Державний університет інтелектуальних технологій і зв'язку
Факультет інформаційних технологій та кібербезпеки
Кафедра кібербезпеки та технічного захисту інформації

"**ЗАТВЕРДЖУЮ**"
Ректор ДУІТЗ
_____ Олександр НАЗАРЕНКО
"____" _____ 2023 року

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ООК-5 Спеціальні вимірювання в галузі ТЗІ

Рівень вищої освіти	другого (магістерського) рівня
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Спеціалізація (за наявності)	
Освітня програма	магістрів
Статус дисципліни	нормативна
Мова викладання	українська

Одеса 2023

Програма навчальної дисципліни Спеціальні вимірювання в галузі ТЗІ для студентів освітнього рівня другий (магістерський) за спеціальністю 125 Кібербезпека та захист інформації

Розробник: викладач Онацький Олексій Віталійович

Навчальна програма затверджена на засіданні кафедри кібербезпеки та технічного захисту інформації

Протокол від "21" березня 2023 року № 8

Завідувач кафедри _____ В.В. Корчинський

"21" березня 2023 року

Програму погоджено з гарантом освітньо-професійних програми магістрів

Гарант освітньо-професійної програми _____ В.В. Корчинський

Програму погоджено з деканом факультету інформаційних технологій та кібербезпеки

Декан факультету _____ Є.В. Василіу

Програму схвалено навчально-методичною радою ДУІТЗ

Голова навчально-методичної ради ДУІТЗ,

Проректор з навчальної роботи _____ А.Г. Ложковський

Протокол № _____ від _____ "____" _____ 2023 р.

ВСТУП

Програма вивчення нормативної навчальної дисципліни «Спеціальні вимірювання в галузі ТЗІ» складена відповідно до освітньо-професійної програми підготовки магістрів в галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека та захист інформації».

У дисципліні розглядається порядок проведення робіт з технічного захисту інформації, а саме: організаційні заходи; заходи з технічного захисту мовної інформації; заходи з технічного захисту інформації, яка обробляється в інформаційно-комунікаційних системах; сутність, шляхи та запобігання утворення технічних каналів витоку інформації: мовної та візуальної інформації, матеріально-речовинні канали витоку інформації, технічні канали витоку інформації, що обробляється основними та допоміжними технічними засобами системи, технічні канали витоку інформації на основі закладних пристроїв. Розглядається порядок розроблення технічного завдання, перелік основних робіт етапу формування технічного завдання, зміст технічного завдання, створення комплексу технічного захисту інформації, модель загроз для інформації: ситуаційний та генеральний план об'єкту інформаційної діяльності, схеми розташування та опис ОТЗС та ДТЗС, обґрунтування можливості створення технічних каналів витоку інформації. Розглядається порядок розроблення та оформлення програм і методик випробувань, проведення атестації комплексу технічного захисту інформації, основні технічні характеристики вимірювальної апаратури, приклади оформлення протоколів спецдослідження або перевірки захищеності виділеного приміщення різної категорії від можливого витоку мовної інформації з обмеженим доступом акустичним, віброакустичним та акустоелектричним каналом.

Дисципліна «Спеціальні вимірювання в галузі ТЗІ» викладається у 5.1 семестрі та кількістю кредитів ECTS – 4.

Предметом вивчення навчальної дисципліни є: аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації; формувати стратегію і політики безпеки інформації в інформаційно-комунікаційних системах; виконувати передпроектні роботи щодо систем та комплексів захисту інформації; проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності; виявляти закладні пристрої на об'єктах інформаційної діяльності; проводити оцінку відповідності (атестацію) комплексів технічного захисту інформації.

Міждисциплінарні зв'язки. Дисципліна базується на професійно-орієнтованих дисциплінах:

Комплексні системи безпеки.

Комплексні системи захисту інформації: проектування, впровадження, супровід.

Методи оцінки інформаційної захищеності.

Методи та засоби захисту інформації.

Забезпечення безпеки телекомунікацій.

Програма навчальної дисципліни складається з змістового модуля:

1. Спеціальні вимірювання в галузі ТЗІ.

1. Мета та завдання навчальної дисципліни

1.1. Метою викладання навчальної дисципліни «Спеціальні вимірювання в галузі ТЗІ» є:

– ознайомлення студентів із методами впровадження систем та комплексів захисту інформації, їх склад і призначення, з застосуванням існуючої нормативної бази в Україні;

– розвиток у студентів практичних навичок у послідовності розробки комплексу технічного захисту інформації;

– підготовка висококваліфікованих фахівців, здатних ставити завдання на виконання етапів технічного проекту і вибирати способи їх реалізації.

1.2. Основними завданнями вивчення дисципліни «Спеціальні вимірювання в галузі ТЗІ» є:

– надання студентові теоретичні знання для задач керування розробкою комплексу технічного захисту інформації;

– аналізувати потреби та вимоги користувачів з метою планування і проведення розробки системи безпеки.

У результаті вивчення навчальної дисципліни студент повинен отримати наступні компетенції відповідно до Стандарту вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» для другого (магістерського) рівня вищої освіти, затвердженого Наказом МОН № 332 від 18.03.2021 р.

Загальні компетентності.

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.

КЗ-2. Здатність проводити дослідження на відповідному рівні.

Фахові компетентності.

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Програмні результати навчання.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

У результаті вивчення навчальної дисципліни студент повинен отримати наступні професійні компетенції (**А**, **Б**, **Д**, **Е**), знання (**З**) та навички/уміння (**У**) з професійного стандарту «Фахівець сфери захисту інформації», затвердженого наказом Адміністрації Держспецзв'язку № 715 від 25.11.2022.

А1. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації.

А1.З1. Поняття та класифікація інформації з обмеженим доступом, державні інформаційні ресурси.

А1.З2. Поняття технічного та криптографічного захисту інформації.

А1.З5. Закони, нормативні акти, нормативні документи, що визначають вимоги із захисту інформації та кіберзахисту.

А1.З6. Політики та етичні норми приватності стосовно безпеки інформації та кібербезпеки.

А1.З7. Принципи та способи захисту інформації, кібербезпеки та приватності.

А1.З10. Поняття комплексних систем захисту інформації та комплексів технічного захисту інформації, їх склад і призначення.

А1.З11. Моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, призначених для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації.

А1.У1. Визначати (формулювати) потреби щодо захисту інформації, що обробляється в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах користувачів (замовників).

А1.У2. Визначати (формулювати) потреби щодо захисту інформації, що озвучується на об'єктах інформаційної діяльності підприємства (організації).

А1.У4. Визначати та аналізувати вимоги щодо захисту інформації та кіберзахисту в інформаційно-комунікаційних системах та на об'єктах інформаційної діяльності підприємства (організації).

А1.У5. Здійснювати попередню оцінку достатності потреб і вимог користувачів (замовників) для забезпечення необхідного рівня захисту інформації та кіберзахисту.

А1.У6. Застосовувати політики безпеки для досягнення цілей безпеки системи.

А1.У7. Аналізувати потреби та вимоги користувачів з метою планування і

проведення розробки системи безпеки.

А1.У8. Використовувати моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації.

А2. Здатність виявляти, досліджувати (оцінювати), системно аналізувати загрози для інформації, аналізувати ризики безпеки інформації та кібербезпеки у разі реалізації загроз.

А2.З1. Класифікація загроз для інформації та кіберзагроз (загрози від несанкціонованих дій з інформацією, технічні канали витоку інформації, спеціальні впливи на засоби обробки інформації).

А2.З2. Методи (способи) та методики виявлення, дослідження та системного аналізу загроз для інформації та кіберзагроз.

А2.З3. Форми та зміст моделей загроз для інформації, моделі порушника інформації; порядок їх розробки.

А2.З5. Підходи, методи (способи) оцінки та аналізу ризиків безпеки інформації та кібербезпеки.

А2.З7. Поняття спеціальних впливів на засоби обробки інформації з метою знищення (спотворення), блокування інформації.

А2.У2. Виявляти загрози для інформації, що озвучується на об’єктах інформаційної діяльності (обґрунтовувати можливість створення певних технічних каналів витоку інформації, що озвучується на конкретному об’єкті інформаційної діяльності).

А2.У3. Досліджувати (оцінювати) та системно аналізувати загрози для інформації та вразливості комп’ютерної системи (систем) для розробки профілю безпеки.

А2.У5. Розробляти модель загроз для інформації від несанкціонованих дій та модель порушника інформації.

А2.У6. Розробляти модель загроз для інформації від витоку технічними каналами.

А2.У7. Розробляти модель загроз для інформації від спеціальних впливів на засоби обробки інформації.

А3. Здатність формувати стратегію і політики безпеки інформації в інформаційно-комунікаційних системах.

А3.З4. Зміст і порядок розробки політики безпеки інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

А3.З5. Поняття профілю безпеки інформації та функціональних послуг безпеки.

А3.З6. Поняття рівня гарантій реалізації функціональних послуг безпеки.

А3.У4. Визначати (розробляти, обґрунтовувати) профіль безпеки інформації в автоматизованих системах різного класу.

А5. Здатність виконувати передпроєктні роботи щодо систем та комплексів захисту інформації.

А5.З1. Середовища функціонування автоматизованих систем.

А5.З2. Загальний порядок створення комплексних систем захисту інформації та комплексів технічного захисту інформації.

А5.З3. Порядок категоріювання об’єктів.

А5.З4. Порядок і методи (способи) обстеження середових функціонування автоматизованих систем та об’єктів інформаційної діяльності.

А5.З5. Порядок розробки моделей загроз для інформації.

А5.З6. Порядок розробки та зміст технічних завдань на створення комплексних систем захисту інформації та комплексів технічного захисту інформації.

А5.У1. Здійснювати категоріювання об’єктів інформаційної діяльності (об’єктів електронно-обчислювальної техніки).

А5.У2. Здійснювати обстеження середовищ функціонування автоматизованих систем.

А5.У3. Здійснювати обстеження об’єктів інформаційної діяльності.

А5.У4. Розробляти моделі загроз для інформації.

А5.У5. Розробляти технічні завдання на створення комплексних систем захисту інформації.

А5.У6. Розробляти технічні завдання на створення комплексів технічного захисту інформації.

А5.У7. Розробляти проекти комплексних систем захисту інформації та комплексів технічного захисту інформації багаторівневими вимогами безпеки або вимогами для обробки кількох рівнів класифікації даних (відкрита інформація, службова інформація, секретна інформація з різними ступенями секретності).

А6. Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об’єктів інформаційної діяльності.

А6.З1. Поняття спеціальних досліджень засобів обробки інформації, технічних засобів.

А6.З2. Поняття спеціальних досліджень об’єктів інформаційної діяльності.

А6.З4. Поняття об’єкта інформаційної діяльності.

А6.З5. Поняття показників захищеності інформації засобів обробки інформації та показників захищеності мовної інформації на об’єкті інформаційної діяльності.

А6.З7. Методики спеціальних досліджень засобів обробки інформації та об’єктів інформаційної діяльності.

А6.У2. Проводити спеціальні дослідження об’єктів інформаційної діяльності (складати схеми спеціальних досліджень, виявляти та вимірювати небезпечні (тестові) акустичні, віброакустичні, акустоелектричні, акустоелектромагнітні, лазерні сигнали, визначати показники захищеності мовної інформації на об’єкті інформаційної діяльності та можливість (неможливість) створення на об’єкті інформаційної діяльності певних технічних каналів витоку інформації).

А6.У3. Визначати вимоги до показників (характеристик) апаратних засобів технічного захисту інформації, які необхідні для забезпечення захищеності інформації в системі або на об’єкті інформаційної діяльності.

А6.У4. Складати протоколи спеціальних досліджень.

А6.У5. Складати приписи на експлуатацію засобів обробки інформації та об’єктів інформаційної діяльності.

А7. Здатність впроваджувати (активізувати) програмні та апаратні засоби захисту інформації в системах і на об’єктах.

А7.З6. Порядок розробки та зміст технічних проектів комплексних систем захисту інформації та комплексів технічного захисту інформації.

А7.У10. Впроваджувати (налаштовувати) апаратні засоби захисту інформації на об’єктах інформаційної діяльності.

А7.У11. Оцінювати якість виконаних робіт з впровадження програмних та апаратних засобів захисту інформації в системах і на об’єктах.

А9. Здатність розробляти, впроваджувати та аналізувати технічні документи, положення, інструкції щодо систем і комплексів захисту інформації.

А9.З1. Систему технічних документів щодо систем і комплексів захисту інформації.

А9.З2. Вимоги до структури та змісту технічних документів щодо систем і комплексів захисту інформації.

А9.З3. Вимоги та підходи до розроблення технічних документів положень, інструкцій, методичних матеріалів щодо систем і комплексів захисту інформації.

А9.З4. Сучасні підходи до формування вимог до захисту інформації в інформаційно-комунікаційних системах і на об’єктах інформаційної діяльності.

А9.У3. Розроблювати (брати участь у розробці) технічної та експлуатаційної документації щодо створення, державної експертизи, (атестації), ведення в експлуатацію, експлуатації систем і комплексів захисту інформації.

А9.У5. Розроблювати плани аварійного відновлення та безперервності операцій в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

А10. Здатність виявляти закладні пристрої на об’єктах інформаційної діяльності.

А10.З1. Поняття закладних пристроїв для зняття інформації, що озвучується та/або обробляється на об’єкті інформаційної діяльності.

А10.З2. Класифікація закладних пристроїв.

А10.З3. Принцип дії закладних пристроїв основних класів.

А10.З4. Методи (способи) виявлення закладних пристроїв на об’єктах інформаційної діяльності.

А10.У1. Розробляти методику виявлення закладних пристроїв на об’єктах інформаційної діяльності.

А10.У2. Здійснювати виявлення (брати участь у виявленні) закладних пристроїв на об’єктах інформаційної діяльності.

А10.У3. Оформлювати акти за результатами виявлення закладних пристроїв на об’єктах інформаційної діяльності.

Б1. Здатність проводити оцінку відповідності (атестацію) комплексів технічного захисту інформації.

Б1.З1. Поняття атестації комплексів технічного захисту інформації.

Б1.З2. Порядок, умови та організація проведення атестації комплексів технічного захисту інформації.

Б1.З3. Поняття та загальний зміст програми та методики проведення атестації комплексів технічного захисту інформації.

Б1.З4. Техніко-технологічне, комп’ютерне, програмне та інше забезпечення атестації комплексів технічного захисту інформації.

Б1.З5. Засоби вимірювальної техніки та методики вимірювань оцінюваних показників комплексів технічного захисту інформації.

Б1.З6. Документи, що оформлюються за результатами атестації комплексів технічного захисту інформації.

Б1.У1. Складати програму та методику атестації комплексу технічного захисту інформації (ТЗІ)

Б1.У2. Здійснювати перевірку повноти і відповідності реалізованих заходів із захисту інформації вимогам технічного завдання на створення комплексу ТЗІ (або на створення КСЗІ в інформаційно-комунікаційних системах в частині вимог до захисту інформації від витоку технічними каналами), нормативно-правових актів та нормативних документів системи ТЗІ.

Б1.У3. Здійснювати інструментальний контроль захищеності інформації на об'єкті інформаційної діяльності від витоку технічними каналами.

Б1.У4. Робити висновки щодо відповідності комплексу ТЗІ вимогам технічного завдання на створення комплексу ТЗІ (або на створення КСЗІ в ІТС в частині вимог до захисту інформації від витоку технічними каналами), нормативно-правових актів і нормативних документів системи ТЗІ.

Б1.У5. Оформлювати протоколи інструментального контролю захищеності інформації на об'єкті інформаційної діяльності.

Б1.У6. Оформлювати акти атестації комплексів ТЗІ та організовувати їх затвердження і реєстрацію.

Б2. Здатність проводити оцінку відповідності (державну експертизу) комплексних систем захисту інформації та засобів технічного захисту інформації.

Б2.З1. Поняття та шляхи проведення державної експертизи комплексних систем захисту інформації та засобів технічного захисту інформації.

Б2.З2. Порядок, умови та організація проведення державної експертизи комплексних систем захисту інформації та засобів технічного захисту інформації.

Б2.З3. Поняття та загальний зміст програми та методики проведення державної експертизи комплексних систем захисту інформації та засобів технічного захисту інформації.

Б2.З4. Методи тестування та оцінки захищеності систем.

Б2.З7. Документи, що оформлюються за результатами державної експертизи комплексних систем захисту інформації та засобів технічного захисту інформації.

Б2.У1. Складати програму та методику проведення державної експертизи комплексних систем захисту інформації.

Б2.У2. Проводити попереднє ознайомлення з об'єктом експертизи та поглиблене обстеження об'єкта експертизи.

Б2.У4. Оформлювати протоколи експертних випробувань та атестати відповідності комплексних систем захисту інформації.

Б2.У5. Здійснювати експертизу комплексних систем захисту інформації шляхом декларування, оформлювати декларації відповідності комплексних систем захисту інформації та організовувати їх затвердження та реєстрацію.

Д2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування щодо системи технічного та криптографічного захисту інформації.

Д2.З1. Порядок розробки та впровадження нормативних документів системи технічного та криптографічного захисту інформації.

Д2.З2. Порядок актуалізації нормативних документів системи технічного та криптографічного захисту інформації.

Д2.У1. Розробляти (брати участь у розробці) нормативні документи системи технічного та криптографічного захисту інформації.

Д2.У2. Писати та публікувати методики та настанови з кіберзахисту та інструктивні матеріали.

Д2.У3. Впроваджувати нормативні документи системи технічного та криптографічного захисту інформації.

Д2.У4. Здійснювати актуалізацію нормативних документів системи технічного та криптографічного захисту інформації.

Д2.У5. Використовувати результати аналізу кращих світових практик, стандартів при розробці нормативних документів системи технічного та криптографічного захисту інформації.

Е1. Здатність здійснювати технічне керівництво фахівцями структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки.

Е1.З1. Керівництва (настанови, інструкції), нормативні акти роботодавця з організації, координації діяльності та взаємодії структурних підрозділів підприємства/ організації.

Е1.З2. Посадові інструкції фахівців структурних підрозділів підприємства/організації, до функцій яких входять питання захисту інформації та кібербезпеки

Е1.З3. Основи управління персоналом.

Е1.У1. Здійснювати методичне та технічне керівництво фахівцями структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки.

Е1.У2. Координувати роботи (брати участь у координації робіт) із захисту інформації та кібербезпеки в структурних підрозділах підприємства/організації.

Е1.У5. Приймати участь в організації та навчанні (підвищенні кваліфікації) працівників структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки, з відповідних питань.

2. Інформаційний обсяг навчальної дисципліни

Змістовий модуль 1. Спеціальні вимірювання в галузі ТЗІ.

1. Поняття комплексних систем захисту інформації та комплексів технічного захисту інформації, їх склад і призначення. Вимоги щодо захисту інформації та кіберзахисту.

Самостійно. Закони, нормативні акти, нормативні документи, що визначають вимоги із захисту інформації та кіберзахисту.

2. Класифікація технічних каналів витоку інформації. Сутність, шляхи та запобігання утворення технічних каналів витоку інформації.

Самостійно. Розробка моделі порушника інформації.

3. Порядок проведення робіт з технічного захисту інформації. Передпроектні роботи щодо систем та комплексів захисту інформації.

Самостійно. Розробка політики безпеки інформаційно-комунікаційних системах.

4. Створення комплексів технічного захисту інформації. Попередні випробування та дослідна експлуатація комплексів технічного захисту інформації.

Самостійно. Розробка моделі загроз на об'єкті інформаційної діяльності.

5. Атестації комплексів технічного захисту інформації.

Самостійно. Розробка програми та методики проведення атестації комплексів технічного захисту інформації

6. Система технічних документів щодо систем і комплексів захисту інформації.

Самостійно. Протокол інструментального контролю захищеності інформації на об'єкті інформаційної діяльності.

7. Порядок проведення робіт з державної експертизи комплексної системи захисту інформації.

Самостійно. Оформлення документації.

3. Рекомендована література

ОСНОВНА

1. Про внесення змін до Закону України "Про інформацію" № 2938-VI від 13.01.2011. – Відомості Верховної Ради України 2011, № 32, ст. 313. – (Серія видань "Законодавство України").

2. Закон України "Про захист персональних даних" № 2297-VI від 01.06.2010. – Відомості Верховної Ради України 2010, № 34, ст. 481. – (Серія видань "Законодавство України").

3. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" № 80/94-ВР від 05.07.1994. – Відомості Верховної Ради України 1994, № 31, ст. 286. – (Серія видань "Законодавство України").

4. НД ТЗИ 1.1-003-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. – (Серія видань "Нормативний документ").

5. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22 від 28.04.99. – (Серія видань "Нормативний документ").

6. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22 від 28.04.1999. – (Серія видань "Нормативний документ").

7. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. – Затверджено наказом ДСТСЗІ СБ України № 125 від 8.11.2005. – (Серія видань "Нормативний документ").

8. Положення про Державну експертизу в сфері технічного захисту інформації. – Затверджено наказом Адміністрації ДССЗЗІ України № 93 від 16.05.07. – Офіційний вісник України. – 2007. – № 52, ст. 2153. – (Серія видань "Нормативний документ").

9. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. – Затверджено наказом Адміністрації ДССЗЗІ України № 65 від 12 березня 2011. – (Серія видань

“Нормативний документ”).

10. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В.Р – Київ.: ООО "Д.В.К.", 2004. – 508 с.

11. Кононович В.Г., Гладиш С.В. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Частина 4: навч. посіб. – Одеса: ОНАЗ ім. О.С. Попова, 2009.

12. Moodle. https://e-learning.suitt.edu.ua/course/view.php?id=27

13. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спеціальності 125 "Кібербезпека" спеціалізації "Системи технічного захисту інформації" / І. Є. Антіпов, А. М. Олейніков, Ю. В. Ликов и др. ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків : ХНУРЕ, 2019. – 216 с.

ДОДАТКОВА

1. НД ТЗІ 1.5-001-2000. Радіовиявлювачі. Класифікація. Загальні технічні вимоги.

2. НД ТЗІ 2.3-001-2001. Радіовиявлювачі вимірювальні.

3. НД ТЗІ 2.3-005-2001. Радіовиявлювачі панорамні.

4. НД ТЗІ 2.3-006-2001. Радіовиявлювачі аналізу вальні.

5. Нелінійний локатор MS-888. Керівництво по експлуатації.

6. SMV-11, SMV-8. Керівництво по експлуатації.

7. Бумеранг-2Г. Керівництво по експлуатації.

8. ST 031 Піранья. Керівництво по експлуатації.

9. Ореол-А. Керівництво по експлуатації.

Інформаційні ресурси

1. https://cip.gov.ua/ua – сайт Державної служби спеціального зв’язку та захисту інформації.

2. https://tzi.ua/ua/index.html – сайт Технічний захист інформації.

3. https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/ – Комплексні системи захисту інформації /[Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Синюгін]

4. Гребенніков Вадим. Комплексні системи захисту інформації. Проектування, впровадження, супровід. https://books.google.com.ua/books?id=GcBlDwAAQBAJ&printsec =frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

5. https://cert.gov.ua/ – сайт Computer Emergency Response Team of Ukraine.

4. **Форма підсумкового контролю успішності навчання:**

залік по закінченні вивчення дисципліни.

5. Засоби діагностики успішності навчання:

Відповіді на практичних заняттях, виконання та захист комплексного завдання.