Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та математики

Кафедра інформаційної та кібернетичної безпеки

імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«___»_____ 2023 р

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ЗАХИСТ ІНФОРМАЦІЇ»

для студентів

спеціальності	122 Комп'ютерні науки
освітнього рівня	першого (бакалаврського)
освітньої програми	122.00.01 Інформатика

КИЇВСЬКИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Програма № 2549/23
(підпис) (прізвище, ініціали)
«___» _____ 2023 р

2023 – 2024 навчальний рік

Розробники:

Довженко Надія Михайлівна, кандидат технічних наук, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Довженко Надія Михайлівна, кандидат технічних наук, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 17.10.2023 р. № 10

Завідувач кафедри _____ (підпис) _____ Павло СКЛАДАННИЙ

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 122.00.01 Інформатика)

___.___. 2023 р.

Керівник освітньої програми _____ (підпис) _____ Ірина МАШКІНА

Робочу програму перевірено

___.___. 2023 р.

Заступник декана _____ (підпис) _____ Євген ІВАНІЧЕНКО

Пролонговано:

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Захист інформації		
Вид дисципліни	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4 / 120	
Курс	4	
Семестр	7	
Кількість змістових модулів з розподілом:	4	
Обсяг кредитів	4	
Обсяг годин, в тому числі:	120	
Аудиторні	56	
Модульний контроль	8	
Семестровий контроль	30	
Самостійна робота	26	
Форма семестрового контролю	іспит	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Захист інформації» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки імені професора Володимира Бурячка на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчального плану спеціальності 122 Комп'ютерні науки, освітньої програми 122.00.01 Інформатика.

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Захист інформації» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Захист інформації» складається з 4х змістовних модулів. Обсяг дисципліни – 120 год (4 кредити).

Метою навчальної дисципліни «Захист інформації» є формування у студентів знань та компетентностей, необхідних для ефективної організації та реалізації захисту інформаційних та телекомунікаційних систем/мереж, комплексного забезпечення інформаційної безпеки систем та мереж, вивчення принципів та одержання практичних навичок створення безпечної мережевої інфраструктури.

Завдання полягає у формування теоретичних знань та практичних умінь у сфері захисту інформаційних та телекомунікаційних систем/мереж та набуття **наступних компетентностей:**

ЗК-2 – Здатність застосовувати знання у практичних ситуаціях;

ЗК-3 – Знання та розуміння предметної області та розуміння професійної діяльності;

ЗК-6 – Здатність вчитися й оволодівати сучасними знаннями;

ЗК-7 – Здатність до пошуку, оброблення та аналізу інформації з різних джерел; до критичної оцінки отриманої інформації, використання логіки і раціональних міркувань;

ЗК-8 – Здатність генерувати нові ідеї (креативність);

ЗК-11 – Здатність приймати обґрунтовані рішення й обґрунтовувати запропоновані рішення на сучасному науково-технічному й професійному рівні;

ЗК-12 – Здатність оцінювати та забезпечувати якість виконуваних робіт, представляти результати роботи;

ЗК-13 – Здатність діяти на основі етичних міркувань.

СК-10 – Здатність застосовувати методології, технології та інструментальні засоби для управління процесами життєвого циклу інформаційних і програмних систем, продуктів і сервісів інформаційних технологій відповідно до вимог замовника;

СК-13 – Здатність до розробки мережевого програмного забезпечення, що функціонує на основі різних топологій структурованих кабельних систем, використовує комп'ютерні системи і мережі передачі даних та аналізує якість роботи комп'ютерних мереж;

СК-14 – Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студент повинен

знати:

- основні види загроз інформаційній безпеці, сучасні проблеми забезпечення безпеки інформаційних технології;
- міжнародні стандарти, рекомендації та політики безпеки в сфері захисту інформації;
- Закони України, що регламентують сферу захисту інформації та кібербезпеки;
- стратегію захисту інформації та механізми забезпечення інформаційної безпеки.

уміти:

- здійснювати аналіз та оцінку сучасних загроз безпеці;
- визначати принципи створення надійної та безпечної мережевої інфраструктури;
- роз'яснювати особливості розповсюдження мережевих атак та атак на ПЗ, наслідків та способів пом'якшення результатів проникнення;
- виокремлювати переваги програмних та апаратних засобів та технологій щодо забезпечення захисту інформації;
- організувати прості топології з використанням сучасних програмно-апаратних комплексів захисту інформації;
- розробляти програмне забезпечення, що функціонує на основі різних топологій структурованих систем;
- досліджувати чинні способи забезпечення захисту конфіденційних даних в сучасних мультисервісних мережах;
- розробляти рекомендацій та застосовувати заходи із забезпечення захисту інформаційних систем та мереж.

та досягти наступних ***програмних результатів*** навчання:

ПР-8 – використовувати методологію системного аналізу об'єктів, процесів і систем для задач аналізу, прогнозування, управління та проектування динамічних процесів в макроекономічних, технічних, технологічних і фінансових об'єктах;

ПР-15 – розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1.							
Тема 1. Вступ до захисту інформації.	6	2			4		
Тема 2. Міжнародна співпраця в сфері кібербезпеки.	4	2					2
Тема 3. Правові аспекти захисту інформації.	8	2			4		2
Тема 4. Стратегії захисту інформації.	4	2					2
Модульний контроль 1	2						
Разом	24	8			8		6
Змістовий модуль 2.							
Тема 5. Основи мережевої безпеки та протоколи безпеки.	12	2			6		4
Тема 6. Дослідження складових елементів комп’ютерних мереж.	12	2			4		6
Модульний контроль 2	2						
Разом	26	4			10		10
Змістовий модуль 3.							
Тема 7. Безпека на рівнях моделі OSI.	10	2			6		2
Тема 8. Дослідження алгоритмів маршрутизації	12	2			6		4
Модульний контроль 3	2						
Разом	24	4			12		6
Змістовий модуль 4.							
Тема 9. Програмно-апаратні комплекси захисту корпоративних та локальних мереж від загроз та кінцевих користувачів	10	2			6		2
Тема 10. Аналіз інцидентів безпеки та концепція аудиту безпеки інформаційних систем	4	2					2
Модульний контроль 4	2						
Разом	16	4			6		4
Підготовка та проходження контрольних заходів	30						
Усього	**120**	**20**			**36**		**26**

5. Програма навчальної дисципліни

Змістовий модуль 1.

Основні питання:

- Вступ до захисту інформації;
- Види загроз і ризиків для інформаційних систем;

- Основні принципи інформаційної безпеки;
- Міжнародна співпраця у сфері кібербезпеки;
- Правові аспекти захисту інформації;
- Особливості механізмів забезпечення конфіденційності, цілісності та доступності даних;
- Стратегії захисту інформації.

Змістовий модуль 2.

Основні питання:

- Основи мережевої безпеки та протоколи безпеки**;**
- Виявлення та захист від мережевих загроз;
- Дослідження складових елементів комп'ютерних мереж.
- Активне та пасивне мережеве устаткування;
- Міжмережевий екран як комплекс апаратних/програмних засобів захисту об'єктів критичної інфраструктури.

Змістовий модуль 3.

Основні питання:

- Особливості забезпечення безпеки на фізичному та канальному рівнях моделі OSI;
- Особливості забезпечення безпеки на мережевому та транспортному рівнях моделі OSI;
- Особливості забезпечення безпеки на сеансовому рівні моделі OSI;
- Особливості забезпечення безпеки на представницькому та прикладному рівнях моделі OSI;
- Характеристики та принципи протоколів безпеки на рівнях моделі OSI;
- Дослідження алгоритмів маршрутизації (RIP, OSPF, IGRP/EIGRP, BGP);

Змістовий модуль 4.

Основні питання:

- Програмно-апаратні комплекси захисту корпоративних та локальних мереж від загроз та кінцевих користувачів.
- Системи виявлення та запобігання вторгнень (IDS/IPS);
- Програмно-апаратні комплекси для виявлення та запобігання вторгнень;
- Головні принципи роботи та алгоритми захисту Cisco Umbrella;
- Особливості розгортання комплексу Symantec Endpoint Protection;
- Оновлення підходів до захисту кінцевих користувачів від ESET Endpoint Security 8;
- Особливості функціонування та розгортання комплексу IBM QRadar;
- Дослідження алгоритмів роботи Cisco Talos;
- Поняття аудиту безпеки та його роль;
- Аналіз інцидентів безпеки та концепція аудиту безпеки інформаційних систем;
- Методи проведення аудиту безпеки інформаційних систем.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної звітності, обов'язковості модульних контролів, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, співбесіда, екзамен.
- *Комп'ютерного контролю:* програми - емулятори
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2		Модуль 3		Модуль 4	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	4	4	2	2	2	2	2	2
Відвідування семінарських занять	1								
Відвідування практичних занять	1								
Відвідування лабораторних занять	1	4	4	5	5	6	6	3	3
Робота на семінарському занятті	10								
Робота на практичному занятті	10								
Лабораторна робота (в тому числі допуск, виконання, захист)	10	4	40	5	50	6	60	3	30
Виконання завдань для самостійної роботи	5	1	5	1	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25	1	25	1	25
Виконання ІНДЗ	30								
Разом		-	78	-	87	-	98		65
Максимальна кількість балів: 328									
Розрахунок коефіцієнта: 328/60=5,47									

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної

компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1.		6	5
1	• Стандарти ISO/IEC з кібербезпеки (ISO/IEC 27001 та ISO/IEC 27002); • Моделі управління мережевими ресурсами.	6	5
Змістовий модуль 2.		10	5
2	• Виявлення мережевих атак шляхом аналізу трафіка; • Команди налаштування протоколів STP, RSTP, MSTP.	10	5
Змістовий модуль 3.		6	5
3	• Керування MAC, IP, ARP та налаштування VLAN; • Створення списки керування доступом (Access Control List).	6	5
Змістовий модуль 4.		4	5
4	• Програмно-апаратні комплекси захисту корпоративних та локальних мереж від загроз та кінцевих користувачів.	4	5
	Разом	**26**	**20**

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульних контролів та критерії оцінювання

Модульні контролі здійснюються відповідно до навчально-методичної карти дисципліни та перевіряють рівень досягнення результатів навчання студентів. Форма проведення – індивідуальне опитування, що складається з 3 запитань відкритої форм. Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі екзамену, умовою допуску до якого є отриманням студентом 35 балів (з врахуванням коефіцієнту) за результатами поточного контролю. Форма проведення екзамену – комбінована. Іспит оцінюється у 40 балів за розподілом: 20 балів – письмове опитування; 20 балів – виконання практико-орієнтованого завдання.

Виконання практичного завдання передбачає перевірку рівня оволодіння студентом теоретичними знаннями та практичними вміннями з ефективної організації та реалізації захисту інформаційних та телекомунікаційних систем/мереж, комплексного забезпечення інформаційної безпеки систем та мереж.

Оцінювання практичного завдання відбувається в межах від 0 до 20 балів, згідно критеріїв оцінювання, й здійснюється з урахуванням: рівнів сформованості аналітико-синтетичних, творчих та методичних умінь необхідних для реалізації захисту інформаційних та телекомунікаційних систем/мереж. Бали за усне опитування та бали за виконання практичного завдання додаються.

Оцінювання результатів засвоєння теоретичних знань та оцінювання сформованості практичних навичок володіння цифровими технологіями студентами, продемонстровані на екзамені, представлене у таблиці.

Підсумкова кількість балів (max – 40)	Оцінка за 4-бальною шкалою
1 – 23	«незадовільно»
24 – 29	«задовільно»
30 – 35	«добре»
36 – 40	«відмінно»

Орієнтовний перелік питань для семестрового контролю

1. Види загроз і ризиків для інформаційних систем;
2. Основні принципи інформаційної безпеки;
3. Виклики в області інформаційної безпеки;
4. Поняття «Кіберпростір» та «кіберборотьба»;
5. Міжнародні організації та консорціуми, що здійснюють регулювання в сфері інформаційної безпеки;
6. Головні проблеми забезпечення кібернетичної безпеки;
7. Правові аспекти безпеки інформаційних систем;
8. Міжнародні закони, положення і стандарти, що регулюють сферу кібербезпеки;
9. Міжнародна співпраця в сфері кібербезпеки;
10. Українське законодавство в сфері регулювання питань інформаційної та кібернетичної безпеки;
11. Закон України «Про кібербезпеку»;
12. Закон України «Про інформацію»;
13. Закон України «Про захист інформації в інформаційних системах»;
14. Закон України «Про інформаційні ресурси інформаційного суспільства»;
15. Стратегії захисту інформації;
16. Значення та компоненти стратегії захисту інформації;
17. Механізми безпеки комп'ютерних мереж;
18. Основи мережевої безпеки та протоколи безпеки;
19. Виявлення та захист від мережевих загроз;
20. Загальні принципи побудови та організації комп’ютерних мереж;
21. Особливості функціонування комп’ютерних мереж;
22. Модель OSI;
23. Безпека на рівнях моделі OSI;
24. Основні характеристики та принципи протоколів безпеки на рівнях моделі OSI;
25. Активне та пасивне мережеве устаткування;
26. Міжмережевий екран як комплекс апаратних/програмних засобів захисту об’єктів критичної інфраструктури;
27. Дослідження алгоритмів маршрутизації (RIP, OSPF, IGRP/EIGRP, BGP);
28. Поняття вторгнень у системи та їх види;
29. Системи виявлення та запобігання вторгнень (IDS/IPS);
30. Програмно-апаратні комплекси для виявлення та запобігання вторгнень;
31. Пом’якшення наслідків вторгнень;
32. Поняття «сигнатури»;
33. Основи криптографічного захисту;
34. Принципи криптографії та її роль у безпеці інформаційних систем;
35. Типи шифрування та криптографічні алгоритми;
36. Використання криптографії для захисту даних;
37. Безпека мобільних пристроїв та хмарних обчислень;
38. Шифрування та захист даних на мобільних пристроях;
39. Захист від загроз IoT-мереж та протоколів;
40. BYOD;
41. Безпека хмарних обчислень;
42. Основи хмарних обчислень та їх безпека;

43. Аналіз інцидентів безпеки та концепція аудиту безпеки інформаційних систем;
44. Виявлення, відновлення та реагування на інциденти;
45. Поняття аудиту безпеки та його роль;
46. Методи проведення аудиту безпеки інформаційних систем.

Шкала відповідності оцінок

Рейтингова оцінка	Сума балів за всі види навчальної діяльності	Значення оцінки
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов'язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре - достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре - в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо - мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання - незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов'язковим повторним вивченням курсу - досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична картка дисципліни

Разом: 120 год., лекції – 20 год., практичні заняття – 36 год., модульний контроль – 8 год., самостійна робота –26 год.

Модулі (назви, бали)	Змістовий модуль 1 (78 балів)		Змістовий модуль 2 (87 балів)		Змістовий модуль 3 (98 балів)		Змістовий модуль 4 (65 балів)	
Лекції (теми, бали)	Вступ до захисту інформації (1 бал)	Міжнародна співпраця в сфері кібербезпеки (1 бал)	Основи мережевої безпеки та протоколи безпеки(1 бал)		Безпека на рівнях моделі OSI(1 бал)		Програмно-апаратні комплекси захисту корпоративних та локальних мереж від загроз та кінцевих користувачів(1 бал)	
	Правові аспекти захисту інформації (1 бал)	Стратегії захисту інформації (1 бал)	Дослідження складових елементів комп'ютерних мереж(1 бал)		Дослідження алгоритмів маршрутизації(1 бал)		Аналіз інцидентів безпеки та концепція аудиту безпеки інформаційних систем(1 бал)	
Лабораторні заняття (теми, бали)	Дослідження та виявлення атак соціальної інженерії (22 бали)	Дослідження мережевих атак та особливостей аудиту безпеки (22 бали)	Налаштування автентифікації AAA на маршрутизаторах Cisco в середовищі Cisco Packet Tracer (22 бали)	Налаштування розширених сценаріїв ACL в середовищі Cisco Packet Tracer (33 бали)	Налаштування функціонування системи запобігання вторгненням IOS (IPS) за допомогою CLI в середовищі Cisco Packet Tracer (33 балів)	Налаштування безпеки VLAN в середовищі Cisco Packet Tracer (33 балів)	Налаштування безпеки VLAN для L2 в середовищі Cisco Packet Tracer (11 балів)	Налаштування IPSec VPN в середовищі Cisco Packet Trace (22 балів)
Самостійна робота	Самостійна робота (5 балів)		Самостійна робота (5 балів)		Самостійна робота (5 балів)		Самостійна робота (5 балів)	
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)		Модульна контрольна робота 2 (25 балів)		Модульна контрольна робота 3 (25 балів)		Модульна контрольна робота 4 (25 балів)	
Підсумковий контроль (вид, бали)	Екзамен (40 балів)							

8. Рекомендовані джерела

Базова:

1. Бурячок В. Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Київ. ДУТ. 2015. 449 с.
2. Тарнавський Ю. А. Технології захисту інформації / Ю. А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
3. Жураковський Б. Ю., Зенів І.О. Комп'ютерні мережі. Частина 1. Навчальний посібник. Київ. КПІ ім. Ігоря Сікорського. 2020. 328 с.
4. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. К. 2015. 220 с.
5. Беседовський О.М., Золотарьова І.О., Євсеєв С.П. Сучасні методи та моделі обробки даних в інформаційних системах. Х. ХНЕУ ім. С. Кузнеця. 2013. 540 с.

Додаткова:

1. Chris Carthern, William Wilson, Noel Rivera. Cisco Networks. Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA. Apress, 2018.1117p.
2. Joseph Muniz, Gary McIntyre, Nadhem AlFardan. Security Operations Center: Building, Operating, and Maintaining your SOC. Cisco Press. 2020. 448 p.
3. Omar Santos, Panos Kampanakis, Aaron Woland. Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP. Cisco Press. 2016. 368 p.