

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
Кафедра комп'ютерних технологій та інформаційної безпеки

Код за ОПІ:

OK7

“ЗАТВЕРДЖУЮ”

Проректор з науково-педагогічної
роботи, к.т.н., доцент



С.О. Слободян

»

2025 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Program of the Discipline

**ТЕХНОЛОГІЇ СТВОРЕННЯ ТА ЗАСТОСУВАННЯ
КОМПЛЕКСІВ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ
ДОСТУПОМ**

**Technologies for creation and application restricted information
trusted protect complexes**

Рівень вищої освіти	<u>другий (магістерський)</u>
Тип дисципліни	<u>обов'язкова</u>
Мова викладання	<u>українська</u>

Миколаїв 2025 рік

Робоча програма навчальної дисципліни «Технології створення та застосування комплексів захисту інформації з обмеженим доступом» є однією із складових підготовки студентів, що навчаються за освітньою програмою ОПП «Системи технічного захисту інформації, автоматизація її обробки», спеціальності F5 «Кібербезпека та захист інформації», галузі знань F «Інформаційні технології»

Розробник: Нужний С.М., доцент кафедри комп'ютерних технологій та інформаційної безпеки, канд. техн. наук, доцент

Проект робочої програми навчальної дисципліни «Технології створення та застосування комплексів захисту інформації з обмеженим доступом» узгоджено з гарантом освітньої програми.

Гарант освітньої програми «Системи технічного захисту інформації, автоматизація її обробки»

Передерій В.І., д.т.н., професор _____

Проект робочої програми навчальної дисципліни «Технології створення та застосування комплексів захисту інформації з обмеженим доступом» розглянуто на засіданні кафедри КТІБ.

Протокол від «24» 04 2025 р. № 12

Завідувач кафедри КТІБ _____ к.т.н., доцент Нужний С.М.

Проект робочої програми навчальної дисципліни «Технології створення та застосування комплексів захисту інформації з обмеженим доступом» розглянуто методичною радою Навчально-наукового інституту автоматики та електротехніки.

Протокол від «15» 05 2025 р. № 5

Заступник голови МР ННІАЕ _____ к.т.н., доцент Новогрецький С.М.

Проект робочої програми навчальної дисципліни «Технології створення та застосування комплексів захисту інформації з обмеженим доступом» погоджено з навчальним відділом

Начальник відділу _____ к.т.н., доцент Лабарткава А.В.

Робоча програма навчальної дисципліни «Технології створення та застосування комплексів захисту інформації з обмеженим доступом» затверджена Навчально-методичною радою НУК

Протокол № 5 від «21» 05 2025 року.

Голова НМР НУК _____ к.т.н., доцент Слободян С.О.

ЗМІСТ

ВСТУП	4
1. Опис навчальної дисципліни	5
2. Мета вивчення навчальної дисципліни	6
3. Передумови для вивчення дисципліни	7
4. Очікувані результати навчання	7
5. Програма навчальної дисципліни	9
6. Методи навчання, засоби діагностики результатів навчання та методів їх демонстрування	20
7. Форми поточного і підсумкового контролю	21
8. Критерії оцінювання результатів навчання	23
9. Засоби навчання	25
10. Рекомендовані джерела інформації	26
Зміни та доповнення	30

ВСТУП

Анотація

Ефективний захист інформації з обмеженим доступом (ІзОД), що циркулює на об'єкті інформаційної діяльності (ОІД), в сучасних умовах можливий тільки при комплексному підході та дотримання вимог нормативних документів Держспецзв'язку. Результатом такого підходу є розробка та експлуатація комплексних системи захисту інформації (КСЗІ). Отримання слухачами курсу теоретичних знань та практичних навичок проектування і експлуатації КСЗІ є базовими програмними результатами навчання та фахових компетентностей.

Програмою передбачається, за умови отримання студентами відповідної форми допуску до ІзОД, ознайомлення слухачів з документами категорії ДСК та «Т».

Ключові слова: комплексна система захисту інформації, модель загроз, модель каналу витоку інформації

Abstract

Effective protection of restricted information (RI), circulating on the object of information activity (OIA), in modern conditions is possible only with a comprehensive approach and compliance with the requirements of the regulatory documents of the State Special Communications Service. The result of this approach is the development and operation of comprehensive information protection systems (CIPS). The students' acquisition of theoretical knowledge and practical skills in the design and operation of CIPS are the basic program results of training and professional competences.

Keywords: complex information protection system, threat model, information leakage channel model, restricted information, object of information activity

1 Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів – 8	Галузь знань F «Інформаційні технології» Спеціальність: F5 «Кібербезпека та захист інформації»	Обов’язкова	
Модулів – 2	Освітня програма «Системи технічного захисту інформації, автоматизація її обробки»	Рік підготовки	
Змістових модулів – 6		1-й	1-й
Загальна кількість годин – 240		Семестр	
		1-й та 2-й	1-й та 2-й
Тижневих годин для денної форми навчання: Аудиторних: 1-й сем. – 3 год; 2-й сем. – 3 год; Самостійної роботи: 1-й сем. – 7 год; 2-й сем. – 3 год.	Рівень вищої освіти: другий (магістерський)	Аудиторні:	
		Лекції, год	
		30	18
		Лабораторні роботи, год	
		30	18
		Практичні роботи, год	
		30	18
		Самостійна робота, год	
		150	186
		Види контролю: екзамен (1-й та 2-й семестри)	
Форма контролю: усна, письмова			

2. Мета та завдання навчальної дисципліни

Метою вивчення навчальної дисципліни «Технології створення та застосування комплексів захисту інформації з обмеженим доступом» є ознайомлення студентів із основами побудови, проектування, впровадження і супроводження роботи КСЗІ на ОІД критичної інфраструктури. В процесі навчання передбачається вивчення нормативних документів та технологій проведення робіт з використанням спеціальних технічних засобів, в тому числі й в умовах забезпечення режиму секретності, на підприємствах, установах, організаціях з різними формами власності, по визначенню рівня захищеності ІзОД.

Вивчення дисципліни повинно забезпечити набуття студентами наступних **компетентностей**:

Інтегральна компетентність:

Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності:

(ЗК-6) Здатність діяти соціально відповідально та громадсько свідомо.

Фахові компетентності:

(КФ-2) Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки;

(КФ-3) Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури;

(КФ-4) Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог;

(КФ-6) Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації;

(КФ-7) Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому;

(КФ-8) Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації;

(КФ-11) Здатність виявляти закладні пристрої на об'єктах інформаційної діяльності (як члени команди);

(КФ-12) Здатність виконувати передпроектні роботи щодо систем та комплексів захисту інформації;

(КФ-13) Здатність проводити спеціалізовані дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності;

(КФ-14) Здатність впроваджувати(активізувати) програмні та апаратні засоби захисту інформації в системах і на об'єктах;

(КФ-15) Здатність адмініструвати системи, мережі та системи безпеки інформації;

(КФ-16) Здатність проводити оцінку відповідності (держану експертизу) програмних засобів технічного та криптографічного захисту інформації;

(КФ-17) Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимог технічного та організаційного спрямування щодо системи технічного криптографічного захисту інформації.

3. Передумови для вивчення навчальної дисципліни

Для ефективного вивчення дисципліни «Технології створення та застосування комплексів захисту інформації з обмеженим доступом», студенти повинні засвоїти матеріал з дисциплін :

- Комплексні системи захисту інформації;
- Методи та засоби захисту інформації;
- Поля і хвилі в системах технічного захисту інформації;
- Безпека інформаційних та комунікаційних систем;
- Управління інформаційною безпекою.

4. Очікувані результати навчання

Основними (програмними) результатами навчання з дисципліни «Технології створення та застосування комплексів захисту інформації з обмеженим доступом» є:

(РН-2) Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах;

(РН-3) Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі;

(РН-5) Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

(РН-6) Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення;

(РН-7) Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки;

(РН-8) Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури;

(РН-9) Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки;

(РН-10) Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації;

(РН-11) Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації;

(РН-12) Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому;

(РН-14) Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій,

бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому;

(РН-19) Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності;

(РН-20) Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та\або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик;

(РН-23) Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та\або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації;

(РН-24) Приймати обґрунтовані рішення з виконання передпроектних робіт щодо систем та комплексів захисту інформації, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

Відповідність результатів навчання Професійним стандартам

№ з/п	ОПП «Системи технічного захисту інформації, автоматизація її обробки»	ПС «Фахівець сфери захисту інформації»		Примітки
1	РН2	A1.31 B1.31 Г1.31	A1.Y2 B1.Y1 Г1.Y5	
2	РН3	B1.31 Г1.31	B1.Y3; B1.Y4 Г2.Y3	
3	РН5	A3.31 B4.33	A3.Y5 B4.Y2; B4.Y3	
4	РН6	B1.31; B1.35; B2.32; B2.34 Г1.31	B1.Y1; B1.Y2; B2.Y1; B2.Y4 Г1.Y3	
5	РН7	B1.33 Г1.36; Г2.37	B1.Y2 Г1.Y5; Г2.Y3	
6	РН8	B3.36 Г1.31; Г1.33; Г2.31 Д1.31	B3.Y1; B3.Y3 Г1.Y2; Г2.Y3; Г2.Y4 Д1.Y3; Д1.Y4	
7	РН9	B2.32 B1.31 Г1.35; Г2.35 Д1.34	B2.Y1 B1.Y1 Г1.Y1; Г1.Y3; Г1.Y4; Г2.Y2 Д1.Y4	
8	РН10	A1.35; A1.37 B1.31; B1.34 B1.31; B2.31; B3.35 Д2.31	A1.Y1; A1.Y4 B1.Y1 B1.Y1; B2.Y1; B3.Y1 Д2.Y1	
9	РН11	B1.35; B2.37 B5.31; B5.32	B1.Y1; B2.Y1 B5.Y3	
10	РН12	A1.37; A2.36 B2.35 B2.31; B3.31; B4.33	A1.Y4; A2.Y2 B2.Y1 B2.Y1; B3.Y1; B4.Y3	
11	РН14	A1.35; A2.31	A1.Y1; A1.Y4; A2.Y2	

		Б1.34 В4.31 Г1.33	Б1.У3 В4.У1 Г1.У1; Г1.У5	
12	РН19	А2.36 В4.32 Г1.31	А2.У2 В4.У4 Г1.У3	
13	РН20	А2.36 В1.31; В4.32 Д1.31	А2.У2 В1.У3; В4.У4 Д1.У5	
14	РН23	А1.31 Б2.31 Г1.31; Г1.36 Д1.31	А1.У1 Б2.У2 Г1.У2 Д1.У1	
15	РН24	Б1.31 В1.31; В4.31 Г1.33; Г1.36 Д1.32	Б1.У1; Б1.У3 В1.У1; В1.У4; В4.У2 Г1.У3 Д1.У41	

5. Програма навчальної дисципліни

Модуль 1

Змістовий модуль 1. Технологія створення КСЗІ на ОІД

Тема 1. Узагальнений алгоритм. Правове та нормативне забезпечення робіт. Концепція безпеки об'єкта. Склад. Вимоги. Аналіз інформаційних та матеріальних потоків, місць їх зберігання та стану захисту інформації на об'єкті. Акти категоріювання інформації, носіїв та приміщень. Комісії, їх склад. [1–5,10, 34,35]

Тема 2. Комісія по визначенню каналів витоку інформації та загроз її захищеності, цілісності та доступності. Їх склад та обов'язки. Технічні вимоги на створення КСЗІ/КТЗЗІ. Наказ на створення КСЗІ/КТЗЗІ. Технічне завдання на КСЗІ. Структура. Вимоги [6,10,11,27,28,34,35]

Тема 3. Ліцензіати та ліцензисти. Розподіл робіт по виконавцям. Розробка РКД. Виконання робіт по реконструкції ОІД та монтажу систем і обладнання. Випробування обладнання та КСЗІ. Навчання персоналу. Нормативні документи по проектуванню та експлуатації КСЗІ [10,11,20,27-29,34,35]

Змістовий модуль 2. Проведення спеціального обстеження приміщення

Тема 4. Методика проведення моніторингу каналів витоку інформації, обстеження та виявлення (локалізації) ТЗР в КЗ. Апаратне та апаратно-технічне забезпечення, яке дозволене до використання ДССЗЗІ. Організаційне та кадрове забезпечення. Розробка «Методики виявлення закладних пристроїв» [7-9,12-26,33]

Тема 5. Проведення спеціального обстеження приміщення. Технічне забезпечення проведення спеціального обстеження приміщення на виявлення та локалізацію закладних пристроїв. [12-18,25,31,33-35]

Тема 6. Проведення спеціального обстеження приміщення. Пошук закладних пристроїв за видами каналів передачі інформації. Особливості проведення спеціального обстеження з використанням апаратно-програмного комплексу АКОР-3ПКМ [12-15,17,18,25,33-35]

Тема 7 Проведення спеціального обстеження приміщення. Дослідження приміщень на наявність акустичного та віброакустичного каналів витоку інформації. [12-15,17,18,25,33-35]

Тема 8. Проведення спеціального обстеження приміщення. Методика виконання робіт на завершеному етапі комплексної перевірки приміщень та програмних комплексів [12,15,21,26,28,29,31-35]

Модуль 2

Змістовий модуль 3. Організація роботи відділу ТЗІ

Тема 9. Організація роботи відділу ТЗІ. Аналіз причин виникнення ТКВІ. Інсайтери – основне джерело інформації для несанкціонованого отримання та перехоплення інформації зловмисниками. Методи виявлення та протидія процедурі вербовки співробітників. [6,34-43]

Тема 10. Методи пошуку та залучення інсайдерів до співпраці по виявленню фактів та намагань вербовки. Взаємодія відділів ТЗІ, РСО та хорони об'єкту. Оцінка ефективності. [34-43]

Змістовий модуль 4. Захищений документообіг

Тема 11. Основні поняття, визначення, класифікація. Системи захисту інформації від НСД на АС-1, 2 та 3 класів. Організаційне, правове, технічне, програмне та інформаційне забезпечення. Стійкість до злому. [31,32,34,43]

Тема 12. Системи захисту інформації від НСД та захищеного документообігу для АС-1 та АС-2 класів. Програмні комплекси «Лоза» та «Гриф». Структура. Організаційне, правове, технічне та інформаційне забезпечення. Демаскуючі фактори. Стійкість до злому. [31,32,34,43]

Тема 13. Системи електронного документообігу Megapolis.DocNet та АСКОД. Структура. Організаційне, правове, технічне та інформаційне забезпечення. Вразливості та стійкість до злому. [31,32,34,43]

Тема 14. Системи електронного документообігу. Захищений документообіг на основі набору програмних засобів Google-додатків. [31,32,34,43]

Тема 15. Програмний комплекс автоматизації центрів надання адміністративних послуг – інформаційна система «Вулик». Проект EGOV4UKRAINE. Система «Трембіта» (платформа обміну даними X-ROAD). [31,32,34,43]

Тема 16. Системи зберігання та надання електронних послуг в Україні. Платформи та портали. Національний реєстр електронних інформаційних ресурсів. Портали електронних послуг «<https://www.rada.gov.ua>», «<https://www.kmu.gov.ua/>» та «<https://diia.gov.ua>». Структура. Організаційне, правове, технічне та інформаційне забезпечення. Вразливості та стійкість до злому. [31,32,34,43]

ТЕМАТИЧНИЙ ПЛАН НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин									
	денна форма					заочна форма				
	усього	у тому числі				усього	у тому числі			
		л	лаб	пр	с.р.		л	лаб	пр	с.р.
Модуль 1 (М1)										
Змістовий модуль 1. Технологія створення КСЗІ на ОІД.										
Тема 1. Узагальнений алгоритм. Правове та нормативне забезпечення робіт. Концепція безпеки об'єкта. Склад. Аналіз інформаційних та матеріальних потоків, місць їх зберігання та стану захисту інформації на об'єкті. Акти категоріювання інформації, носіїв та приміщень. Комісії, їх склад.	15	2	0	2	11	60	4	0	2	18
Тема 2. Комісія по визначенню каналів витоку інформації та загроз її захищеності, цілісності та доступності. Їх склад та обов'язки. Технічні вимоги на створення КСЗІ/КТЗЗІ. Наказ на створення КСЗІ/КТЗЗІ. Технічне завдання на КСЗІ. Структура. Вимоги	15	2	0	2	11					18
Тема 3. Ліцензіати та ліцензисти. Розподіл робіт по виконавцям. Розробка РКД. Виконання робіт по реконструкції ОІД та монтажу систем і обладнання. Випробування та експлуатація обладнання та КСЗІ. Навчання персоналу. Нормативні документи по проектуванню та експлуатації КСЗІ	15	2	0	0	13					18
Разом за змістовим модулем 1	45	6	0	4	35	60	4	0	2	54
Змістовий модуль 2. Проведення спеціального обстеження приміщення										

Назви змістових модулів і тем	Кількість годин									
	денна форма					заочна форма				
	усього	у тому числі				усього	у тому числі			
		л	лаб	пр	с.р.		л	лаб	пр	с.р.
Тема 4. Методика проведення моніторингу каналів витоку інформації, обстеження та виявлення (локалізації) ТЗР в КЗ. Апаратне та апаратно-технічне забезпечення, яке дозволене до використання ДССЗЗІ. Організаційне та кадрове забезпечення. Розробка «Методики виявлення закладних пристроїв»	15	2	0	3	10	90	5	9	7	14
Тема 5. Проведення спеціального обстеження приміщення. Технічне забезпечення проведення спеціального обстеження приміщення на виявлення та локалізацію закладних пристроїв.	30	2	6	2	20					14
Тема 6. Проведення спеціального обстеження приміщення. Пошук закладних пристроїв за видами каналів передачі інформації. Особливості проведення спеціального обстеження з використанням апаратно-програмного комплексу АКОР-ЗПКМ	15	2	4	2	7					14
Тема 7 Проведення спеціального обстеження приміщення. Дослідження приміщень на наявність акустичного та віброакустичного каналів витоку інформації.	15	2	3	2	8					14
Тема 8. Проведення спеціального обстеження приміщення. Методика виконання робіт на завершеному етапі комплексної перевірки приміщень та програмних комплексів	30	1	2	2	25					13
Разом за змістовим модулем 2	105	9	15	11	70	90	5	9	7	69
Разом за модулем 1	150	15	15	15	105	150	9	9	9	123

Назви змістових модулів і тем	Кількість годин									
	денна форма					заочна форма				
	усього	у тому числі				усього	у тому числі			
		л	лаб	пр	с.р.		л	лаб	пр	с.р.
Модуль 2 (М2)										
Змістовий модуль 3. Організація роботи відділу ТЗІ										
Тема 9. Організація роботи відділу ТЗІ. Аналіз причин виникнення ТКВІ. Інсайдери – основне джерело інформації для несанкціонованого отримання та перехоплення інформації зловмисниками. Методи виявлення та протидія процедурі вербовки співробітників	15	2	2	2	9	30	2	2	2	12
Тема 10. Методи пошуку та залучення інсайдерів до співпраці по виявленню фактів та намагань вербовки. Взаємодія відділів ТЗІ, РСО та хорони об’єкту. Оцінка ефективності	15	2	2	2	9					12
Разом за змістовим модулем 3	30	4	4	4	18	30	2	2	2	24
Змістовий модуль 4. Організація роботи відділу ТЗІ										
Тема 11. Основні поняття, визначення, класифікація. Системи захисту інформації від НСД на АС-1, 2 та 3 класів. Організаційне, правове, технічне, програмне та інформаційне забезпечення. Стійкість до злому	15	2	2	4	7	60	7	7	7	7
Тема 12. Системи захисту інформації від НСД та захищеного документообігу для АС-1 та АС-2 класів. Програмні комплекси «Лоза» та «Гриф». Структура. Організаційне, правове, технічне та інформаційне забезпечення. Демаскуючі фактори. Стійкість до злому	15	2	2	4	7					7

Назви змістових модулів і тем	Кількість годин									
	денна форма					заочна форма				
	усього	у тому числі				усього	у тому числі			
		л	лаб	пр	с.р.		л	лаб	пр	с.р.
Тема 13. Системи електронного документообігу Megapolis.DocNet та АСКОД. Структура. Організаційне, правове, технічне та інформаційне забезпечення. Вразливості та стійкість до злому	10	2	2	3	3					6
Тема 14. Системи електронного документообігу Захищений документообіг на основі набору програмних засобів Google-додатків	7	2	2	0	3					6
Тема 15. Програмний комплекс автоматизації центрів надання адміністративних послуг – інформаційна система «Вулик». Проект EGOV4UKRAINE. Система «Трембіта» (платформа обміну даними X-ROAD)	8	2	2	0	4					7
Тема 16. Системи зберігання та надання електронних послуг в Україні. Платформи та портали. Національний реєстр електронних інформаційних ресурсів. Портали електронних послуг « https://www.rada.gov.ua », « https://www.kmu.gov.ua/ » та « https://diia.gov.ua ». Структура. Організаційне, правове, технічне та інформаційне забезпечення. Вразливості та стійкість до злому	5	1	1	0	3					6
Разом за змістовим модулем 4	60	11	11	11	27	60	7	7	7	39
Разом за модулем 2	90	15	15	15	45	90	9	9	9	63
Разом за дисципліну	240	30	30	30	150	240	18	18	18	186

ТЕМИ ЛАБОРАТОРНИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин
1	Апаратура для пошуку пристроїв несанкціонованого доступу до конфіденційної аудіоінформації. Апаратно-програмний комплекс «АКОР-2»	4
2	Дослідження методів протидії витоку мовної інформації за межі контрольованої зони при використанні зловмисником мікрофонів направленої дії	4
3	Апаратура для пошуку пристроїв несанкціонованого доступу до конфіденційної аудіоінформації. Апаратно-програмний комплекс DiGiScan EX	4
4	Апаратура для пошуку пристроїв несанкціонованого доступу. Тепловизор FLIR E4	4
5	Апаратура для пошуку пристроїв несанкціонованого доступу. Індикатор поля	2
6	Захищений документообіг. Системи захисту інформації «Лоза».	2
7	Захищений документообіг. Системи захисту інформації «Гриф»	2
8	Оцінювання відповідності систем, комплексів та засобів захисту інформації вимогам нормативних документів та умовам	2
9	Виявлення та дослідження (оцінювання) загроз для інформаційних ресурсів об'єкту критичної інфраструктури на базі відкритої інформації	2
10	Оцінювання відповідності (атестація) комплексу технічного, криптографічного та програмного захисту інформації об'єкту критичної інфраструктури	2
11	Дослідження систем і комплексів захисту інформації, моніторинг та аудит загроз для автоматизованої системи обробки інформації на основі ОС Windows 11 та/або Linux	2
Разом		30¹

Примітка.

1) Студенти заочної форми виконують лабораторні роботи згідно індивідуального графіку бригади, загальним об'ємом 9 годин із переліку вказаних тем лабораторних робіт

ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин
1	Концепція безпеки об'єкта. Акти категоріювання інформації, носіїв та приміщень.	2
2	Комісія по визначенню каналів витоку інформації та загроз її захищеності, цілісності та доступності. Наказ на створення КСЗІ/КТЗЗІ. Технічне завдання на КСЗІ	2
3	Розробка РКД. Виконання робіт по реконструкції ОІД та монтажу систем і обладнання. Випробування та експлуатація обладнання та КСЗІ.	2
4	Методика проведення моніторингу каналів витоку інформації, обстеження та виявлення (локалізації) ТЗР в КЗ.	2
5	Методика проведення спеціального обстеження приміщення. Технічне забезпечення проведення спеціального обстеження приміщення на виявлення та локалізацію закладних пристроїв.	2
6	Методика проведення обстеження приміщення з використанням апаратно-програмного комплексу АКОР-ЗПКМ	2
7	Методика проведення обстеження приміщення на наявність акустичного та віброакустичного каналів витоку інформації	2
8	Методика проведення обстеження приміщення на завершеному етапі комплексної перевірки приміщень та програмних комплексів	1
9	Організація роботи відділу ТЗІ. Методи виявлення та протидія процедурі вербовки співробітників	2
10	Методи пошуку та залучення інсайдерів до співпраці по виявленню фактів та намагань вербовки.	2
11	Системи захисту інформації від НСД на АС-1, 2 та 3 класів. Організаційне, технічне та інформаційне забезпечення.	2
12	Системи захисту інформації від НСД для АС-1 та АС-2 класів. Програмні комплекси «Лоза» та «Гриф».	2
13	Системи електронного документообігу Megapolis.DocNet та АСКОД.	2
14	Захищений документообіг на основі набору програмних засобів Google-додатків	2
15	Інформаційна система «Вулик». Проект EGOV4UKRAINE. Система «Трембіта» (платформа обміну даними X-ROAD)	2
16	Системи зберігання та надання електронних послуг в Україні. Платформи та портали. Національний реєстр електронних інформаційних ресурсів.	1
Разом		30

САМОСТІЙНА РОБОТА

Метою самостійної роботи є повторення й осмислення студентом основних питань кожної теми, висвітлених на лекційних, практичних і лабораторних заняттях.

Самостійна робота проводиться в лабораторіях НУК, читальних залах, на об'єктах майбутньої діяльності і/або вдома. Результати цієї роботи фіксуються студентом в індивідуальному робочому зошиті (конспекті).

№ з/п	Назва теми	Кількість годин	
		Денна форма навчання	Заочна форма навчання
Модуль 1 (М1)			
1	До теми 1. Узагальнений алгоритм. Правове та нормативне забезпечення робіт. Концепція безпеки об'єкта. Склад. Аналіз інформаційних та матеріальних потоків, місць їх зберігання та стану захисту інформації на об'єкті. Акти категоріювання інформації, носіїв та приміщень. Комісії, їх склад.	11	18
2	До теми 2. Комісія по визначенню каналів витоку інформації та загроз її захищеності, цілісності та доступності. Їх склад та обов'язки. Технічні вимоги на створення КСЗІ/КТЗЗІ. Наказ на створення КСЗІ/КТЗЗІ. Технічне завдання на КСЗІ. Структура. Вимоги	11	18
3	До теми 3. Ліцензіати та ліцензисти. Розподіл робіт по виконавцям. Розробка РКД. Виконання робіт по реконструкції ОІД та монтажу систем і обладнання. Випробування та експлуатація обладнання та КСЗІ. Навчання персоналу. Нормативні документи по проектуванню та експлуатації КСЗІ	13	18
4	До теми 4. Методика проведення моніторингу каналів витоку інформації, обстеження та виявлення (локалізації) ТЗР в КЗ. Апаратне та апаратно-технічне забезпечення, яке дозволене до використання ДССЗІ. Організаційне та кадрове забезпечення. Розробка «Методики виявлення закладних пристроїв»	10	14
5	До теми 5. Проведення спеціального обстеження приміщення. Технічне забезпечення проведення спеціального обстеження приміщення на виявлення та локалізацію закладних пристроїв.	20	14
6	До теми 6. Проведення спеціального обстеження приміщення. Пошук закладних пристроїв за видами каналів передачі інформації. Особливості проведення спеціального обстеження з використанням апаратно-програмного комплексу АКОР-ЗПКМ	7	14
7	До теми 7. Проведення спеціального обстеження приміщення. Дослідження приміщень на наявність акустичного та віброакустичного каналів витоку інформації.	8	14
8	До теми 8. Проведення спеціального обстеження приміщення. Методика виконання робіт на завершеному етапі комплексної перевірки приміщень та програмних комплексів	25	13
Разом за модулем 1		105	123

№ з/п	Назва теми	Кількість годин	
		Денна форма навчання	Заочна форма навчання
9	До теми 9. Організація роботи відділу ТЗІ. Аналіз причин виникнення ТКВІ. Інсайтери – основне джерело інформації для несанкціонованого отримання та перехоплення інформації зловмисниками. Методи виявлення та протидія процедури вербовки співробітників.	9	12
10	До теми 10. Методи пошуку та залучення інсайдерів до співпраці по виявленню фактів та намагань вербовки. Взаємодія відділів ТЗІ, РСО та хорони об'єкту. Оцінка ефективності	9	12
11	До теми 11. Основні поняття, визначення, класифікація. Системи захисту інформації від НСД на АС-1, 2 та 3 класів. Організаційне, правове, технічне, програмне та інформаційне забезпечення. Стійкість до злому.	7	7
12	До теми 12. Системи захисту інформації від НСД та захищеного документообігу для АС-1 та АС-2 класів. Програмні комплекси «Лоза» та «Гриф». Структура. Організаційне, правове, технічне та інформаційне забезпечення. Демаскуючі фактори. Стійкість до злому	7	7
13	До теми 13. Системи електронного документообігу Megapolis.DocNet та АСКОД. Структура. Організаційне, правове, технічне та інформаційне забезпечення. Вразливості та стійкість до злому.	3	6
14	До теми 14. Системи електронного документообігу Захищений документообіг на основі набору програмних засобів Google-додатків	3	6
15	До теми 15. Програмний комплекс автоматизації центрів надання адміністративних послуг – інформаційна система «Вулик». Проект EGOV4UKRAINE. Система «Трембіта» (платформа обміну даними X-ROAD)	4	7
16	До теми 16. Системи зберігання та надання електронних послуг в Україні. Платформи та портали. Національний реєстр електронних інформаційних ресурсів. Портالي електронних послуг « https://www.rada.gov.ua », « https://www.kmu.gov.ua/ » та « https://diia.gov.ua ». Структура. Організаційне, правове, технічне та інформаційне забезпечення. Вразливості та стійкість до злому	3	6
Разом за модулем 2		45	63
Разом		150	186

Навчальний матеріал дисципліни, передбачений для засвоєння здобувачем вищої освіти в процесі самостійної роботи, включається в завдання поточного контролю разом із навчальним матеріалом, який опрацьовувався при проведенні навчальних занять.

Денна форма навчання

Розподіл годин самостійної роботи для денної форми навчання:

- підготовка до лекційних занять – 1 год. / 1 год. занять;
- самостійне опрацювання лекційних матеріалів – 1 год. / 1 год. занять;
- підготовка до лабораторних робіт – 2,0 год. / 1 год. занять;
- підготовка до практичних робіт – 0,8 год. / 1 год. занять;
- підготовка до контрольних заходів – 1,0 год. на 1 захід.

Заочна форма навчання

Розподіл годин самостійної роботи для заочної форми навчання:

- підготовка до лекційних занять – 3 год. / 1 год. занять;
- самостійне опрацювання лекційних матеріалів – 3 год. / 1 год. занять;
- підготовка до лабораторних робіт – 2,0 год. / 1 год. занять;
- підготовка до практичних робіт – 2 год. / 1 год. заняття;
- підготовка до контрольних заходів – 3 год. на 1 захід.

Розподіл годин підготовки самостійної роботи

№	Вид роботи	Кількість годин	
		Денна форма навчання	Заочна форма навчання
1	Підготовка до лекцій	30	42
2	Самостійне опрацювання окремих тем навчальної дисципліни	30	42
3	Підготовка до лабораторних робіт	30	18
4	Підготовка до практичних робіт	12	18
5	Підготовка до модульних контрольних робіт	3	3
Усього годин за модуль 1		105	123 ,
1	Підготовка до лекцій	15	21
2	Самостійне опрацювання окремих тем навчальної дисципліни	15	21
3	Підготовка до практичних робіт	9	15
4	Підготовка до модульних контрольних робіт	6	6
Усього годин за модуль 2		45	63
Разом за курсом		150	186

6. Методи навчання, засоби діагностики результатів навчання та методи їх демонстрування

Здобувач зобов'язаний вивчити теоретичний матеріал та здобути практичні навички у відповідності до тематичного плану навчальної дисципліни.

Методами навчання є:

- пояснення, демонстрування;
- лекція; відеометод;
- лабораторна робота, інструктаж;
- репродуктивний метод;
- проблемного викладу.

Засобами оцінювання результатів навчання є:

- модульні контрольні роботи;
- звіти з лабораторних робіт;
- індивідуальні та групові завдання;
- завдання на лабораторному обладнанні;
- комплексна контрольна робота (за необхідністю).

Методами демонстрування результатів навчання є:

- усні відповіді;
- письмові відповіді;
- виконання завдань із застосуванням комп'ютерної техніки;
- оформлення звітів з лабораторних робіт;
- презентації результатів виконаних завдань та досліджень.

Допускається застосування дистанційних технологій для діагностики результатів навчання.

7. Форми поточного та підсумкового контролю

Досягнення здобувача вищої освіти оцінюються за 100-бальною системою Університету.

Поточний контроль проводиться в межах навчальних занять і передбачає оцінювання теоретичної підготовки здобувачів вищої освіти із зазначених тем (у тому числі, самостійно опрацьованого матеріалу) та практичних навичок, набутих під час виконання лабораторних робіт.

Поточний контроль здійснюється протягом семестру в наступних формах:

- перевірка та захист звітів з лабораторних робіт;
- проведення та перевірка модульних контрольних робіт;
- контрольна робота на заочній формі навчання;
- семестрова атестація;
- перевірка конспекту лекцій;
- контроль відвідування занять.

Перевірка звіту з лабораторної роботи включає оцінювання правильності та повноти виконання завдання, правильності та повноти висновків, правильності оформлення звіту.

Процедура захисту звіту з лабораторної роботи включає один або декілька елементів:

- письмове викладення відповідей на запитання за тематикою роботи;
- усне опитування за тематикою роботи;
- виконання завдань із застосуванням комп'ютерної техніки.

При виконанні модульних контрольних робіт здобувач вищої освіти відтворює засвоєні знання шляхом надання письмових відповідей на поставлені запитання. На теоретичні запитання необхідно давати розгорнуті відповіді, супроводжуючи їх прикладами та ілюстраціями. Повнота відповідей оцінюється згідно з теоретичним матеріалом, наведеним у джерелах інформації для кожної теми. На тестові запитання потрібно вказати номер правильної відповіді та її формулювання.

Контрольна робота на заочній формі навчання має ті ж вимоги, виконується протягом семестру і здається до проведення підсумкового контролю.

Поточний модульний контроль проводиться з урахуванням даних поточного контролю за відповідний змістовний модуль і має на меті оцінку

результатів знань студента після вивчення матеріалу з логічно-завершеної частини дисципліни – змістового модуля.

Семестрова атестація дає змогу здійснити проміжну оцінку досягнень здобувача вищої освіти. В період семестрової атестації викладач оцінює результати поточного контролю та атестує чи не атестує здобувача вищої освіти.

За рішенням кафедри студентам, які брали участь у науково-дослідній роботі – роботі конференцій, студентських наукових гуртків, підготовці публікацій, а також були учасниками олімпіад, конкурсів, тощо можуть присуджуватися додаткові бали. Додаткові бали також можуть присуджуватися за результатами перевірки конспекту лекцій, контролю відвідування занять та за активність на лекціях і практичних заняттях.

За всі поточні контрольні заходи протягом семестру, з урахуванням додаткових балів, студент сумарно може отримати від 0 до 100 балів.

Умовою допуску студента до семестрового підсумкового контролю є мінімальна сума у 60 балів, яку студент повинен набрати у разі виконання всіх елементів модулів.

Семестровий підсумковий контроль з дисципліни проводиться відповідно до навчального плану у вигляді *екзамену* в терміни, встановлені графіком навчального процесу, та в обсязі навчального матеріалу, визначеному робочою програмою навчальної дисципліни.

Студент, який набрав за всі поточні контрольні заходи менше 60 балів або хоче отримати додаткові бали, пише додаткову семестрову залікову роботу (проводиться у письмовій формі), до якої він допускається, якщо має за виконання всіх передбачених елементів модулів не менше 40 балів. Максимальна кількість балів за залікову роботу становить 20 балів.

Зарахування кредитів навчального курсу можливо тільки після досягнення результатів, запланованих РПНД, що виражається в одній з позитивних оцінок, передбачених чинним законодавством.

8. Критерії оцінювання результатів навчання

При оцінюванні лабораторних робіт враховуються наступні критерії:

- виконання роботи та правильність виконання;
- наявність звіту, вчасність подачі та якість звіту;
- захист звіту.

Максимальна оцінка за кожну лабораторну роботу для ДФН – 6 балів.

Максимальна сумарна кількість балів для ДФН та ЗФН за лабораторні роботи – $6 \times 6 = 36$ балів (модуль 1), $5 \times 6 = 30$ балів (модуль 2)

Критерії оцінювання лабораторних робіт

Кількість балів	Критерії оцінювання
6	Роботу виконано самостійно, завдання виконано правильно. Звіт здано у встановлений термін, оформлення звіту повністю відповідає вимогам, у висновках проведено коректну інтерпретацію результатів. Студент надав правильні відповіді на всі питання захисту.
5	Робота виконана правильно з консультаціями викладача. Звіт здано у встановлений термін, можливі несуттєві помилки в оформленні звіту та незначні некоректності у висновках. Студент надав принципово правильні відповіді на питання захисту (без суттєвих помилок).
4	Роботу виконано із підказками викладача та незначними помилками. Звіт містить неточності у висновках та окремі помилки. Студент відповів на питання захисту частково чи з принциповими помилками.
2	Завдання виконано у повному об'ємі але з помилками. Звіт містить неточності у висновках та окремі помилки. Студент не відповів на питання захисту.
1	Завдання виконано не у повному об'ємі (не менше 70%). Надано звіт, що містить неточності і помилки. Студент не відповів на питання захисту.
0	Робота не виконана.

Для поточного модульного контролю студентами виконуються по 2 (дві) модульних контрольні роботи за матеріалами змістовних модулів за Модулем. Максимальний бал за кожне питання (тему) МКР – 3 бали. Загальна сума балів за модульні контрольні роботи для кожного модуля:

	Модуль 1			Модуль 2		
Контрольні роботи	МКР1	МКР2	Разом за модуль	МКР3	МКР4	Разом за модуль
Кількість балів	$3 \times 3 = 9$	$5 \times 3 = 15$	24	$3 \times 3 = 9$	$3 \times 3 = 9$	24

За заочною формою навчання в кінці кожного семестру виконується підсумкова залікова робота. Максимальна оцінка за підсумкову залікову роботу – 24 бали.

Критерії оцінювання задач та практичних завдань в МКР

Правильних відповідей, %	100	90	80	70	60	50	40	30	20	10
бал	3	2,7	2,4	2,1	1,8	1,5	1,2	0,9	0,6	0,3

Розподіл оцінки за змістовними модулями та видами контролю

Модуль 1	Денне форма		Заочна форма	
	Вид роботи	Кількість балів	Вид роботи	Кількість балів
ЗМ 1	Практичні роботи	2	Практичні роботи	2
	МКР 1	9	–	0
ЗМ 2	Лабораторні роботи	36	Лабораторні роботи	36
	Практичні роботи	5	Практичні роботи	5
	МКР 2	15	–	0
А	Атестація	5	–	0
КР	–	0	Контрольна робота	24
Конспект лекцій	Конспект	8	Конспект	13
Екзамен	Екзамен	20	Екзамен	20
Сума		100		100

Модуль 2	Денне форма		Заочна форма	
	Вид роботи	Кількість балів	Вид роботи	Кількість балів
ЗМ 3	Лабораторні роботи	15	Лабораторні роботи	15
	Практичні роботи	2	Практичні роботи	2
	МКР 3	6	–	0
ЗМ 4	Лабораторні роботи	15	Лабораторні роботи	15
	Практичні роботи	15	Практичні роботи	15
	МКР 4	14	–	0
А	Атестація	5	–	0
КР	–	0	Контрольна робота	20
Конспект лекцій	Конспект	8	Конспект	13
Екзамен	Екзамен	20	Екзамен	20
Сума		100		100

**Рівні підсумкової оцінки екзамену з дисципліни
(перерахунковий коефіцієнт – 0,4)**

Оцінка за 100-бальною шкалою університету / Grade according to 100-points scale of University	Оцінка за шкалою ЄКТС / Grade according to ECTS scale
90-100 (творчий рівень)/(creative level)	A (відмінно) / (excellent)
82-89 (високий рівень)/(high level)	B (дуже добре) / (very good)
74-81 (добрий рівень)/(good level)	C (добре) / (good)
64-73 (середній рівень)/(average level)	D (посередньо) / (average)
60-63 (задовільний рівень)/(satisfactory level)	E (достатньо) / (satisfactory)
35-59 (низький рівень)/(low level)	FX (незадовільно з можливістю повторного складання) / (unsatisfactory with the possibility to repass the exam)
1-34 (незадовільний рівень)/(unsatisfactory level)	F (незадовільно з обов'язковим повторним вивченням) / (unsatisfactory with the compulsory repeating of the course)

9. Засоби навчання

Апаратне забезпечення, необхідне для вивчення навчальної дисципліни, включає персональний комп'ютер (настільний або ноутбук) та спеціалізовані лабораторні стенди.

Програмне забезпечення, необхідне для вивчення навчальної дисципліни, включає операційну систему, спеціалізоване програмне забезпечення для інженерних розрахунків та моделювання технічних засобів, текстовий процесор та редактор растрових зображень (для підготовки звітів з практичних робіт); pdf-, djv-переглядач (для ознайомлення з джерелами інформації, представленими в електронному виді).

10. Рекомендовані джерела інформації

Базові

1. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва.
2. НД ТЗІ 1.1-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення.
3. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
4. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
5. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення.
6. НД ТЗІ 1.4-001-00 Типове положення про службу захисту інформації в автоматизованій системі.
7. НД ТЗІ 1.4-002-08 Радіолокатори нелінійні. Класифікація. Рекомендовані методи та засоби випробувань.
8. НД ТЗІ 1.5-001-00 Радіовиявлювачі. Класифікація. Загальні положення.
9. НД ТЗІ 1.5-002-12 Класифікатор засобів технічного захисту інформації.
10. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.
11. НД ТЗІ 1.6-005-13 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці”
12. НД ТЗІ 2.1-002-07 Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення.
13. НД ТЗІ 2.3-001-01 Радіовиявлювачі вимірювальні. Методи та засоби випробувань.
14. НД ТЗІ 2.3-002-01 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби пасивного

приховування мовної інформації. Нелінійні атенюатори та загороджувальні фільтри. Методика випробувань.

15. НД ТЗІ 2.3-003-01 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби активного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань.

16. НД ТЗІ 2.3-004-01 Радіовиявлювачі індикаторні. Методи та засоби випробувань.

17. НД ТЗІ 2.3-005-01 Радіовиявлювачі панорамні. Методи та засоби випробувань.

18. НД ТЗІ 2.3-006-01 Радіовиявлювачі аналізувальні. Методи та засоби випробувань.

19. НД ТЗІ 2.5-006-99 Класифікатор засобів копіювально-розмножувальної техніки.

20. НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.

21. НД ТЗІ 2.7-001-99 Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт.

22. НД ТЗІ 2.7-002-99 Методичні вказівки з використання засобів копіювально-розмножувальної техніки.

23. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.

24. НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу

25. НД ТЗІ 2.7-011-12 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки «Методики виявлення закладних пристроїв».

26. НД ТЗІ 2.7-013-16 Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99

27. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Перед проектні роботи.

28. НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

29. НД ТЗІ 3.6-001-00 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

30. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (Зі зміною № 1).

31. НД ТЗІ 3.7-002-99 Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова).

32. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

33. НД ТЗІ 4.7-001-01 Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби визначення наявності та віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань.

34. Наказ Держспецзв'язку №023 (ДСК) від 19.06.2015 р. зі змінами наказ № 01т від 23.01.2023 р.

35. Бюлетень 28 Інформаційно-аналітичний бюлетень. Системи і засоби технічних розвідок та їх носії. Випуск 28 за 2022 рік

36. Кара-Мурза С. Маніпуляція свідомістю. – «ЕКСМО-Прес», 2001

37. Exposure of Enemy Set-Ups. Електронний ресурс. Режим доступу: <https://drive.google.com/file/d/16t59k0G381jlasvlZM5i49MZ2wTnwsyA/view>

38. Intelligence Targets Abroad. Електронний ресурс. Режим доступу: <https://drive.google.com/file/d/1dWB8ak89PeNiQppP7IYNqc7FIO6TZmGM/view>

39. Political Intelligence from USSR Territory. Електронний ресурс. Режим доступу: <https://drive.google.com/file/d/1XxulRAgcXO4XIFW-YrNhi57uzAx3dGwB/view>

40. Communication with Agents. Електронний ресурс. Режим доступу: <https://drive.google.com/file/d/1NQPERpdFYjCkrQEO-mIcmDVk5PMDQzmm/view>

41. Acquisition and Training of Agent Recruiters. Електронний ресурс. Режим доступу: <https://drive.google.com/file/d/1EesGYnEONyKHuApCNtCcDOm84ZxnLeRG/view>

42. Use of Soviet Cultural Committee. Електронний ресурс. Режим доступу: https://drive.google.com/file/d/1kbcWaaaEbxz_lIFXNg9BRDtZKfo-xD1e/view

43. Зачепило В.С. Схорона державної таємниці: навч. посіб. / В.С. Зачепило, З.А. Шандра, І.Р. Опірський, І.Я. Тишик, Л.В. Мороз. – Львів: Видавництво Львівської політехніки, 2015. – 168 с.

Допоміжна

1. Комплексні системи санкціонованого доступу: навч. посіб. / О.І. Гарасимчук, В. Б. Дудикевич, В. А. Ромака; Нац. ун-т «Львів. політехніка». — Л. Вид-во Львів. політехніки, 2010. — 212 с.

2. Захист засобів і каналів телефонного зв'язку: навч. посіб. / В.Б. Дудикевич, В. В. Хома, Л. Т. Пархуць; Нац. ун-т «Львів. політехніка». — Л. : Вид-во Львів. політехніки, 2012. — 210 с.

3. Захист засобів і каналів телефонного зв'язку: навч. посіб. / В.Б. Дудикевич, В.В. Хома, Л.Т. Пархуць, Нац. ун-т «Львівська політехніка». — Львів: Вид-во Львівської політехніки, 2012

Зміни та доповнення