МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський державний екологічний університет

ЗАТВЕРДЖЕНО
на засіданні групи забезпечення
спеціальності 122 Комп'ютерні науки
від «22» 09 2020 року
протокол № 5
Голова групи (Мещеряков В.І.)

УЗГОДЖЕНО
Декан факультету
комп'ютерних наук, управління
та адміністрування
(Коваленко Л.Б.)

СИЛЛАБУС

навчальної дисципліни
ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЇ
(назва навчальної дисципліни)

122 Комп'ютерні науки
(шифр та назва спеціальності)

Комп'ютерні науки
(назва освітньої програми)

бакалавр	денна
(рівень вищої освіти)	(форма навчання)

4	8	4 / 120	екзамен
(рік навчання)	(семестр навчання)	(кількість кредитів ЄКТС/годин)	(форма контролю)

Інформаційних технологій
(кафедра)

Одеса, 2020 р.

Автори:

Фразе-Фразенко О.О., доцент кафедри інформаційних технологій, к.т.н., доцент

(прізвище, ініціали, посада, науковий ступінь, вчена звання)

(прізвище, ініціали, посада, науковий ступінь, вчена звання)

Поточна редакція розглянута на засіданні кафедри інформаційних технологій від «31» серпня 2020 року, протокол № 1.

Викладачі: лекції: Фразе-Фразенко О.О., доцент кафедри ІТ, к.т.н., доцент

(вид навчального заняття: прізвище, ініціали, посада, науковий ступінь, вчена звання)

лабораторні роботи: Бучинська І.В., ст. викладач кафедри ІТ

(вид навчального заняття: прізвище, ініціали, посада, науковий ступінь, вчена звання)

Перелік попередніх редакцій

Прізвища та ініціали авторів	Дата, № протоколу	Дата набуття чинності

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета	Закласти термінологічний фундамент, навчити студентів правильно проводити аналіз погроз інформаційній безпеці, основним методам, принципам, алгоритмам захисту інформації в комп'ютерних системах з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників.
Компетентність	СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури
Результат навчання	ПР15. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.
Базові знання	1. сучасні погрози безпеці інформаційним системам; 2. технічні методи і засоби захисту інформації; 3. криптографічні методи захисту інформації; 4. програмні методи і засоби захисту; 5. методи захисту інформації в розподілених інформаційних системах; 6. організаційно-правове забезпечення захисту інформації.
Базові вміння	1. аналізувати можливості несанкціонованого здобуття інформації потенційними порушниками; 2. аналізувати вплив комп'ютерних вірусів і шкідливих програм на безпеку комп'ютерних систем; 3. організовувати та виконувати практичні дій посадових осіб відділу захисту інформації відповідно до інструкцій і обов'язків.
Базові навички	1. Вирішення складних непередбачуваних задач і проблем у спеціалізованих сферах професійної діяльності та/або навчання, яке передбачає збирання та інтерпретацію інформації (даних), вибір методів та інструментальних засобів, застосування інноваційних підходів.
Пов'язані силлабуси	немає
Попередня дисципліна	БЖД та основи охорони праці

Наступна дисципліна	немає
Кількість годин	лекції: 27 практичні заняття: - лабораторні заняття: 27 семінарські заняття: - самостійна робота студентів: 66

2. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

2.1. Лекційні модулі

Код	Назва модуля та тем	Кількість годин	
		аудиторні	СРС
ЗМ-Л1	**Інформаційні загрози та несанкціонований доступ**		
	• Історія та основні принципи розвідки	2	2
	• Канали несанкціонованого отримання інформації	2	2
	• Класифікація каналів витоку інформації	2	
	• Канали витоку інформації при експлуатації ЕОМ	2	2
	• Методи і засоби несанкціонованого отримання інформації	2	2
	• Методи і засоби руйнування інформації	2	2
	• Інформаційне протиборство	2	2
	• Загрози інформації	2	2
ЗМ-Л2	**Методи та засоби захисту інформації**		
	• Підходи до створення КСЗІ	2	2
	• Технічні методи і засоби ЗІ	2	4
	• Програмні методи захисту	2	2
	• Криптографічний захист	2	2
	• Скремблювання.	2	
	• Стеганографія	1	2
	Разом:	27	26

Консультації:
Фразе-Фразенко Олексій Олексійович,
четвер, ауд. 319 НЛК № 1., час: 13.00-14.00

2.2. Практичний модуль

Код	Назва модуля та тем	Кількість годин	
		аудиторні	СРС
ЗМ-П1	• Формування паролів та методи їх зламу за допомогою атак	4	5
	• Криптографія та криптоаналіз, алгоритми шифрування та способи атак для розкриття зашифрованих даних	8	5
ЗМ-П2	• Алгоритми шифрування DES та 3DES, режими їх роботи та програмна реалізація	5	4
	• Алгоритм шифрування AES, режими його роботи та програмна реалізація	5	4
	• Систему RSA, режими її роботи та програмна реалізація	5	2
	Разом:	27	20

Лабораторні роботи проводяться в комп'ютерних класах кафедри інформаційних технологій (ауд. 319, 324, 327, 328, 329). Під час проведення лабораторних робіт використовується наступне програмне забезпечення: ПК з ОС Windows, Sublime Text, MS Excel, Спеціалізоване ПЗ для дослідження шифрів.

Консультації:
Бучинська Ірина Вікторівна, четвер, ауд. 330 НЛК № 1., час 14.00-15.00

2.3. Самостійна робота студента та контрольні заходи

Код модуля	Завдання на СРС та контрольні заходи	Кількість годин	Строк проведення
ЗМ-Л1	• Підготовка до лекційних занять • Підготовка до модульної контрольної роботи № 1	10 4	1-4 тижні 1-4 тижні
ЗМ-Л2	• Підготовка до лекційних занять • Підготовка до модульної контрольної роботи № 2	8 4	5-9 тижні 5-9 тижні
ЗМ-П1	• підготовка до усного опитування напередодні відповідної лабораторної роботи (обов'язкове) • підготовка до захисту звіту з лабораторних робіт (обов'язкове)	6 4	1-4 тижні 1-4 тижні
ЗМ-П2	• підготовка до усного опитування напередодні відповідної лабораторної роботи (обов'язкове) • підготовка до захисту звіту з лабораторних робіт (обов'язкове)	6 4	5-9 тижні 5-9 тижні
	Підготовка до іспиту	20	Сесія
	Разом:	66	

1. Методика проведення та оцінювання контрольного заходу для ЗМ-Л1.

Контроль проводиться після вивчення лекційного матеріалу модулів ЗМ-Л1 в формі тестової модульної контрольної роботи із використанням системи дистанційного навчання університету, МКР-1 тестового типу в якій студенти відповідають на 25 питань, які автоматично генеруються із банку тестових питань за відповідними лекціями. Результати роботи оцінюються в автоматичному режимі із використанням системи дистанційного навчання. Час, що виділяється на виконання МКР-1 не перевищує 1 академічної години.

Максимальна оцінка за контрольну роботу складає 25 балів або 1 бал за одну правильну відповідь. Критерії оцінювання результатів контрольного заходу: модуль вважається зарахованим, якщо надана вірна відповідь на 15 та більше питань тесту.

2. Методика проведення та оцінювання контрольного заходу для ЗМ-Л2.

Контроль проводиться після вивчення лекційного матеріалу модулів ЗМ-Л2, в формі тестової модульної контрольної роботи із використанням системи

дистанційного навчання університету, МКР-2 тестового типу в якій студенти відповідають на 25 питань що автоматично генеруються із банку тестових питань за відповідними лекціями. Результати роботи оцінюються в автоматичному режимі із використанням системи дистанційного навчання. Час, що виділяється на виконання МКР-1 не перевищує 1 академічної години.

Максимальна оцінка за контрольну роботу складає 25 балів або 1 бал за одну правильну відповідь. Критерії оцінювання результатів контрольного заходу: модуль вважається зарахованим, якщо надана вірна відповідь на 15 та більше питань тесту.

3. Методика підсумкового оцінювання контрольних заходів для всіх лекційних модулів.

Підсумкова оцінка за всі лекційні модулі дорівнює сумі набраних балів за лекційні модулі ЗМ-Л1, ЗМ-Л2 яка не може перевищувати 50 балів.

4. Методика проведення та оцінювання контрольного заходу для ЗМ-П1.

Методика проведення та оцінювання контрольного заходу для ЗМ-П1.

За весь практичний модуль встановлена максимальна оцінка 20 балів. За кожну з 2 лабораторних робіт встановлена максимальна оцінка 10 балів.

Контроль по кожній лабораторній роботі проводиться в формі:

усного опитування при підготовці до кожної лабораторної роботи з метою допуску до її виконання (кількість запитань – до 5, максимальна кількість балів – 4),

захисту результатів лабораторної роботи наведених у звіті до лабораторної роботи (кількість запитань залежить від ходу виконання студентом роботи і якості звіту, максимальна кількість балів – 6).

Для кожної лабораторної роботи, якщо студент за усне опитування одержав 2 і менше балів він не допускається до виконання роботи, а якщо більше – допускається.

Для кожної лабораторної роботи при захисті результатів студент може одержати до 6 балів.

Підсумковою оцінкою за кожну лабораторну роботу буде сума балів за усне опитування і захист результатів.

Підсумковою оцінкою за весь практичний модуль буде сума балів за всі лабораторні роботи.

5. Методика проведення та оцінювання контрольного заходу для ЗМ-П2.

За весь практичний модуль встановлена максимальна оцінка 30 балів. За кожну з 3 лабораторних робіт встановлена максимальна оцінка 10 балів.

Контроль по кожній лабораторній роботі проводиться в формі:

усного опитування при підготовці до кожної лабораторної роботи з метою допуску до її виконання (кількість запитань – до 5, максимальна кількість балів – 4),

захисту результатів лабораторної роботи наведених у звіті до лабораторної

роботи (кількість запитань залежить від ходу виконання студентом роботи і якості звіту, максимальна кількість балів – 6).

Для кожної лабораторної роботи, якщо студент за усне опитування одержав 2 і менше балів він не допускається до виконання роботи, а якщо більше – допускається.

Для кожної лабораторної роботи при захисті результатів студент може одержати до 6 балів.

Підсумковою оцінкою за кожну лабораторну роботу буде сума балів за усне опитування і захист результатів.

Підсумковою оцінкою за весь практичний модуль буде сума балів за всі лабораторні роботи.

6. Методика оцінювання за всіма змістовними модулями.

Підсумковою оцінкою за всіма змістовними модулями (ОЗ) буде сума балів за лекційні та практичні модулі.

7. Методика проведення та оцінювання підсумкового контрольного заходу.

Підсумковий контрольний захід проводиться у формі екзамену тестового типу в якій студенти відповідають на 50 запитань із використанням системи е-навчання університету Moodle. Питання формуються по першій та другій частині курсу. Правильна відповідь на кожне з тестових завдань оцінюється в залежності від складності від 1 до 3 балів. (15х1+20х2+15х3) Максимальна оцінка за складання іспиту дорівнює 100 балам. Час, що виділяється на виконання екзаменаційної роботи визначається при видачі завдання і не перевищує 2 академічні години. Студент може бути допущений до складання підсумкового контролю лише за отримання більше, ніж 30 балів за практичну частину.

8. Методика підсумкового оцінювання за дисципліну.

Загальна кількісна оцінка є усередненою між кількісною оцінкою поточних контролюючих заходів (до 50 балів за МКР1 та МКР2, до 50 балів та виконання та захист лабораторних робіт) та кількісною оцінкою семестрового контролюючого заходу (до 100 балів).

3. РЕКОМЕНДАЦІЇ ДО САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

Рекомендується наступний порядок вивчення дисципліни «Технології захисту інформації»:

–зміст кожної теми курсу вивчається за допомогою навчальної та методичної літератури, що наведена в списку;

–після засвоєння змісту кожної теми курсу потрібно відповісти на «запитання самоперевірки», що наведені у даних методичних вказівках і відповідній літературі;

–якщо виникли питання при вивченні теоретичного матеріалу або при виконанні контрольних робіт, то потрібно звернутись до викладача, який читав лекції.

3.1. Модуль ЗМ-Л1 „ Інформаційні загрози та несанкціонований доступ ”

3.1.1. Повчання

В результаті засвоєння матеріалу змістовного модуля «Інформаційні загрози та несанкціонований доступ», студент повинен знати історію та основні принципи розвідки. Канали несанкціонованого отримання інформації. Класифікація каналів витоку інформації . Інформаційне протиборство . Загрози інформації. Канали витоку інформації при експлуатації ЕОМ. Аналітичне забезпечення ІБ . Методи і засоби несанкціонованого отримання інформації. Методи і засоби руйнування інформації.

3.1.2. Питання для самоперевірки

Питання, які мають бути засвоєнні в ході вивчення змістовного модуля ЗМ-Л1 і являють собою необхідний мінімум знань, який потрібний для засвоєння дисципліни «Технології захисту інформації”, наведені нижче (ті, що формують базові результати навчання виділені курсивом):

1. *Надайте визначення інформаційної сфери. [2, с. 25]*
2. *Надайте визначення єдиного інформаційного простору країни. [2, с. 31]*
3. *Надайте визначення інформаційних ресурсів. [2, с. 37]*
4. *Надайте визначення інформаційної війни. [2, с. 43]*
5. *Надайте визначення інформаційної зброї. [2, с. 49]*
6. *Надайте визначення загрози інформаційній безпеці. [2, с. 55]*
7. *Надайте визначення незаконного використання інформаційних і телекомунікаційних систем і інформаційних ресурсів. [2, с. 61]*
8. *Надайте визначення несанкціонованого втручання в інформаційні і телекомунікаційні системи й інформаційні ресурси. [2, с. 67]*
9. *Надайте визначення життєво важливих структур. [2, с. 73]*
10. *Надайте визначення міжнародного інформаційного тероризму. [2, с. 79]*
11. *Надайте визначення міжнародної інформаційної злочинності. [2, с. 85]*
12. *Які складові включає у себе інформаційна інфраструктура? [2, с. 91]*
13. *Надайте визначення організаційних структур. [2, с. 97]*
14. *Надайте визначення інформаційно-телекомунікаційних структур. [2, с. 103]*
15. *Надайте визначення інформаційної безпеки. [2, с. 109]*
16. Які базові засади інформаційної безпеки нашої держави закладено у статтях 17, 19, 31, 32, 34, 50, 57 та 64 Конституції України? [2, с. 115]
17. Які правові основи інформаційної діяльності закладено у Закон України“Про інформацію”? [2, с. 121]
18. Надайте визначення інформації згідно зі ст. 1 Закону України “Про інформацію”. [2, с. 127]
19. Які основні види інформації визначаються у Законі України “Про інформацію”?

[2, с. 133]
20. Як поділяється інформація за режимом доступу до неї? [2, с. 139]
21. Як здійснюється контроль за режимом доступу до інформації? [2, с. 145]
22. Як поділяється за своїм правовим режимом інформація з обмеженим доступом? [2, с. 151]
23. Яка інформація відноситься до конфіденційної? [2, с. 157]
24. Яка інформація не може бути конфіденційною? [2, с. 163]
25. Яка інформація відноситься до таємної інформації? [2, с. 169]
26. Чим та як визначається інформація, що складає державну таємницю? [2, с. 175]
27. Чим визначається ступень таємності інформації? [2, с. 181]
28. Які грифи таємності можуть надаватися інформації та який їх терміни дії? [2, с. 187]
29. Яка інформація входить до інформаційних ресурсів України? [2, с. 193]
30. Чим забезпечується інформаційний суверенітет України? [2, с. 199]
31. Які національні інтереси України потрібно захищати у відповідності до Закону України "Про основи національної безпеки України" та "Концепції національної безпеки України"? [2, с. 205]
32. Що визначає "Концепція національної безпеки України"? [2, с. 211]
33. Коли та як була затверджена "Концепція технічного захисту інформації в Україні"? [2, с. 217]
34. Що визначає та має забезпечити "Концепція технічного захисту інформації в Україні"? [2, с. 223]

3.2. Модуль ЗМ-Л2 „ Методи та засоби захисту інформації "

3.2.1. Повчання

Розділи модуля ЗМ-Л2 формують у студентів уявлення про класифікацію технічних засобів забезпечення ІБ. Класифікація програмних та криптографічних засобів забезпечення ІБ . Підходи до створення КСЗІ. Загрози безпеки . Технічні методи і засоби ЗІ. Програмні методи захисту. Системна класифікація та характеристики технічних засобів забезпечення ІБ . Криптографічний захист. Скремблювання. Стеганографія. Електронна ідентифікація користувачів.

3.2.2. Питання для самоперевірки

Питання, які мають бути засвоєнні в ході вивчення змістовного модуля ЗМ-Л2 і являють собою необхідний мінімум знань, який потрібний для засвоєння дисципліни «Технології захисту інформації", наведені нижче (ті, що формують базові результати навчання виділені курсивом):

1. *Надайте визначення ТЗІ. [3, с. 31]*
2. *Чим зумовлені загрози безпеці інформації в Україні? [3, с. 38]*
3. *Чим зумовлюється стан ТЗІ в Україні? [3, с. 45]*

4. *Надайте визначення системи ТЗІ. [3, с. 52]*
5. *Що складає правову основу забезпечення ТЗІ в Україні? [3, с. 59]*
6. *Які принципи формування і проведення державної політики у сфері ТЗІ? [3, с. 66]*
7. *Які основні функції організаційних структур системи ТЗІ? [3, с. 73]*
8. *Які основні напрями державної політики у сфері ТЗІ? [3, с. 80]*
9. *Які першочергові заходи щодо реалізації державної політики у сфері ТЗІ? [3, с. 87]*
10. *Які складові інформаційної безпеки держави відносяться до технічного аспекту інформаційної безпеки? [3, с. 94]*
11. *Яке призначення технічного захисту інформації? [3, с. 101]*
12. *Яке призначення криптографічного захисту інформації? [3, с. 108]*
13. *Надайте визначення поняття технічного каналу витоку інформації [3, с. 115]*
14. *Надайте визначення поняття небезпечного фізичного сигналу [3, с. 122]*
15. *Яка класифікація ТКВІ прийнята в Україні? [3, с. 129]*
16. *Що таке природні ТКВІ? Наведіть приклади таких каналів. [3, с. 136]*
17. *Що таке штучні ТКВІ? Наведіть приклади таких каналів. Яким шляхом утворюються штучні ТКВІ? [3, с. 143]*
18. *Намалюйте схему загальної класифікації видів інформації, яка може бути об'єктом злочинних посягань. [3, с. 150]*
19. *В чому полягає сутність та основні завдання ТЗІ? [3, с. 157]*
20. *Намалюйте класичну схему обробки, розповсюдження та захисту інформації. [3, с. 164]*
21. Що є основними об'єктами захисту інформації? [3, с. 171]
22. Які технічні засоби і системи звуться додатковими технічними засобами і системами? [3, с. 178]
23. Яка фізична сутність акустичного сигналу? [3, с. 185]
24. Яка фізична сутність акустично-електричних перетворень? [3, с. 192]
25. Що є частотою та періодом коливань? [3, с. 199]
26. Які частоти коливань відносяться до звукового діапазону частот? [3, с. 206]
27. Які частоти коливань відносяться до інфразвукового діапазону частот? [3, с. 213]
28. Які частоти коливань відносяться до ультразвукового діапазону частот? [3, с. 220]
29. Яка фізична сутність мікрофону та гучномовця? [3, с. 227]
30. Як утворюється мікрофонний ефект та яка його фізична сутність? [3, с. 234]
31. Яка головна особливість радіозв'язку? [3, с. 241]
32. В чому полягає фізична сутність процесу модуляції? [3, с. 248]
33. Який сигнал має більшу частоту: сигнал-переносник, чи модулюючий сигнал? [3, с. 255]
34. Чому сигнал, що модулюється, звуть несучим коливанням? [3, с. 262]
35. Які види модуляції використовуються для передавання інформації по радіозв'язку? [3, с. 269]
36. В чому полягає процес демодуляції (детектування)? [3, с. 276]

3.3. Модуль ЗМ-П1

При вивченні практичного модуля студенти набувають уміння Аналізувати та формувати вимоги до захисту інформації, Користуватись спеціалізованим ПЗ у галузі ІБ, Виявляти та визначати атаки, обирати методи протистояння;

3.4. Модуль ЗМ-П2

При вивченні практичного модуля студенти набувають уміння Аналізувати відомі алгоритми шифрування; Модифікувати алгоритми відповідно до потреб, створювати власні; Розробляти програмну реалізацію алгоритмів.

Питання для самоперевірки та захисту лабораторних робіт за модулями ЗМ-П1, П2 (ті, що формують базові результати навчання виділені курсивом):

1. *Як і де утворюються паразитні випромінювання? [4, с. 18]*
2. *Який механізм утворення наводок? Де вони виникають? [4, с. 24]*
3. *В чому полягає небезпека паразитних випромінювань та наводок? [4, с. 30]*
4. *Дайте визначення організаційних заходів із захисту об'єкту. [4, с. 36]*
5. *Які основні організаційні та режимні заходи відносяться до основних? [4, с. 42]*
6. *Дайте визначення технічних заходів із захисту об'єкту. [4, с. 48]*
7. *Які основні складові технічних заходів? [4, с. 54]*
8. *Який порядок проведення робіт з ТЗІ? [4, с. 60]*
9. *В чому полягає особливість використання беззаходових способів зняття інформації? [4, с. 66]*
10. *В чому полягає фізична сутність способу високочастотного нав'язування для зняття інформації? [4, с. 72]*
11. *Чим визначається власна резонансна частота коливального контуру? Запишіть формулу визначення резонансної частоти. [4, с. 78]*
12. *За яким принципом побудовано детальний розподіл ТКВІ? [4, с. 84]*
13. *Що є комбінованими каналами витоку інформації? [4, с. 90]*
14. *Які є канали витоку акустичної інформації? [4, с. 96]*
15. *Які способи та засоби використовуються для зняття акустичної інформації? [4, с. 102]*
16. *Які є види радіозакладних пристроїв? [4, с. 108]*
17. *Які є канали витоку електромагнітної та електронної інформації? [4, с. 114]*
18. *Якими способами та засобами знімається електромагнітна та електронна інформація? [4, с. 120]*
19. *Які є канали зняття письмової інформації? [4, с. 126]*
20. *Якими способами та засобами знімається письмова інформація? [4, с. 132]*
21. *Дайте визначення об'єкту технічного захисту інформації. [4, с. 138]*
22. Коли використовується комплексний захист інформації? [4, с. 144]
23. Дайте визначення основних технічних засобів. [4, с. 150]
24. Дайте визначення допоміжних технічних засобів. [4, с. 156]

25. Дайте визначення поняття загрози для інформації. [4, с. 162]
26. Дайте визначення поняття рівня технічного захисту інформації. [4, с. 168]
27. Дайте визначення поняття активний захист інформації. [4, с. 174]
28. Дайте визначення поняття пасивний захист інформації. [4, с. 180]
29. Чим відрізняється пасивний захист від активного захисту інформації? [4, с. 186]
30. Який порядок проведення робіт з технічного захисту інформації на об'єкті? [4, с. 192]
31. Які фізичні явища покладені у методи та засоби захисту акустичної інформації від витоку по вібраційних каналах? [4, с. 198]
32. В чому полягає метод "завантаження мембрани", що використовується для придушення мікрофонів? [4, с. 204]
33. Які прилади використовуються для захисту акустичної інформації, що циркулює у приміщенні, від зняття з телефону? [4, с. 210]
34. Які засоби захисту акустичної інформації використовуються для її захисту при передаванні по телефонних мережах у проміжку від телефону до АТС? [4, с. 216]
35. Які прилади використовуються для виявлення засобів зняття акустичної інформації з телефонних мереж у проміжку від телефону до АТС? [4, с. 222]
36. Які засоби захисту акустичної інформації використовують для її захисту по всьому ланцюгу передавання у телефонній мережі між двома телефонами? [4, с. 228]
37. На що потрібно звертати увагу при візуальному пошуку радіозакладних пристроїв? [4, с. 234]
38. Які методи використовують для виявлення радіозакладних пристроїв? [4, с. 240]
39. Які функції виконують програми моніторингу ефіру? [4, с. 246]
40. Який алгоритм виявлення радіозакладних пристроїв з використанням методу моніторингу ефіру? [4, с. 252]
41. Які функції виконують сканери? [4, с. 258]
42. Які функції виконують індикатори електромагнітного поля? [4, с. 264]
43. Які функції виконують нелінійні локатори? [4, с. 270]
44. Які багатофункціональні прилади використовують для виявлення засобів зняття інформації? [4, с. 276]
45. Які методи пошуку радіозакладних пристроїв, побудованих на використанні способу ВЧ-нав'язування? [4, с. 282]
46. Як використовуються генератори шуму для захисту акустичної інформації? [4, с. 288]
47. На яких принципах будуються генератори шуму? [4, с. 294]
48. Які методи та засоби використовуються для виявлення та захисту акустичної інформації від несанкціонованого запису звукозаписувальними пристроями? [4, с. 300]
49. Які методи та засоби використовуються для захисту електронної та електромагнітної інформації? [4, с. 306]
50. Які технічні методи та засоби використовуються для захисту письмової інформації? [4, с. 312]

4. ПИТАННЯ ДО ЗАХОДІВ ПОТОЧНОГО, ПІДСУМКОВОГО ТА СЕМЕСТРОВОГО КОНТРОЛЮ»

4.1. Тестові завдання до модульної контрольної роботи модуля ЗМ-Л1.

1. Під цим терміном в Законі України "Про електронні документи та електронний документообіг" розуміють інформацію, представлену в формальному вигляді, зручному для її оброблення електронними пристроями. [1,с. 336]
2. На першому місці в законодавчій ієрархії щодо інформаційної безпеки стоїть закон України ... [1, с. 158]
3. Інформація, яка знаходиться в розпорядженні чи володінні окремих фізичних чи юридичних осіб, які самі визначають її статус і режим доступу до неї - це … [1, с. 386]
4. Що - являє собою сукупність організаційних та інженерних заходів, програмно-апаратних засобів, що забезпечують захист інформації, і відповідно, спрямованих на забезпечення безпеки підприємства. [1, с. 247]
5. Що складає правову основу забезпечення ТЗІ в Україні? [2, с. 304]
6. Процедура підтвердження компетентності центру сертифікації ключів, відповідно до закону, називається [3, с. 396]
7. Чи є вірним наступне твердження?: юридична сила документа може бути опротестована на тій підставі, що він електронний [2, с. 199]
8. Який закон України визначає види секретної інформації, прописує процедури віднесення відомостей до категорій секретної, а також інформації, визначає обов'язки державних органів щодо захисту державної таємниці? [3, с. 553]
9. Згідно «НД ТЗІ 1.1-005-07.» Визначення відповідності виконаних робіт зі створення комплексу ТЗІ на об'єкті інформаційної діяльності вимогам нормативних документів - це… [2, с. 516]
10. Згідно «НД ТЗІ 1.1-005-07.» Сукупність аналітичних, експериментальних і вимірювальних робіт, виконуваних на об'єктах інформаційної діяльності, з метою визначення повноти виконання вимог щодо захисту від витоку інформації з обмеженим доступом технічними каналами, а також визначення повноти заходів щодо захисту інформації - це… [2, с. 239]
11. Згідно «НД ТЗІ 1.1-005-07.» Сукупність інформаційних, інженерних і технічних засобів, призначених для захисту інформації з обмеженим доступом технічними каналами на об'єктах інформаційної діяльності - це… [3, с. 213]
12. Згідно «НД ТЗІ 1.1-005-07.» Будинки, приміщення, транспортні засоби або інші інженерно-технічні споруди, функціональне призначення яких передбачає обіг інформації з обмеженим доступом - це… [3, с. 590]
13. Складовими системи безпеки підприємства є: [2, с. 377]
14. Згідно «НД ТЗІ 1.1-005-07.» Хто є суб'єктом відносин при створенні комплексів ТЗІ. [1, с. 79]
15. З точки зору закону, ... - це комплекс правових, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації і належний порядок доступу до неї. [1, с. 50]
16. Інформація, яка містить відомості, що містять державну або іншу передбачену

законом таємницю, розголошення якої може завдати шкоди державі, суспільству або окремим особам - це... [2, с. 257]

17. Які складові інформаційної безпеки держави відносяться до технічного аспекту інформаційної безпеки? [3, с. 247]
18. Центром сертифікації ключів не може бути [2, с. 470]
19. Яке призначення технічного захисту інформації? [1, с. 128]
20. Яке призначення криптографічного захисту інформації? [2, с. 228]
21. Відповідно до Закону України "Про електронні документи та електронний документообіг", суб'єкт, якій призначається електронний документ - це... [3, с. 203]
22. Коли електронний документ не може бути оригіналом? [2, с. 38]
23. Порядок доступу до секретної інформації визначається законом України [1, с. 352]
24. Складовими системи безпеки підприємства не є: [2, с. 167]
25. Відповідно до Закону України "Про електронні документи та електронний документообіг", особа, яка надає послуги взаємодії суб'єктів, обмениваючимся електронними документами - це... [3, с. 380]
26. Чи може у електронного документа бути більш одного оригіналу? [4, с. 318]
27. Чи може бути опротестована юридична сила документа бути опротестована на тій підставі, що він електронний? [5, с. 562]
28. Економічне шпигунство (розвідка)… [2, с. 312]
29. Особистий ключ в ЕЦП - це: [3, с. 370]
30. Відповідно до Закону України "Про електронні документи та електронний документообіг", особа, яка створила документ - це... [2, с. 347]
31. Оригіналом електронного документа вважається: [3, с. 115]
32. Закон визначає режим доступу до інформації як передбачений законом порядок отримання, використання, поширення та зберігання інформації. У цьому сенсі закон поділяє інформацію на: [2, с. 201]
33. Складовими системи безпеки підприємства є: [2, с. 221]
34. Відповідно до Закону України "Про електронні документи та електронний документообіг", автор це... [3, с. 498]
35. Закон України "Про електронний цифровий підпис" визначає склад суб'єктів, які є учасниками процесу постановки і застосування електронного цифрового підпису. Вкажіть зайвий пункт: [3, с. 150]
36. Документ – це… [2, с. 47]
37. Закон України "Про інформацію" визначає інформацію як [1, с. 83]
38. Відповідно до Закону України "Про електронні документи та електронний документообіг", власник - це... [1, с. 194]
39. Організаційні методи при забезпеченні інформаційної безпеки [2, с. 403]
40. Закон України "Про електронний цифровий підпис" визначає електронний цифровий підпис, як вид електронного підпису, отриманого за результатом криптографічного перетворення набору даних, який додається до цього набору або логічно з ним об'єднується і дає можливість перевірки цілісності цього набору, а також ідентифікації підписанта [3, с. 146]
41. Сукупність організаційних та інженерно-технічних засобів і методів захисту

інформації - це … [2, с. 93]
42. Питання інформаційної безпеки підприємства актуальні ... [1, с. 67]
43. Відповідно до Закону України "Про електронні документи та електронний документообіг", адресат - це... [2, с. 262]
44. Сукупність процесів створення, обробки, відправлення, передавання, одержання, зберігання, використання та знищення, що виконуються за дотриманням процедур перевірки подлінності- це … [3, с. 233]
45. Центром сертифікації ключів може бути [2, с. 455]
46. Хто відповідає за визначення рівню безпеки інформації? [1, с. 86]
47. Хто є найбільш вірогідними порушниками інформаційної безпеки? [2, с. 227]
48. Хто відповідає за забезпечення захисту інформації? [3, с. 319]
49. Що найбільше впливає на впевненість у забезпеченні захисту? [2, с. 200]
50. Що таке політики безпеки? [2, с. 227]

4.2. Тестові завдання до модульної контрольної роботи модуля ЗМ-Л1.

1. Що є основою для вибору засобів захисту? [2, с. 118]
2. Що таке тактичне планування захисту? [3, с. 222]
3. Гарантованість безпеки визначається: [1, с. 320]
4. У чому полягає ціль аналізу ризиків? [2, с. 467]
5. Яким чином формально визначається аналіз ризиків? [3, с. 279]
6. Чому перевага віддається якісному аналізу загроз [2, с. 583]
7. Що являє собою стандарт ISO/IEC 27799? [1, с. 203]
8. Що являє собою стандарт NIST 800-60; [2, с. 343]
9. Що являє собою стандарт BS 17799; [3, с. 406]
10. Що являє собою стандарт ISO 27000; [2, с. 293]
11. Оберіть вірне визначення основних технічних засобів. [1, с. 188]
12. Оберіть вірне визначення допоміжних технічних засобів. [2, с. 231]
13. Оберіть вірне визначення поняття загрози для інформації. [3, с. 592]
14. Оберіть вірне визначення поняття рівня технічного захисту інформації. [2, с. 236]
15. Оберіть вірне визначення поняття активний захист інформації. [2, с. 185]
16. Оберіть вірне визначення поняття пасивний захист інформації. [3, с. 332]
17. Як називається процедура шифрування, що передбачає переставляння символів за визначеними правилами? [4, с. 330]
18. Як називається процедура шифрування, що передбачає заміну символів на символи іншого алфавіту або алфавітів? [5, с. 461]
19. Як називається процедура шифрування, що передбачає по символьне складання символів відкритого тексту із символами спеціальної послідовності? [6, с. 334]
20. Несанкціонований виток інформації це: [7, с. 461]
21. Захист інформації це: [8, с. 132]
22. Основна задача захисту інформації полягає у [9, с. 322]
23. Ризик вимірюється у [10, с. 303]
24. Перевірка правильності суб’єкта на основі його ідентифікатору це [11, с. 266]
25. У відповідності до вимог “Жовтогарячої книги” унікальні ідентифікатори

повинні мати [12, с. 131]

26. Відповідність засобів безпеки задачам захисту визначає [13, с. 351]
27. Закритий ключ до шифру використовується для [14, с. 533]
28. Спосіб управління доступом у відповідності до якого кожному об’єкту системи надається відповідна мітка його критичності, називається [15, с. 334]
29. Організаційними вимогами до системи захисту є [16, с. 55]
30. Вибіркова політика безпеки визначається матрицею доступу через [17, с. 269]
31. Основу політики безпеки складає [18, с. 349]
32. Кожному суб’єкту у матриці доступу відповідає [19, с. 222]
33. Який спосіб криптоаналізу є найменш затратним? [20, с. 162]
34. Які недоліки притаманні несиметричним системам? [21, с. 508]
35. Яка із наук вивчає математичні методи захисту інформації? [22, с. 396]
36. Цілісність інформації забезпечується методами [23, с. 432]
37. Множина знаків, що використовується для кодування інформації називається [24, с. 518]
38. Недоліком дискретних моделей політики безпеки є [25, с. 176]
39. Першим етапом розробки системи захисту є [26, с. 582]
40. Які технічні засоби і системи звуться додатковими технічними засобами і системами? [27, с. 208]
41. Доступ до об’єкту у системі при наявності вибіркової політики безпеки відповідає [28, с. 104]
42. Надійність систем захисту інформації визначається [29, с. 342]
43. Політика інформаційної безпеки це [30, с. 113]
44. Захист конфіденційності інформації забезпечується [31, с. 159]
45. Який із видів крипто аналізу є найменш затратним для алгоритму RSA? [32, с. 298]
46. Нормативний документ, що визначає всі аспекти безпеки програмного продукту називається [33, с. 337]
47. Два ключа використовуються у криптографічних системах [34, с. 465]
48. Переваги апаратної реалізації криптографічного захисту [35, с. 243]
49. Принцип, у відповідності до якого користувачам надаються тільки необхідні права доступу це [36, с. 144]
50. Головним параметром криптографічної системи є показник [37, с. 74]
51. Довжиною ключа національного стандарту шифрування ГОСТ 28147-89 [38, с. 429]
52. Надання кожному об’єкту унікального коду це [39, с. 307]
53. Недоліком матричних моделей безпеки є [40, с. 426]
54. Чим визначається власна резонансна частота коливального контуру? Вкажіть формулу визначення резонансної частоти. [41, с. 372]
55. На що потрібно звертати увагу при візуальному пошуку радіозакладних пристроїв? [42, с. 362]

4.3. Тестові завдання до Іспиту

1. Під цим терміном в Законі України "Про електронні документи та електронний

документообіг" розуміють інформацію, представлену в формальному вигляді, зручному для її оброблення електронними пристроями. (1 бал) [1,с. 336]

2. На першому місці в законодавчій ієрархії щодо інформаційної безпеки стоїть закон України ... (1 бал) [1, с. 158]
3. Інформація, яка знаходиться в розпорядженні чи володінні окремих фізичних чи юридичних осіб, які самі визначають її статус і режим доступу до неї - це … (1 бал) [1, с. 386]
4. Що - являє собою сукупність організаційних та інженерних заходів, програмно-апаратних засобів, що забезпечують захист інформації, і відповідно, спрямованих на забезпечення безпеки підприємства. (1 бал) [1, с. 247]
5. Що складає правову основу забезпечення ТЗІ в Україні? (1 бал) [2, с. 304]
6. Процедура підтвердження компетентності центру сертифікації ключів, відповідно до закону, називається (1 бал) [3, с. 396]
7. Чи є вірним наступне твердження?: юридична сила документа може бути опротестована на тій підставі, що він електронний (1 бал) [2, с. 199]
8. Який закон України визначає види секретної інформації, прописує процедури віднесення відомостей до категорій секретної, а також інформації, визначає обов'язки державних органів щодо захисту державної таємниці? (1 бал) [3, с. 553]
9. Згідно «НД ТЗІ 1.1-005-07.» Визначення відповідності виконаних робіт зі створення комплексу ТЗІ на об'єкті інформаційної діяльності вимогам нормативних документів - це… (1 бал) [2, с. 516]
10. Згідно «НД ТЗІ 1.1-005-07.» Сукупність аналітичних, експериментальних і вимірювальних робіт, виконуваних на об'єктах інформаційної діяльності, з метою визначення повноти виконання вимог щодо захисту від витоку інформації з обмеженим доступом технічними каналами, а також визначення повноти заходів щодо захисту інформації - це… (1 бал) [2, с. 239]
11. Згідно «НД ТЗІ 1.1-005-07.» Сукупність інформаційних, інженерних і технічних засобів, призначених для захисту інформації з обмеженим доступом технічними каналами на об'єктах інформаційної діяльності - це… (1 бал) [3, с. 213]
12. Згідно «НД ТЗІ 1.1-005-07.» Будинки, приміщення, транспортні засоби або інші інженерно-технічні споруди, функціональне призначення яких передбачає обіг інформації з обмеженим доступом - це… (1 бал) [3, с. 590]
13. Складовими системи безпеки підприємства є: (1 бал) [2, с. 377]
14. Згідно «НД ТЗІ 1.1-005-07.» Хто є суб'єктом відносин при створенні комплексів ТЗІ. (1 бал) [1, с. 79]
15. З точки зору закону, ... - це комплекс правових, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації і належний порядок доступу до неї. (1 бал) [1, с. 50]
16. Інформація, яка містить відомості, що містять державну або іншу передбачену законом таємницю, розголошення якої може завдати шкоди державі, суспільству або окремим особам - це... (1 бал) [2, с. 257]
17. Які складові інформаційної безпеки держави відносяться до технічного аспекту інформаційної безпеки? (1 бал) [3, с. 247]
18. Що є основою для вибору засобів захисту? (1 бал) [2, с. 118]
19. Що таке тактичне планування захисту? (1 бал) [3, с. 222]

20. Гарантованість безпеки визначається: (1 бал) [1, с. 320]
21. У чому полягає ціль аналізу ризиків? (1 бал) [2, с. 467]
22. Яким чином формально визначається аналіз ризиків? (1 бал) [3, с. 279]
23. Чому перевага віддається якісному аналізу загроз (1 бал) [2, с. 583]
24. Що являє собою стандарт ISO/IEC 27799? (1 бал) [1, с. 203]
25. Що являє собою стандарт NIST 800-60; (1 бал) [2, с. 343]
26. Що являє собою стандарт BS 17799; (1 бал) [3, с. 406]
27. Що являє собою стандарт ISO 27000; (1 бал) [2, с. 293]
28. Оберіть вірне визначення основних технічних засобів. (1 бал) [1, с. 188]
29. Оберіть вірне визначення допоміжних технічних засобів. (1 бал) [2, с. 231]
30. Оберіть вірне визначення поняття загрози для інформації. (1 бал) [3, с. 592]
31. Оберіть вірне визначення поняття рівня технічного захисту інформації. (1 бал) [2, с. 236]
32. Оберіть вірне визначення поняття активний захист інформації. (1 бал) [2, с. 185]
33. Закон України "Про інформацію" визначає інформацію як (1 бал) [1, с. 83]
34. Відповідно до Закону України "Про електронні документи та електронний документообіг", власник - це... (1 бал) [1, с. 194]
35. Організаційні методи при забезпеченні інформаційної безпеки (1 бал) [2, с. 403]
36. Закон України "Про електронний цифровий підпис" визначає електронний цифровий підпис, як вид електронного підпису, отриманого за результатом криптографічного перетворення набору даних, який додається до цього набору або логічно з ним об'єднується і дає можливість перевірки цілісності цього набору, а також ідентифікації підписанта (1 бал) [3, с. 146]
37. Сукупність організаційних та інженерно-технічних засобів і методів захисту інформації - це … (1 бал) [2, с. 93]
38. Питання інформаційної безпеки підприємства актуальні ... (1 бал) [1, с. 67]
39. Оберіть вірне визначення поняття пасивний захист інформації. (1 бал) [3, с. 332]
40. Як називається процедура шифрування, що передбачає переставляння символів за визначеними правилами? (1 бал) [4, с. 330]
41. Як називається процедура шифрування, що передбачає заміну символів на символи іншого алфавіту або алфавітів? (1 бал) [5, с. 461]
42. Як називається процедура шифрування, що передбачає по символьне складання символів відкритого тексту із символами спеціальної послідовності? (1 бал) [6, с. 334]
43. Несанкціонований виток інформації це: (1 бал) [7, с. 461]
44. Захист інформації це: (1 бал) [8, с. 132]
45. Центром сертифікації ключів не може бути (2 бали) [2, с. 470]
46. Яке призначення технічного захисту інформації? (2 бали) [1, с. 128]
47. Яке призначення криптографічного захисту інформації? (2 бали) [2, с. 228]
48. Відповідно до Закону України "Про електронні документи та електронний документообіг", суб'єкт, якій призначається електронний документ - це... (2 бали) [3, с. 203]
49. Коли електронний документ не може бути оригіналом? (2 бали) [2, с. 38]
50. Порядок доступу до секретної інформації визначається законом України (2 бали) [1, с. 352]

51. Складовими системи безпеки підприємства не є: (2 бали) [2, с. 167]
52. Відповідно до Закону України "Про електронні документи та електронний документообіг", особа, яка надає послуги взаємодії суб'єктів, обмінюючимся електронними документами - це... (2 бали) [3, с. 380]
53. Чи може у електронного документа бути більш одного оригіналу? (2 бали) [4, с. 318]
54. Чи може бути опротестована юридична сила документа бути опротестована на тій підставі, що він електронний? (2 бали) [5, с. 562]
55. Економічне шпигунство (розвідка)… (2 бали) [2, с. 312]
56. Особистий ключ в ЕЦП - це: (2 бали) [3, с. 370]
57. Відповідно до Закону України "Про електронні документи та електронний документообіг", особа, яка створила документ - це... (2 бали) [2, с. 347]
58. Оригіналом електронного документа вважається: (2 бали) [3, с. 115]
59. Закон визначає режим доступу до інформації як передбачений законом порядок отримання, використання, поширення та зберігання інформації. У цьому сенсі закон поділяє інформацію на: (2 бали) [2, с. 201]
60. Складовими системи безпеки підприємства є: (2 бали) [2, с. 221]
61. Відповідно до Закону України "Про електронні документи та електронний документообіг", автор це... (2 бали) [3, с. 498]
62. Закон України "Про електронний цифровий підпис" визначає склад суб'єктів, які є учасниками процесу постановки і застосування електронного цифрового підпису. Вкажіть зайвий пункт: (2 бали) [3, с. 150]
63. Документ – це… (2 бали) [2, с. 47]
64. Основна задача захисту інформації полягає у (2 бали) [9, с. 322]
65. Ризик вимірюється у (2 бали) [10, с. 303]
66. Перевірка правильності суб’єкта на основі його ідентифікатору це (2 бали) [11, с. 266]
67. У відповідності до вимог “Жовтогарячої книги” унікальні ідентифікатори повинні мати (2 бали) [12, с. 131]
68. Відповідність засобів безпеки задачам захисту визначає (2 бали) [13, с. 351]
69. Закритий ключ до шифру використовується для (2 бали) [14, с. 533]
70. Спосіб управління доступом у відповідності до якого кожному об’єкту системи надається відповідна мітка його критичності, називається (2 бали) [15, с. 334]
71. Організаційними вимогами до системи захисту є (2 бали) [16, с. 55]
72. Вибіркова політика безпеки визначається матрицею доступу через (2 бали) [17, с. 269]
73. Основу політики безпеки складає (2 бали) [18, с. 349]
74. Кожному суб’єкту у матриці доступу відповідає (2 бали) [19, с. 222]
75. Який спосіб криптоаналізу є найменш затратним? (2 бали) [20, с. 162]
76. Які недоліки притаманні несиметричним системам? (2 бали) [21, с. 508]
77. Яка із наук вивчає математичні методи захисту інформації? (2 бали) [22, с. 396]
78. Цілісність інформації забезпечується методами (2 бали) [23, с. 432]
79. Множина знаків, що використовується для кодування інформації називається (2 бали) [24, с. 518]
80. Недоліком дискретних моделей політики безпеки є (2 бали) [25, с. 176]

81. Першим етапом розробки системи захисту є (2 бали) [26, с. 582]
82. Відповідно до Закону України "Про електронні документи та електронний документообіг", адресат - це... (3 бали) [2, с. 262]
83. Сукупність процесів створення, обробки, відправлення, передавання, одержання, зберігання, використання та знищення, що виконуються за дотриманням процедур перевірки подлінності- це … (3 бали) [3, с. 233]
84. Центром сертифікації ключів може бути (3 бали) [2, с. 455]
85. Хто відповідає за визначення рівню безпеки інформації? (3 бали) [1, с. 86]
86. Хто є найбільш вірогідними порушниками інформаційної безпеки? (3 бали) [2, с. 227]
87. Хто відповідає за забезпечення захисту інформації? (3 бали) [3, с. 319]
88. Що найбільше впливає на впевненість у забезпеченні захисту? (3 бали) [2, с. 200]
89. Що таке політики безпеки? (3 бали) [2, с. 227]
90. Які технічні засоби і системи звуться додатковими технічними засобами і системами? (3 бали) [27, с. 208]
91. Доступ до об’єкту у системі при наявності вибіркової політики безпеки відповідає (3 бали) [28, с. 104]
92. Надійність систем захисту інформації визначається (3 бали) [29, с. 342]
93. Політика інформаційної безпеки це (3 бали) [30, с. 113]
94. Захист конфіденційності інформації забезпечується (3 бали) [31, с. 159]
95. Який із видів крипто аналізу є найменш затратним для алгоритму RSA? (3 бали) [32, с. 298]
96. Нормативний документ, що визначає всі аспекти безпеки програмного продукту називається (3 бали) [33, с. 337]
97. Два ключа використовуються у криптографічних системах (3 бали) [34, с. 465]
98. Переваги апаратної реалізації криптографічного захисту (3 бали) [35, с. 243]
99. Принцип, у відповідності до якого користувачам надаються тільки необхідні права доступу це (3 бали) [36, с. 144]
100. Головним параметром криптографічної системи є показник (3 бали) [37, с. 74]
101. Довжиною ключа національного стандарту шифрування ГОСТ 28147-89 (3 бали) [38, с. 429]
102. Надання кожному об’єкту унікального коду це (3 бали) [39, с. 307]
103. Недоліком матричних моделей безпеки є (3 бали) [40, с. 426]
104. Чим визначається власна резонансна частота коливального контуру? Вкажіть формулу визначення резонансної частоти. (3 бали) [41, с. 372]
105. На що потрібно звертати увагу при візуальному пошуку радіозакладних пристроїв? (3 бали) [42, с. 362]

5. ЛІТЕРАТУРА ДЛЯ ВИВЧЕННЯ ДИСЦИПЛІНИ

Основна література.

1. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. — Киев: Издательство «Юниор», 2003, — 504 с.
2. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защити информации. Т1 — Несанкционированное получение информации. — Киев: «Арий», 2008, — 464 с.
3. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. Т2 — Информационная безопасность. — Киев: «Арий», 2008, — 344 с.
4. Максименко Г.А., Хорошко В.А.. Методы выявления, обработки и идентификции сигналов радиозакладных устройств. — Киев: ООО «ПолиграфКонсалтинг», 2004. — 317 с.
5. Пархуць Л.Т. Методи і засоби захисту інформації. Конспект лекцій. Частина 1. «Захист інформації від витоку по технічних каналах». НУ ЛП, — Львів: 2008. — 67с. Частина 2. «Методи і засоби пошуку електронних пристроїв перехоплення інформації». НУ ЛП, — Львів: 2009. — 84с.

Додаткова література.

1. www.library-odeku.16mb.com
2. Рибальський О.В. Інформаційна безпека правоохоронних органів. Курс лекцій / Рибальський О.В., Хахановський В.Г., Шорошев В.В., Грищенко О.І.,Сторожев С.В., Кобець М.В. – К.: НАВСУ, 2003. – 160 с.
3. Термінологічний довідник з питань технічного захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В. / За ред. проф. В.О.Хорошка. – К.: ДУІКТ, 2007. – 365 с.
4. Хорошко В.О. Основи інформаційної безпеки /Хорошко В.О., Чередниченко В.С., Шелест М.Є./ За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 186с.
5. Каторин Ю.Ф. Большая энциклопедия промышленного шпионажа / Каторин Ю.Ф., Куренков Е.В., Лысов А.