МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Харківський національний університет внутрішніх справ
Факультет № 4
Кафедра протидії кіберзлочинності
Факультет № 6
Кафедра кібербезпеки та DATA-технологій

ЗАТВЕРДЖЕНО
на спільному засіданні
кафедри протидії кіберзлочинності
факультету № 4 та
кафедри кібербезпеки та DATA-
технологій факультету № 6
протокол № 2 від 22.06.2023.
Завідувач кафедри
протидії кіберзлочинності
_____**Олександр МАНЖАЙ**
Завідувач кафедри
кібербезпеки та DATA-технологій
_____ **Юрій ГНУСОВ**

МЕТОДИ ТА ЗАСОБИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ (ОК.21)

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кафедра	Кафедра кібербезпеки та DATA-технологій (https://univd.edu.ua/uk/dir/1740/kafedra-kiberbezpeky-ta-DATA-tekhnologiy)
Контактний телефон	+38 057 73-98-014 (роб.)
E-mail	Vlatu1969@ukr.net
ЛЕКТОР (ЛЕКТОРИ)	
	**Тулупов Володимир Володимирович**, доцент кафедри кібербезпеки та DATA-технологій факультету №6, кандидат технічних наук, доцент E-mail: Vlatu1969@ukr.net **Лекційний потік:** факультет № 6, КБдср/зср-22-1

Назва освітньо-професійної програми	Кібербезпека та захист інформації (безпека інформаційних та комунікаційних систем) Cybersecurity and information protection (security of information and communication systems)
Рівень вищої освіти	Перший (бакалаврський) (НРК України – 6 рівень та перший цикл вищої освіти Рамки кваліфікацій Європейського простору вищої освіти)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Статус дисципліни	Нормативна компонента освітньо-професійної програми вивчається у 4,5,6 семестрі навчання.
Мета вивчення дисципліни	Отримання здобувачами вищої освіти необхідних знань та навичок щодо застосування на об'єктах інформаційної діяльності необхідних заходів і засобів технічного захисту інформації, 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).
Завдання вивчення дисципліни	- 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; - Перевірка ефективності застосованих заходів та засобів захисту інформації, у тому числі шляхом проведення інструментальних досліджень у відповідності до методик оцінки.
Обсяг дисципліни в кредитах ECTS/годинах	8 кредитів ECTS (загальний обсяг – 240 годин) З них (денна/заочна):
	- аудиторна робота: 120/24 годин.
	- самостійна робота: 120/216 годин.
Форми та види проведення навчальних занять	Форма навчання –денна Види навчальних занять: - лекції: 60 годин; - практичні заняття: 24 годин; - лабораторні заняття: 36 годин.

	Форма навчання – заочна Види навчальних занять: - лекції: 8 годин; - практичні заняття: 6 годин; - лабораторні заняття:10 годин.
Самостійна робота	Опрацювання рекомендованої літератури, поширене вивчення теоретичних питань лекційних занять за кожною темою, виконання індивідуальних завдань до практичних занять та опрацювання завдань з метою підготовки до виконання лабораторних занять.
Індивідуальні завдання	Наукові доповіді, індивідуальні завдання до лабораторних занять.
Необхідне обладнання	Мультимедійне обладнання (ноутбук та проектор), комп'ютерне забезпечення з виходом у мережу Інтернет.
Мова викладання	Українська
Контроль	Поточний та підсумковий контроль. Поточний: опитування на практичних заняттях; участь в дискусіях, веб-квестах, обговоренні доповідей, підготовка доповідей, тестування, виконання самостійних робіт, захист лабораторних робіт. Критерії оцінки поточного контролю викладач повідомляє на першому занятті та перед кожними оцінюванням. Підсумковий контроль: залік, екзамен.
Інтегральна компетентність, загальні компетентності (ЗК)	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційних технологій (кібербезпека), що передбачає ідентифікацію та використання інформації для прийняття рішень. ЗК 2. Знання та розуміння предметної області та розуміння професії.
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. 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 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.

ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ТЕМАМИ

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 секретної інформації. Державна таємниця.

Переліки відомостей, згідно до яких інформацію відносять до певного виду. Переліки службової інформації, наприклад (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’єнання 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 нав’язування.

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 розвідок 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. Виявлювачі порожнечь. Металошукачі. Рентгенівські апарати. Класифікація засобів радіовиявлення: індикатори електромагнітного поля, радіочастотоміри та інтерцептори. Прилади виявлення пристроїв прихованого знімання інформації. Багатофункціональні пошукові прилади. 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 та 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 секретної 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 секретної 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 контрою 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. 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.	
Програмні результати навчання (ПРН)	ПРН 5. Адаптуватися в умовах часто зміни технологій професійно діяльності, прогнозувати кінцевий результат ПРН 16. Реалізовувати комплексн системи захисту інформації автоматизованих системах (АС організації (підприємства) відповідно д вимог нормативно-правових документів ПРН 36. Виявляти небезпечні сигнали технічних засобів. ПРН 37 Вимірювати параметри небезпечних та завадових сигналів під

	час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
Критерії оцінювання результатів навчання	Оцінювання навчальної дисципліни проводиться за результатами поточного та підсумкового контролю: - поточний контроль - 50 балів; - підсумковий контроль - 50 балів. Оцінка за поточний контроль складається з оцінювання аудиторної та самостійної роботи здобувача вищої освіти. Оцінка за аудиторну роботу визначається як середнє арифметичне балів, які ним отримані на заняттях (здобувач має отримати не менш 5 позитивних оцінок) з коефіцієнтом 5. Оцінка за самостійну роботу визначається як середнє арифметичне балів, які отримані здобувачем за: реферати, програми

	(здобувач має підготувати не менш 2 проектів) з коефіцієнтом 5. Підсумкові бали з навчальної дисципліни визначаються як сума балів, які отримані здобувачем протягом семестру, та балів, які набрані на підсумковому контролі (екзамені).

ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS

Оцінка в балах	**Оцінка за національною шкалою**	**Оцінка за шкалою ECTS**	
		Оцінка	**Пояснення**
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.
94-96			
90-93			
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.
80-84			
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.

70-74	Задовільно (“зараховано”)	D	**„Задовільно”** – теоретичний зміст курсу освоєний не повністю, але прогалинине 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.
65-69			
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.
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
21-40			
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 приведе до значимого підвищення якості виконання навчальних

			завдань, робота, що потребує повної переробки

Перелік питань, 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 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 (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 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.

ОСНОВНА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна та наукова література:

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. Лаптєв О.А. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. – К. ДУТ, 2020 – 326 с.
3. Лаптєв О.А. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: Навчальний посібник / О.А. Лаптєв, 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.

ДОДАТКОВА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна та наукова література:

5. 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.
6. 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.

7. 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.
8. 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.
9. 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:

10. 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.
11. 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.
12. 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.
13. 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.
14. 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.

Інформаційні ресурси в Інтернеті:

1. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws.
2. 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.
3. 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/.
4. 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.
5. 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.