НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних систем, мереж та кібербезпеки

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г. Глазунова
"___" _____ 2023 р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем, мереж та кібербезпеки
Протокол №10 від "17" травня 2023 р.
Завідувач кафедри
(доц. Касаткін Д.Ю.)

РОЗГЛЯНУТО
Гарант ОП
«Кібербезпека»
_____
Гарант ОП
_____ (проф. Лахно В.А.)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ОСНОВИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ»

Спеціальність	125 «Кібербезпека»
Освітня програма	«Кібербезпека»
Факультет	інформаційних технологій
Розробник:	Кулініч О.М., к.т.н., доцент.

Київ – 2023

1. Опис навчальної дисципліни «Основи технічного захисту інформації»

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	Бакалавр	
Галузь знань	12 – Інформаційні технології	
Спеціальність	125 – Кібербезпека	
Освітня програма	«Кібербезпека»	
Характеристика навчальної дисципліни		
Вид	обов'язкова	
Загальна кількість годин	120	
Кількість кредитів ECTS	4	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
Форма контролю	екзамен	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	2	
Семестр	4	
Лекційні заняття, год.	30	
Практичні, семінарські заняття	-	
Лабораторні заняття, год.	26	
Самостійна робота, год.	60	
МКР	4	
Кількість тижневих аудиторних годин для денної форми навчання	4	

2. Мета, завдання та компетентності навчальної дисципліни

Мета: вивчення сучасних методів захисту інформації, отримання студентами необхідних базових знань, щодо порядку створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. В рамках курсу передбачено проведення теоретичних та практичних завдань щодо класифікації, шляхів утворення технічних каналів витоку інформації, а також сучасних методів та засобів технічного захисту інформації.

Завдання навчальної дисципліни: є теоретична та практична підготовка студентів до застосування сучасних методів захисту інформації, а також навиків щодо розроблення, впровадження та експлуатації систем технічного захисту інформації на об’єктах інформаційної діяльності.

В результаті вивчення навчальної дисципліни студент повинен

- знати: основні поняття та принципи технічного захисту інформації; загальні аспекти технічного захисту інформації; вимоги щодо розміщення режимних приміщень для функціонування інформації з обмеженим доступом; види технічних каналів витоку інформації, класифікацію та шляхи їх утворення; сучасні методи та засоби технічного захисту інформації; основні положення та сутність створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності; порядок проведення атестації комплексів технічного захисту інформації.

- вміти: застосовувати знання, навички для розв’язування задач аналізу та синтезу визначення загроз інформаційної безпеки; вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах; вміти класифікувати канали витоку інформації; розробляти та впроваджувати заходи з технічного захисту інформації на об’єктах інформаційної діяльності; вирішувати задачі виявлення технічних каналів витоку інформації та запобігання витоку інформації такими каналами; проводити атестацію комплексів технічного захисту інформації.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

Спеціальні (фахові, предметні) компетентності (СК):

СК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

СК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

СК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

В результаті вивчення навчальної дисципліни студент набуде певні програмні результати (РН), а саме

ПРН5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН13. Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних.

ПРН14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

ПРН17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

ПРН18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.

ПРН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

ПРН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

ПРН32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

ПРН36. Виявляти небезпечні сигнали технічних засобів.

ПРН37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН50. Забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

ПРН51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.

ПРН52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

В контексті зазначених вище компетентностей та програмних результатів навчання задачі викладання дисципліни визначають необхідний комплекс знань і вмінь, що отримують студенти під час вивчення дисципліни.

Навчальна програма розрахована на студентів, які навчаються за освітньою програмою підготовки бакалавра за спеціальністю «Кібербезпека».

Програма побудована за вимогами кредитно-модульної системи організації навчального процесу у закладах вищої освіти і використанням академічної системи оцінювання досягнень студентів та шкали оцінок Європейської кредитно-трансферної системи (ECTS).

Робоча навчальна програма з курсу «Основи технічного захисту інформації» є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма дисципліни «Основи технічного захисту інформації» розроблена на підставі наступних документів:

- освітня програма підготовки фахівців за спеціальністю 125 «Кібербезпека»;
- навчальний план підготовки фахівців за спеціальністю 125 «Кібербезпека».

Навчальна програма характеризує шляхи перетворення інформації, що одержується студентом впродовж вивчання курсу, і відбиває зміст курсу, розподілення його на розділи та їх обсяги, дані про форми вивчення та контролю знань.

Теоретичною базою для вивчення курсу «Основи технічного захисту інформації» є курс «Методи та засоби захисту інформації».

Курс «Основи технічного захисту інформації» є базовим для вивчення наступних дисциплін: «Технології безпечного програмування» та «Системне програмування».

3.Програма та структура навчальної дисципліни

– повного терміну денної (заочної) форми навчання;

Назви змістових модулів і тем	Кількість годин												
	денна форма							Заочна форма					
	тиж-ні	всьо-го	у тому числі					всьо-го	у тому числі				
			л	п	лр	ін д	с.р.		л	п	лр	ін д	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Змістовий модуль 1. Сутність технічного захисту інформації.													
Тема 1. Загальні аспекти технічного захисту інформації.	1	6	2				4						
Тема 2. Загальні положення та вимоги щодо розміщення режимних приміщень.	2	8	2		2		4						
Тема 3. Технічні канали витоку інформації та їх класифікація (ч.1).	3	6	2				4						
Тема 4. Технічні канали витоку інформації та їх класифікація (ч.2).	4	8	2		2		4						
Тема 5. Сутність та шляхи утворення технічних каналів витоку інформації – електромагнітні, електричні, параметричні.	5	8	2		2		4						
Тема 6. Сутність та шляхи утворення технічних каналів витоку інформації – акустичні, акусто-вібраційні, акусто-електричні, акусто-оптичні.	6	8	2		2		4						
Тема 7. Сутність та шляхи утворення технічних каналів витоку інформації – матеріально-речовинні, канали зв’язку, візуальної інформації.	7	6	2				4						
Тема 8. Сутність та класифікація засобів несанкціонованого	8	10	2		4		4						

перехоплення інформації.													
МКР	8	2			2								
Разом за змістовим модулем 1		**62**	**16**		**14**		**32**						
Змістовий модуль 2. Механізми технічного захисту інформації на об'єктах інформаційної діяльності.													
Тема 1. Основні положення та сутність створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності.	9	8	2		2		4						
Тема 2. Передпроектні роботи при створенні комплексів технічного захисту інформації на об'єктах інформаційної діяльності.	10	10	2		4		4						
Тема 3. Розроблення технічного проекту комплексу технічного захисту інформації.	11	10	2		4		4						
Тема 4. Сутність та оформлення моделі загроз при створенні комплексу технічного захисту інформації.	12	6	2				4						
Тема 5. Розробка та впровадження заходів з технічного захисту інформації на об'єктах інформаційної діяльності.	13	8	2		2		4						
Тема 6. Порядок проведення атестації комплексів технічного захисту інформації.	14	8	2		2		4						
Тема 7. Фізична безпека інформаційних систем та об'єктів інформаційної діяльності.	15	6	2				4						
МКР	15	2			2								
Разом за змістовим модулем 2		**58**	**14**		**16**		**28**						
Всього годин		**120**	**30**		**30**		**60**						

4. Теми практичних занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

Теми семінарських занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Вирішення завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах.	2
2	Формування вимог щодо розміщення режимних приміщень.	2
3	Вирішення задач виявлення технічних каналів витоку інформації.	2
4	Вирішення задач запобігання витоку інформації технічними каналами.	2
5	Вирішення задач запобігання витоку інформації шляхом несанкціонованого перехоплення.	4
6	Складання розпорядчого документу щодо створення комплексу технічного захисту інформації.	2
7	Розроблення технічного завдання на створення комплексу технічного захисту інформації.	4
8	Розроблення моделі загроз при створенні комплексу технічного захисту інформації.	4
9	Розроблення паспорту на комплекс технічного захисту інформації.	2
10	Оформлення заявки на проведення атестації комплексів технічного захисту інформації.	2
	Всього	30

Курсове проектування - Не передбачено робочим навчальним планом

САМОСТІЙНА РОБОТА СТУДЕНТІВ

Самостійна робота студентів передбачає:

- систематичне відвідання усіх видів аудиторних занять і ведення конспекту лекцій;

- систематичне вивчення лекційного матеріалу і навчальної літератури, що рекомендуються;

- сумлінну підготовку до лабораторних занять;
- вчасне і якісне оформлення звітів про лабораторні роботи.

6. Контрольні питання, комплекти тестів для визначення рівня засвоєння знань студентами

6.1. Питання для перевірки знань студентів:

1. Технічні канали витоку інформації та їх класифікація.
2. Технічні канали витоку інформації, що обробляється в основних технічних засобах і системах.
3. Технічні канали витоку мовної інформації.
4. Витік інформації через засоби несанкціонованого перехоплення.
5. Витік інформації в каналах зв’язку, витік видової інформації та матеріально-речовинні канали витоку інформації.
6. Основні положення та сутність створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності.
7. Передпроектні роботи при створенні комплексів технічного захисту інформації на об’єктах інформаційної діяльності.
8. Сутність та оформлення моделі загроз при створенні комплексу технічного захисту інформації.
9. Розробка та впровадження заходів із захисту інформації на об’єктах інформаційної діяльності.
10. Випробування та атестація комплексів технічного захисту інформації на об’єктах інформаційної діяльності.
11. Основні напрями захисту.
12. Концепція забезпечення захисту інформації.
13. Основні загрози інформації.
14. Політика безпеки інформації.
15. Комплекс засобів захисту і об'єкти комп’ютерної системи.
16. Сутність несанкціонованого доступу.
17. Сутність моделі порушника.
18. Основні принципи забезпечення захисту інформації.
19. Планування захисту і керування системою захисту.
20. Основні принципи керування доступом.
21. Сутність безперервного захисту.
22. Сутність атрибутів доступу.
23. Довірче і адміністративне керування доступом.
24. Забезпечення персональної відповідальності.
25. Сутність послуг безпеки.
26. Сутність гарантій безпеки.
27. Основні принципи реалізації програмно-технічних засобів.
28. Функції і механізми захисту.
29. Реалізація комплексу засобів захисту.
30. Концепція диспетчера доступу.

31. Методи протидії і виявлення троянських програм.
32. Методи протидії і виявлення черв’яків.
33. Методи протидії і виявлення вірусів.
34. Методи нейтралізації шкідливого програмного забезпечення.
35. Методи і засоби сканування і захисту веб-серверів та веб-застосунків.
36. Механізми захисту від DoS/DDoS атак.
37. Захист від SQL-ін‘єкцій.
38. Інструменти тестування веб-ресурсів на вразливість до атак.
39. Методи протидії криптографічним атакам.
40. Сутність криптографічного захисту інформації.

6.2. Приклади тестів з дисципліни:

1. Етапи здійснення технічного захисту інформації:

А) визначення й аналіз загроз, розроблення системи захисту інформації, реалізація плану захисту інформації; контроль функціювання та керування системою захисту інформації;

В) визначення завдання захисту інформації, аналіз ризиків, розроблення моделі загроз, розроблення моделі порушника, підготовка до введення в дію, пусконалагоджувальні роботи;

С) визначення загальної структури та складу системи захисту інформації, вимоги до можливих заходів, методів та засобів захисту інформації, допустимі обмеження щодо застосування певних заходів і засобів захисту, введення в дію і функціонування.

2. Комплекс засобів захисту – це ...

А) сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

В) це сукупність всіх програмно-апаратних засобів, в тому числі програм ПЗП, задіяних під час реалізації політики безпеки;

С) взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

3. Технічний захист інформації – це ...

А) вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

В) взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

С) вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

7. Методи навчання

Виконання лабораторних робіт з використанням ПЗ; виконання індивідуальних навчально-дослідних завдань.

8. Форми контролю

Систематичний контроль за самостійною роботою студентів і якістю засвоєння ними поточного навчального матеріалу:

- на лабораторних роботах шляхом перевірки підготовки до виконання роботи;
- роботу над індивідуальними завданнями до лабораторних робіт;
- вивчення літератури, що рекомендувалася, та конспекту лекцій;
- оформлення звітів про виконання лабораторним роботам.

Поточний контроль знань студентів проводиться:

- на лабораторних роботах оцінюється підготовка до роботи, обсяг її виконання, результати захисту звіту;
- на лекційних заняттях виконується вибіркове опитування студентів;
- шляхом проведення модульних контролів знань студентів та виставлення рейтингових оцінок знань студентів по усім видам занять.

9. Розподіл балів, які отримують студенти.

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл. 1 «ПОЛОЖЕННЯ про екзамени та заліки у НУБіП України» (наказ про уведення в дію від «26» квітня 2023 р. протокол № 10):

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзамен	**Залік**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

Для визначення рейтингу студента із засвоєння дисципліни $R_{дис}$ (до 100 балів) одержаний рейтинг з атестації $R_{АТ}$ (до 30 балів) додається до рейтингу студента з навчальної роботи $R_{НР}$ (до 70 балів): $R_{дис}=R_{НР}+R_{АТ}$.

10.Методичне забезпечення

1. Електронний навчальний курс на платформі Moodle вміщує повне методичне забезпечення включаючи: лекції, презентації до лекцій, методичні вказівки до виконання лабораторних робіт, глосарій термінів тощо.

11. Рекомендована література

Основна:

1. НД ТЗІ 3.7-003 -2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» // Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. Київ. 2005. – С. 22.

2. Закон України «Про захист інформації в автоматизованих системах» // Відомості Верховної Ради України, 1994. - № 31. – С. 286.

3. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.].Вінниця : ВНТУ, 2018. - 118 с.

4. Проєктування комплексних систем захисту інформації. Підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. 320 с

5. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. – К.: ІСЗЗІ НТУУ «КПІ», 2015. – 104 с.

6. Методи та засоби інженерно-технічного захисту інформації навч. посіб. / В.В. Богданов, О.В.Волков, О.В.Жук, В.В.Мартинюк – К.: ВІТІ НТУУ «КПІ», 2013.

7. НД ТЗІ 1.1-002-1999 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. [в редакції станом на 28.12.2012. Київ. ДСТСЗІ СБ України, 2012, ст. 21.

8. НД ТЗІ 3.6-003-2016 Порядок проведення робіт зі створення та атестації комплексу технічного захисту інформації.

9. Постанова Кабінету Міністрів України від 16.02.1998 № 180 «Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах».

10. Постанова Кабінету Міністрів від 29.03.2006 № 373 «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

11.Технічні канали витоку інформації: навч. посіб. / Ю.Б. Науменко, Н.А. Паламарчук, С.А. Паламарчук, О.Є. Ткаленко – К.: ВІТІ НТУУ «КПІ», 2010.

12. Технічно-експлуатаційна документація до відповідних технічних засобів, систем та комплексів технічного захисту інформації, що вивчаються.

13. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95).

14. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ – ПЕМВН-95).

15. Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах.

16. ДСТУ 3396 0-96. Захист інформації. Технічний захист інформації. Основні положення.

17. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

18. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

19. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.

20. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення

21. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.

22. 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.

23. НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.

24. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі.

25. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

26. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

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

28. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.

Допоміжна

1. Кузнецов О.О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2011. – 510 с.

Інформаційні ресурси

1. АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=81998&cat_id=38835