

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ**

Кафедра кібербезпеки та DATA – технологій факультету № 6

РОБОЧА ПРОГРАМА

навчальної дисципліни "Методи та засоби технічного захисту інформації"
обов'язкових компонент
освітньої програми першого (бакалаврського) 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.

Опис навчальної дисципліни

Найменування показників	Шифри та назви галузі знань, код та назва спеціальності, ступінь вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 8 Загальна кількість годин – 240 Кількість тем – 15	12 Інформаційні технології 125 Кібербезпека бакалавр	Навчальний курс – 2, 3 Семестр – 4, 5, 6 Види підсумкового контролю: залік, екзамен
Розподіл навчальної дисципліни за видами занять:		
денна форма навчання		заочна форма навчання
Лекції – 60;		Лекції – 8;
Практичні заняття – 24;		Практичні заняття – 6;
Лабораторні заняття – 36;		Лабораторні заняття – 10;
Самостійна робота – 120;		Самостійна робота – 216;
Індивідуальні завдання:		Індивідуальні завдання:
Курсова робота – не передбачено		Курсова робота – не передбачено
Реферати –		Реферати –

1. Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни «Методи та засоби технічного захисту інформації» є отримання здобувачами вищої освіти необхідних знань та навичок щодо застосування на об'єктах інформаційної діяльності (далі – ОІД) необхідних заходів і засобів технічного захисту інформації (далі – ТЗІ), у тому числі інформації, що віднесена до державної таємниці, а також перевірка ефективності запроваджених заходів та засобів щодо витоку інформації технічними каналами (протидія технічним розвідкам).

Основними завданнями вивчення дисципліни «Методи та засоби технічного захисту інформації» є отримання здобувачами вищої освіти знань щодо причин виникнення технічних каналів витоку інформації на об'єктах інформаційної діяльності, вміння правильно обрати необхідні методи та засоби захисту інформації під час створення комплексної системи захисту інформації, перевірити ефективність застосованих заходів та засобів захисту інформації, у тому числі шляхом проведення інструментальних досліджень у відповідності до методик оцінки.

Міждисциплінарні зв'язки: «Фізика», «Правові засади захисту інформації», «Метрологія та вимірювання», «Електроніка та схемотехніка», «Теорія інформації та кодування», «Управління та організація в сфері

інформаційної безпеки».

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

знати:

- основні положення та терміни, що стосуються галузі інформаційної безпеки та технічного захисту інформації;
- зміст і вимоги загальнодержавних нормативно-правових актів у сфері кібербезпеки та окремих нормативних документів у сфері технічного захисту інформації (далі – НД ТЗІ);
- класифікацію об'єктів інформаційної діяльності, інформації, що на них циркулює та в якому вигляді;
- класифікацію технічних каналів витоку інформації (далі – ТКВІ) та причини їх виникнення;
- можливі ТКВІ на об'єктах де розміщені технічні засоби обробки, передачі, зберігання та відображення інформації (далі – ТЗПІ);
- види та засоби технічних розвідок;
- методи, способи та засоби запобігання виникнення ТКВІ;
- класифікацію технічних засобів захисту інформації, їхні можливості та основні характеристики;
- типові заходи та засоби ТЗІ;
- вимоги до умов експлуатації систем (комплексів) урядового або спеціального зв'язку від витоку інформації;
- типові технічні характеристики та особливості застосування засобів технічного захисту інформації (протидії технічним розвідкам);
- основні методики контролю ефективності протидії технічним розвідкам;
- основні методики спеціальних досліджень та інструментального контролю ефективності технічного захисту інформації;
- 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;
- обирати необхідні технічні засоби для захисту інформації від її витоку через ймовірні канали витоку;
- 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;

- оцінювати ефективність застосованих на об'єкті інформаційної діяльності заходів та засобів протидії технічним розвідкам;

- у відповідності до затверджених методик проводити спеціальні дослідження та здійснювати інструментальний контроль ефективності технічного захисту інформації;

- узагальнювати передовий досвід роботи фахівців з організації захисту інформації щодо стандартизації, уніфікації методів, способів, засобів і заходів забезпечення безпеки інформаційної сфери суспільства.

Програмні компетентності, які формуються при вивченні навчальної дисципліни:		
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційних технологій (кібербезпека), що передбачає ідентифікацію та використання інформації для прийняття рішень.	
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.
Спеціальні (фахові, предметні) 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.
	ФК 2	Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
	ФК 3	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. Інформація: визначення, її види та носії, в якому вигляді циркулює, її вартість.

Термін «інформація», його визначення. Інформація, що підлягає захисту.

Види інформації за режимом доступу. Відкрита інформація та інформація з обмеженим доступом. Види інформації за правовим режимом. Конфіденційна інформація. Персональні дані. Службова інформація. Типи інформації. Державна таємниця.

Переліки відомостей, згідно до яких інформацію відносять до певного виду. Переліки службової інформації в МВС України та Національній поліції України. Звід відомостей, що становлять державну таємницю (ЗВДТ).

Класифікація носіїв інформації. Матеріальні носії інформації. Нематеріальні носії інформації (фізичні поля). Людина як носій інформації.

Вартість інформації. Собівартість інформації. Збитки через несанкціонований доступ до інформації чи її втрату.

Тема № 2. 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.

Легальні та нелегальні організації, що мають у своєму складі підрозділи технічної розвідки.

Види та характеристика радіоелектронної розвідки та її складових: радіорозвідка, радіотехнічна розвідка, радіолокаційна розвідка, комп'ютерна

розвідка, радіотепловізорна розвідка. Оптико-електронна розвідка. Акустична розвідка.

Тема № 3. Об'єкти інформаційної діяльності: визначення, види та технічні засоби.

Визначення терміну «об'єкт інформаційної діяльності». Види об'єктів інформаційної діяльності: виділені приміщення; копіювально-розмножувальна техніка; автоматизовані системи.

Призначення виділених приміщень. Види обладнання, що використовуються у приміщення: основні та допоміжне. Основні технічні засоби (ОТЗ). Допоміжні технічні засоби та системи (ДТЗС). Інженерні системи та комунікації у приміщенні.

Види та принципи роботи копіювально-розмножувальної техніки.

Класифікація автоматизованих систем. Типові складові частини автоматизованих систем та принципи їх роботи.

Небезпечні сигнали та їх джерела.

Тема № 4. Технічні канали витоку інформації: визначення та класифікації.

Класифікація каналів витоку інформації.

Різні класифікації технічних каналів витоку інформації: у нормативних актах та вченими. Штучні та природні канали витоку інформації.

Загальні характеристики технічних каналів витоку інформації. Середовища поширення інформації в технічних каналах витоку інформації.

Тема № 5. Методи та засоби несанкціонованого отримання інформації технічними каналами.

Засоби для негласного проникнення у приміщення.

Класифікація засобів технічної розвідки. Поділ за принципом роботи: активні та пасивні.

Типові характеристики пристроїв для: прослуховування приміщень; телефонних ліній. Радіозакладки.

Методи і засоби встановлення та під'єднання технічних засобів розвідки.

Методи і засоби дистанційного керування та отримання інформації із технічного засобу розвідки.

Системи прихованого відеоспостереження.

Методи та засоби перехоплення інформації з автоматизованих систем.

Тема № 6. Акустичні технічні канали витоку інформації.

Класифікація акустичних технічних каналів витоку інформації: повітряний, віброакустичний, акустоелектричний, оптико-електронний, параметричний. Причини виникнення та середовище поширення.

Засоби технічної розвідки з акустичних технічних каналів витоку інформації.

Мікрофони: їх класифікація. Мікрофонний ефект. Високочастотне навіязування.

Тема № 7. Телекомунікаційні технічні канали витоку інформації.

Класифікація телекомунікаційних технічних каналів витоку інформації: електричний; радіоелектронний; побічного електромагнітного випромінювання та наведення. Причини виникнення та середовище поширення.

Низькочастотні і високочастотні випромінювання технічних засобів. Витік інформації по ланцюгах електроживлення. Витік інформації по цілях заземлення.

Засоби технічної розвідки з телекомунікаційних технічних каналів витоку інформації.

Тема № 8. Візуально-оптичні технічні канали витоку інформації.

Класифікація візуально-оптичних технічних каналів витоку інформації. Причини виникнення та середовище поширення.

Засоби технічної розвідки з візуально-оптичних технічних каналів витоку інформації.

Тема № 9. Матеріально-речовинні технічні канали витоку інформації.

Класифікація матеріально-речовинних технічних каналів витоку інформації. Причини виникнення та середовище поширення.

Засоби технічної розвідки з матеріально-речовинних технічних каналів витоку інформації.

Тема № 10. Пошукова техніка для виявлення засобів технічних розвідок.

Виявлення каналів витоку інформації на об'єктах інформаційної діяльності. Обстеження об'єкту інформаційної діяльності.

Класифікація засобів для пошуку технічних пристроїв негласного перехоплення інформації: активні та пасивні.

Виявители пустот. Металошукачі. Рентгенівські апарати.

Класифікація засобів радіовиявлення: індикатори електромагнітного поля, радіочастотоміри та інтерцептори.

Універсальний прилад виявлення пристроїв прихованого знімання інформації СРМ-700 «Акула». Багатофункційний пошуковий прилад ST-031 «Піранья».

Радіомоніторинг у структурі загальних методів захисту акустичної інформації: основна мета радіомоніторингу при захисті акустичної інформації, основні вимоги до структури і параметрів засобів радіомоніторингу.

Вимірювальні засоби радіомоніторингу. Селективні мікровольтметри і нановольтметри. Панорамні засоби радіомоніторингу. Аналізуючі засоби радіомоніторингу.

Методи пошуку з використанням пошукової техніки.

Тема № 11. Засоби технічного захисту інформації.

Класифікація засобів технічного захисту інформації.

Сертифікація засобів технічного захисту інформації.

Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Тема № 12. Методи технічного захисту інформації.

Методи технічного захисту інформації: пасивні та активні.

Вимоги (рекомендації) щодо забезпечення захисту інформації (протидії технічним розвідкам).

Створення комплексної системи захисту інформації на об'єкті інформаційної діяльності.

Тема № 13. Оцінка ефективності захисту інформації від витоку технічними каналами витоку.

Загальні підходи до оцінки ефективності інформаційної захищеності. Цілі та задачі технічного контролю ефективності заходів захисту інформації.

Ефективність технічного захисту інформації (протидії технічній розвідці).

Перелік методик контролю ефективності протидії технічним розвідкам.

Проведення інструментальних досліджень у відповідності до методик оцінки ефективності.

Норми ефективності захисту інформації (протидії технічній розвідці).

Дотримання вимог з режиму секретності під час проведення інструментальних досліджень та проведення оцінки ефективності протидії технічним розвідкам.

Тема № 14. Методики технічного контролю ефективності заходів технічного захисту інформації від витоку електромагнітними полями.

Методика вимірювання ПЕМВН від засобів електронно-обчислювальної техніки.

Види вимірювань, вимоги до вимірювачів, вибір тестів.

Вибір тестів для вимірювання ПЕМВН цифрових сигналів монітора.

Методика контролю захищеності від ПЕМВН периферійних засобів персональних ЕОМ.

Тема № 15. Методики оцінки ефективності захищеності інформації від витоку акустичними каналами та каналами акустоелектричних перетворень.

Основні поняття щодо вимірювань технічних каналів витоку мовної інформації.

Методи захисту та порядок проведення контролю захищеності виділених приміщень від витоку акустичної мовної інформації.

Дослідження впливу акустичного поля на допоміжні технічні засоби та системи.

Вимоги до методики й обладнання для вимірювання каналів витоку з акустоелектричними перетвореннями.

Вимоги до методики й обладнання для вимірювання каналів витоку з будівельних конструкції та інженерних комунікації за рахунок віброакустичних перетворень.

4. Структура навчальної дисципліни

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

№ з/п	Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
		Всього	з них:					
			Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 4								
1.	Тема № 1. Інформація: визначення, її види та носії, в якому вигляді циркулює, її вартість.	14	4		2	4	4	
2.	Тема № 2. Цілі, задачі та організація технічної розвідки.	18	4				14	
3.	Тема № 3. Об'єкти інформаційної діяльності: визначення, види та технічні засоби.	14	4		2		8	
4.	Тема № 4. Технічні канали витоку інформації: визначення та класифікації.	16	4		2		10	
5.	Тема № 5. Методи та засоби несанкціонованого отримання інформації по технічних каналах.	28	4		2	8	14	
Всього за семестр № 4:		90	20		8	12	50	Залік
Семестр № 5								
6.	Тема № 6. Акустичні технічні канали витоку інформації.	19	4			4	11	
7.	Тема № 7. Телекомунікаційні технічні канали витоку інформації.	10	4				6	
8.	Тема № 8. Візуально-оптичні технічні канали витоку інформації.	12	4		4		4	
9.	Тема № 9. Матеріально-речовинні технічні канали витоку інформації.	6	2				4	
10.	Тема № 10. Пошукова техніка для	28	6		4	8	10	

	виявлення засобів технічних розвідок.							
Всього за семестр № 5:		75	20		8	12	35	Залік
Семестр № 6								
11.	Тема № 11. Засоби технічного захисту інформації.	19	4		4		11	
12.	Тема № 12. Методи технічного захисту інформації.	18	4		4		10	
13.	Тема № 13. Оцінка ефективності захисту інформації від витоку технічними каналами витоку.	10	4				6	
14.	Тема № 14. Методики технічного контролю ефективності заходів технічного захисту інформації від витоку електромагнітними полями.	14	4			6	4	
15.	Тема № 15. Методики оцінки ефективності захищеності інформації від витоку акустичними каналами та каналами акустоелектричних перетворень.	14	4			6	4	
Всього за семестр № 6:		75	20		8	12	35	Екзамен
Загалом		240	60		24	36	120	

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

№ з/п	Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
		Всього	з них:					
			Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 4								
1.	Тема № 1. Інформація: визначення, її види та носії, в якому вигляді циркулює, її вартість.	16					16	
2.	Тема № 2. Цілі, задачі та організація технічної розвідки.	16					16	
3.	Тема № 3. Об'єкти інформаційної діяльності: визначення, види та технічні засоби.	16					16	
4.	Тема № 4. Технічні канали витоку інформації: визначення та класифікації.	26	2		2	2	20	
5.	Тема № 5. Методи та засоби несанкціонованого отримання	16					16	

	<i>інформації по технічних каналах.</i>							
Всього за семестр № 4:		90	2		2	2	84	Залік
Семестр № 5								
6.	<i>Тема № 6. Акустичні технічні канали витоку інформації.</i>	19	4		2		13	
7.	<i>Тема № 7. Телекомунікаційні технічні канали витоку інформації.</i>	13					13	
8.	<i>Тема № 8. Візуально-оптичні технічні канали витоку інформації.</i>	13					13	
9.	<i>Тема № 9. Матеріально-речовинні технічні канали витоку інформації.</i>	13					13	
10.	<i>Тема № 10. Пошукова техніка для виявлення засобів технічних розвідок.</i>	17				4	13	
Всього за семестр № 5:		75	4		2	4	65	Залік
Семестр № 6								
11.	<i>Тема № 11. Засоби технічного захисту інформації.</i>	20	4		2		14	
12.	<i>Тема № 12. Методи технічного захисту інформації.</i>	16	2				14	
13.	<i>Тема № 13. Оцінка ефективності захисту інформації від витоку технічними каналами витоку.</i>	13					13	
14.	<i>Тема № 14. Методики технічного контролю ефективності заходів технічного захисту інформації від витоку електромагнітними полями.</i>	13					13	
15.	<i>Тема № 15. Методики оцінки ефективності захищеності інформації від витоку акустичними каналами та каналами акустоелектричних перетворень.</i>	13					13	
Всього за семестр № 6:		75			2		67	Екзамен
Загалом		240	8		6	10	216	

4.1.3. Питання, що виносяться на самостійне опрацювання

Перелік питань до тем навчальної дисципліни	Література
Тема № 1. Інформація: визначення, її види та носії, в якому вигляді циркулює, її вартість.	
1. Види інформації за правовим режимом. Конфіденційна інформація. Персональні дані. Службова інформація. Типи інформації. Державна таємниця. 2. Переліки службової інформації в МВС України та Національній поліції України. 3. Звід відомостей, що становлять державну таємницю (ЗВДТ).	31, 35, 37, 39, 40, 41, 59, 60
Тема № 2. Цілі, задачі та організація технічної розвідки.	
1. Відомі історичні операції у сфері негласного застосування засобів технічних розвідок. 2. Операція «Златоуст» (герб у посольстві США в СРСР). 3. Операція «Берлінський тунель».	20, 21, 22, 23, 24, 25, 27, 28
Тема № 3. Об'єкти інформаційної діяльності: визначення, види та	

<i>технічні засоби.</i>	
<ol style="list-style-type: none"> 1. Основні технічні засоби (ОТЗ). 2. Допоміжні технічні засоби та системи (ДТЗС). 3. Інженерні системи та комунікації у приміщенні. 4. Типові складові частини автоматизованих систем та принципи їх роботи. 	3, 4, 8, 20, 21
Тема № 4. <i>Технічні канали витоку інформації: визначення та класифікації.</i>	
<ol style="list-style-type: none"> 1. Загальні характеристики технічних каналів витоку інформації. 2. Середовища поширення інформації в технічних каналах витоку інформації. 	10, 11, 12, 13, 14, 15, 50, 51, 52
Тема № 5. <i>Методи та засоби несанкціонованого отримання інформації по технічних каналах.</i>	
<ol style="list-style-type: none"> 1. Класифікація засобів технічної розвідки. 2. Методи і засоби встановлення та під'єднання технічних засобів розвідки. 3. Методи і засоби дистанційного керування та отримання інформації із технічного засобу розвідки. 4. Методи та засоби перехоплення інформації з автоматизованих систем. 	15, 19, 20, 21, 22, 23, 24, 25, 27
Тема № 6. <i>Акустичні технічні канали витоку інформації.</i>	
<ol style="list-style-type: none"> 1. Причини виникнення акустичних технічних каналів витоку. 2. Мікрофони: їх класифікація. 3. Мікрофонний ефект. 	13, 14, 24, 25
Тема № 7. <i>Телекомунікаційні технічні канали витоку інформації.</i>	
<ol style="list-style-type: none"> 1. Низькочастотні і високочастотні випромінювання технічних засобів. 2. Витік інформації по ланцюгах електроживлення. 3. Витік інформації по цілях заземлення. 4. Засоби технічної розвідки з телекомунікаційних технічних каналів витоку інформації. 	13, 14, 24, 25
Тема № 8. <i>Візуально-оптичні технічні канали витоку інформації.</i>	
<ol style="list-style-type: none"> 1. Засоби технічної розвідки з візуально-оптичних технічних каналів витоку інформації. 	20, 21, 23, 24, 25
Тема № 9. <i>Матеріально-речовинні технічні канали витоку інформації.</i>	
<ol style="list-style-type: none"> 1. Засоби технічної розвідок з матеріально-речовинних технічних каналів витоку інформації. 	20, 21, 23, 24, 25
Тема № 10. <i>Пошукова техніка для виявлення засобів технічних розвідок.</i>	
<ol style="list-style-type: none"> 1. Виявлювачі порожнеч. 2. Металошукачі. 3. Рентгенівські апарати. 4. Вимірювальні засоби радіомоніторингу. 5. Селективні мікровольтметри і нановольтметри. 6. Панорамні засоби радіомоніторингу. 7. Аналізуючи засоби радіомоніторингу. 	65, 66, 67, 68
Тема № 11. <i>Засоби технічного захисту інформації.</i>	
<ol style="list-style-type: none"> 1. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. 	63, 64, 66
Тема № 12. <i>Методи технічного захисту інформації.</i>	
<ol style="list-style-type: none"> 1. Методи технічного захисту інформації. 2. Створення комплексної системи захисту інформації на об'єкті інформаційної діяльності. 	3, 4, 36, 38, 50, 52, 53, 54, 55, 56, 57, 58, 70, 71, 80, 81

Тема № 13. <i>Оцінка ефективності захисту інформації від витоку технічними каналами витоку.</i>	
1. Загальні підходи до оцінки ефективності інформаційної захищеності. 2. Цілі та задачі технічного контролю ефективності заходів захисту інформації.	16, 17, 18, 61, 62, 89
Тема № 14. <i>Методики технічного контролю ефективності заходів технічного захисту інформації від витоку електромагнітними полями.</i>	
1. Методика вимірювання ПЕМВН від засобів електронно-обчислювальної техніки.	61, 62, 74, 75, 77, 78, 83, 84, 85, 87
Тема № 15. <i>Методики оцінки ефективності захищеності інформації від витоку акустичними каналами та каналами акустоелектричних перетворень.</i>	
1. Основні поняття щодо вимірювань технічних каналів витоку мовної інформації. 2. Методи захисту та порядок проведення контролю захищеності виділених приміщень від витоку акустичної мовної інформації.	61, 62, 72, 73, 76, 84, 86, 88

5. Індивідуальні завдання

5.1.1. Теми рефератів

1. Державна політика забезпечення інформаційної безпеки.
2. Основні завдання забезпечення безпеки інформації.
3. Безпека інформаційних ресурсів.
4. Державні інформаційні ресурси.
5. Права на доступ до інформації.

5.1.2. Теми наукових робіт

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 навчання

За темами навчальної дисципліни передбачається використання таких методів навчання:

- викладання матеріалу під час лекційних занять з використанням мультимедіа;
- формування професійних вмінь і навичок використання інформаційних технологій під час практичних занять;

- формування навичок використання інформаційних технологій для пошуку та аналізу інформації під час самостійної роботи.

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

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 ТЗП.
 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 (пустот), 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 радіочастотомірювачів.
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 витоків технічними каналами на об'єктах ТЗП.
71. Перелічити основні рекомендації щодо захисту інформації від витоків технічними каналами на об'єктах ТЗП при розробці технічного проекту.

8. Критерії та засоби оцінювання результатів навчання здобувачів

Контрольні заходи оцінювання результатів навчання включають в себе поточний та підсумковий контроль.

Поточний контроль. До форм поточного контролю належить оцінювання:

- рівня знань під час практичних, лабораторних занять;
- якості виконання самостійної роботи.

Поточний контроль здійснюється під час проведення семінарських, практичних та лабораторних занять і має на меті перевірку набутих здобувачем вищої освіти (далі – здобувач) знань, умінь та інших компетентностей 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 національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Оцінки за самостійну роботу виставляються в журналі 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 робота (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 формі, передбаченій в робочою програмою 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**.

$$\begin{array}{l} \text{Загальна} \\ \text{кількість балів} \\ \text{(перед} \\ \text{підсумковим} \\ \text{контролем)} \end{array} = \left(\begin{array}{l} \text{Результат} \\ \text{навчальних} \\ \text{занять} \\ \text{за семестр} \end{array} + \begin{array}{l} \text{Результат} \\ \text{самостійної} \\ \text{роботи за} \\ \text{семестр} \end{array} \right) / 2 * 10$$

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 реєструється в журналах обліку роботи академічної групи. Результати підсумкового контролю з дисциплін відображаються 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).

$$\begin{array}{l} \text{Підсумкові бали} \\ \text{навчальної} \end{array} = \begin{array}{l} \text{Загальна кількість} \\ \text{балів (перед} \end{array} + \begin{array}{l} \text{Кількість балів за} \\ \text{підсумковим} \end{array}$$

*дисципліни**підсумковим
контролем)**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.

Так як 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.

$$\text{Підсумкові бали навчальної дисципліни} = \frac{\text{Сума підсумкових балів за семестри}}{\text{Кількість семестрів}}$$

У цьому розділі також повинні бути розроблені чіткі критерії оцінювання здобувачів вищої освіти під час поточного контролю (*робота на 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 робота	Підсумковий контроль
Отримати не менше 4 позитивних оцінок	Підготувати реферат, підготувати конспект за темою самостійної роботи, виконати практичне завдання тощо	Отримати за підсумковий контроль не менше 30 балів

Підсумковий контроль – екзамен.

9. Шкала оцінювання: за національною шкалою, 100-бальною шкалою, шкалою ЄКТС.

Оцінка в балах	Оцінка за національною шкалою	Оцінка	
		Оцінка	Пояснення
97-100	Відмінно	A	«Відмінно» – теоретичний зміст курсу засвоєний

94-96	(«зараховано»)				цілком , необхідні практичні навички роботи з освоєним матеріалом сформовані, усі навчальні завдання, які передбачені програмою навчання виконані в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
90-93					
85-89	Добре («зараховано»)	В			«Дуже добре» – теоретичний зміст курсу засвоєний цілком , потрібні практичні навички роботи з освоєним матеріалом в основному сформовані, усі навчальні завдання, які передбачені програмою навчання, виконані , якість виконання більшості з них оцінена числом балів, близьким до максимального , робота з двома-трьома незначними помилками.
80-84					
75-79					
70-74	Задовільно («зараховано»)	С			«Добре» – теоретичний зміст курсу засвоєний цілком , практичні навички роботи з освоєним матеріалом в основному сформовані, усі навчальні завдання, які передбачені програмою навчання, виконані , якість виконання жодного з них не оцінена мінімальним числом балів, деякі види завдань виконані з помилками , робота з декількома незначними помилками, або з однією-двома значними помилками.
65-69					
60-64					
41-59	Незадовільно («не зараховано»)	Б			«Задовільно» – теоретичний зміст курсу засвоєний частково , але прогалини не несуть істотний характер, потрібні практичні навички роботи з освоєним матеріалом в основному сформовані більшість передбачених програмою
21-40					
1-20					
		Е			«Достатньо» – теоретичний зміст курсу освоєний частково , деякі практичні навички роботи не сформовані , частина передбачених програмою навчання навчальних завдань не виконана , або якість виконання деяких з них оцінена числом
		FX			«Умовно незадовільно» – теоретичний зміст курсу засвоєний частково , потрібні практичні навички роботи несформовані , більшість передбачених програмою навчання, навчальних завдань не виконано , або якість їхнього виконання оцінено числом балів, близьким до мінімального ; при додатковій самостійній
		Е			«Безумовно незадовільно» – теоретичний зміст курсу неосвоєний , потрібні практичні навички роботи несформовані , всі виконані навчальні завдання містять грубі помилки , додаткова самостійна робота над матеріалом курсу не

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

Основна

1. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. - К.: ІСЗЗІ НТУУ «КПІ», 2019. - 104 с.
2. Лаптев О.А. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. – К. ДУТ, 2020 – 326 с.
3. Лаптев О.А. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: Навчальний посібник / О.А. Лаптев, В.А. Савченко, Г.В. Шуклін. – К. ДУТ, 2020 – 126 с.
4. 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.
5. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2018. Частина 13: Захист інформації в системах електронного урядування / [О.М. Хошаба]. – К.: ФОП Москаленко О. М., 2018. – 72 с.
6. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – Національний університет “Одеська юридична академія” та Київський інститут інтелектуальної власності та права – К.: КІВП, 2018. – 128 с.
7. Борисова Л.В. Основи інформаційної безпеки. Конспект лекцій. – Національний університет цивільного захисту України – Х.: НУЦЗУ, 2019. – 105 с.
8. Дмитренко В. П. Поля і хвилі в телекомунікаціях: навчальний посібник для студентів вищих навчальних закладів / В.П. Дмитренко, С.М. Романенко, Г.В. Мороз – Запоріжжя: НУ«ЗП», 2019. – 289 с.
9. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / укл.: Г.І.Ластівка, П.М.Шпатар – Чернівці: Чернівецький національний університет, 2018. – 252 с.
- 10.Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання. – К.: ВД “Гельветика”, 2017. – 168 с.
- 11.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, 2020. 218 с.
- 12.Програма навчальної дисципліни «Методи та засоби захисту інформації». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2022 р.
- 13.Робоча програма навчальної дисципліни «Методи та засоби захисту інформації». Спеціальність 125 «Кібербезпека». Тулупов В.В. – м. Харків: Харківський національний університет внутрішніх справ, 2022 р.
- 14.Тулупов В.В. Методи та засоби захисту інформації. Електронний курс

лекцій. Харків, ХНУВС, 2022 р.

15. Тулупов В.В. Електронний курс методичних розробок до практичних та лабораторних занять з дисципліни "Методи та засоби захисту інформації". Харків, ХНУВС, 2022 р.
16. Тихонов Ю.О. Теорія кіл і сигналів в інформаційному та кіберпросторах: Завдання та методичні вказівки до виконання курсової роботи / Ю.О. Тихонов, В.М. Ахрамовіч, О.А. Лаптев. – К. ДУТ, 2019 – 22 с.

Додаткова

17. 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.
18. 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.
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.1. / за ред. д-ра техн. наук, проф. В. М. Карташова. Харків : СМІТ, 2019. 339 с.
20. 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, 2019. 230 с.
21. 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, 2019. 187 с.

Нормативно-правові акти

22. 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>.
23. 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>.
24. 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>.
25. 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>.
26. 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>.
 27. 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>.
 28. 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>.
 29. 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>.
 30. 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>.
 31. 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>.
 32. 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>.
 33. 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>.
 34. 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>.
 35. 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>.
 36. 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>.
 37. 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>.
 38. 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>.
39. 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>.
40. 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>.
41. 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.
42. 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>
43. 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.
44. 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://zakonodavstvo.com/download/nakaz-vid-23122020-383-pro-zatverdjennya-zvodu-2020-87459.html>
45. ДСТУ EN 50117-11-1:2019 Кабелі коаксіальні. Частина 11-1. Групові технічні умови на коаксіальні кабелі для передавання аналогових і цифрових сигналів. Розподільні та магістральні кабелі для систем, що працюють на частоті від 5 МГц до 1000 МГц (EN 50117-11-1:2019, IDT)
46. ДСТУ EN 50117-11-2:2021 Кабелі коаксіальні. Частина 11-2. Групові технічні умови на коаксіальні кабелі для передавання аналогових та цифрових сигналів. Розподільні та магістральні кабелі для систем, що працюють на частоті від 5 МГц до 2000 МГц (EN 50117-11-2:2019, IDT)
47. ДСТУ EN 55016-1-3:2021 Технічні вимоги до апаратури для вимірювання радіозбурень і несприйнятливості та методи вимірювання. Частина 1-3. Апаратура для вимірювання радіозбурень і несприйнятливості. Допоміжне обладнання. Потужність збурень (EN 55016-1-3:2006; A1:2016; A2:2020,

- IDT; CISPR 16-1-3:2004; A1:2016; A2:2020, IDT)
- 48.ДСТУ EN IEC 55015:2021 Обладнання освітлювальне та аналогічне електричне. Норми та методи вимірювання характеристик радіозавод (EN IEC 55015:2019, A11:2020, IDT; CISPR 15:2018, IDT)
 - 49.ДСТУ EN IEC 55016-1-1:2021 Технічні вимоги до апаратури для вимірювання радіозбурень і несприйнятливості та методи вимірювання. Частина 1-1. Апаратура для вимірювання радіозбурень і несприйнятливості. Вимірювальна апаратура (EN IEC 55016-1-1:2019, IDT; CISPR 16-1-1:2019, IDT)
 - 50.ДСТУ EN IEC 55016-1-4:2021 Технічні вимоги до апаратури для вимірювання радіозбурень і несприйнятливості та методи вимірювання. Частина 1-4. Апаратура для вимірювання радіозбурень і несприйнятливості. Антени та випробувальні майданчики для вимірювання випромінюваних збурень (EN IEC 55016-1-4:2019; A1:2020, IDT; CISPR 16-1-4:2019; A1:2020, IDT)
 - 51.ДСТУ EN IEC 61000-4-3:2021 Електромагнітна сумісність. Частина 4-3. Методики випробування та вимірювання. Випробування на несприйнятливість до радіочастотних електромагнітних полів (EN IEC 61000-4-3:2020, IDT; IEC 61000-4-3:2020, IDT)
 - 52.ДСТУ EN ISO 41001:2021 Системи управління інфраструктурою. Вимоги та настанови щодо застосування (EN ISO 41001:2018, IDT; ISO 41001:2018, IDT)
 - 53.ДСТУ ETSI EG 202 057-2:2021 Якість передавання мовної та мультимедійної інформації. Визначення та оцінювання показників якості послуг, які стосуються користувачів. Частина 2. Голосова телефонія, факс групи 3, SMS та послуги передавання даних з використанням модему (ETSI EG 202 057-2 V1.3.2 (2011-04), IDT)
 - 54.ДСТУ ETSI EG 202 057-3:2021 Оброблення мовної інформації, передавання сигналів, показники якості послуг. Визначення та оцінювання показників якості послуг, які стосуються користувачів. Частина 3. Показники якості послуг, призначені для наземних мереж рухомого зв'язку загального користування (ETSI EG 202 057-3 V1.1.1 (2005-04), IDT)
 - 55.ДСТУ ETSI EG 202 057-4:2021 Оброблення мовної інформації, передавання сигналів, показники якості послуг. Визначення та оцінювання показників якості послуг, які стосуються користувачів. Частина 4. Доступ до інтернету (ETSI EG 202 057-4 V1.2.1 (2008-07), IDT)
 - 56.ДСТУ ETSI ES 202 057-1:2021 Оброблення мовної інформації, передавання сигналів, показники якості послуг. Визначення та оцінювання показників якості послуг, які стосуються користувачів. Частина 1. Загальні положення (ETSI ES 202 057-1 V2.1.1 (2013-01), IDT)
 - 57.ДСТУ ITU-T Y.2617:2021 Механізми гарантованої якості послуг та модель робочих характеристик мереж пакетного передавання даних загального користування (ITU-T Y.2617 (06/2016), IDT)
 - 58.ДСТУ ETSI EN 319 122-1:2021 Електронні підписи та інфраструктури (ESI). Цифрові підписи CAdES. Частина 1. Структурні блоки та базові підписи

- CAdES (ETSI EN 319 122-1 V1.2.1 (2021-10), IDT)
- 59.ДСТУ ETSI EN 319 122-2:2021 Електронні підписи та інфраструктури (ESI). Цифрові підписи CAdES. Частина 2. Розширені підписи CAdES (ETSI EN 319 122-2 V1.1.1 (2016-04), IDT)
- 60.ДСТУ ETSI EN 319 162-1:2021 Електронні підписи та інфраструктури (ESI). Контейнери пов'язаних підписів (ASiC). Частина 1. Структурні блоки та базові контейнери ASiC (ETSI EN 319 162-1 V1.1.1 (2016-04), IDT)
- 61.ДСТУ ETSI EN 319 162-2:2021 Електронні підписи та інфраструктури (ESI). Контейнери пов'язаних підписів (ASiC). Частина 2. Додаткові контейнери ASiC (ETSI EN 319 162-2 V.1.1.1 (2016-04), IDT)
- 62.ДСТУ ISO 21043-1:2021 Криміналістика. Частина 1. Терміни та визначення (ISO 21043-1:2018, IDT)
- 63.ДСТУ ISO 21043-2:2021 Криміналістика. Частина 2. Виявлення, фіксування, вилучання, транспортування та зберігання об'єктів (ISO 21043-2:2018, IDT)

Інформаційні ресурси в Інтернеті

- 64.База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws>.
- 65.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.
- 66.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/>.
- 67.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.
- 68.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.
- 69.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/>.
- 70.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/>.
- 71.Каталог скануючих приймачів та іншого радіобладнання// Digital and Analog Systems : офіційний вебсайт. URL: <https://www.das-ua.com/katalog/skanuyuchi-prijmachi/>.
- 72.Каталог обладнання та пристроїв для фізичного огляду // Digital and Analog

Systems : офіційний вебсайт. URL: <https://www.das-ua.com/katalog/tehnika-dlya-fizichnogo-oglyadu/>.