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 «ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ»

для студентів

спеціальності	125 Кібербезпека та захист інформації
освітнього рівня	першого (бакалаврського)
освітньої програми	125.00.01 Безпека інформаційних і комунікаційних систем

2023 – 2024 навчальний рік

Розробник:
Бржевська Зореслава Михайлівна, доктор філософії з кібербезпеки, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:
Бржевська Зореслава Михайлівна, доктор філософії з кібербезпеки, 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 01.09.2022 р. № 12

Завідувач кафедри _____ (підпис) _____ Павло СКЛАДАННИЙ

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 2022 р.
Керівник освітньої програми _____ (підпис) Артем ПЛАТОНЕНКО

Робочу програму перевірено
___.___. 2022 р.
Заступник декана _____ (підпис) _____ Євген ІВАНІЧЕНКО

Пролонговано:
на 2023/2024 н.р. _____ (підпис) _____ (ПІБ), «23» 08 2023 р., протокол № 8
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
Вид дисципліни	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	2 / 60	
Курс	1	
Семестр	2	
Кількість змістових модулів з розподілом:	2	
Обсяг кредитів	2	
Обсяг годин, в тому числі:	60	
Аудиторні	28	
Модульний контроль	4	
Семестровий контроль	-	
Самостійна робота	28	
Форма семестрового контролю	залік	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Теоретичні аспекти захищених інформаційно-комунікаційних технологій» 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 125 Кібербезпека та захист інформації, освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем.

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 «Теоретичні аспекти захищених інформаційно-комунікаційних технологій» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Теоретичні аспекти захищених інформаційно-комунікаційних технологій» складається з 2-х змістових модулів: 1. Основні парадигми і моделі захисту інформації від несанкціонованого доступу в обчислювальних системах. 2. Політика безпеки,стандартизовані моделі, принципи побудови і напрямки розвитку сучасних технологій створення захищених інформаційно-комунікаційних систем. Обсяг дисципліни – 60 год. (2 кредити).

Метою викладання навчальної дисципліни «Теоретичні аспекти захищених інформаційно-комунікаційних технологій» є отримання компетентностей та навичок щодо обґрунтування застосування механізмів захисту та оцінки рівня захищеності інформаційно-комунікаційних систем і технологій від несанкціонованого доступу до ресурсів.

Завдання:

- надання студентам теоретичних знань щодо проблем, завдань і особливостей технологій захисту інформації на об'єктах інформаційної діяльності від несанкціонованого доступу до ресурсів;

− формування у студентів категоріальних понять з основ процесів, що притаманні функціонуванню об’єктів інформаційної діяльності в умовах зовнішніх і внутрішніх негативних впливів;

− формування у студентів знань і умінь щодо формування політики безпеки інформаційно-комунікаційних систем;

− стимулювання студентів до активної аналітико-пошукової роботи, що спрямована на визначення ефективних шляхів розвитку у сфері захисту інформації.

У результаті вивчення навчальної дисципліни формуються

загальні компетентності:

КЗ-2: Здатність до здобування нових знань, накопичення наукових та педагогічних вмінь і навичок та їх застосування в практичних ситуаціях

КЗ-3: Здатність до виявлення, генерування, дослідження та вирішення проблем за професійним спрямуванням.

фахові компетентності:

КФ-1: Здатність до застосування сучасних інформаційних і безпекових технологій у сфері захисту інформації

КФ-5: Здатність до забезпечення захисту інформації, що обробляється в інформаційно-комунікаційних системах, здійснення адміністрування таких систем та проведення їх експлуатації.

3. Результати навчання за дисципліною

При вивченні курсу «Теоретичні аспекти захищених інформаційно-комунікаційних технологій» студенти повинні

знати:

- про правові і нормативні акти, які визначають систему захисту інформації від несанкціонованого доступу;
- про сутність сучасної теорії захищених інформаційних систем;
- про сукупність основних теоретичних положень складових захищених інформаційних технологій: гарантовано захищених обчислювальних систем; процесів забезпечення безпеки обчислювальних систем; механізмів захисту інформаційних технологій; програмного забезпечення для вирішення завдань захисту інформації; критеріїв безпеки інформаційних технологій;
- про основні моделі, методи, принципи і правила побудови систем захисту інформації від несанкціонованого доступу на об’єктах інформаційної діяльності (інформаційно-комунікаційних системах);
- особливості забезпечення безпеки сучасних інформаційних технологій.

уміти:

- обґрунтовувати застосування механізмів захисту та оцінки рівня захищеності інформаційної системи (технології);
- визначати моделі, принципи і правила побудови систем захисту від несанкціонованого доступу об’єктів і інформаційно-комунікаційних систем;
- моделювати основні процеси забезпечення безпеки об’єктів і інформаційно-комунікаційних систем.

та досягнути наступні ***програмні результати***:

ПРз-2: - вміти виявляти і формулювати актуальні наукові проблеми, генерувати та інтегрувати нові ідеї та нові знання у сфері захисту інформації, інформаційної та/або кібербезпеки;
- вміти оцінювати уразливості й методи їх застосування в різних інформаційно-комунікаційних технологіях;
- вміти обґрунтовувати основні вимоги до програмного забезпечення, що вирішує завдання захисту інформації;

- вміти обґрунтовувати застосування національних та міжнародних стандартів безпеки інформаційних технологій;
- вміти характеризувати особливості забезпечення безпеки сучасних інформаційних технологій;

ПРз-3: - знати методи оцінки вразливостей й методи оцінки ефективності систем захисту інформації від несанкціонованого доступу інформаційно-комунікаційних системах;
- вміти виявляти ризики експлуатації загроз несанкціонованого доступу до ресурсів інформаційно-комунікаційних систем
- вміти обґрунтовувати положення політики захисту інформації від несанкціонованого доступу в інформаційно-комунікаційних системах;

ПРз-7: - вміти оцінювати загрози інформації в інформаційно-комунікаційних системах;
- вміти визначати вимоги до методів і способів попередження експлуатації загроз несанкціонованого доступу до ресурсів інформаційно-комунікаційних систем;

ПРз-9: - володіти практичними навичками формування вимог до політики безпеки інформаційно-комунікаційних систем.

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	
Змістовий модуль 1. Основні поняття мережевих технологій						
Тема 1. Сучасні мережеві технології	6	2				4
Тема 2. Базова конфігурація захищених систем	12	2		2	2	6
Тема 3. Протоколи та моделі	10	2		2	2	4
Модульний контроль	2					
Разом	30	6		4	4	14
Змістовий модуль 2. Основи мережевої безпеки та побудова сучасних захищених інформаційних технологій						
Тема 4. Взаємодія мережевих застосунків	6	2		2	2	4
Тема 5. Основи мережевої безпеки	12	2		2		6
Тема 6. Приклади побудови сучасних захищених інформаційних технологій.	10	2			2	4
Модульний контроль	2					
Разом	30	6		4	4	14
Усього	60	12		8	8	28

5. Програма навчальної дисципліни

Змістовий модуль 1. Основні поняття мережевих технологій

Тема 1. Сучасні мережеві технології

Вплив мереж життя людей. Компоненти мережі, принципи роботи з хостами та мережевими пристроями. Уявлення та топології мереж. Основні типи мереж. Підключення до інтернету. Поняття надійних мереж. Тенденції розвитку мереж, політика BYOD (використання в офісі власних пристроїв), спільна робота через Інтернет, відеозв'язок та хмарні обчислення та способи нашої взаємодії один з одним. Забезпечення мережної безпеки. Фахівеці у сфері IT

Тема 2. Базова конфігурація захищених систем

Доступ до Cisco IOS, доступ до пристрою під керуванням Cisco IOS для налаштування. Навігація по IOS, налаштовування мережевих пристроїв у Cisco IOS. Структура команд. Базове налаштування пристроїв. Збереження конфігурацій. Порти та адреси, принципи обміну даними між пристроями в мережевих середовищах. Налаштування IP-адресації. Перевірка підключення.

Тема 3. Протоколи та моделі

Правила, типи правил, яких необхідно дотримуватися для успішного передавання даних. Протоколи. Стеки протоколів. Організації зі стандартизації, роль організацій зі стандартизації при створенні протоколів для забезпечення мережної сумісності. Еталонні моделі, як моделі TCP/IP і OSI використовуються для полегшення стандартизації процесу передавання даних. Інкапсуляція даних. Доступ до даних.

Змістовий модуль 2. Основи мережевої безпеки та побудова сучасних захищених інформаційних технологій

Тема 4. Взаємодія мережевих застосунків

Фізичний рівень. Системи числення. Канальний рівень. Мережевий рівень. Транспортний рівень. Прикладний рівень.

Тема 5. Основи мережевої безпеки

Загрози безпеці та вразливості. Мережеві атаки. Нейтралізація мережевих атак. Захист пристроїв, захисні функції з метою пом'якшення загроз безпеці.

Тема 6. Приклади побудови сучасних захищених інформаційних технологій.

Реалізація схеми для невеликої мережі, що включає маршрутизатор, комутатор і кінцеві пристрої. Пристрої у невеликій мережі. Програми та протоколи невеликої мережі. Розгортання мереж, як невелика мережа створює основу для більших мереж. Перевірка з'єднання, використання результатів команд ping і tracert для перевірки з'єднання та підтримки відповідної працездатності мережі. Команди хоста і IOS для отримання інформації про пристрої у мережі. Методи пошуку та усунення несправностей. Сценарії пошуку та усунення несправностей.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної звітності, обов’язковості модульного контролю, 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 та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. 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, фронтальне опитування, співбесіда, залік.
- *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;
- виконання тестових завдань.

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	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	3	3	3	3
Відвідування семінарських занять	1				
Відвідування практичних занять	1	2	2	2	2
Відвідування лабораторних занять	1	2	2	2	2
Робота на семінарському занятті	10				
Робота на практичному занятті	10	2	20	2	20
Лабораторна робота (в тому числі допуск, виконання, захист)	10	2	20	2	20
Виконання завдань для самостійної роботи	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25
Виконання ІНДЗ	30				
	Разом	-	77	-	77
	Максимальна кількість балів: 154				
	Розрахунок коефіцієнта: 154/100=1,54				

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. Основні поняття мережевих технологій		14	5
1	Тема 1. Основи мережевого з’єднання та передачі даних. Тема 2. Ethernet-концепції. Тема 3. Базове налаштування маршрутизатора.	14	5

Змістовий модуль 2. Основи мережевої безпеки та побудова сучасних захищених інформаційних технологій		14	5
2	Тема 4. IP-адресація. Тема 5. Взаємодія мережевими застосунками. Тема 6. Приклади побудови сучасних захищених інформаційних технологій.	14	5
	Разом	28	10

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 модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – комп'ютерний тест, що складається 20 запитань закритої та відкритої форм.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі заліку, умовою допуску до якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Орієнтовний перелік питань для самоконтролю

1. Пояснити переваги сучасних мережних технологій.
2. Пояснити, як використовуються вузли та мережні пристрої.
3. Пояснити способи подання мереж і те, як вони використовуються у мережних топологіях.
4. Описати чотири основні критерії надійної мережі.
5. Пояснити як такі тенденції як BYOD, онлайн-співпраця, відео і хмарні обчислення змінюють спосіб нашої взаємодії.
6. Визначити деякі основні загрози мережній безпеці та рішення для запобігання ним.
7. Пояснити як отримати доступ до пристрою під керуванням Cisco IOS з метою налаштування.
8. Пояснити як орієнтуватися у Cisco IOS для конфігурування мережних пристроїв.
9. Описати структуру команд програмного забезпечення Cisco IOS.
10. Налаштування пристрою під керуванням Cisco IOS за допомогою CLI.
11. Пояснити, як мережні протоколи дозволяють пристроям отримувати доступ до локальних і віддалених мережних ресурсів.
12. Пояснити роль організацій зі стандартизації у створенні протоколів для забезпечення мережної сумісності.
13. Пояснити як моделі TCP/IP і OSI використовуються для полегшення стандартизації процесу передавання даних.
14. Пояснити, як протоколи, служби та мережні середовища фізичного рівня підтримують

зв'язок між мережами передавання даних.
15. Перетворення чисел між десятковою, двійковою та шістнадцятковою системами.
16. Пояснити, як керування доступом до середовища передавання даних на Канальному рівні підтримує зв'язок між мережами.
17. Пояснити, як працює Ethernet у комутованій мережі.
18. Пояснити, як маршрутизатори використовують протоколи і служби мережного рівня для забезпечення наскрізного з'єднання.
19. Пояснити, як ARP і ND дозволяють спілкуватися у мережі.
20. Початкові налаштування на маршрутизаторі та кінцевих пристроях.
21. Обчислення схеми підмереж IPv4 для ефективного сегментування мережі.
22. Описати структуру адреси IPv4, включаючи мережну частину, вузлову частину і маску підмережі.
23. Пояснити як підмережі сегментують мережу для забезпечення кращої комунікації.
24. Пояснити, як створити гнучку схему адресації за допомогою маски підмережі змінної довжини (VLSM).
25. Пояснити, як налаштовувати статичні глобальні індивідуальні адреси та локальні адреси каналу мережі IPv6.
26. Пояснити, як динамічно налаштовувати глобальні індивідуальні адреси.
27. Використання різних засобів для перевірки мережного з'єднання. Пояснити як протокол ICMP використовується для перевірки мережного з'єднання.
28. Порівняти операцій протоколів транспортного рівня з точки зору підтримки наскрізного з’єднання.
29. Пояснити роботу протоколів прикладного рівня при наданні підтримки застосункам кінцевого користувача.
30. Пояснити, чому на мережних пристроях слід запроваджувати основні заходи безпеки.
31. Визначити протоколи і застосунки, які використовуються у невеликій мережі.
32. Описати традиційні методи виявлення і усунення несправностей у мережі.

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: 60 год., лекції – 12 год., практичні заняття –8 год., лабораторні роботи – 8 год., модульний контроль –4 год., самостійна робота –28 год.

Модулі (назви, бали)	**Змістовий модуль 1. Основні поняття мережевих технологій (77 балів)**			**Змістовий модуль 2. Основи мережевої безпеки та побудова сучасних захищених інформаційних технологій (77 балів)**		
Лекції (теми, бали)	Сучасні мережеві технології (1 бал)	Базова конфігурація захищених систем (1 бал)	Протоколи та моделі (1 бал)	Взаємодія мережевих застосунків (1 бал)	Основи мережевої безпеки (1 бал)	Приклади побудови сучасних захищених інформаційних технологій (1 бали)
Практичні, семінарські заняття (теми, бали)		Базові налаштування комутатора та кінцевого пристрою. (11 балів)	Дослідження моделей TCP/IP і OSI (11 балів)	Базові налаштування пристрою (11 балів)	Захист мережних пристроїв (11 балів)	
Лабораторні заняття (теми, бали)		Під'єднання дротової і бездротової локальної мережі (11 балів)	Дослідження ARP-таблиці (11 балів)	Проектування та впровадження VLSM (11 балів)		Відпрацювання комплексних практичних навичок (11 балів)
Самостійна робота	Самостійна робота (5 балів)				Самостійна робота (5 балів)	
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)				Модульна контрольна робота 2 (25 балів)	
Підсумковий контроль (вид, бали)	Залік					

8. Рекомендовані джерела

Основна

1. Богуш В.М., Довидьков О.А. Основи захищених інформаційних технологій. – К.: ДУІКТ, 2005 - 450 с.
2. Бурячок В.Л., Семко В.В., Складанний П.М., Лукова-Чуйко Н.В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. – К.: ДУТ - КНУ, 2016. – 178с.

Додаткова

3. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: термінологічний навчальний довідник. – К.: ООО “Д.В.К.” 2004. – 508 с.
4. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
5. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
6. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
7. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
8. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розроблення технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
9. Common Criteria for Information Technology Security Evaluation. National Institute of Standards and Technology \& National Security Agency (USA), Communication Security Establishment (Canada), UK IT Security and Certification Scheme (United Kingdom), Bundesamt fur Sichereit in der Informationstechnik (Germany), Service Central de la Securite des Systemes (France), National Communications Security Agency (Netherlands). Version 2.1. August 1999.
10. Common Methodology for Information Technology Security Evaluation. National Institute of Standards and Technology \& National Security Agency (USA), Communication Security Establishment (Canada), UK IT Security and Certification Scheme (United Kingdom), Bundesamt fur Sichereit in der Informationstechnik (Germany), Service Central de la Securite des Systemes (France), National Communications Security Agency (Netherlands). Version 0.95. June 2000.
11. ISO/IEC 7498-2. Information processing systems Open Systems Interconnection Basic Reference Model. Part 2: Security Architecture. Switzeland, 1989. 32 pp.

9. Додаткові ресурси

1. Cisco Networks Engineers’ Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA
2. CCENT/CCNA ICND1 Official Exam Certification Guide, Second Edition
3. Сайт мережевої академії Cisco [електроний ресурс] https://www.netacad.com/
4. Сайт Інституту інженерів з електротехніки та електроніки (IEEE, Institute of Electrical and Electronics Engineers) [електроний ресурс] http://www.ieee.org