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
«01» 09 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ»

для студентів

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

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Програма № 0974/23
(підпис) (прізвище, ініціали)

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	4 / 120	
Курс	2	
Семестр	3	
Кількість змістових модулів з розподілом:	3	
Обсяг кредитів	4	
Обсяг годин, в тому числі:	120	
Аудиторні	42	
Модульний контроль	6	
Семестровий контроль	30	
Самостійна робота	42	
Форма семестрового контролю	Екзамен	

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 навчальних планів 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. Забезпечення гарантій виконання вимог політик безпеки. 2. Стандартизовані моделі та методи оцінки ефективності захисту. Обсяг дисципліни. – 120 год. (4 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	Індивідуальні	
Змістовий модуль 1. Забезпечення гарантій виконання вимог політик безпеки							
Тема 1. Сучасні загрози мережевій безпеці	8	2					6
Тема 2. Забезпечення безпеки мережевих пристроїв	16	2		2	4		8
Тема 3. Авторизація, аутентифікація, аудит	10	2		2			6
Модульний контроль	2						
Разом	36	6		4	4		20
Змістовий модуль 2. Стандартизовані моделі та методи оцінки ефективності захисту							
Тема 4. Впровадження технологій міжмережевого екрану	16	2		2	4		8
Тема 5. Впровадження системи запобігання вторгненням	10	2		2			6
Тема 6. Безпека локальної мережі (LAN)	24	4		6	6		8
Модульний контроль	4						
Разом	54	8		10	10		22
Підготовка та проходження контрольних заходів	30						
Усього	120	14		14	14		42

5. Програма навчальної дисципліни

Змістовий модуль 1. Забезпечення гарантій виконання вимог політик безпеки

Тема 1. Сучасні загрози мережевій безпеці

Захист мереж. Мережеві загрози, опис загроз та атак різного типу. Нейтралізація загроз, інструменти та процедури для нейтралізації наслідків впливу шкідливого програмного забезпечення та поширених мережевих атак.

Тема 2. Забезпечення безпеки мережевих пристроїв

Захист доступу до пристроїв, конфігурація безпечного адміністративного доступу. Призначення адміністративних ролей, конфігурація авторизації команд з використанням рівнів привілеїв та CLI на основі ролей. Моніторинг пристроїв та керування ними, впровадження захищеного керування та моніторингу мережевих пристроїв. Використання автоматичних функцій забезпечення безпеки.

Тема 3. Авторизація, аутентифікація, аудит

Призначення AAA, способи застосування AAA для захисту мережі. Локальна автентифікація AAA, впровадження аутентифікації AAA, під час якої виконується звірка користувачів з локальною базою даних, Серверне рішення AAA, серверна автентифікація AAA та її комунікаційні протоколи. Серверна автентифікація AAA, впровадження серверної автентифікації з використанням протоколів TACACS+ та RADIUS. Серверна авторизація та облік AAA, конфігурація серверної авторизації та обліку AAA.

Змістовий модуль 2. Стандартизовані моделі та методи оцінки ефективності захисту

Тема 4. Впровадження технологій міжмережевого екрану

Списки контроля доступу, впровадження списків контролю доступу (ACL) для фільтрації трафіку та нейтралізації мережевих атак. Технології міжмережевих екранів, налаштування класичного міжмережевого екрану для нейтралізації мережевих атак. Зональні міжмережеві екрани, використання зонального міжмережевого екрану за допомогою інтерфейсу командного рядка (CLI).

Тема 5. Впровадження системи запобігання вторгненням

Технологии IPS, способи застосування AAA для захисту мережі. Сигнатури IPS, способи застосування сигнатур для виявлення шкідливого мережевого трафіку. Використання IPS, конфігурація операцій Cisco IOS IPS за допомогою інтерфейсу командного рядка (CLI).

Тема 6. Безпека локальної мережі (LAN)

Безпека кінцевих пристроїв, вразливості кінцевих пристроїв та способів захисту. Чинники, які необхідно враховувати при забезпеченні безпеки на рівні 2, впровадження функцій безпеки на рівні 2.

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:* тестові програми.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних і лабораторних 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	4	4
Відвідування семінарських занять					
Відвідування практичних занять	1	2	2	5	5
Відвідування лабораторних занять	1	2	2	5	5
Робота на семінарському занятті					
Робота на практичному занятті	10	2	20	5	50
Лабораторна робота (в тому числі допуск, виконання, захист)	10	2	20	5	50
Виконання завдань для самостійної роботи	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25
	Разом	-	77	-	144
Максимальна кількість балів: 221					
Розрахунок коефіцієнта: 221/60=3,68					

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом позааудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмного 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. Забезпечення гарантій виконання вимог політик безпеки		**20**	**5**
Тема 1. Криптографічні системи. Тема 2. Використання віртуальних приватних мереж (VPN).		20	5
Змістовий модуль 2. Стандартизовані моделі та методи оцінки ефективності захисту		**22**	**5**
Тема 3. Використання багатофункціонального пристрої захисту Cisco Adaptive Security Appliance. Тема 4. Багатофункціональний пристрій безпеки Cisco ASA з розширеним функціоналом.		22	5

Тема 5. Управління безпечною мережею.		
Разом	**42**	**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.	1 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	1 бали
3	Дотримання вимог щодо технічного оформлення	-
	Разом	2 бали

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 4 бали.

Форми проведення семестрового контролю та критерії оцінювання

Студент дає відповіді на запитання та завдання електронного тесту на платформі мережевої академії Cisco. Тест містить 60 питань. 40 питань містять одну правильну відповідь і оцінюються по 1 балу за правильну відповідь. 20 питань містять декілька правильних відповідей і оцінюються по 3 бали (3 бали – обрані всі варіанти відповідей правильно, 2 бали – не всі обрані варіанти обрано правильно, 1 бал – тільки одна відповідь з обраних є правильною). Всі питання закритого типу (вибір правильної відповіді із запропонованих варіантів), які передбачають автоматичну (комп'ютерну) перевірку. Загальна сума балів за тест на платформі мережевої академії Cisco складає 100 балів.

Екзамен проводиться із суворим дотриманням принципів академічної доброчесності, що передбачає недопустимість списування, фальсифікацій та обману. При порушенні студент відсторонюється від подальшого проходження екзаменаційного тесту із підсумковою оцінкою Fx за дисципліну. При виконанні завдань допускається користування довідковою літературою, матеріалами курсу CCNA Security.

Підсумкова оцінка за дисципліну в балах (максимально 100 балів) за дисципліну є сумою результату поточного контролю за семестр (60%) та відповіді на екзамені (40%).

Орієнтовний перелік питань для семестрового контролю

1. Пояснення того, що таке мережеві загрози, техніки нейтралізації та основи безпеки мережі.
2. Пояснення інструментів та процедур для нейтралізації наслідків впливу шкідливого ПЗ та поширених мережевих атак.
3. Захист адміністративного доступу до маршрутизаторів Cisco.
4. Захист адміністративного доступу з використанням AAA.
5. Пояснення способів застосування AAA для захисту мережі.
6. Пояснення серверної автентифікації AAA та її комунікаційних протоколів.
7. Впровадження технологій міжмережевого екрану для захисту периметра мережі.
8. Впровадження списків контролю доступу (ACL) для фільтрації трафіку та нейтралізації мережевих атак.
9. Використання зонального міжмережевого екрану за допомогою інтерфейсу командного рядка (CLI).

10. Конфігурування IPS для нейтралізації атак на мережу.
11. Пояснення способів застосування AAA для захисту мережі.
12. Пояснення способів застосування сигнатур для виявлення шкідливого мережевого трафіку.
13. Опис факторів, які необхідно враховувати для забезпечення безпеки LAN, та способів впровадження функцій безпеки рівня 2 та кінцевих пристроїв.
14. Пояснення вразливостей кінцевих пристроїв та способів захисту.
15. Опис методів забезпечення конфіденційності та цілісності даних.
16. Пояснення способів спільного застосування типів шифрування, хешей та цифрових підписів для забезпечення конфіденційності, цілісності та аутентифікації.
17. Пояснення способів застосування криптографічних хешів для забезпечення цілісності та автентифікації даних.
18. Пояснення способів застосування алгоритмів шифрування для забезпечення конфіденційності даних.
19. Пояснення способів застосування інфраструктури відкритих ключів для забезпечення конфіденційності та аутентифікації даних.
20. Використання захищених віртуальних приватних мереж (VPN).
21. Пояснення призначення мереж VPN.
22. Пояснення принципу роботи мереж IPsec VPN.
23. Конфігурація мережі Site-to-Site IPsec VPN (між двома пунктами) з автентифікацією за допомогою спільного ключа за допомогою інтерфейсу командного рядка (CLI).
24. Використання конфігурації міжмережевого екрана ASA з використанням командного інтерфейсу рядки (CLI).
25. Пояснення того, як пристрій ASA функціонує як розширений міжмережевий екран із збереженням стану.
26. Використання конфігурації міжмережевого екрана ASA та мереж VPN за допомогою ASDM.
27. Перевірка безпеки мережі та створення технічної політики безпеки.
28. Пояснення різних методів та інструментів, що використовуються для тестування безпеки мережі.
29. Пояснення призначення комплексної політики щодо інформаційної безпеки.

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 карта дисципліни

Разом: 120 год., лекції – 14 год., практичні заняття – 14 год., лабораторні роботи – 14 год., модульний контроль – 6 год., самостійна робота – 42 год., семестровий контроль – 30 год.

Модулі (назви, бали)	**Змістовий модуль 1. Забезпечення гарантій виконання вимог політик безпеки** (77 балів)			**Змістовий модуль 2. Стандартизовані моделі та методи оцінки ефективності захисту** (144 бали)		
Лекції (теми, бали)	Сучасні загрози мережевій безпеці (1 бал)	Забезпечення безпеки мережевих пристроїв (1 бал)	Авторизація, аутентифікація, аудит (1 бал)	Впровадження технологій міжмережевого екрану (1 бал)	Впровадження системи запобігання вторгненням (1 бал)	Безпека локальної мережі (LAN) (2 бали)
Лабораторні заняття (теми, бали)		Захист маршрутизатора для адміністративного доступу (22 бали)		Налаштування списків ACL для IP-адрес з метою нейтралізації атак (11 балів)	Конфігурування IOS IPS за допомогою інтерфейсу командного рядка (CLI) (11 балів)	Безпека VLAN на 2-му рівні. (33 бали)
Практичні заняття (теми, бали)		Налаштування операцій SYSLOG, NTP і SSH на маршрутизаторах CISCO (11 балів)	Налаштування аутентифікації AAA на маршрутизаторах Cisco (11 бали)	Налаштування розширених ACL списків за сценарієм 1 (22 бали)		Конфігурування та перевірка IPsec VPN між двома пунктами (site-to-site). Конфігурація базових налаштувань ASA та міжмережевого екрана за допомогою інтерфейсу командного рядка (CLI) (33 бали)
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)	Екзамен (40 балів)					

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

1. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: термінологічний навчальний довідник. – К.: ООО “Д.В.К.” 2004. – 508 с.
2. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
3. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
4. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
5. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
6. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розроблення технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
7. 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.
8. 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.
9. 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 CCENT/CCNA ICND1 Official Exam Certification Guide, Second Edition Сайт мережевої академії Cisco [електроний ресурс] https://www.netacad.com/
2. Сайт Інституту інженерів з електротехніки та електроніки (IEEE, Institute of Electrical and Electronics Engineers) [електроний ресурс] http://www.ieee.org