НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних систем, мереж та кібербезпеки

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г. Глазунова
"__" _____ 2023 р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем, мереж та кібербезпеки
Протокол №10 від «17» травня 2023 р.
Завідувач кафедри
(доц. Касаткін Д.Ю.)

РОЗГЛЯНУТО
Гарант ОП
«Кібербезпека»
_____
Гарант ОП
_____ (проф. Лахно В.А.)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ»

Спеціальність	125 «Кібербезпека»
Освітня програма	«Кібербезпека»
Факультет	інформаційних технологій
Розробник:	Кулініч О. М., к.т.н., доцент.

Київ – 2023

1. Опис навчальної дисципліни «Комплексні системи захисту інформації»

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	Бакалавр	
Галузь знань	12 – Інформаційні технології	
Спеціальність	125 – Кібербезпека	
Освітня програма	«Кібербезпека»	
Характеристика навчальної дисципліни		
Вид	обов’язкова	
Загальна кількість годин	120	
Кількість кредитів ECTS	4	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
Форма контролю	екзамен	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	2	
Семестр	4	
Лекційні заняття, год.	30	
Практичні, семінарські заняття	-	
Лабораторні заняття, год.	26	
Самостійна робота, год.	60	
МКР, год.	4	
Кількість тижневих аудиторних годин для денної форми навчання	4	

2. Мета, завдання та компетентності навчальної дисципліни

Мета: вивчення організаційних та інженерно-технічних заходів, спрямованих на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу, знайомство з базовими організаційними заходами для комплексних систем захисту інформації, а також інженерно-технічними заходами, засвоєння функціональних можливостей та методів побудови комплексних систем захисту інформації, опановування необхідними прийомами та практичними навичками при налаштуванні та конфігуруванні сучасного мережевого обладнання.

Завдання навчальної дисципліни: є теоретична та практична підготовка студентів до застосування методів побудови комплексних систем захисту інформації, навичок при налаштуванні та конфігуруванні сучасного мережевого обладнання.

В результаті вивчення навчальної дисципліни студент повинен

- знати: основні поняття та принципи побудови комплексної системи захисту інформації; нормативно – правову базу, що регулює етапи побудови, аудиту та впровадження КСЗІ; методики визначення об'єктів КСЗІ, їх класифікації та оцінки джерел дестабілізуючого впливу; принципи класифікації інформації, що підлягає захисту в КСЗІ підприємств та організацій різної форми власності; механізми та методи забезпечення організаційної, криптографічної, інженерно-технічної складових КСЗІ; методологію розробки та складанні моделей порушника та моделі загроз з врахуванням особливостей протікання бізнес-процесів на підприємстві чи організації; етапи проектування, розробки та підтримки КСЗІ та принципи сертифікації створюваних систем захисті інформації; принципи розробки політики безпека підприємства або організації різних форм власності.

- вміти:

вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; здійснювати оцінку рівня захищеності інформації що обробляється в інформаційно-телекомунікаційних системах використовувати інструментальні засоби оцінювання; готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної безпеки і \або кібербезпеки; розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; виконувати аналіз реалізації прийнятої політики інформаційної і /або кібербезпеки; проектувати та реалізувати комплексні системи захисту інформації в автоматизованих системах організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації; вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах; визначати рівень

захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 8. Здатність до абстрактного і системного мислення, аналізу та синтезу.

Спеціальні (фахові, предметні) компетентності (СК):

СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

СК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

СК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

СК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

СК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

СК9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

СК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

СК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

СК13. Здатність розробляти апаратне, алгоритмічне та програмне забезпечення, компоненти комп’ютерних систем захисту інформації.

В результаті вивчення навчальної дисципліни студент набуде певні програмні результати (ПРН), а саме

ПРН6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПРН10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

ПРН11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.

ПРН13. Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних.

ПРН16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.

ПРН20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

ПРН21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

ПРН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

ПРН25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

ПРН28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.

ПРН30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

ПРН35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-

телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.

ПРН36. Виявляти небезпечні сигнали технічних засобів.

ПРН37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.

ПРН50. Забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

В контексті зазначених вище компетентностей та програмних результатів навчання задачі викладання дисципліни визначають необхідний комплекс знань і вмінь, що отримують студенти під час вивчення дисципліни.

Навчальна програма розрахована на студентів, які навчаються за освітньою програмою підготовки бакалавра за спеціальністю «Кібербезпека».

Програма побудована за вимогами кредитно-модульної системи організації навчального процесу у закладах вищої освіти і використанням академічної системи оцінювання досягнень студентів та шкали оцінок Європейської кредитно-трансферної системи (ECTS).

Робоча навчальна програма з курсу «Комплексні системи захисту інформації» є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма дисципліни «Комплексні системи захисту інформації» розроблена на підставі наступних документів:

- освітня програма підготовки фахівців за спеціальністю 125 «Кібербезпека»;
- навчальний план підготовки фахівців за спеціальністю 125 «Кібербезпека».

Навчальна програма характеризує шляхи перетворення інформації, що одержується студентом впродовж вивчання курсу, і відбиває зміст курсу, розподілення його на розділи та їх обсяги, дані про форми вивчення та контролю знань.

Теоретичною базою для вивчення курсу «Комплексні системи захисту інформації» є курси «Організаційне забезпечення захисту інформації» та «Інформаційна безпека держави».

Курс «Комплексні системи захисту інформації» є базовим для вивчення наступної дисципліни: «Безпека інформації в інформаційно-комунікаційних системах».

3.Програма та структура навчальної дисципліни

– повного терміну денної (заочної) форми навчання;

Назви змістових модулів і тем	Кількість годин												
	денна форма							Заочна форма					
	тиж-ні	всьо-го	у тому числі					всьо-го	у тому числі				
			л	п	лр	інд	с.р.		л	п	лр	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Змістовий модуль 1. Порядок проведення робіт із створення комплексної системи захисту інформації.													
Тема 1. Нормативно-методичне забезпечення з питань побудови КСЗІ та проведення їх державної експертизи.	1	6	2				4						
Тема 2.Автоматизовані системи. Класифікація, типи інформації, які обробляються в автоматизованих системах.	2	8	2		2		4						
Тема 3. Формування загальних вимог до КСЗІ в ІТС.	3	8	2		2		4						
Тема 4. Визначення об'єктів захисту. Оцінка загроз та джерел загроз безпеці інформації, що циркулює на об’єкті інформаційної діяльності.	4	6	2				4						
Тема 5. Сутність моделі порушника інформаційної безпеки в ІТС при створенні комплексної системи захисту інформації.	5	10	2		4		4						
Тема 6. Вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій, які	6	8	2		2		4						

регламентують використання захищених технологій обробки інформації в ІТС.													
Тема 7. Визначення вимог із захисту оброблюваної в ІТС, вибір послуг безпеки ІТС.	7	10	2		4		4						
Тема 8. Обґрунтування і прийняття проектних рішень, які дають змогу реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію різних компонентів КСЗІ.	8	4	2				2						
МКР	8	4			2		2						
Разом за змістовим модулем 1		**64**	**16**		**16**		**32**						
Змістовий модуль 2. Визначення відповідності комплексної системи захисту інформації технічному завданню.													
Тема 1. Введення КСЗІ в дію та оцінка захищеності інформації в ІТС.	9	8	2		2		4						
Тема 2. Розробка програми та методики державної експертизи комплексної системи захисту інформації.	10	8	2		2		4						
Тема 3. Етапи проведення державної експертизи комплексної системи захисту інформації.	11	6	2				4						
Тема 4. Створення комплексу технічного захисту інформації, порядок розробки та відмінності в застосуванні.	12	10	2		4		4						
Тема 5. Декларація про відповідність, порядок розробки та відмінності в застосуванні.	13	8	2		2		4						
Тема 6. Порядок створення та впровадження організаційно-	14	8	2		2		4						

технічного рішення на комплексну систему захисту інформації.													
Тема 7. Організація служби захисту інформації (СЗІ) та організаційне проектування діяльності СЗІ.	15	4	2				2						
МКР	15	4			2		2						
Разом за змістовим модулем 2		**56**	**14**		**14**		**28**						
Всього годин		**120**	**30**		**30**		**60**						

4. Теми практичних занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

Теми семінарських занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Класифікація інформації, яка обробляється в автоматизованих системах.	2
2	Формування загальних вимог до КСЗІ в ІТС.	2
3	Розроблення плану робіт із захисту інформації в ІТС.	4
4	Розроблення вимог до КЗЗ в частині захисту від несанкціонованого доступу в ІТС.	2
5	Визначення вимог із захисту оброблюваної в ІТС, вибір послуг безпеки ІТС.	4
6	Розроблення вимог до КСЗІ в частині захисту ІТС від несанкціонованого доступу.	2
7	Розроблення інструкції з модернізації КСЗІ.	2
8	Розроблення інструкції адміністратора безпеки та інструкції системного адміністратора.	2
9	Створення комплексу технічного захисту інформації, порядок розробки та відмінності в застосуванні.	4
10	Розроблення положення про службу захисту інформації на підприємстві.	2
	Всього	**26**

Курсове проектування - Не передбачено робочим навчальним планом

САМОСТІЙНА РОБОТА СТУДЕНТІВ

Самостійна робота студентів передбачає:

- систематичне відвідання усіх видів аудиторних занять і ведення конспекту лекцій;

- систематичне вивчення лекційного матеріалу і навчальної літератури, що рекомендуються;
- сумлінну підготовку до лабораторних занять;
- вчасне і якісне оформлення звітів про лабораторні роботи.

6. Контрольні питання, комплекти тестів для визначення рівня засвоєння знань студентами

6.1. Питання для перевірки знань студентів:

1. Етапи створення КСЗІ.
2. Формування загальних вимог до КСЗІ в ІТС.
3. Обґрунтування необхідності створення КСЗІ.
4. Порядок обстеження середовищ функціонування ІТС.
5. Формування завдання на створення КСЗІ.
6. Порядок розробки політики безпеки інформації в ІТС.
7. Вибір варіанту КСЗІ.
8. Порядок розробки плану захисту інформації.
9. Порядок розробки технічного завдання на створення КСЗІ.
10. Порядок розробки проекту КСЗІ.
11. Сутність ескізного проекту КСЗІ.
12. Сутність технічного проекту КСЗІ.
13. Сутність робочого проекту КСЗІ.
14. Порядок підготовки КСЗІ до введення в дію.
15. Навчання користувачів КСЗІ і ІТС.
16. Оцінка захищеності інформації в ІТС.
17. Комплектування КСЗІ.
18. Будівельно-монтажні роботи при побудові КСЗІ.
19. Пусконалагоджувальні роботи КСЗІ.
20. Порядок проведення попередніх випробувань КСЗІ.
21. Порядок проведення дослідної експлуатації КСЗІ.
22. Порядок проведення державної експертизи КСЗІ.
23. Організація служби захисту інформації.
24. Організаційне проектування діяльності служби захисту інформації.
25. Порядок створення служби захисту інформації.
26. Склад нормативних документів, що регламентують діяльність служб захисту інформації.
27. Сутність декларації про відповідність.
28. Порядок розробки декларації про відповідність.
29. Порядок розробки програми державної експертизи комплексної системи захисту інформації.
30. Порядок розробки методики державної експертизи комплексної системи захисту інформації.
31. Сутність моделі загроз.
32. Сутність моделі порушника.
33. Сутність автоматизованих систем.
34. Класифікація автоматизованих систем.
35. Типи інформації, які обробляються в автоматизованих системах.
36. Визначення об'єктів захисту.

6.2. Приклади тестів з дисципліни:

1. Об'єктами захисту в системі є:

А) володільці інформації, власники системи, користувачі;

В) спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи;

С) інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

2. Комплексна система захисту інформації - це ...

А) організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

В) взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

С) діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

3. Метою пусконалагоджувальних робіт є: ...

А) встановлення і налагодження КЗЗ;

В) приймання робіт з оцінкою їх відповідності вимогам ТЗ;

С) перевірка працездатності КСЗІ та визначення можливості прийняття її у дослідну експлуатацію.

7. Методи навчання

Виконання лабораторних робіт з використанням ПЗ; виконання індивідуальних навчально-дослідних завдань.

8. Форми контролю

Систематичний контроль за самостійною роботою студентів і якістю засвоєння ними поточного навчального матеріалу:

- на лабораторних роботах шляхом перевірки підготовки до виконання роботи;
- роботу над індивідуальними завданнями до лабораторних робіт;
- вивчення літератури, що рекомендувалася, та конспекту лекцій;
- оформлення звітів про виконання лабораторним роботам.

Поточний контроль знань студентів проводиться:

- на лабораторних роботах оцінюється підготовка до роботи, обсяг її виконання, результати захисту звіту;
- на лекційних заняттях виконується вибіркове опитування студентів;
- шляхом проведення модульних контролів знань студентів та виставлення рейтингових оцінок знань студентів по усім видам занять.

9. Розподіл балів, які отримують студенти.

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл. 1 «ПОЛОЖЕННЯ про екзамени та заліки у НУБіП України» (наказ про уведення в дію від «26» квітня 2023 р. протокол № 10):

Рейтинг здобувача вищої освіти, бали	Оцінка національна за результати складання екзаменів заліків	
	Екзамен	**Залік**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

Для визначення рейтингу студента із засвоєння дисципліни $R_{дис}$ (до 100 балів) одержаний рейтинг з атестації $R_{АТ}$ (до 30 балів) додається до рейтингу студента з навчальної роботи $R_{НР}$ (до 70 балів): $R_{дис}=R_{НР}+R_{АТ}$.

10. Методичне забезпечення

1. Електронний навчальний курс на платформі Moodle вміщує повне методичне забезпечення включаючи: лекції, презентації до лекцій, методичні вказівки до виконання лабораторних робіт, глосарій термінів тощо.

11. Рекомендована література

Основна:

1. НД ТЗІ 3.7-003 -2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» // Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. Київ. 2005. – С. 22.
2. Закон України «Про захист інформації в автоматизованих системах» // Відомості Верховної Ради України, 1994. - № 31. – С. 286.
3. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.].Вінниця : ВНТУ, 2018. - 118 с.
4. Проєктування комплексних систем захисту інформації. Підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. 320 с
5. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. – К.: ІСЗЗІ НТУУ «КПІ», 2015. – 104 с.
6. Методи та засоби інженерно-технічного захисту інформації навч. посіб. / В.В. Богданов, О.В.Волков, О.В.Жук, В.В.Мартинюк – К.: ВІТІ НТУУ «КПІ», 2013.
7. НД ТЗІ 1.1-002-1999 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. [в редакції станом на 28.12.2012. Київ. ДСТСЗІ СБ України, 2012, ст. 21.
8. НД ТЗІ 3.6-003-2016 Порядок проведення робіт зі створення та атестації комплексу технічного захисту інформації.
9. Постанова Кабінету Міністрів України від 16.02.1998 № 180 «Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах».
10. Постанова Кабінету Міністрів від 29.03.2006 № 373 «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».
11. Технічні канали витоку інформації: навч. посіб. / Ю.Б. Науменко, Н.А. Паламарчук, С.А. Паламарчук, О.Є. Ткаленко – К.: ВІТІ НТУУ «КПІ», 2010.
12. Технічно-експлуатаційна документація до відповідних технічних засобів, систем та комплексів технічного захисту інформації, що вивчаються.

13. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95).

14. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ – ПЕМВН-95).

15. Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах.

16. ДСТУ 3396 0-96. Захист інформації. Технічний захист інформації. Основні положення.

17. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

18. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

19. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.

20. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення

21. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.

22. НД ТЗІ 3.3-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

23. НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.

24. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі.

25. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

26. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

27. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

28. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.

Допоміжна

1. Кузнецов О.О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2011. – 510 с.

Інформаційні ресурси

1. АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=81998&cat_id=38835