ЗАТВЕРДЖЕНО
Вченою радою факультету
інформаційно-комп'ютерних технологій
31 серпня 2023 р., протокол № 5
Голова Вченої ради
Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ОК 27 «СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності 125 «Кібербезпека та захист інформації»
освітньо-професійна програма «Кібербезпека та захист інформаційя»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

Схвалено на засіданні
кафедри комп'ютерної інженерії та кібербезпеки
28 серпня 2023 р., протокол № 7
Завідувач кафедри
Андрій ЄФІМЕНКО
Гарант освітньо-
професійної програми
Андрій ЄФІМЕНКО

Розробник: кандидат технічних наук, доцент, доцент кафедри комп'ютерної інженерії та кібербезпеки Котенко Володимир Миколайович

Житомир
2026-2027 н.р.

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітній ступінь	Характеристика навчальної дисципліни
		денна форма навчання
Кількість кредитів – 4	Галузь знань: 12 «Інформаційні технології»	Нормативна
Модулів – 1	Спеціальність: 125 «Кібербезпека та захист інформації»	Рік підготовки:
Змістових модулів – 2		4-й
Загальна кількість годин - 120		Семестр
		7-й
		Лекції
Тижневих годин для денної форми навчання: аудиторних – 4 самостійної роботи студента – 3,5	Освітній ступінь «бакалавр»	32 год.
		Практичні, семінарські
		—
		Лабораторні
		32 год.
		Самостійна робота
		56 год.
		Вид контролю: екзамен

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 53 % аудиторних занять, 47 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є формування теоретичних знань та практичних навичок дослідження технологій передачі та обробки інформації в інформаційно-комунікаційних системах з метою виявлення можливих каналів несанкціонованого отримання інформації, вивчення причин і джерел виникнення технічних каналів просочування інформації, методів і способів несанкціонованого доступу до інформації і її руйнування, методів і технічних засобів захисту інформації, принципів побудови і експлуатації технічних засобів виявлення і захисту каналів передачі інформації.

Завданнями вивчення дисципліни є:

засвоєння фізичних основ утворення причин і джерел технічних каналів просочування інформації та проведення їх аналізу;

оволодіння методами і засобами несанкціонованого отримання інформації по технічним каналам, методами і засобами руйнування інформації;

оволодіння технічними методами і засобами пошуку та усунення каналів витоків інформації, забезпечення захисту інформації;

оволодіння технічними засобами пошуку та заглушення каналів несанкціонованого витоку інформації.

Зміст навчальної дисципліни направлений на формування наступних **компетентностей**, визначених стандартом вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації»:

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 5. Здатність до пошуку, оброблення та аналізу інформації.

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів навчання** за спеціальністю 125 «Кібербезпека та захист інформації»:

РН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

РН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

РН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

РН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

РН 21. 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.

РН 36. Виявляти небезпечні сигнали технічних засобів.

РН 37. 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.

РН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

РН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

3. Програма навчальної дисципліни

Змістовий модуль 1. Технічні канали витоку інформації. Комплекси технічного захисту інформації

Тема 1. Введення в дисципліну. Загальна характеристика методів розвідки. Канали поширення інформації та способи несанкціонованого доступу до інформації

Предмет і завдання навчальної дисципліни. Канали поширення інформації та способи несанкціонованого доступу до інформації. Система захисту інформації. Технічні канали просочування інформації.

Тема 2. Шляхи формування технічних каналів витоку інформації та система захисту інформації

Шляхи формування технічних каналів витоку інформації. Система захисту інформації.

Тема 3. Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності

Основні поняття та визначення. Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності.

Тема 4. Випробування та атестація комплексів технічного захисту інформації на об'єктах інформаційної діяльності

Випробування комплексів ТЗІ. Атестація комплексів ТЗІ.

Тема 5. Канали побічних електромагнітних випромінювань. Канали побічних електромагнітних випромінювань основних технічних засобів та допоміжних технічних засобів та систем

Засоби передачі електричних сигналів. Види провідних електричних ліній зв'язку. Параметри ліній зв'язку. Електромагнітні випромінювання елементів технічних засобів передачі інформації. Електромагнітні випромінювання персональних комп'ютерів.

Тема 6. Канали побічних електромагнітних наведень. Канали просочування інформації по ланцюгах заземлення та живлення

Наведення електромагнітних випромінювань технічних засобів передачі інформації. Просочування інформаційних сигналів в ланцюгах електроживлення. Паразитні зв'язки через ланцюги живлення. Просочування інформаційних сигналів в ланцюги заземлення.

Тема 7. Канал витоку інформації через закладні пристрої

Апаратні закладки. Способи установки. Акустичні закладки. Електромагнітні закладки

Тема 8. Акустичні та віброакустичні канали витоку інформації

Основні визначення акустики. Джерела утворення акустичних каналів. Заходові методи. Беззаходові методи. Фізичні перетворювачі.

Змістовий модуль 2. Методи та засоби виявлення і захисту інформації

Тема 9. Вимоги до обладнання території та приміщень щодо захисту інформації. Екранування приміщень

Вимоги до обладнання території та приміщень. Екранування приміщень. Конструктивні особливості приміщень.

Тема 10. Детектори поля. Багатофункціональний пошуковий прилад ST 032

Детектори поля. Загальні відомості. Конструктивні особливості приладів. Схемні рішення. Технічні характеристики. Багатофункціональний пошуковий прилад ST-032. Загальна характеристика приладу. Канали виявлення прибору. Технічні характеристики

Тема 11. Скануючі приймачі. Сканери безпровідних відеокамер . Нелінійні локатори. Активні засоби захисту інформації

Скануючий приймач AR8200 Mk3. Цифровий генератор шуму DNGD2300. Сканер безпровідних відеокамер C-Hunter 935. Нелінійні локатори.

Тема 12. Пошуковий комплекс DigiScan EX

Програмне забезпечення управління перестройкою РПП – Digi Scan EX 2.0. Склад комплекту ПАК DigiScan EX.

Тема 13. Системи охоронної та тривожно-викликної сигналізації

Принцип побудови систем. Засоби виявлення для приміщень та території. Засоби збору та обробки інформації.

Тема 14. Застосування технічних засобів відео спостереження для контроля території

Принципи побудови систем. Телевізійні камери. Пристрої для оснащення телевізійних камер. Реєстратори.

Тема 15. Системи контроля і управління доступом

Принцип побудови систем. Периферійне обладнання і носії інформації систем контролю доступу. Засоби ідентифікації і аутентифікації.

Тема 16. Системи пожежно-охоронної сигналізації

Принцип побудови систем. Засоби виявлення. Засоби збору та обробки інформації.

4. Структура (тематичний план) навчальної дисципліни

Змістовні модулі	Кількість годин			
	Всього	Лекції	Лабораторні	Самостійна робота
2	3	4	5	6
Модуль 1				
Змістовий модуль 1. Технічні канали витоку інформації. Комплекси технічного захисту інформації				
Тема 1. Введення в дисципліну. Загальна характеристика методів розвідки. Канали поширення інформації та способи несанкціонованого доступу до інформації	8	2	2	4
Тема 2. Шляхи формування технічних каналів витоку інформації та система захисту інформації	6	2	2	2
Тема 3. Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності	8	2	2	4
Тема 4. Випробування та атестація комплексів технічного захисту інформації на об'єктах інформаційної діяльності	6	2	2	2
Тема 5. Канали побічних електромагнітних випромінювань. Канали побічних електромагнітних випромінювань основних технічних засобів та допоміжних технічних засобів та систем.	8	2	2	4
Тема 6. Канали побічних електромагнітних наведень. Канали просочування інформації по ланцюгах заземлення та живлення	8	2	2	4
Тема 7. Канал витоку інформації через закладні пристрої	8	2	2	4
Тема 8. Акустичні та віброакустичні канали витоку інформації	8	2	2	4
Разом змістовий модуль 1	**60**	**16**	**16**	**28**
Змістовий модуль 2. Методи та засоби виявлення і захисту інформації				
Тема 9. Вимоги до обладнання території та приміщень щодо захисту інформації. Екранування приміщень	8	2	2	4
Тема 10. Детектори поля. Багатофункціональний пошуковий прилад ST 032	6	2	2	2
Тема 11. Скануючі приймачі. Сканери безпровідних відеокамер. Нелінійні локатори. Активні засоби захисту інформації	8	2	2	4
Тема 12. Пошуковий комплекс DigiScan EX	6	2	2	2
Тема 13. Системи охоронної та тривожно-викликної сигналізації	8	2	2	4
Тема 14. Застосування технічних засобів відео спостереження для контроля території	8	2	2	4
Тема 15. Системи контроля і управління доступом	8	2	2	4
Тема 16. Системи пожежно-охоронної сигналізації	8	2	2	4
Разом змістовий модуль 2	**60**	**16**	**16**	**28**
ВСЬОГО	**120**	**32**	**32**	**56**

5. Теми лабораторних занять

№	Назва теми	Кількість годин
1.	Дослідження ослаблення радіохвиль на шляху розповсюдження у приміських зонах і в сільській місцевості	4
2.	Дослідження ослаблення радіохвиль на шляху розповсюдження у міських умовах	4
3.	Розрахунок електромагнітної доступності до джерела радіовипромінювань	4
4.	Дослідження ефективності екранування приміщень	2
5.	Дослідження параметрів небезпечного сигналу при попаданні в систему заземлення	2
6.	Дослідження ймовірності послівного розпізнавання мовної інформації в залежності від спектрального рівня шуму в октавних смугах	2
7.	Дослідження ймовірності послівного розпізнавання мовної інформації в залежності від спектрального рівня шуму в рівноартикуляційних смугах	2
8.	Дослідження ймовірності виявлення порушника при проникненні на об’єкт охорони	2
9.	Дослідження ймовірність виявлення порушника при комбінації засобів виявлення	2
10.	Дослідження параметрів оптичних інфрачервоних засобів випромінювання	4
11.	Дослідження технічних характеристик засобів відеоспостереження	4
РАЗОМ		**32**

6. Завдання для самостійної роботи

Тема 1 Тема 1. Введення в дисципліну. Загальна характеристика методів розвідки. Канали поширення інформації та способи несанкціонованого доступу до інформації

1. Опрацювання матеріалу лекції 1. Підготовка до тестування.
2. Аналітичне представлення електромагнітної обстановки.
3. Фізичні перетворювачі.
4. Класифікація візуально-оптичних каналів просочування інформації.

Тема 2. Шляхи формування технічних каналів витоку інформації та система захисту інформації

1. Опрацювання матеріалу лекції 2. Підготовка до тестування.
2. . Механізм виникнення ПЕМВ в засобах цифрової електронної техніки.
3. Оцінка рівня ПЕМВ **.**
4. Методи і засоби віддаленого отримання інформації:

Тема 3. Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності

1. Опрацювання матеріалу лекції 3. Підготовка до тестування.
2. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.
3. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

Тема 4. Випробування та атестація комплексів технічного захисту інформації на об'єктах інформаційної діяльності

1. Опрацювання матеріалу лекції 4. Підготовка до тестування.
2. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.
3. НД ТЗІ 2.1-002-07 Захист інформації на об'єктах інформаційної діяльності.

Тема 5. Канали побічних електромагнітних випромінювань. Канали побічних електромагнітних випромінювань основних технічних засобів та допоміжних технічних засобів та систем.

1. Опрацювання матеріалу лекції 5. Підготовка до тестування.
2. Електромагнітні випромінювання на частотах самозбудження ПНЧ ТЗПІ.
3. Інформативність ПЕМВ персональних комп'ютерів.

Тема 6. Канали побічних електромагнітних наведень. Канали просочування інформації по ланцюгах заземлення та живлення

1. Опрацювання матеріалу лекції 6. Підготовка до тестування.
2. Зняття інформації по електричним каналам витоку інформації.
3. Параметричний канал витоку інформації.

Тема 7. Канал витоку інформації через закладні пристрої

1. Опрацювання матеріалу лекції 7. Підготовка до тестування.
2. Мікрофонні радіозакладки.
3. Телефонні закладки.
4. Методи пошуку радіозакладних пристроїв.

Тема 8. Акустичні та віброакустичні канали витоку інформації

1. Опрацювання матеріалу лекції 8. Підготовка до тестування.
2. Лазерні мікрофони.
3. Спрямовані мікрофони.
4. Електронні стетоскопи.

Тема 9. Вимоги до обладнання території та приміщень щодо захисту інформації. Екранування приміщень.

1. Опрацювання матеріалу лекції 9. Підготовка до тестування.
2. Параметри звукоізоляції деяких видів віконних та дверних отворів.
3. Захист від НСВ по комунікаційних каналах .

Тема 10. Детектори поля. Багатофункціональний пошуковий прилад ST 032

1. Опрацювання матеріалу лекцій 10. Підготовка до тестування.
2. Методика пошуку радіовипромінювань з допомогою детекторів поля.

Тема 11. Скануючі приймачі. Сканери безпровідних відеокамер . Нелінійні локатори. Активні засоби захисту інформації

1. Опрацювання матеріалу лекції 11. Підготовка до тестування.
2. Методика пошуку радіовипромінювань з допомогою скануючих радіоприймачів.
3. Методика пошуку відеокамер та скритих засобів несанкціонованого зняття інформації.

Тема 12. Пошуковий комплекс DigiScan EX

1. Опрацювання матеріалу лекцій 12. Підготовка до тестування.
2. Методика застосування пошукової системи ***DigiScan EX.***
3. Методика сканування баз даних.

Тема 13. Системи охоронної та тривожно-викликної сигналізації

1. Опрацювання матеріалу лекції 13. Підготовка до тестування.
2. Принцип побудови датчиків охоронної системи Orion NOVA II
3. Принцип побудови системи збору і передачі інформації охоронної системи Orion NOVA II

Тема 14. Застосування технічних засобів відео спостереження для контроля території

1. Опрацювання матеріалу лекції 14. Підготовка до тестування.
2. Бездротові системи відеоспостереження, організація передачі інформації.
3. Побудова мереж IP-відеоспостереження.

Тема 15. Системи контроля і управління доступом

1. Опрацювання матеріалу лекції 15. Підготовка до тестування.
2. Особливості організації розподілених СКУД.
3. Побудова мереж СКУД.

Тема 16. Системи пожежно-охоронної сигналізації

1. Опрацювання матеріалу лекції 16. Підготовка до тестування.
2. Принцип побудови датчиків пожежної системи Tiras PRIME A

3. Принцип побудови системи збору і передачі інформації пожежної системи Tiras PRIME A

7. Індивідуальні завдання

1. Концепція технічного захисту інформації в Україні, затвердженої постановою Кабінету Міністрів України від 08.10.97 р., № 1126
2. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 р. №1229.
3. Сигнал і його опис. Сигнали та перешкоди.
4. Джерела утворення акустичних каналів витоку інформації.
5. Визначення послівної розбірливості мови з відповідним інтегральним рівнем при її прослуховуванні в умовах «мовноподібного» шуму і проходженні мовного сигналу через середовище з рівномірною амплітудно-частотною характеристикою.
6. Розрахунок послівної розбірливості при представленні спектру мовного сигналу 20-рівноартикуляційними смугами та октавними смугами.
7. Класифікація електричних каналів просочування інформації.
8. Методи і засоби несанкціонованого отримання інформації з автоматизованих систем
9. Методи і засоби несанкціонованого прослуховування
10. Методи і засоби руйнування інформації
11. Технічні засоби захисту території і об'єктів.
12. Захист ліній зв'язку. Методи і засоби захисту телефонних ліній. Методи контролю дротяних ліній
13. Багатофункціональний пошуковий прилад ST 032
14. Сканер безпровідних відеокамер C-Hunter 935
15. Нелінійний локатор Лорнет
16. Радіоприймач AR8200
17. Детектор поля PROTECT 1203.

8. Методи навчання

1. Словесні.
2. Наочні.
3. Практичні.
4. Робота з книгою.
5. Відео-метод.
6. Створення ситуацій зацікавленості та новизни.

При цьому здійснення навчально-пізнавальної діяльності проводиться у формі пояснення, роз’яснення, розповіді, лекцій, ілюстрацій, демонстрацій та лабораторних досліджень.

9. Методи контролю

1. Експрес-опитування на лекціях; контрольна робота.
2. Конспект самостійно опрацьованих питань.
3. Тестування на лабораторних заняттях.
4. Тестування на заліку та екзамені, екзаменаційні білети.

10. Розподіл балів

Поточне тестування та самостійна робота																Сума
ЗМ 1								ЗМ 2								
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	Т11	Т12	Т13	Т14	Т15	Т16	100
5	7	6	6	7	6	6	6	6	6	6	6	6	7	7	7	

Шкала оцінювання

За шкалою	Екзамен	Залік	Бали
A	Відмінно	Зараховано	90-100
B	Добре	Зараховано	82-89
C			74-81
D	Задовільно	Зараховано	64-73
E			60-63
FX	Незадовільно	Не зараховано	35-59
F		Не зараховано	0-34

11. Рекомендована література

Основна література

1. Закон України «Про інформацію».
2. Закон України «Про державну таємницю».
3. Барило Г.І., Вісьтак М.В., Готра З.Ю., Лесінський В.В., Політанський Л.Ф. Електронні елементи та пристрої систем безпеки й охорони: Навчальний посібник .- За ред. Готри З.Ю. – Чернівці: Рута, 2017. – 216 с.
4. Даутов А. Л. Внедрение и развитие систем контроля и управления доступом на предприятии / А. Л. Даутов, А. С. Пуряев // Инновационная наука. — 2016. — №. 5–1 (17).
5. Волхонский В. В. Системы контроля и управления доступом / В. В. Волхонский. — СПб. : Университет ИТМО. — 2015.

6. Поповський В.В., Персіков А.В. Захист інформації в телекомунікаційних системах. Том 1, Том 2.-Харків 2008.

7. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техниче-скими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

8. В.О.Хорошко, О.Д. Азаров, Г.О.Максименко, Ю.Є.Яремчук. Пошук та локалізація радіозакладних пристроїв. Навчальний посібник.-Вінниця: ВНТУ, 2007.-333 с.

9. Поисковое программное обеспечение DigiScan EX. Для приемников AOR, ICOM. Версия 1.1 (15.01.03). Техническое описание.

10. Сканирующий приемник AR8200. Инструкция по эксплуатации.

11. Краткая инструкция управления прибором ST032 Ver.1.0.

Допоміжна література

1. Болдырев А.И., Василевский И.В., Сталенков С.Е. Методические рекомендации по поиску и нейтрализации средств негласного съема информации. Практическое пособие. — М.: НЕЛК, 2001. — 138 с.

2. Бузов Г.А.., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие.-М.: Горячая линия-Телеком, 2005.-416 с.

3. Куприянов А.И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений/ А.И.Куприянов, А.В. Сахаров, В.А. Шевцов.-М.: Издательский центр ”Академия”, 2006.-256 с.

4. Инженерно-техническая защита информации: учеб. пособие для студентов, обучающихся по специальностям в обл. информ. безопасности/ А.А. Торокин.-М.: Гелиос АРВ, 2005.-960 с.

5. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. - М.: Логос; ПБОЮЛ Н.А. Егоров, 2001. - 264 с : ил.

6. Положення про технічний захист інформації в Україні УП №1229/99 від 27.09.99.

7. Концепція технічного захисту інформації в Україні, затверджена постановою Кабінету Міністрів України від 08.10.97 р., № 1126.

8. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 р. №1229.

9. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22.

10. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

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

12. 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.

13. НБУ № 243 04.07.07 Правила з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи.

12. Інформаційні ресурси в Інтернеті

1. http://www.DAS
2. https://cip.gov.ua/ua
3. https://data.gov.ua/dataset/1f3e38a5-ca00-4fa9-be1a-810a206ed1fe
4. https://algorytmx.com.ua/products-and-solutions/certification
5. https://cip.gov.ua/ua/news/zasobi-tzi-yaki-mayut-ekspertnii-visnovok-pro-vidpovidnist-do-vimog-tekhnichnogo-zakhistu-informaciyi
6. https://zakon.rada.gov.ua/go/z0640-01
7. https://ips.ligazakon.net/document/REG3698
8. https://iit.com.ua/
9. http://ca.mil.gov.ua/normative-documentation
10. https://tzi.ua/ua/organzacjn_metodi_zahistu_nformac.html