Міністерство освіти і науки України
Чернігівський національний технологічний університет
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

(ВБ12.1)

Освітня програма «*Інженерія програмного забезпечення*»

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	3	6	РГР	3

Чернігів – 2020 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 і комп'ютерних систем НУ «Чернігівська політехніка», к.т.н., доцент _____ *(Є.В. Риндич)*
(підпис) (прізвище та ініціали)

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

Протокол від "__" серпня *2020* року № __

Завідувач кафедри *інформаційних технологій та програмної інженерії*

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

Abstract

Computer network protection systems (VB 12.1)
2020/2021 Sem. 8

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="4">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>Загальна кількість годин – 150</td><td>8-й</td></tr>
<tr><td rowspan="8">Тижневих годин: аудиторних – 3; самостійної роботи і індивідуальної студента – 6</td><td rowspan="8">Освітньо-кваліфікаційний рівень:
бакалавр</td><td>Лекції</td></tr>
<tr><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 студентів 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.

– ЗК7. Здатність працювати в команді.

– ЗК 31. 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.

– ФК25. Здатність реалізовувати фази та ітерації життєвого циклу програмних систем та інформаційних технологій на основі відповідних моделей і підходів розробки програмного забезпечення.

– 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.

– ПР05. Знати і застосовувати відповідні математичні поняття, методи доменного, системного і об'єктно-орієнтованого аналізу та математичного моделювання для розробки програмного забезпечення.

– ПР10. Проводити передпроектне обстеження предметної області, системний аналіз об'єкта проектування.

– ПР11.Вибирати вихідні дані для проектування, керуючись формальними методами опису вимог та моделювання.

– 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.

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 :

– існуючі мережеві протоколи, що необхідні для функціонування мережі;

– існуючи мережні стандарти та протоколи захищеної передачі даних;

– основні напрямки захисту обчислювальних мереж;

– перспективи розвитку обчислювальних мереж;

– принципи організації взаємодії між прикладними програмами на різних комп'ютерах в локальних та глобальних мережах;

– планування адресного простору IP мереж та налаштування динамічної маршрутизації;

– організація системних мережних сервісів (DNS, XNTP, DHCP та ін.);

– організація та підтримка базових мережних сервісів (SMTP, HTTP, FTP та ін.);

– особливості сучасних комп'ютерних систем передачі даних.

вміти :

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

– робити вибір методу доступу до каналу передачі даних;

– забезпечувати взаємодію комп’ютерів у мережному середовищі з врахуванням цілої низки додаткових вимог;

– реалізувати прикладну програму засобами транспортного протоколу, протоколів автентифікації та конфіденційної передачі даних;

– аналізувати ефективність функціонування обчислювальної мережі;

– створювати віртуальні приватні мережі;

– 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 до 19 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**:

– особливість побудови локальних та глобальних мереж;

– існуючи мережні стандарти та протоколи забезпечення конціденційності та цілосності;

– перспективи розвитку обчислювальних мереж;

– принципи організації взаємодії між локальними та глобальними мережами та системами;

– організація сучасних мережних операційних систем;

– основи криптографічних алгоритмів;

– види та особливості моделей комп’ютерних систем та мереж.

2) **вміє**:

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

– робити вибір методу доступу до каналу передачі даних;

– забезпечувати взаємодію комп’ютерів у мережному середовищі з врахуванням цілої низки додаткових вимог;

– реалізувати прикладну програму засобами транспортного протоколу, протоколів автентифікації та конфіденційної передачі даних;

– аналізувати ефективність функціонування обчислювальної мережі;

– створювати віртуальні приватні мережі;

– створювати мережні сервіси автентифікації, авторизації та обліку.

5 Засоби діагностики результатів навчання

Для визначення рівню засвоєння навчального матеріалу застосовуються наступні методи контролю:

- поточне опитування на лекціях;
- оцінки за захист лабораторних робіт;

- підсумковий 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

Предмет та завдання курсу “ Системи захисту обчислювальних мереж ”. Класифікація мережних топологій. 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

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.

Змістовий модуль 2. Системи захисту обчислювальних мереж

Тема 4. Мережеві екрани

Системи захисту обчислювальних мереж. Мережеві екрани.

Тема 5. Системи виявлення порушника

Системи захисту обчислювальних мереж. Системи виявлення порушника.

Змістовий модуль 3. Моделі безпеки комп’ютерних систем. Протоколи безпеки.

Тема 6. Моделі безпеки комп’ютерних систем.

Критерії оцінки інформаційної безпеки. Моделі безпеки комп’ютерних систем. Мандатна, дискреційна та рольова політики безпеки комп’ютерних систем.

Тема 7. Протоколи безпеки.

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

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	20	4		16
3	Мережеві протоколи ідентифікації та автентифікації	24	4	4	16
	Разом за змістовим модулем 1	**50**	**10**	**4**	**36**
Змістовий модуль 2. Системи захисту обчислювальних мереж					
4	Мережеві екрани	22	4	4	14
5	Системи виявлення порушника	26	6	4	16
	Разом за змістовим модулем 2	**48**	**10**	**8**	**30**
Змістовий модуль 3. Моделі безпеки комп'ютерних систем. Протоколи безпеки					
6	Моделі безпеки комп'ютерних систем	20	4	4	12
7	Протоколи безпеки	22	6	4	12
	Разом за змістовим модулем 3	**42**	**10**	**8**	**24**
	РГР	**10**	**-**	**-**	**10**
	Усього годин за дисципліну	**150**	**30**	**20**	**100**

8 Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Створення віртуальної приватної мережі на базі PPTP сервера POPTOP	4
2	Налаштування автентифікації, авторизації та обліку VPN користувачів за допомогою RADIUS сервера FreeRADIUS, з використанням модуля	4
3	Налаштування поштового серверу Postfix	4
4	Перетворення мережевих адрес та статистика в фільтрах IPTABLES. Типові рішення захисту мереж.	4
5	Налаштування HTTP-проксі сервера Squid	4
Разом		**20**

9 Самостійна робота

№ з/п	Назва теми	Кількість годин
Семестр 9		
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 поштових серверів; б) алгоритми генерації псевдовипадкових чисел	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].

11 Методи контролю

Оцінювання знань ЗВО здійснюється відповідно до «Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти Національного університету «Чернігівська політехніка», погодженого вченою радою НУ «Чернігівська політехніка» (протокол № 6 від 31.08.2020 р.) та затвердженого наказом ректора НУ «Чернігівська політехніка» від 31.08.2020 р. №26.

Політика дотримання академічної доброчесності ґрунтується на «Кодексі академічної доброчесності Національного університету “Чернігівська політехніка”», погодженого вченою радою НУ “Чернігівська політехніка” (протокол № 6 від 31.08.2020 р.) та введеного в дію наказом ректора НУ “Чернігівська політехніка” від 31.08.2020 р. №26.

З дисципліни студент може набрати до 60% підсумкової оцінки за виконання всіх видів робіт, що виконуються протягом семестру і до 40% 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 студентами під час лекцій та консультацій та опитувань студентів під час захисту лабораторних робіт [14.1].

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

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

Семестровий контроль у вигляді *заліку* проводиться на останньому тижні навчального семестру (заліковий тиждень) з двома запитаннями. Оцінка за результатами вивчення дисципліни формується шляхом додавання підсумкових результатів поточного контролю до залікової оцінки. Ті студенти, які не виконали всі обов'язкові види робіт та за результатами роботи в семестрі набрали менше 20 балів, мають пройти повторний курс вивчення дисципліни. Взаємозв'язок між набраними балами і оцінкою наведений у розділі 12.

Якщо відповідь повна і зміст відповіді студента повністю відповідає сутності поставлених запитань, можна отримати від 33 до 40 балів. В тому випадку, коли студент відповідає без грубих помилок, можна отримати від 24 до 32 балів. Якщо при відповіді студент допускає грубі помилки, і всі запитання вирішені менш, ніж на половину, можна отримати від 17 до 24 балів. За не відповідь хоча б на одне запитання, не можна отримати більше 16 балів.

Складання заліку є обов'язковим елементом підсумкового контролю знань для студентів, які претендують на оцінку «добре» або «відмінно». Якщо студент виконав всі види робіт протягом семестру та набрав 60% підсумкової оцінки (тобто «задовільно»), 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 пакеті документів на дисципліну.

Переліки залікових питань знаходяться в пакеті документів на дисципліну. У випадку, якщо студент 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 (20), він не допускається до складання екзамену під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань студентів НУ «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. Моделі безпеки комп'ютерних систем. Протоколи безпеки	**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 Теоретичні питання	0…	30
2 Результат поточного контролю	0…	30
Змістовий модуль 2	**0…**	**60**
1 Теоретичні питання	0…	30
2 Результат поточного контролю	0…	30
Змістовий модуль 3	**0…**	**60**
1 Теоретичні питання	0…	30
2 Результат поточного контролю	0…	30
Зважена модульна оцінка	**0…**	**60**

Підсумковий семестровий контроль

Вид контролю	**Кількість балів**	
1 Теоретичні питання	0…	40
2 Зважена модульна оцінка	0…	60
Семестрова оцінка	**0…**	**100**

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	**Оцінка ECTS**	**Оцінка за національною шкалою**
		для екзамену, курсового проекту
90 – 100	**A**	відмінно
82-89	**B**	добре
74-81	**C**	
64-73	**D**	задовільно
60-63	**E**	

35-59	**FX**	незадовільно з можливістю повторного складання
0-34	**F**	незадовільно з обов’язковим повторним вивченням дисципліни

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. Програмні засоби мережевих технологій. 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. Програмні засоби мережевих технологій. Методичні вказівки з 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. Коллинз М. Защита сетей. Подход на основе анализа данных. – М.: ДМК, 2019. – 308 с.
2. Олифер В.Г. Олифер Н.А. Компьютерные сети: 2-ое изд. – М.: Вильямс, 2007. – 1410 с.
3. Буров Е. Комп'ютерні мережі. Львів, БаК, 2003, -584 с., ил.
4. Таненбаум Э. Компьютерные сети. СПб, Питер, 2002, -948 с., ил.
5. Довгаль С.И., Литвинов Б.Ю., Сбитнев Ф.И. Персональные ЭВМ : Локальные сети. Киев,”Информсистема сервис ” 1993.-440с.,ил.
6. Craig Hunt. TCP/IP network administration. O’Relly & Associates, Inc, 1994-1998,2004. 472 pages.
7. 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. Крёнке Д. Теория и практика построения баз данных. 8-е изд. / Д. Крёнке. – СПб.: Питер, 2003. – 800 с.
4. Райордан Р. Основы реляционных баз данных Пер. с англ. / Р. Райордан – М. : Издательско-торговый дом «Русская Редакция», 2001. – 384 с.
5. Козленко Л. Информационная безопасность в современных системах управления базами данных / Л. Козленко. – КомпьютерПресс № 3, 2002.
6. Фуфаев Э. В. Разработка и эксплуатация удаленных баз данных : учебник для студ. сред. проф. образования / Э. В. Фуфаев, Д. Э. Фуфаев. – М.: Издательский центр «Академия», 2008. – 256 с.
7. К. Луни Oracle Database 10g Настольная книга администратора баз данных / [Кевин Луни, Боб Брила и эксперты TUSC]. – Издательство "Лори", 2008. – 729 с.
8. Информационные технологии в бизнесе / Под ред. М. Желены. – СПб: Питер, 2002. – 1120 е.: ил. – (Серия «Бизнес-класс»).
9. Томаси У. Электронные системы связи. М.: Техносфера, 2007.–1360 с..
10. Абрамова О. Методика експертної оцінки варіантів проектів прийняття рішень // Укр. ін вест. журн. Welcome. — 1999. — № 12. — С. 33—45
11. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд-е 2-е, испр.: Пер с англ.–М.: "Вильямс", 2003.–1104 с.
12. Гаранин М.В., Журавлев В.И., Кунегин С.В. Системы и сети передачи информации.–М.: Радио и связь,2001.–336 с.
13. Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В. Широкополосные беспроводные сети передачи информации. – М.: Техносфера, 2005. –592 с.
14. Шахнович И.В. Современные технологии беспроводной связи. –М.: Техносфера, 2006.– 288 с.
15. Величко В.В. Передача данных в сетях мобильной связи третьего поколения. – М.: Радио и связь,2005.– 332 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