань та документування програмного забезпечення.

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

– 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.

– ПР25. Мати навички виконання певних ролей в IT-проектах будь-якої складності.

Основними завданнями вивчення дисципліни "*Системи захисту обчислювальних мереж* " є:

1) Вивчення побудови, принципу дії, систем захисту обчислювальних мереж, таких як брандмауери та IDS.

2) Вивчення мережевих протоколів, що використовуються для автентифікації, обміну ключами, конфіденційного обміну повідомленнями.

3) Набуття практичних навичок роботи з сучасними системами організації віртуальних приватних мереж.

Згідно з вимогами освітньо-професійної програми студенти повинні:

знати :

– існуючи мережні стандарти та протоколи забезпечення конціденційності та цілосності;

– основні мережеві протоколи безпеки та автентифікації

– основні моделі інформаційної безпеки;

– основи криптографічних алгоритмів;

– види та особливості моделей комп'ютерних систем та мереж;

– засоби попередження та вивлення мережевих атак;

– методи захисту від атак в дротових та бездротових мережах.

вміти :

– робити вибір протоколів та мережевого обладнання, необхідного для забезпечення інформаційної безпеки;

– робити вибір методу доступу до каналу передачі даних;

– створювати віртуальні приватні мережі;

– створювати мережні сервіси автентифікації, авторизації та обліку

– встановлювати та налаштовувати мережеві екрани;

– налаштовувати системи виявлення та запобігання вторгнень;

– попереджувати та захищати мережі від найбільш поширених типів атак.

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 до 39 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 здобувач:

1) **знає**:

– існуючи мережні стандарти та протоколи забезпечення конціденційності та цілосності;

– основні мережеві протоколи безпеки та автентифікації

– основні моделі інформаційної безпеки;

– основи криптографічних алгоритмів;
– види та особливості моделей комп'ютерних систем та мереж;
– засоби попередження та вивлення мережевих атак;
– методи захисту від атак в дротових та бездротових мережах.

2) **вміє**:

– робити вибір протоколів та мережевого обладнання, необхідного для забезпечення інформаційної безпеки;
– робити вибір методу доступу до каналу передачі даних;
– створювати віртуальні приватні мережі;
– створювати мережні сервіси автентифікації, авторизації та обліку
– встановлювати та налаштовувати мережеві екрани;
– налаштовувати системи виявлення та запобігання вторгнень;
– попереджувати та захищати мережі від найбільш поширених типів атак.

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

Змістовий модуль 1. Протоколи та засоби ідентифікації, авторизації, автентифікації та обліку мережевих ресурсів.

Тема 1. Вступ

Централізоване та розподілене управління мережею. Проблеми що виникають при створенні комп'ютерних мереж і систем. Особливості інформації, що передається в системах. База для вивчення дисципліни - операційні систем Linux та FreeBSD. Основні джерела інформації: стандарти ICTT/ITU, рекомендовані стандарти RFC, а також документація до програмних пакетів що вивчаються. Допоміжні джерела інформації в мережі Інтернет.

Тема 2. Типи інформації та моделі інформаційної безпеки

Критерії оцінки інформаційної безпеки. Моделі безпеки комп'ютерних систем. Мандатна, дискреційна та рольова політики безпеки комп'ютерних систем. Класифікація типів інформації. Визначення необхідних заходів для забезпечення конфіденційності даних.

Тема 3. Мережеві протоколи ідентифікації та автентифікації

Мережеві протоколи: Kerberos, CHAP, PAP, RADIUS, DIAMETER, LDAP. Системи AAA на основі протоколу RADIUS та його розширень. Налагодження серверу AAA на основі FreeRADIUS та PostgreSQL. Налагодження сереверу на основі FreeDIAMETER та PostgreSQL. Налагодження серверу AAA на основі

пакету OpenLDAP. Методика планування дерева LDAP. Протокол SSL / TLS. Переваги і недоліки автентифікації на різних рівнях моделі ISO / OSI.

Тема 4. Протоколи безпеки.

Протоколи обміну ключами. Протоколи без арбітра. Протоколи з арбітром. Алгоритми цифрового підпису. Схеми ідентифікації. Спеціальні алгоритми для протоколів.

Змістовий модуль 2. Системи захисту обчислювальних мереж

Тема №5. Засоби захисту локальних мереж при підключенні до Інтернет

Міжмережеві екрани (МЕ). Місце і роль МЕ в забезпеченні мережевої безпеки. Класифікація МЕ. Вимоги до МЕ. Основні можливості та схеми розгортання МЕ. Переваги і недоліки МЕ. Побудова правил фільтрації. Методи мережевий трансляції адрес (NAT). Шлюзи рівня додатків. Реалізація мережевої політики безпеки з використанням МЕ. Методи обходу міжмережевих екранів.

Тема № 6. Захист серверів і робочих станцій. Засоби та методи запобігання та виявлення вторгнень

Системи виявлення вторгнень (СВВ). Призначення та можливості засобів виявлення вторгнень на хости, протоколи і мережеві служби. Місце і роль засобів виявлення вторгнень в загальній системі забезпечення мережної безпеки. Класифікація СОВ. Виявлення атак на основі сигнатур атак і виявлення аномалій. Аудит прикладних служб. Засоби виявлення вразливостей мережевих служб. Способи протидії вторгненням. Системи віртуальних пасток (Honey Pot і Padded Cell).

Змістовий модуль 3. Механізми реалізації атак та захист від них.

Тема № 7. Механізми реалізації атак в дротових та бездротових мережах

Атаки направлені на переривання підключення. MITM атаки. Особливості бездротових мереж та атаки на них. Різновиди атак на бездротові мережі. Атаки, спрямовані на мережеву інфраструктуру.

Тема № 8. Захист від атак дротових та бездротових мереж

Основні заходи для попередження вторгнень до дротових та бездротових мереж та усунення їх вразливостей до атак. Виявлення та локалізація вторгнень до дротових та бездротових мереж.

Тема № 9. Механізми реалізації атак в мережах TCP / IP

Типи атак в мережах TCP/IP. Атаки, спрямовані на відмову в обслуговуванні. Віддалене визначення версії ОС з використанням особливостей реалізації стека протоколів TCP / IP. Методи сканування портів. Методи виявлення пакетних сніфера. VPN та їх вразливості. Методи обходу МЕ. Імперсонації наосліп. Десинхронізація TCP-з'єднань.

Тема №10. Захист від атак в TCP/IP мережах

Технічні заходи захисту від мережевих атак. Недоліки протоколів сімейства TCP / IP з точки зору забезпечення безпеки інформації.

7 Структура навчальної дисципліни

Назви змістових модулів і тем		Кількість годин для денної форми навчання			
		Всього	У тому числі		
			Лек.	Лаб.	С.р.
Модуль 1					
Змістовий модуль 1. Протоколи та засоби ідентифікації, авторизації, автентифікації та обліку мережевих ресурсів					
1	Вступ	6	2		4
2	Типи інформації та моделі інформаційної безпеки	10	2		8
3	Мережеві протоколи ідентифікації та автентифікації	24	4	4	16
4	Протоколи безпеки.	10	2		8
	Разом за змістовим модулем 1	**50**	**10**	**4**	**36**
Змістовий модуль 2. Системи захисту обчислювальних мереж					
5	Засоби захисту локальних мереж при підключенні до Інтернет	22	4	4	14
6	Захист серверів і робочих станцій. Засоби та методи запобігання та виявлення вторгнень	26	6	4	16
	Разом за змістовим модулем 2	**48**	**10**	**8**	**30**
Змістовий модуль 3. Механізми реалізації атак та захист від них.					
7	Механізми реалізації атак в дротових та бездротових мережах	12	4		8
8	Захист від атак дротових та бездротових мереж	8	4	4	10
9	Механізми реалізації атак в мережах TCP / IP	13	6		7
10	Захист від атак в TCP/IP мережах	19	6	4	9
	Разом за змістовим модулем 3	**52**	**20**	**8**	**24**
	Усього годин за дисципліну	**150**	**30**	**20**	**100**

8 Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Протоколи аутентифікації на транспортному рівні. Протокол SSL / TLS	4
2	Створення віртуальної приватної мережі на базі PPTP сервера PPTPd Налаштування автентифікації, авторизації та обліку VPN користувачів за допомогою RADIUS сервера FreeRADIUS, з використанням модуля	4
3	Налаштування мережевого екрану та використання його для попередження атак.	4

4	Система виявлення вторгнень та її налаштування	4
5	Налаштування HTTP-проксі сервера Squid для виділення доступу до веб ресурсів	4
Разом		**20**

9 Самостійна робота

№ з/п	Назва теми	Кількість годин
Семестр 8		
1	Засвоєння лекційного матеріалу	16
2	Підготовка до лабораторних робіт	16
3	Підготовка звітів по лабораторним роботам	16
4	Робота з методичними вказівками, основною та додатковою літературою	16
5	Самостійне вивчення на основі навчальної літератури наступних питань: а) особливості налаштування системи виявлення вторгнень; б) мережеві протоколи автентифікації	18
6	Виконання РГР	18
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 налаштуванні систем захисту для віртуального сервера певного призначення. 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. Протоколи та засоби ідентифікації, авторизації, автентифікації та обліку мережевих ресурсів	**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. Системи захисту обчислювальних мереж	**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. Механізми реалізації атак та захист від них.	**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, диференційованого заліку	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. 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 прикладного програмного забезпечення навчальних лабораторій з мережевим обладнанням.

14 Методичне забезпечення

1. Системи захисту обчислювальних мереж. Методичні вказівки до виконання лабораторних робіт для студентів спеціальності 121 «Інженерія програмного забезпечення». – Чернігів: ЧНТУ, 2019. – 34 с. – Електронні данні. – Режим доступу: http://eln.stu.cn.ua/course/view.php?id=1106, обмежений. – Заголовок з екрану.
2. Системи захисту обчислювальних мереж. 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=1106, 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. Коллинз М. Защита сетей. Подход на основе анализа данных. – М.: ДМК, 2019. – 308 с.
4. Прикладна криптологія:системи шифрування:підручник/ О.Г. Корченко, В.П. Сіденко, Ю.О. Дрейс.–К.:ДУТ,2014. –448с.:іл.
5. 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.
6. Олифер В.Г. Олифер Н.А. Компьютерные сети: 2-ое изд. – М.: Вильямс, 2007. – 1410 с.
7. Технології захисту інформації: підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. –Київ : КПІ ім. Ігоря Сікорського, 2018. –162с.
8. Буров Е. Комп'ютерні мережі. – Львів, БаК, 2003, – 584 с., ил.
9. Брюс Шнайер Прикладная криптография. – "Триумф", 2002. – 816с.

Допоміжна

1. Є.М.Чернихівський. Математичне моделювання телекомунікаційних систем та мереж. Навч. посібник.: Львів.: Видавництво Львівської політехніки, 2011 р.: 280 с.: іл..
2. Глоба Л.С. Математичні основи побудови інформаційно-телекомунікаційних систем.: Навч. посібник.: Київ.: Норіта-плюс., 2007 р.: 360 с.: іл.
3. Томаси У. Электронные системы связи. М.: Техносфера, 2007.–1360 с..
4. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд-е 2-е, испр.: Пер с англ.–М.: "Вильямс", 2003.–1104 с.
5. Гаранин М.В., Журавлев В.И., Кунегин С.В. Системы и сети передачи информации.–М.: Радио и связь,2001.–336 с.
6. Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В. Широкополосные беспроводные сети передачи информации. – М.: Техносфера, 2005. –592 с.

16 Електронні інформаційні ресурси

1. Система дистанційного навчання НУ «Чернігівська політехніка». Курс: Системи захисту обчислювальних мереж. – [Електронний ресурс]. – Режим доступу : https://eln.stu.cn.ua/course/view.php?id=1106
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