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

ПРОГРАМНІ ЗАСОБИ МЕРЕЖЕВИХ ТЕХНОЛОГІЙ

(ВБ12.2)

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	3	6		З

Чернігів – 2020 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:
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

Network defending technology software (VB 12.2)

2020/2021 Sem.1

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
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 – 4</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.

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.

– 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.

– ФК 29. Здатність до розробки і реалізації методів тестування та випробування програмних комплексів.

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.

– 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.

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

– засоби і методи збереження і передачі автентифікаційної інформації;

– 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.

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 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 20 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:

– засоби і методи збереження і передачі автентифікаційної інформації;

– 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.

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;
– 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;
- підсумковий 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. Механізми реалізації атак в мережах TCP / IP

Віддалене визначення версії ОС з використанням особливостей реалізації стека протоколів TCP / IP. Методи сканування портів. Методи виявлення пакетних сніфера. Методи обходу МЕ.

Змістовний модуль 2.

Тема № 3. Методи перехоплення мережевих з'єднань в мережах TCP/IP

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

Тема №4. Приклади мережевих 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. Технічні зоходи захисту від мережевих атак.

Змістовний модуль 3. Криптографічні методи захисту інформації в комп'ютерних мережах

Тема № 5. 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 № 6. 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 4.

Тема № 7. Розробка захищених мережевих додатків

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

Тема №8. 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 № 9. 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).

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. Механізми реалізації атак в мережах TCP/IP	17		3				4		10	
	Разом за змістовим модулем 1	**30**		**6**				**4**		**20**	
	Модуль 2.										
3	Тема № 3. Методи перехоплення мережевих з'єднань в мережах TCP/IP	17		3				4		10	
4	Тема №4. Приклади мережевих атак в мережах TCP/IP	13		3						10	
	Разом за змістовим модулем 2	**30**		**6**		**0**		**4**		**20**	
	Модуль 3.										
5	Тема № 5. Криптографічні протоколи забезпечення безпеки	13		3						10	
6	Тема № 6. Захист віртуальних приватних мереж (VPN)	17		3				4		10	
	Разом за змістовим модулем 3	**30**		**6**				**4**		**20**	
	Модуль 4.										
7	Тема № 7. Розробка захищених мережевих додатків	13		3						10	
8	Тема №8. Засоби захисту локальних мереж при підключенні до Інтернет	17		3				4		10	
9	Тема № 9. Захист серверів і робочих станцій. Засоби та методи запобігання та виявлення вторгнень			6				4		20	
	Разом за змістовим модулем 4	**30**		**12**				**8**		**40**	
	Усього годин за дисципліну	**150**		**30**				**20**		**100**	

8 Теми лабораторних занять

№ з/п	Назва теми	Кількість годин (д/з)
1	Протоколи аутентифікації на прикладному рівні. Протокол Kerberos	4
2	Протоколи аутентифікації на транспортному рівні. Протокол SSL / TLS	4
3	Інструментальні засоби проведення мережевих атак	4
4	Розгортання VPN з використанням IPSEC	4
5	Реалізація мережевої політики безпеки з використанням МЕ. Методи обходу міжмережевих екранів	4
6	Системи віртуальних пасток (Honey Pot і Padded Cell).	4
Разом		**20**

9 Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Підготовка до лабораторних робіт	45
2	Підготовка до тестів	10
3	Засвоєння лекційного матеріалу	45
	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
Модуль 1.	**0… 12**
1 Повнота ведення конспектів занять.	0… 1
2 Рішення завдань до захисту лабораторних робот.	0… 1
3 Самостійність виконання лабораторних робіт.	0… 5
4 Своєчасність виконання лабораторних робіт.	0… 5
Модуль 2.	**0… 12**
1 Повнота ведення конспектів занять.	0… 1
2 Рішення завдань до захисту лабораторних робіт.	0… 1
3 Самостійність виконання лабораторної роботи.	0… 5
4 Своєчасність виконання лабораторної роботи.	0… 5
Модуль 3.	**0… 12**
1 Повнота ведення конспектів занять.	0… 1
2 Рішення завдань до захисту лабораторної роботи.	0… 1
3 Самостійність виконання лабораторних робіт.	0… 5
4 Своєчасність виконання лабораторних робіт.	0… 5
Модуль 4.	**0… 24**
1 Повнота ведення конспектів занять.	0… 2
2 Рішення завдань до захисту лабораторної роботи.	0… 2
3 Самостійність виконання лабораторних робіт.	0… 10
4 Своєчасність виконання лабораторних робіт.	0… 10
Семестрова оцінка поточного контролю	**0 60**

Для *захисту лабораторної роботи* студент повинен відповісти на всі контрольні запитання з методичних вказівок та на два запитання за вибором викладача з лекційного курсу за темою лабораторної роботи. Для *денної форми навчання* за кожну лабораторну роботу студент отримує певну кількість балів з урахуванням максимальної кількості балів згідно наведеної вище таблиці. При цьому враховується якість оформлення звіту та повнота відповідей на запитання при захисті лабораторної роботи.

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 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=3427, обмежений. – Заголовок з екрану.

15 Рекомендована література

Базова

1. Дейт К. Введение в системы баз данных, 7-е издание.: Пер. с англ. / К. Дейт. – М. : Издательский дом «Вильямс», 2001. – 1072с.
2. Коннолли Т. Базы данных. Проектирование, реализация и сопровождение. Теория и практика. 3-е издание. : Пер. с англ. / Т. Коннолли, К. Бегг. – М. : Издательский дом "Вильямс", 2003. – 1440 с.
3. Хомоненко А. Д. Базы данных: Учебник для высших учебных заведений / А. Д. Хомоненко, В. М. Цыганков, М. Г. Мальцев Под ред. проф. А. Д. Хомоненко. – 4-е изд., доп. и перераб. – СПб. : КОРОНА принт, 2004. – 736 с.
4. Цикритзис Д. Модели данных / Д. Цикритзис, Ф. Лоховски / Пер. с англ. – М. : Финансы и статистика, 1985. – 344с.

5. Р. Гринвальд Oracle llg. Основы, 4-е издание. – Пер. с англ. / Р. Гринвальд, Р. Стаковьяк, Дж. Стерн. – СПб. : Символ-Плюс, 2009. – 464 с.
6. Есин В. И. Безопасность информационных систем и технологий / В. И. Есин, А. А. Кузнецов, Л. С. Сорока. – Х. : ООО «ЭДЭНА», 2010. – 656 с.
7. Разрушающие программные воздействия: Учебно-методическое пособие / [А.Б. Вавренюк, Н.П. Васильев, Е.В. Вельмякина и др.; под ред. М.А. Иванова.] – М. : НИЯУ МИФИ, 2011. – 328 с.
8. 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
9. 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
10. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» затверджений наказом ДСТСЗІ СБ України від 04.12.2000 р. № 53. http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article;jsessionid=97BBACF714A05BF6459C5F476282F024?art_id=39738&cat_id=38835
11. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу», затверджений наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22. http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article;jsessionid=BA075F688F4E729D7C88A20E1C636EA4?art_id=40393&cat_id=38835
12. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу», затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22. http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40396&cat_id=38835
13. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22. http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40386&cat_id=38835
14. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу», затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22. http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40381&cat_id=38835
15. НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі»

затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22. http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40374&cat_id=38835

Допоміжна

1. Крёнке Д. Теория и практика построения баз данных. 8-е изд. / Д. Крёнке. – СПб.: Питер, 2003. – 800 с.
2. Райордан Р. Основы реляционных баз данных Пер. с англ. / Р. Райордан – М. : Издательско-торговый дом «Русская Редакция», 2001. – 384 с.
3. Цаленко М. Ш. Моделирование семантики в базах данных / М. Ш. Цаленко. – М. : Наука. Гл. ред.физ-мат.лит., 1989. – 288с.
4. Козленко Л. Информационная безопасность в современных системах управления базами данных / Л. Козленко. – КомпьютерПресс № 3, 2002.
5. 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.
6. К. Луни Oracle Database 10g Настольная книга администратора баз данных / [Кевин Луни, Боб Брила и эксперты TUSC]. – Издательство "Лори", 2008. – 729 с.
7. Информационные технологии в бизнесе / Под ред. М. Желены. – СПб: Питер, 2002. – 1120 е.: ил. – (Серия «Бизнес-класс»).
8. Томаси У. Электронные системы связи. М.: Техносфера, 2007.–1360 с..
9. Абрамова О. Методика експертної оцінки варіантів проектів прийняття рішень // Укр. ін вест. журн. Welcome. — 1999. — № 12. — С. 33—45
10. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд-е 2-е, испр.: Пер с англ.–М.: "Вильямс", 2003.–1104 с.
11. Гаранин М.В., Журавлев В.И., Кунегин С.В. Системы и сети передачи информации.–М.: Радио и связь,2001.–336 с.
12. Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В. Широкополосные беспроводные сети передачи информации. – М.: Техносфера, 2005. –592 с.
13. Шахнович И.В. Современные технологии беспроводной связи. –М.: Техносфера, 2006.– 288 с.
14. Величко В.В. Передача данных в сетях мобильной связи третьего поколения. – М.: Радио и связь,2005.– 332 с.
1. http://www.citforum.ru/database/classics/chen/

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