МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

Кафедра кібербезпеки та DATA – технологій факультету № 6

РОБОЧА ПРОГРАМА

навчальної дисципліни "Методи та засоби захисту інформації"
вибіркових компонент
освітньої програми першого рівня вищої освіти
125 "Кібербезпека" (Безпека інформаційних та комунікаційних систем)

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30.08.2023 № 7

СХВАЛЕНО
Вченою радою факультету № 6
Протокол від 25.08.2023 № 7

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 29.08.2023 № 7

Розглянуто на засіданні кафедри кібербезпеки та DATA-технологій факультету № 6 *(протокол від 15.08.2023 № 8)*

Розробник: доцент кафедри кібербезпеки та DATA – технологій факультету № 6 Харківського національного університету внутрішніх справ, к.т.н. доцент Тулупов В.В.

Рецензенти:
професор кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ, к.т.н. доцент Носов В.В.

завідувач кафедри проектування та експлуатації електронних апаратів Харківського національного університету радіоелектроніки, к.т.н. доцент Хорошайло Ю.Є.

1. Опис навчальної дисципліни

<table>
<tr><th>Найменування показників</th><th>Шифри та назви галузі знань,
код та назва спеціальності,
ступінь вищої освіти</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><td>Кількість кредитів ECTS – 6
Загальна кількість годин – 180
Кількість тем – 12
Індивідуальні завдання:
Реферат-1</td><td>12 Інформаційні технології
(шифр та назва галузі знань)
125 Кібербезпека
(шифр,спеціальність)
бакалавр
(назва СВО)</td><td>Цикл вибіркових дисциплін.
Навчальний курс- 3
Семестр - 5
Види контролю:
Підсумковий контроль - екзамен</td></tr>
<tr><td colspan="3">Розподіл навчальної дисципліни за видами занять</td></tr>
<tr><td>денна форма навчання

Лекції – 30 год;
Практичні заняття – 28 год;
Лабораторні заняття – 32 год;
Самостійна робота – 90 год;</td><td colspan="2">заочна форма навчання

Лекції – 12 год;
Практичні заняття – 8 год;
Лабораторні заняття – 8 год;
Самостійна робота – 152 год;</td></tr>
</table>

2. Мета та завдання навчальної дисципліни

Метою дисципліни «Методи та засоби захисту інформації» є отримання студентами необхідних знань щодо застосування заходів та засобів, спрямованих на технічний захист інформації (ТЗІ) на об'єктах технічних засобів обробки, передачі, зберігання та відображення інформації (ТЗПІ).

Дисципліна спрямована на вивчення:

- фізичних явищ, притаманних технічним каналам витоку інформації (ТКВІ) на об'єктах ТЗПІ;
- принципів дії засобів захисту інформації, їх основних характеристик та можливостей.

Основними завданнями вивчення дисципліни «Методи та засоби захисту інформації» є: узагальнення передового досвіду роботи фахівців з організації захисту інформації щодо стандартизації, уніфікації методів, способів, засобів і заходів забезпечення безпеки інформаційної сфери суспільства.

Міждисциплінарні зв'язки: математика, фізика, фізичні методи перетворення сигналів, теорія інформації та кодування, правові засади захисту інформації, управління та організація в сфері інформаційної безпеки.

Очікуванні результати навчання: у результаті вивчення навчальної дисципліни здобувач вищої освіти повинен:

знати:

основні положення та терміни, що стосуються галузі інформаційної безпеки; зміст і вимоги окремих нормативних документів технічного захисту інформації; класифікацію технічних каналів витоку інформації та методи та засоби запобігання їх виникнення; види технічних розвідок та засобів, що вони використовують; методи та способи захисту інформації; класифікацію технічних засобів захисту інформації, їхні можливості та основні характеристики; типові заходи та засоби ТЗІ; можливі ТКВІ на об'єктах ТЗПІ; порядок розробки та реалізації заходів ТЗІ на об'єктах ТЗПІ.

вміти:

на основі аналізу реальної обстановки розробити моделі загроз інформації; ефективно застосовувати технічні засоби захисту у різних ситуаціях; визначати сукупність усіх можливих методів технічної розвідки для визначеної ситуативної моделі об'єкта захисту; оцінювати можливості різноманітних технічних засобів розвідки; визначати сукупність усіх можливих методів захисту інформації для визначеної ситуативної моделі об'єкта захисту; ефективно використовувати методи захисту інформації; оцінювати можливості різноманітних технічних засобів захисту інформації; ефективно використовувати технічні засоби захисту інформації; проводити аналіз можливих ТКВІ; розробляти пропозиції з ТЗІ на об'єктах ТЗПІ.

Програмні компетентності, які формуються при вивченні навчальної дисципліни:	
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується

	комплексністю та неповною визначеністю умов.
Загальні компетентності (ЗК)	ЗК 1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Знання та розуміння предметної області та розуміння професії. ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.
Фахові компетентності (ФК)	ФК 1. Здатність застосовувати нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. ФК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. ФК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. ФК 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах, з метою реалізації встановленої політики інформаційної та/або кібербезпеки. ФК 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. ФК 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

3. Програма навчальної дисципліни

ТЕМА № 1. Цілі, задачі та організація технічної розвідки

Виникнення, історичне становлення й розвиток технічної розвідки, радіоелектронної боротьби, інформаційної війни, інформаційного тероризму: технічна розвідка, радіоелектронна боротьба, інформаційна війна, інформаційний тероризм. Види та характеристика радіоелектронної розвідки та її складових: радіорозвідка, радіотехнічна розвідка, радіолокаційна розвідка, комп'ютерна розвідка, радіотепловізорна розвідка. Оптико-електронна розвідка. Акустична розвідка.

ТЕМА № 2. Концепція інженерно-технічного захисту інформації

Основні положення концепції інженерно-технічного захисту інформації. Системний підхід до інженерно-технічного захисту інформації: основні положення системного підходу до інженерно-технічного захисту інформації, цілі, завдання та ресурси системи захисту інформації, загрози безпеки інформації й заходи для їхнього запобігання.

ТЕМА № 3. Характеристика захищеної інформації

Захист інформації як інтегральна проблема та шляхи її вирішення. Умови безпеки інформації. Державна політика і система ТЗІ в Україні. Нормативно-правова база України в сфері ТЗІ. Структура системи захисту інформації.

Поняття та характеристика захищеної інформації. Види інформації, що захищається. Види загроз безпеки інформації. Джерела загроз безпеки інформації. Джерела загроз безпеки інформації. Небезпечні сигнали і їх джерела.

ТЕМА № 4. Електромагнітні випромінювання та наведення

Побічні електромагнітні випромінювання та наведення. Побічні перетворення акустичних сигналів в електричні сигнали. Низькочастотні і високочастотні випромінювання технічних засобів. Електромагнітні випромінювання розподілених джерел. Витік інформації по ланцюгах електроживлення. Витік інформації по цілях заземлення.

ТЕМА № 5. Типова структура та види технічних каналів витоку інформації (ТКВІ).

Загальна характеристика технічного каналу витоку інформації. Класифікація та характеристика технічних каналів витоку інформації, що обробляється ТЗПІ. Особливості витоку інформації технічними каналами. Типова структура та види технічних каналів витоку інформації.

ТЕМА № 6. Технічні канали витоку акустичної інформації

Загальна характеристика акустичного каналу витоку інформації. Основна класифікаційна ознака технічних каналів витоку інформації. Класифікація акустичних закладних пристроїв: особливості технічних характеристик радіоакустичних закладних пристроїв, ознакова структура радіоакустичних закладних пристроїв. Радіомоніторинг у структурі загальних методів захисту акустичної інформації: основна мета радіомоніторингу при захисті акустичної інформації, основні вимоги до структури і параметрів засобів радіомоніторингу.

ТЕМА № 7. Технічні канали витоку інформації, що обробляється ТЗПІ.

Технічні канали витоку інформації, що обробляється ТЗПІ і передається каналами зв'язку.Електричні лінії зв'язку. Електромагнітні канали витоку інформації. Електромагнітні випромінювання елементів ТЗПІ. Електромагнітні випромінювання на частотах роботи генераторів ВЧ ТЗПІ і ВТЗС. Електромагнітні випромінювання на частотах самозбудження УНЧ ТЗПІ. Побічні електромагнітні випромінювання персонального комп'ютера.

ТЕМА № 8. Методи та засоби захисту інформації оброблюваної ТЗПІ від витоку технічними каналами.

Екранування засобів ТЗПІ. Властивості та вимоги щодо засобів екранування. Заземлення засобів ТЗПІ. Типові системи заземлення технічних засобів. Особливості та вимоги до засобів фільтрування інформаційних сигналів.

ТЕМА № 9. Методи та засоби технічного захисту інформації від витоку технічними каналами.

Методи та засоби блокування технічних каналів витоку інформації. Основні загальні положення технічного захисту інформації. Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами. Захист інформації від несанкціонованого запису звукозаписувальними пристроями. Захист електронної інформації. Захист письмової інформації від оптичного зняття.

ТЕМА № 10. Методи та засоби технічного захисту акустичної інформації.

Методи та засоби виявлення та блокування технічних каналів витоку акустичної інформації. Захист акустичної інформації від зняття радіозакладними пристроями. Методи пошуку радіозакладних пристроїв.

ТЕМА № 11. Методи пошуку електронних пристроїв перехоплення інформації. Класифікація методів та засобів пошуку електронних пристроїв перехоплення інформації.

Методи пошуку електронних пристроїв з використанням виявлювачів порожнеч, металошукачів і рентгенівських апаратів. Методи пошуку з використанням індикаторів електромагнітного поля, радіо частотомірів та інтерцепторів: інформативні побічні електромагнітні випромінювання; методи пошуку сигналів ПЕМВН; прилади для вимірювання ПЕМВН; вибір детектора; призначення селективного мікровольтметра SMV 8.5.

ТЕМА № 12. Засоби пошуку електронних пристроїв перехоплення інформації Класифікація засобів радіовиявлення. Індикаторні засоби радіомоніторингу. Інтерсептори.

Універсальний прилад виявлення пристроїв прихованого знімання інформації СРМ-700 «Акула». Багатофункційний пошуковий прилад ST-031 «Піранья». Вимірювальні засоби радіомоніторингу. Селективні мікровольтметри і

нановольтметри. Панорамні засоби радіомоніторингу. Аналізуючі засоби радіомоніторингу.

4. Структура навчальної дисципліни

4.1.1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни					Література	Вид контролю
	Всього	з них:					
		лекції	Практичні заняття	Лабораторні заняття	Самостійна робота		
Семестр № 5							
ТЕМА № 1. Цілі, задачі та організація технічної розвідки	8	4			4	1-5, 27-31	**екзамен**
ТЕМА № 2. Концепція інженерно-технічного захисту інформації	10	2	4		4	1-5, 27-45	
ТЕМА № 3. Характеристика захищеної інформації	14	2	2		10	1- 8, 12, 13, 27-45	
ТЕМА № 4. Електромагнітні випромінювання та наведення	16	2	2	4	8	1-8, 12, 13, 27-52	
ТЕМА № 5. Типова структура та види технічних каналів витоку інформації (ТКВІ)	14	2	2	2	8	1-8, 12, 13, 27-45	
ТЕМА № 6. Технічні канали витоку акустичної інформації	12	2	2	2	6	1-8, 12, 13, 27-52	
ТЕМА № 7. Технічні канали витоку інформації, що обробляється ТЗПІ	18	4	2	4	8	1-8,12, 13, 27-51	
ТЕМА № 8. Методи та засоби захисту інформації оброблюваної ТЗПІ від витоку технічними каналами	16	2	4	2	8	1-8, 9,12, 13, 27-45	
ТЕМА № 9. Методи та засоби технічного захисту інформації від витоку технічними каналами	12	2	2		8	1-8, 12, 13, 27-51	
ТЕМА № 10. Методи та засоби технічного захисту акустичної інформації	16	2	2	4	8	1-5, 7, 8, 12, 13,	
ТЕМА № 11. Методи пошуку електронних пристроїв перехоплення інформації. Класифікація методів та засобів пошуку	18	4	2	4	8	1-5, 7, 8, 12, 13, 16,18,27-	

електронних пристроїв перехоплення інформації.						56	
ТЕМА № 12. Засоби пошуку електронних пристроїв перехоплення інформації. Класифікація засобів радіовиявлення. Індикаторні засоби радіомоніторингу. Інтерсептори.	24	4	4	8	8	1-8, 12-15, 16,18,27-56	
Всього за семестр :	**180**	**30**	**28**	**32**	**90**		

4.1.2. Розподіл часу навчальної дисципліни за темами (заочна форма навчання)

Номер та назва навчальної теми	**Кількість годин, відведених на вивчення навчальної дисципліни**					**Література**	**Вид контролю**
	Всього	**з них:**					
		лекції	**Практичні заняття**	**Лабораторні заняття**	**Самостійна робота**		
Семестр № 5							
ТЕМА № 1. Цілі, задачі та організація технічної розвідки	12				12	1-5, 27-31	
ТЕМА № 2. Концепція інженерно-технічного захисту інформації	12				12	1-5, 27-45	
ТЕМА № 3. Характеристика захищеної інформації	12				12	1- 8, 12, 13, 27-45	
ТЕМА № 4. Електромагнітні випромінювання та наведення	12				12	1-8, 12, 13, 27-52	
ТЕМА № 5. Типова структура та види технічних каналів витоку інформації (ТКВІ)	**20**	**2**	**2**	**2**	**14**	1-8, 12, 13, 27-45	
ТЕМА № 6. Технічні канали витоку акустичної інформації	12				12	1-8, 12, 13, 27-52	
ТЕМА № 7. Технічні канали витоку інформації, що обробляється ТЗПІ	12				12	1-8,12, 13, 27-51	
ТЕМА № 8. Методи та засоби захисту інформації оброблюваної ТЗПІ від витоку технічними каналами	**22**	**4**	**2**	**2**	**14**	1-8, 9,12, 13, 27-45	
ТЕМА № 9. Методи та засоби технічного захисту інформації від витоку технічними каналами.	12				12	1-8, 12, 13, 27-51	**екзамен**
ТЕМА № 10. Методи та засоби технічного захисту акустичної	**20**	**2**	**2**	**2**	**14**	1-5,7, 8, 12, 13,	

інформації							
ТЕМА № 11. Методи пошуку електронних пристроїв перехоплення інформації. Класифікація методів та засобів пошуку електронних пристроїв перехоплення інформації.	**22**	**4**	**2**	**2**	**14**	1-5, 7, 8, 12, 13, 16,18,27-56	
ТЕМА № 12. Засоби пошуку електронних пристроїв перехоплення інформації. Класифікація засобів радіовиявлення. Індикаторні засоби радіомоніторингу. Інтерсептори.	12				12	1-8, 12-15, 16,18,27-56	
Всього за семестр :	**180**	**12**	**8**	**8**	**152**		

4.1.3. Питання, що виносяться на самостійне опрацювання

Завдання що виносяться на самостійну роботу студента	Літера-тура:
Семестр № 5	
Тема № 1. Цілі, задачі та організація технічної розвідки. Відпрацювати лекцію №1. Види та характеристика радіоелектронної розвідки та її складових.	1-5,27-31
Тема № 2. Концепція інженерно-технічного захисту інформації. Відпрацювати лекцію №2. Системний підхід до інженерно-технічного захисту інформації. Основні положення концепції інженерно-технічного захисту інформації.	1-5,7-45
Тема № 3. Характеристика захищеної інформації. Відпрацювати лекцію № 3. Характеристика джерел загроз безпеки інформації.	1- 8,12,13, 27-45
Тема №4. Електромагнітні випромінювання та наведення. Відпрацювати лекцію № 4. Низькочастотні та високочастотні випромінювання технічних засобів.	1-8,12,13, 27-52
Тема № 5. Типова структура та види технічних каналів витоку інформації (ТКВІ). Відпрацювати лекцію № 5. Дослідження побічних електромагнітних випромінювань та наведень ПЕМВН у діапазоні частот 30 – 1000 МГц із використанням селективного мікровольтметру SMV 8.5.(1)	1-8, 12,13, 27-45
Тема № 6. Технічні канали витоку акустичної інформації. Відпрацювати лекцію № 6. Загальна характеристика речового каналу витоку інформації. Дослідження побічних електромагнітних випромінювань та наведень ПЕМВН у діапазоні частот 30 – 1000 МГц із використанням селективного мікровольтметру SMV 8.5.(2). Захист інформації від витоку з акустично-оптичного каналу.	1-8,12,13, 27-52
Тема №7. Технічні канали витоку інформації, що обробляється ТЗПІ.	1-8,12,13,

Технічні канали витоку інформації, що обробляються ТЗПІ. Відпрацювати лекцію № 7. Побічні електромагнітні випромінювання персонального комп'ютера. Дослідження відеокамери на базі ПЗЗ - матриць та відикону. Захист мовної інформації від витоку з акустичного каналу методом енергетичного приховування.	27-51
Тема № 8. Методи та засоби захисту інформації оброблюваної ТЗПІ від витоку технічними каналами. Відпрацювати лекцію № 8. Технічні канали витоку інформації, що обробляється ТЗПІ і передається каналами зв'язку. Електричні лінії зв'язку. Електромагнітні канали витоку інформації. Електромагнітні випромінювання елементів ТЗПІ. Електромагнітні випромінювання на частотах роботи генераторів ВЧ ТЗПІ і ВТЗС. Електромагнітні випромінювання на частотах самозбудження УНЧ ТЗПІ. Побічні електромагнітні випромінювання персонального комп'ютера.	1-8, 9,12, 13, 27-45
Тема № 9. Методи та засоби технічного захисту інформації від витоку технічними каналами. Відпрацювати лекцію № 9. Методи та засоби блокування технічних каналів витоку інформації. Основні загальні положення технічного захисту інформації. Захист інформації від витоку по технічних каналах, утворених допоміжними технічними засобами. Захист інформації від несанкціонованого запису звукозаписувальними пристроями. Захист електронної інформації. Захист письмової інформації від оптичного зняття.	1-8,12,13, 27-51
Тема № 10. Методи та засоби технічного захисту акустичної інформації. Відпрацювати лекцію № 10. Методи та засоби технічного захисту акустичної інформації. Загальна характеристика речового каналу витоку інформації.	1-5, 7, 8, 12, 13,
Тема № 11. Методи пошуку електронних пристроїв перехоплення інформації. Відпрацювати лекцію № 11. Класифікація методів та засобів пошуку електронних пристроїв перехоплення інформації. Методи пошуку електронних пристроїв з використанням виявлювачів поражнечь, металошукачів і рентгенівських апаратів. Методи пошуку з використанням індикаторів електромагнітного поля, радіо частотомірів та інтерцепторів: інформативні побічні електромагнітні випромінювання.	1-5, 7, 8, 12,13, 16,18,27-56
Тема № 12. Засоби пошуку електронних пристроїв перехоплення інформації. Відпрацювати лекцію № 12. Методи пошуку сигналів ПЕМВН. Закінчити рішення задач практичного заняття. Прилади для вимірювання ПЕМВН. Вибір детектора. призначення селективного мікровольтметру SMV 8.5.	1-8, 12-15, 16,18,27-56

5. Індивідуальні навчально-дослідні завдання

5.1.1. Теми рефератів

1. Нормативна база забезпечення безпеки інформації в інформаційно-телекомунікаційних мережах.
2. Дослідження властивостей побічного електромагнітного випромінювання та оцінка ефективності захисту інформації.
3. Методи просторової обробки сигналів для захисту інформації в радіоелектронних засобах.
4. Проблеми розробки універсальних засобів захисту інформації.
5. Технічні засоби захисту мовної інформації в приміщеннях та каналах зв'язку.
6. Методи захисту акустичної інформації від витоку по технічних каналах.
7. Класифікація засобів виявлення, локалізації і нейтралізації закладних пристроїв.
8. Електромагнітні канали витоку інформації.
6. Електричні канали витоку інформації.
7. Параметричні канали витоку інформації.
8. Повітряні канали витоку акустичної інформації.
9. Вібраційні канали витоку акустичної інформації.
10. Електроакустичні канали витоку акустичної інформації.
11. Оптико-електронний канал витоку акустичної інформації, його характеристика, методи блокування.
12. Пасивні й активні методи і засоби захисту мовної інформації.
13. Звукоізоляція приміщень як метод блокування витоку акустичної інформації.
14. Методи та засоби виявлення та подавлення диктофонів.
15. Методи і засоби захисту телефонних ліній.
16. Методи і засоби пошуку електронних закладних засобів.
17. Методи пошуку закладок з використанням індикаторів поля, інтерсепторів і радіочастотомірів.
18. Методи пошуку закладок з використанням металошукачів.
19. Спеціальні перевірки виділених приміщень.
20. Сертифікація засобів захисту інформації. Основні поняття.

6. Методи навчання

Аудиторні заняття проводяться у формі візуального представлення аналітично-графічного матеріалу дисципліни, на яких студенти повинні виконувати відповідні розумові, обчислювальні та практичні дії.

Самостійна робота за кожною темою передбачає вивчення теоретичних питань лекційних занять, опрацювання завдань практичних занять. Індивідуальна робота передбачає написання рефератів.

7. Перелік питань та завдань, що виносяться на підсумковий контроль

Контроль проводиться по тестових завданнях на підсумковому контролі – екзамену.

1. Охарактеризувати складові інформаційної безпеки.
2. Класифікувати джерела загроз та загрози інформації.

3. Розкрити сутність технічного каналу витоку інформації.
4. Привести загальну класифікацію каналів витоку інформації.
5. Перелічити та охарактеризувати електромагнітні канали витоку інформації.
6. Перелічити та охарактеризувати електричні канали витоку інформації.
7. Пояснити принцип утворювання параметричного каналу витоку інформації.
8. Перелічити та охарактеризувати повітряні канали витоку акустичної інформації.
9. Перелічити та охарактеризувати вібраційні канали витоку акустичної інформації.
10. Перелічити та охарактеризувати електроакустичні канали витоку акустичної інформації.
11. Оптико-електронний канал витоку акустичної інформації, його характеристика, методи блокування.
12. Охарактеризувати індукційний метод перехоплення інформації при її передачі по каналах зв'язку.
13. Класифікація, принцип роботи акустичних закладок.
14. Класифікація, принцип роботи віброакустичних закладок.
15. Класифікація, принцип роботи спрямованих мікрофонів.
16. Класифікація, принцип роботи панорамних скануючих приймачів.
17. Класифікація, принцип роботи аналізаторів спектру та пеленгаторів.
18. Охарактеризувати програмно-апаратні комплекси радіо-, радіотехнічної розвідки.
19. Охарактеризувати методи та засоби отримання інформації з дротяних ліній зв'язку
20. Розкрити фізичні принципи роботи засобів перехоплення факсимільних передач.
21. Охарактеризувати засоби візуальної розвідки.
22. Охарактеризувати системи спостереження за транспортними засобами. Радіомаяки. Радіонавігаційний приймач.
23. Класифікація методів та засобів захисту інформації від витоку технічними каналами.
24. Дайте визначення поняттю технічний канал витоку інформації згідно з ДСТУ.
25. Назвіть можливі види акустичних каналів витоку інформації.
26. Наведіть класифікацію акустичних і радіоакустичних закладних пристроїв.
27. Назвіть види сигналів, що використовуються у сучасних радіоакустичних закладних пристроях з детермінованими та випадковими базами.
28. Яка особливість застосування радіоакустичних закладних пристроїв із сигналами ППРЧ і які існують засоби для їх виявлення?
29. Назвіть сигнальну ознакову структуру радіоакустичних закладних пристроїв.
30. Назвіть ознакову структуру зовнішнього вигляду радіоакустичних закладних пристроїв.
31. Назвіть основні методи захисту акустичної інформації від витоку по технічних каналах.
32. Наведіть класифікацію засобів виявлення, локалізації і нейтралізації закладних пристроїв.
33. Назвіть основні цілі радіомоніторингу при захисті мовної інформації.
34. Назвіть основні вимоги до структури і параметрів засобів радіомоніторингу при захисті мовної інформації.
35. Нарисуйте функціональну схему радіовиявлювача закладних пристроїв, які використовують сигнали ППРЧ.

36. Розкрити зміст організаційних методів захисту інформації від витоку технічними каналами.
37. Розкрити зміст технічних методів захисту інформації від витоку технічними каналами.
38. Охарактеризуйте пасивні методи та засоби захисту інформації.
39. Охарактеризуйте активні методи та засоби захисту інформації.
40. Перелічити активні методи і засоби захисту інформації, що циркулює в ТЗПІ.
41. Розкрити фізичні принципи просторового і лінійного зашумлення.
42. Охарактеризуйте пасивні й активні методи і засоби захисту мовної інформації.
43. Звукоізоляція приміщень як метод блокування витоку акустичної інформації.
44. Охарактеризувати методи та засоби виявлення та подавлення диктофонів.
45. Охарактеризувати методи і засоби захисту телефонних ліній.
46. Охарактеризувати методи і засоби пошуку електронних закладних засобів.
47. Охарактеризувати методи пошуку закладок з використанням індикаторів поля, інтерсепторів і радіочастотомірів.
48. Охарактеризувати методи пошуку закладок з використанням нелінійних локаторів, виявителі порожнеч (поражнечь), металошукачів і рентгенівських апаратів
49. Перелічити засоби пошуку пристроїв перехоплення інформації. Сканерні приймачі й аналізатори спектру.
50. Засоби пошуку пристроїв перехоплення інформації.
51. Програмно-апаратні та спеціальні комплекси контролю сигналів.
52. Охарактеризувати засоби контролю провідних ліній.
53. Охарактеризувати засоби пошуку пристроїв перехоплення інформації, що використовують фізичні властивості навколишнього середовища.
54. Нелінійні локатори. Фізичні принципи роботи.
55. Металошукачі. Фізичні принципи роботи.
56. Виявлювачі порожнеч. Фізичні принципи роботи.
57. Рентгенівські апарати. Фізичні принципи роботи.
58. Перелічити методи пошуку електронних пристроїв перехоплення інформації.
59. Перелічити методи пошуку з застосуванням індикаторів поля, інтерсепторів та радіочастотовимірювачів.
60. Охарактеризувати методи пошуку з застосуванням с використанням сканерних приймачів і програмно-апаратних комплексів контролю.
61. Охарактеризувати методи пошуку електронних пристроїв перехоплення інформації.
62. Охарактеризувати методи контролю телефонних ліній.
63. Охарактеризувати методи пошуку закладок з використанням металошукачів.
64. Як здійснюються спеціальні перевірки виділених приміщень.
65. Перелічити види спеціальних перевірок.
66. Розкрити послідовність перевірок виділених приміщень.
67. Державне ліцензування діяльності в області захисту інформації.
68. Сертифікація засобів захисту інформації. Основні поняття.
69. Атестування об’єктів інформатизації. Основні поняття.
70. Етапи організації робіт із захисту інформації від витоку технічними каналами на об’єктах ТЗПІ.

71. Перелічити основні рекомендації щодо захисту інформації від витоку технічними каналами на об’єктах ТЗПІ при розробці технічного проекту.

8. Критерії та засоби оцінювання результатів навчання здобувачів

Контрольні заходи включають у себе поточний та підсумковий контроль.

Поточний контроль.

До форм поточного контролю належить оцінювання:

- рівня знань під час практичних і лабораторних занять;
- якості виконання індивідуальної та самостійної роботи.

Поточний контроль здійснюється під час проведення практичних та лабораторних занять і має за мету перевірку засвоєння знань, умінь і навичок здобувачем вищої освіти (далі – здобувач) з навчальної дисципліни.

У ході поточного контролю проводиться систематичний вимір приросту знань, їх корекція. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національної системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Оцінки за самостійну та індивідуальну роботи виставляються в журнали обліку роботи академічної групи окремою графою за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Результати цієї роботи враховуються під час виставлення підсумкових оцінок.

При розрахунку успішності здобувачів враховуються такі види робіт: навчальні заняття (практичні, лабораторні тощо); самостійна та індивідуальна роботи (виконання домашніх завдань, ведення конспектів першоджерел та робочих зошитів, виконання розрахункових завдань, підготовка рефератів, наукових робіт, публікацій, розроблення спеціальних технічних пристроїв і приладів, моделей, комп’ютерних програм, виступи на наукових конференціях, семінарах та інше); контрольні роботи (виконання тестів, контрольних робіт у вигляді, передбаченому в робочій програмі навчальної дисципліни). Вони оцінюються за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Здобувач, який отримав оцінку «незадовільно» за навчальні заняття або самостійну роботу, зобов’язаний перескласти її.

Загальна кількість балів (оцінка), отримана здобувачем за семестр перед підсумковим контролем, розраховується як середньоарифметичне значення з оцінок за навчальні заняття та самостійну роботу, та для переводу до 100-бальної системи помножується на коефіцієнт **10**.

Загальна кількість балів (перед підсумковим контролем) **=((** ***Результат навчальних занять за семестр*** **+** ***Результат самостійної роботи за семестр*** **) /** ***2)*** ****10***

Підсумковий контроль. Підсумковий контроль проводиться з метою оцінки результатів навчання на певному ступені вищої освіти або на окремих його завершених етапах.

Для обліку результатів підсумкового контролю використовується поточно-накопичувальна інформація, яка реєструються в журналах обліку роботи академічної

групи. Результати підсумкового контролю з дисциплін відображуються у відомостях обліку успішності, навчальних картках здобувачів, залікових книжках. ***Присутність здобувачів на проведенні підсумкового контролю (заліку, екзамену) обов'язкова.*** Якщо здобувач вищої освіти не з'явився на підсумковий контроль (залік, екзамен), то науково-педагогічний працівник ставить у відомість обліку успішності відмітку «не з'явився».

Підсумковий контроль (екзамен, залік) оцінюється за національною шкалою. Для переводу результатів, набраних на підсумковому контролі, з національної системи оцінювання в 100-бальну вводиться коефіцієнт **10**, таким чином максимальна кількість балів на підсумковому контролі (екзамені, заліку), які використовуються при розрахунку успішності здобувачів, становить **50.**

Підсумкові бали з навчальної дисципліни визначаються як сума балів, отриманих здобувачем протягом семестру, та балів, набраних на підсумковому контролі (екзамені, заліку).

$$\textit{Підсумкові бали навчальної дисципліни} = \textit{Загальна кількість балів (перед підсумковим контролем)} + \textit{Кількість балів за підсумковим контролем}$$

Здобувач вищої освіти, який під час складання підсумкового контролю (екзамен, залік) отримав незадовільну оцінку, складає його повторно. Повторне складання підсумкового екзамену чи заліку допускається не більше двох разів з кожної навчальної дисципліни: один раз – викладачеві, а другий – комісії, до складу якої входить керівник відповідної кафедри та 2-3 науково-педагогічних працівники.

Якщо дисципліна вивчається протягом двох і більше семестрів з семестровим контролем у формі екзамену чи заліку, то результат вивчення дисципліни в поточному семестрі визначається як середньоарифметичне значення балів, набраних у поточному та попередньому семестрах.

$$\textit{Підсумкові бали навчальної дисципліни} = \textit{Підсумкові бали за поточний семестр} + \textit{Підсумкові бали за попередній семестр} : 2$$

У цьому розділі також повинні бути розроблені чіткі критерії оцінювання здобувачів вищої освіти під час поточного контролю *(робота на семінарських, практичних, лабораторних та інших аудиторних заняттях, самостійна робота, виконання індивідуальних творчих завдань)* та підсумкового контролю. Кафедра визначає вимоги до здобувачів стосовно засвоєння змісту навчальної дисципліни, а саме: кількість оцінок, яку він повинен отримати під час аудиторної роботи, самостійної роботи. Наприклад:

Робота під час навчальних занять	**Самостійна та індивідуальна робота**	**Підсумковий контроль**
Отримати не менше 4 позитивних оцінок	Підготувати реферат, підготувати конспект за темою самостійної роботи, розв'язати задачі.	Отримати за підсумковий контроль не

		менше 30 балів

9. Шкала оцінювання: національна та ECTS

Оцінка в балах		Оцінка за національною шкалою	Оцінка за шкалою ECTS	
			Оцінка	Пояснення
12	97-100	Відмінно ("зараховано")	A	**"Відмінно"** – теоретичний зміст курсу освоєний **цілком,** необхідні практичні навички роботи з освоєним матеріалом сформовані, **всі** навчальні завдання, які передбачені програмою навчання **виконані** в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
11	94-96			
10	90-93			
9	85 – 89	Добре ("зараховано")	B	**"Дуже добре"** – теоретичний зміст курсу освоєний **цілком**, необхідні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **всі** навчальні завдання, які передбачені програмою навчання **виконані**, якість виконання **більшості** з них оцінено числом балів, близьким до **максимального,** робота з двома – трьома незначними помилками.
8	80-84			
7	75 – 79		C	**"Добре"** – теоретичний зміст курсу освоєний **цілком**, практичні навички роботи з освоєним матеріалом **в основному** сформовані, **всі** навчальні завдання, які передбачені програмою навчання **виконані**, якість виконання **жодного** з них **не оцінено мінімальним** числом балів, деякі види завдань виконані **з помилками,** робота з декількома незначними помилками, або з однією – двома значними помилками.
6	70 –74	Задовільно ("зараховано")	D	**"Задовільно"** – теоретичний зміст курсу освоєний **не повністю**, але **прогалини не носять істотного** характеру, необхідні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **більшість** передбачених програмою навчання навчальних завдань **виконано, деякі** з виконаних завдань, містять **помилки,** робота з трьома значними помилками.
5	65-69			
4	60 – 64		E	**"Достатньо"** – теоретичний зміст курсу освоєний **частково, деякі** практичні навички роботи **не сформовані, частина** передбачених програмою навчання навчальних завдань **не виконані,** або якість виконання деяких з них оцінено числом балів, близьким до **мінімального**, робота, що задовольняє мінімуму критеріїв оцінки.
3	40–59	Незадовільно ("не зараховано")	FX	**"Умовно незадовільно"** – теоретичний зміст курсу освоєний **частково**, необхідні практичні навички роботи **не сформовані, більшість** передбачених програм навчання, навчальних завдань **не виконано**, або якість їхнього виконання оцінено числом балів, близьким до **мінімального**; при **додатковій самостійній** роботі над матеріалом курсу **можливе підвищення якості** виконання навчальних завдань (**з можливістю повторного складання**), робота, що потребує доробки
2	21-40			
1	1–20		F	**"Безумовно незадовільно"** – теоретичний зміст курсу **не освоєно**, необхідні практичні навички роботи **не сформовані, всі виконані** навчальні завдання містять грубі **помилки, додаткова самостійна** робота над матеріалом курсу **не**

Оцінка в балах		Оцінка за національною шкалою	Оцінка за шкалою ECTS	
			Оцінка	Пояснення
				приведе до значимого **підвищення якості** виконання навчальних завдань, робота, що потребує повної переробки

10. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Програма навчальної дисципліни «Методи та засоби захисту інформації». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2023 р.
2. Робоча програма навчальної дисципліни «Методи та засоби захисту інформації». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2023 р.
3. Тулупов В.В. Методи та засоби захисту інформації. Електронний курс лекцій. Харків, ХНУВС, 2023 р.
4. Тулупов В.В. Електронний курс методичних розробок до практичних та лабораторних занять з дисципліни "Методи та засоби захисту інформації". Харків, ХНУВС, 2023 р.
5. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спец. 125 «Кібербезпека» спеціалізації «Системи технічного захисту інформації» / І. Є. Антіпов та ін. ; Харків. нац. ун-т радіоелектроніки. Харків : Панов, 2019. 215 с.
6. Технічний захист інформації в інформаційних та телекомунікаційних системах : навчальний посібник / уклад. Ластівка Г. І., Шпатар П. М. Чернівці: Чернівецький національний університет, 2018. 252 с.

Додаткова

7. Нужний С. М., Турти М. В. Методичні вказівки до виконання практичних робіт з дисципліни «Організаційне забезпечення технічного захисту інформації» в 2 ч. Ч. 1 / під ред. д-ра техн. наук О. В. Блінцова ; Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : СНУК, 2018. 54 с.
8. Блінцов О. В., Корицький В. І. Методичні вказівки до виконання лабораторних робіт з дисципліни «Мікропроцесорні засоби обробки даних в системах технічного захисту інформації» / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2018. 78 с.
9. Олейніков А.М. Методи та засоби захисту інформації навчальний посібник / А. М. Олейніков. – Харків: НТМТ, 2014. - 298 с.
10. Термінологічний довідник з питань технічного захисту інформації / ред. В. О. Хорошко. 3. вид., доп. і перероб. К. : ТОВ «ПоліграфКонсалтинг», 2003. 286 с.
11. Коженевський С. Р. Термінологічний довідник з питань технічного захисту інформації. Вид. 4-те, доп. і перероб. К. : ДУІКТ, 2007. 365 с.
12. Рибальський О.В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації : посібник для курсантів ВНЗ МВС України. К. : Вид. Національної академії внутріш. справ, 2012. 104 с.

13. Методи і засоби технічного захисту інформації : навч. посіб. / уклад. Ластівка Г. І., Шпатар П. М.; Чернів. нац. ун-т ім. Ю. Федьковича. Чернівці : Чернів. нац. ун-т, 2010. 248 с.
14. Шепета О. В. Адміністративно-правові засади технічного захисту інформації : монографія /Акад. наук вищ. освіти України, Global organization of allied leadership, Acad. of open society security. К. : О. С. Ліпкан, 2012. 295 с.
15. Політанський Л. Ф., Зумшан І. М. Поля і хвилі в системах технічного захисту інформації : навч. посіб. / Чернів. нац. ун-т ім. Ю. Федьковича. Чернівці : Чернівецький нац. ун-т, 2011. 60 с.
16. Романенко С. М., Дмитренко В. П., Карпуков Л. М. Поля і хвилі в задачах технічного захисту інформації : навч. посіб. для студентів ВНЗ, які навчаються за напрямом підгот. «Кібербезпека» / Запоріз. нац. техн. ун-т. Запоріжжя : ЗНТУ, 2016. 280 с.
17. Основи теорії кіл, сигналів та процесів в системах технічного захисту інформації : підруч. для студ. вищ. навч. закл., які навчаються за напрямом «Системи технічного захисту інформації» / за заг. ред. В. М. Шокала ; Харк. нац. ун-т радіоелектрон. Х. : НТМТ, 2011. Ч. 1. Ю. О. Коваль та ін. 2011. 542 с.
18. Тимошенко Л. П. Схемотехніка пристроїв технічного захисту інформації : навч. посіб. для студ. вищ. навч. закл., які навчаються за напрямом «Системи технічного захисту інформації» : у 2 ч. Ч.1. / за ред. д-ра техн. наук, проф. В. М. Карташова. Харків : СМІТ, 2012. 339 с.
19. Тимошенко Л. П. Схемотехніка пристроїв технічного захисту інформації : навч. посіб. для студ. вищ. навч. закл., які навчаються за напрямом «Системи технічного захисту інформації» : у 2 ч. Ч.2. / за ред. д-ра техн. наук, проф. В. М. Карташова. Харків : СМІТ, 2015. 230 с.
20. Інформаційна безпека. Технічні канали витоку та системи ідентифікації особи людини : навч. посіб. для студ. вищ. навч. закл., які навч. за напрямом «Системи технічного захисту інформації» з навч. дисциплін «Методи та засоби технічного захисту інформації», «Системи банківської безпеки» та «Технічні засоби охорони об'єктів» / М. В. Захарченко та ін. ; за ред. чл.-кор. МАЗ, канд. техн. наук, доц. В. Г. Кононовича ; Держ. служба спец. зв'язку та захисту інформації України, Адмін. держ. служби спец. зв'язку та захисту інформації України, Одес. нац. акад. зв'язку ім. О. С. Попова, Каф. інформ. безпеки та передачі даних. О. : ОНАЗ ім. О.С. Попова, 2012. 187 с.
21. Голев Д. В., Кононович В. Г., Хомич С. В. Методики оцінки інформаційної захищеності телекомунікацій : навч. посіб. / за ред. чл.-кор. МАЗ В. Г. Кононовича. Одеса : ОНАЗ ім. О.С. Попова, 2013. 218 с.
22. Програми та методики державної експертизи інформаційної захищеності телекомунікацій : навч. посіб. у галузі знань 1701 «Інформаційна безпека» за спец. 7.17010201, 8.17010201 – Системи технічного захисту інформації, автоматизація її обробки / С. М. Горохов та ін. ; за ред. чл.-кор. МАЗ В. Г. Кононовича ; Одес. нац. акад. зв'язку ім. О. С. Попова, Каф. інформ. безпеки та передачі даних. О. : ОНАЗ ім. О. С. Попова, 2013. 251 с.
23. Методики оцінки інформаційної захищеності телекомунікацій : навч. посіб. галузі знань 1601, 1701 «Інформаційна безпека» за спец. 7.17010201, 8.17010201 – Системи

технічного захисту інформації, автоматизації її обробки / Голев Д. В., Кононович В. Г., Хомич С. В. ; за ред. чл.-кор. МАЗ В. Г. Кононовича ; Одес. нац. акад. зв'язку ім. О. С. Попова, Каф. інформ. безпеки та передачі даних. О. : ОНАЗ ім. О. С. Попова, 2013. 217 с.
24. Носов В. В., Манжай А. В. Організація та забезпечення безпеки інформації : навчальний посібник. Харків : ХНУВС, 2007. 216 с.

Нормативно-правові акти

25. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.
26. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3475-15.
27. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
28. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
29. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3855-12.
30. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17.
31. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19.
32. Про ліцензування видів господарської діяльності : Закон України від 02.03.2015 № 222-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/222-19.
33. Про основні засади державного нагляду (контролю) у сфері господарської діяльності : Закон України від 05.04.2007 № 877-V // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/877-16.
34. Про акредитацію органів з оцінки відповідності : Закон України від 17.05.2001 № 2407-III // База даних «Законодавство України» / Верховна Рада України. URL https://zakon.rada.gov.ua/laws/show/2407-14:
35. Про наукову і науково-технічну експертизу : Закон України від 10.02.1995 № 51/95-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/51/95-%D0%B2%D1%80.
36. Про метрологію та метрологічну діяльність : Закон України від 05.06.2014 № 1314-VII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1314-18.
37. Про основні засади забезпечення кібербезпеки України : Закон України від

05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19.
38. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27.09.1999 № 1229 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1229/99.
39. Про затвердження Концепції технічного захисту інформації в Україні : постанова Кабінету Міністрів України від 08.10.1997 № 1126 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF.
40. Про затвердження Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України : постанова Кабінету Міністрів України від 03.09.2014 № 411 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF.
41. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Кабінету Міністрів України від 29.03.2006 № 373 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF.
42. Про деякі питання захисту інформації, охорона якої забезпечується державою : постанова Кабінету Міністрів України від 13.03.2002 № 281 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/281-2002-%D0%BF.
43. Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації : постанова Кабінету Міністрів України від 04.02.1998 № 121 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/281-2002-%D0%BF.
44. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення: НД ТЗІ 1.1-005-07. К. : Державна служба спеціального зв'язку та захисту інформації України, 2007. 5 с. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102265&cat_id=46556.
45. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі : НД ТЗІ 3.7-003-2005: чинний від 2005-11-08. К. : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2005. 17 с. URL: http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106350.
46. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва. ДБН А.2.2-96. Видання інформаційне. К. : Держкоммістобудування України, 1996. 18 с.
47. Про затвердження Зводу відомостей, що становлять державну таємницю : наказ Служби безпеки України від 23.12.2020 № 383 // База даних «Законодавство України» / Верховна Рада України. URL: https://законодавство.com/download/nakaz-vid-23122020-383-pro-zatverdjennya-zvodu-2020-87459.html

Інформаційні ресурси в Інтернеті

48. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws.
49. Фонд нормативних документів у сфері технічного та криптографічного захисту інформації // Державна служба спеціального зв'язку та захисту інформації України : офіційний вебсайт. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/category?cat_id=89734.
50. Перелік нормативно-методичних документів в галузі захисту інформації // Облікові документи для секретного діловодства / ТОВ «НІКС» : офіційний вебсайт. URL: https://sites.google.com/a/nics.com.ua/price/.
51. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом // Державна служба спеціального зв'язку та захисту інформації України : офіційний вебсайт. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/category?cat_id=39181.
52. Відомості про засоби технічного захисту інформації, на які закінчився термін дії сертифікатів відповідності та експертних висновків // Державна служба спеціального зв'язку та захисту інформації України : офіційний вебсайт. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=234241&cat_id=39181.
53. Каталог обладнання для виявлення каналів витоку інформації // Digital and Analog Systems : офіційний вебсайт. URL: https://www.das-ua.com/katalog/obladnannya-dlya-viyavlennya-kanaliv-vitoku-informacii/.
54. Каталог обладнання для протидії засобам знімання інформації// Digital and Analog Systems : офіційний вебсайт. URL: https://www.das-ua.com/katalog/obladnannya-protidii-zasobam-znimannya-informacii/.
55. Каталог скануючих приймачів та іншого радіообладнання// Digital and Analog Systems : офіційний вебсайт. URL: https://www.das-ua.com/katalog/skanuyuchi-prijmachi/.
56. Каталог обладнання та пристроїв для фізичного огляду // Digital and Analog Systems : офіційний вебсайт. URL: https://www.das-ua.com/katalog/texnika-dlya-fizichnogo-oglyadu/.