Форма № Н - 3.04

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

"Стандарти інформаційної та кібернетичної безпеки"
зі спеціальності 125 – «Кібербезпека»
(шифр і назва напряму підготовки)
Освітня програма «Кібербезпека»

факультет інформаційних технологій
(назва факультету)

Київ – 2023 р.

Опис навчальної дисципліни

_____Стандарти інформаційної та кібернетичної безпеки _____

(назва)

Галузь знань, напрям підготовки, спеціальність, освітньо-кваліфікаційний рівень		
Галузь знань	Інформаційні технології	
Спеціальність	125 – «Кібербезпека»	
другий (магістерський) рівень	Бакалавр	
Характеристика навчальної дисципліни		
Вид	Вибіркова	
Загальна кількість годин	150	
Кількість кредитів ECTS	5	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
Форма контролю	Іспит	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	2023-2024	
Семестр	6	
Лекційні заняття	30 год.	
Практичні, семінарські заняття	30 год.	
Лабораторні заняття	-	
Самостійна робота	60 год.	
Індивідуальні завдання		
Кількість тижневих годин для денної форми навчання: аудиторних	4 год.	

1. Мета та завдання навчальної дисципліни

Мета дисципліни “Стандарти інформаційної та кібернетичної безпеки” полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для визначення місця і ролі кібербезпеки в загальній системі національної безпеки, стану та принципів забезпечення інформаційної безпеки особистості, суспільства та держави, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів ефективного та безпекового поводження з інформацією незалежно від її походження та виду в умовах широкого використання сучасних інформаційних технологій.

Дисципліна «Стандарти інформаційної та кібернетичної безпеки**»** взаємопов’язана з такими дисциплінами, як «Комплексні системи захисту інформації» та «Організаційне забезпечення захисту інформації».

В результаті вивчення курсу „Стандарти інформаційної та кібернетичної безпеки” студенти повинні:

– засвоїти основні фундаментальні поняття і закони нормативно-правового забезпечення кібербезпеки для їх використання в сучасних системах;

– розуміти взаємозв’язок інформаційної безпеки з інформаційним суверенітетом, національною безпекою та правами людини;

– знати основи державної та міжнародної політики у сфері забезпечення інформаційної безпеки (ІБ) та зміст основних положень нормативно-правових актів у сфері інформаційної безпеки;

– знати основні закони, принципи та правила поводження з інформацією;

– виявляти реальні та потенційні загрози у сфері інформаційної безпеки та законодавчі шляхи їх запобігання;

– знати основні методи маніпулювання свідомістю людини, впливу на суспільну думку з використанням сучасних інформаційно-комунікаційних технологій;

– знати основні положення юридичної відповідальності за правопорушення в інформаційній сфері та зміст основних міжнародних договорів з питань ІБ;

– розуміти основні проблеми правового забезпечення ІБ.

Завдання лекційних занять

Мета проведення лекцій полягає у тому, щоб ознайомити студентів із головними питаннями курсу «Стандарти інформаційної та кібернетичної безпеки».

Завдання проведення лекцій полягає у: викладенні студентам у відповідності з програмою та робочим планом основних питань курсу «Стандарти інформаційної та кібернетичної безпеки» та формуванні у студентів цілісної системи теоретичних знань з курсу «Стандарти інформаційної та кібернетичної безпеки».

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

Загальні компетентності:

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ2. Знання та розуміння предметної області та розуміння професії.

Спеціальні (фахові) компетентності:

СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

СК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

В результаті вивчення навчальної дисципліни студент набуде певні програмні результати, а саме:

ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;

ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.

Навчальна програма з курсу «Стандарти інформаційної та кібернетичної безпеки» є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма дисципліни «Стандарти інформаційної та кібернетичної безпеки» розроблена на підставі наступних документів:

-освітньо-професійна програма підготовки фахівців за спеціальністю «Кібербезпека»;

-навчальний план підготовки бакалаврів за спеціальністю «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.

2. Програма навчальної дисципліни

Змістовий модуль №1. Стандарти кібербезпеки.

Тема 1. Характеристика стандартів із забезпечення кібербезпеки.

Характеристика ефективних стандартів з кібербезпеки. Повнота стандартів.

Доступність стандартів. Корисність та актуальність стандартів. Форми представлення стандартів.

Тема 2. Міжнародний стандарт з оцінювання безпеки інформаційних технологій (ISO/IEC 15408).

Завдання стандарту ISO/IEC 15408. Зміст «Загальних критеріїв», структура стандарту ISO/IEC 15408, область застосування «Загальних критеріїв» та недоліки стандарту. Розроблення ІТ-продукту та його кваліфікаційний аналіз. Етапи здійснення кваліфікаційного аналізу. Специфікації функцій захисту. Заявка на відповідність профілю захисту.

Тема 3. Стандарт ISO/IEC 27002 «Інформаційні технології - Методики безпеки - Практичні правила управління безпекою інформації».

Загальні відомості про стандарт. Структура й основний зміст стандарту. Сфера застосування. Оцінювання й оброблення ризиків. Організація забезпечення безпеки інформації. Управління інцидентами безпеки інформації.

Тема 4. Міжнародний стандарт безпеки ISO/IEC 17799.

Загальні відомості. Стисла суть розділів стандарту. Розподіл відповідальності стосовно забезпечення безпеки. Класифікація та управління інформаційними ресурсами. Безпека в процесі роботи співробітника. Безпека носіїв даних. Контроль доступу в ОС. Використання системних утиліт. Безпека системних файлів. Захист даних, які використовуються в процесі тестування систем. Відповідність системи захисту основним вимогам.

Змістовий модуль 2. Нормативно-правове забезпечення кібербезпеки в зарубіжних країнах та Україні.

Тема 5. Порівняння підходів за ISO 17799 і BSI.

Німецький стандарт для вибору критерію аудиту BSI. Порівняння підходів за ISO 17799 і BSI. Міжнародний стандарт з управління СУІБ ISO 27001. Оцінювання ефективності існуючої системи захисту ІС на основі стандарту.

Тема 6. Інформаційна безпека як об’єкт правовідносин.

Сутність понять «суспільні відносини» та «правовідносини». Життєво важливі інтереси в інформаційній сфері. «Національні інтереси» - поняття та сутність. «Національні інтереси в інформаційній сфері» - поняття та сутність. Взаємозв`язок інформаційної безпеки з правовідносинами.

Тема 7. Поняття кібербезпеки, кіберзлочинності та кібертероризму в різних країнах.

Визначення поняття «кібернетична безпека» (кібербезпека). Стратегія кібербезпеки України. Конвенції про кіберзлочинність. Кібертероризм. Органи безпеки НАТО. Принципи та мінімальні стандарти політики безпеки НАТО. Вимоги щодо промислової та

індустріальної безпеки. Норми поводження з несекретною інформацією НАТО. Національні стратегії кібербезпеки різних країн. Національна стратегія кібербезпеки США. Національна стратегія кібербезпеки Європейського Союзу. Конвенція про кіберзлочинність.

Тема 8. Основна правова база забезпечення інформаційної та кібернетичної безпеки в Україні.

Доктринальні та концептуальні засади забезпечення інформаційної та кібернетичної безпеки. Основні законодавчі акти щодо забезпечення інформаційної та кібернетичної безпеки. Доктрина інформаційної безпеки України. Стратегія кібербезпеки України. Інформаційна війна. Захист службової інформації. Захист персональних даних (інформації про особу) в Україні.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Стандарти кібербезпеки.												
Тема 1. Характеристика стандартів із забезпечення кібербезпеки.	14	2	2			10						
Тема 2. Міжнародний стандарт з оцінювання безпеки інформаційних технологій (ISO/IEC 15408).	18	4	4			10						
Тема 3. Стандарт ISO/IEC 27002 «Інформаційні технології - Методики безпеки - Практичні правила управління безпекою інформації».	18	4	4			10						
Тема 4. Міжнародний стандарт безпеки ISO/IEC 17799.	23	4	4			15						
Разом за змістовим модулем 1	**73**	**14**	**14**			**45**						
Змістовий модуль 2. Нормативно-правове забезпечення кібербезпеки в зарубіжних країнах та Україні.												
Тема 5. Порівняння підходів за ISO 17799 і BSI.	18	4	4			10						
Тема 6. Інформаційна безпека як об'єкт правовідносин.	18	4	4			10						
Тема 7. Поняття кібербезпеки, кіберзлочинності та кібертероризму в різних країнах.	18	4	4			10						
Тема 8. Основна правова база забезпечення інформаційної та кібернетичної безпеки в Україні.	23	4	4			15						
Разом за змістовим модулем 2	**77**	**16**	**16**			**45**						
Усього годин за курс	**150**	**30**		**30**		**90**						

7. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1.	Практична робота №1. Характеристика стандартів із забезпечення кібербезпеки.	2
2.	Практична робота №2. Міжнародний стандарт з оцінювання безпеки інформаційних технологій (ISO/IEC 15408).	4
3.	Практична робота №3. Стандарт ISO/IEC 27002 «Інформаційні технології - Методики безпеки - Практичні правила управління безпекою інформації».	4
4.	Практична робота №4. Міжнародний стандарт безпеки ISO/IEC 17799.	4
5.	Практична робота №5. Стандартизація аудиту системи управління інформаційною безпекою на основі стандарту ISO 17799.	4
6.	Практична робота №6. Поняття кібербезпеки, кіберзлочинності та кібертероризму в різних країнах.	4
7.	Практична робота №7. Організаційна робота із захисту інформації з обмеженим доступом в країнах НАТО і ЄС.	4
8	Практична робота №8. Міжнародні правові інструменти і механізми протидії інформаційним порушенням та кіберзлочинності.	4
	Разом	**30**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1.	Національна стратегія кібербезпеки США.	6
2.	Національна стратегія кібербезпеки Європейського Союзу	6
3.	Оцінювання ефективності існуючої системи захисту ІС на основі стандарту.	6
4.	Характеристика ефективних стандартів з кібербезпеки.	6
5.	Інформаційна безпека як об’єкт правовідносин.	6
6.	Міжнародні правові інструменти і механізми протидії інформаційним порушенням та кіберзлочинності.	6
7.	Основна правова база забезпечення інформаційної та кібернетичної безпеки в Україні.	6
8.	Доктринальні та стратегічні нормативно-правові акти України в сфері забезпечення інформаційної безпеки.	6
9.	Основна правова база забезпечення інформаційної та кібернетичної безпеки в Україні.	6
10.	Оцінювання ефективності існуючої системи захисту ІС на основі стандарту.	6
11.	Принципи та мінімальні стандарти політики безпеки НАТО. Вимоги щодо промислової та індустріальної безпеки.	6
12.	Національна стратегія кібербезпеки Європейського Союзу. Конвенція про кіберзлочинність.	6
13.	Розподіл відповідальності стосовно забезпечення безпеки. Класифікація та управління інформаційними ресурсами.	6
14.	Основні суб`єкти створення небезпечної інформації.	6
15.	Основні суб`єктивні причини складності правового забезпечення інформаційної безпеки.	6
	Разом	**90**

9. Індивідуальні завдання
(ПЕРЕЛІК ПИТАНЬ ДЛЯ САМОСТІЙНОЇ РОБОТИ)

1. Визначення сутності інформації.
2. Основні показники класифікації носіїв інформації.
3. Засоби передачі та сприйняття інформації.
4. Основні властивості інформації які визначають її небезпечність.
5. Розкриття сутності інформаційної небезпеки.
6. Особисте бачення ролі та місця інформаційної безпеки у життєдіяльності суспільства у сучасних умовах.
7. Визначення поняття «інформаційна безпека».
8. Особисте бачення трансформації ролі та місця інформаційної безпеки в системі національної безпеки.
9. Особисте бачення трансформації ролі та місця інформаційної безпеки в системі національної безпеки.
10. Розкриття сутності безпечності інформації.
11. Основні чинники, які впливають на небезпечність інформації.
12. Розкриття визначення поняття «безпека інформації».
13. Основні суб`єкти створення небезпечної інформації.
14. Основні чинники визначення об’єктів інформаційної небезпеки.
15. Основні чинники визначення ієрархії об’єктів інформаційної небезпеки.
16. Головний принцип, якій забезпечує необхідний рівень інформаційної безпеки
17. Об’єкти інформаційної небезпеки та їх обґрунтування.
18. Коротка характеристика прав і свобод людини, громадянина та їх обов’язків в інформаційній сфері.
19. Коротка характеристика прав суспільства в інформаційній сфері.
20. Коротка характеристика обов’язків держави в інформаційній сфері.
21. Основна об`єктивна причина складності правового забезпечення інформаційної безпеки.
22. Основні суб`єктивні причини складності правового забезпечення інформаційної безпеки.
23. Коротке обґрунтування визначення кібернетики як об`єкту небезпеки.
24. Сутність поняття «кібернетична безпека» (кібербезпека).
25. Чинники які визначають взаємозв`язок понять «інформаційна безпека - ІБ» та «кібербезпека».
26. Чинники які визначають застосування термінів «ІБ» та «кібербезпека».
27. Сутність, поняття та правове визначення інформаційної діяльності.
28. Складові інформаційної діяльності.
29. Особисте розуміння співвідношення понять «національна безпека», «ІБ» та «кібернетична безпека».
30. У чому полягають основні відмінності у сутності понять «ІБ» та «кібербезпека».
31. Чинники які визначають взаємозв`язок інформаційної діяльності та інформаційної безпеки.
32. Сутність інформаційного насильства.
33. Суб`єкти інформаційної діяльності та їх вплив на процеси забезпечення ІБ.
34. Основні чинники які визначають особливості здійснення інформаційної діяльності в умовах постіндустріального суспільства.
35. Сутність маніпуляції.
36. Найбільше розповсюджені види маніпуляції.
37. Суб`єкти інформаційної діяльності та їх вплив на процеси забезпечення кібербезпеки.
38. Особливості маніпулювання свідомістю у сучасних умовах.
39. Наведіть приклади проявів інформаційного насильства.
40. Оцінка ролі маніпулювання в системі державного управління.
41. Оцінка місця маніпулювання в політичної системі.
42. Оцінка ролі та місце маніпулювання в системі міжнародних відносин.
43. Трансформація ролі та значення інформації на різних етапах розвитку людства.
44. Перспективи розвитку та механізми здійснення інформаційного насильства.
45. Механізми впливу інформації на поведінку людини.

46. В чому полягають тотожності та відмінності об`єктів інформаційної небезпеки та інформаційної безпеки?
47. Чому інформаційна діяльність є апріорі небезпечною з точки національної безпеки?
48. Спрямованість розвитку інформаційної діяльності.
49. Роль та значення інформаційних ресурсів у розвитку людства.
50. Тенденції змін у системі доступу до інформаційних ресурсів.
51. Оцінка стану національного інформаційного суверенітету у сучасних умовах.
52. Чинники які впливають на інформаційний суверенітет.
53. Витоки глобалізації інформаційного простору.
54. Механізми та засоби глобалізації інформаційного простору.
55. Основні принципові наслідки глобалізації інформаційного простору.
56. Витоки та наслідки соціальних мереж.
57. Перспективи розвитку соціальних мереж.
58. Структура нормативно-правової бази забезпечення захисту інформації.
59. Розкриття поняття «інформаційно-комунікаційна технологія» (ІКТ).
60. Розкриття понять «глобальна інформаційна система» та «глобальна мережа».
61. Природа інформаційного тероризму.
62. Розкриття поняття «соціалізація».
63. Поняття об`єктності та суб`єктності в системі правовідносин.

10. Методи навчання

Проведення лекцій з використанням технічних засобів навчання. Проведення практичних робіт та самостійної роботи засобами інформаційно-комунікаційних технологій в освіті. Використовується електронний навчальний курс на платформі Moodle «Стандарти інформаційної та кібернетичної безпеки».

11. Форми контролю

Наприкінці кожного змістовного модуля проводиться контрольна робота у вигляді тесту, що створений у комп'ютерному навчальному середовищі. Підсумкова атестація: іспит.

12. 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): $R_{дис}=R_{НР}+R_{АТ}$.

Оцінка виконання та захисту практичних робіт за кожний модуль здійснюється у наступній відповідності:

№ Практичної роботи	**Кількість балів**	**Загальна кількість балів**
1 модуль		
Практична робота № 1	15	70
Практична робота № 2	15	
Практична робота № 3	15	

Практична робота №4	15	
Самостійна робота	10	
Модульна контрольна		30
2 модуль		
Практична робота № 4	15	70
Практична робота № 5	15	
Практична робота № 6	15	
Практична робота № 7	15	
Самостійна робота	10	
Модульна контрольна		30

13. Методичне забезпечення

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

14. Рекомендовані джерела інформації

Базові

1. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017 // Офіційний вісник Президента України. – 2017. – № 5. – С. 15. – Ст. 102.
2. Довгань О.Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти: монографія; НАПрН України, НДІІП, НАН України, Нац. б-ка ім. В.І. Вернадського. – Київ, 2015. – 388 с.
3. Інформаційна безпека держави : підручник / [В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін.] ; в 2 т. – Т.1. / за аг. ред.. В.В. Остроухова. – К. : ДНУ «Книжкова палата Україна», 2016. – 264 с.
4. Стратегія кібербезпеки України: Указ Президента України від 15.03.2016 р. № 96/2016// Офіційний вісник України. – 2016. – № 23. – С. 69. – Ст. 899.
5. Стратегія національної безпеки України : Указ Президента України від 06.05.2015 р. № 287/2015// Офіційний вісник України. – 2015. – № 43. – С. 14. – Ст. 1353.
6. Воєнна доктрина України: Указ Президента України від 24.09.2015 р. №555/2015 // Офіційний вісник України. – 2015. – № 78. – С. 38. – Ст. 2592.
7. Законодавчі основи забезпечення інформаційної безпеки України: наукова доповідь / Пилипчук В.Г., Корж І.Ф., Петришин О.В., Савінова Н.А., Фурашев В.М. (За заг. ред. Пилипчука В.Г.) – К: НДІІП НАПрН України, 2014. – 60 с.
8. Конституція України : Закон України від 28.06.96 р. № 254к/96-ВР // Відомості Верховної Ради України (ВВР). – 1996. – № 30. – Ст. 141.
9. Концепція розвитку сектору безпеки і оборони України : Указ Президента України від 14.03.2016 р. № 92/2016 // Офіційний вісник України. – 2016. – № 23. – С. 12. – Ст. 898.
10. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори:проблеми безпеки, методи та засоби боротьби: Підручник. – К.: ДУТ, 2015. – 449 с.
11. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. – Житомир: ЖНАЕУ, 2016. – 636 с.
12. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л.Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа]; за заг. ред. д-ра техн. наук, професора В.Б. Толубка.— К.: ДУТ, 2015.— 288 с.

Допоміжні

1. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Василіу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ЦП «Компринт» О.В., 2020. – 444 с.

2. Параметри оцінки ефективності інформаційного права / П.В. Кіндрат // Право і суспільство. – 2016. – № 5. – С. 102–107. ISSN 2078–3736

3. Правові засади та пріоритети розвитку протидії негативним інформаційним впливам на дітей / О. Г. Радзієвська // Інформація і право. – 2017. – № 2(21)/2017. – С. 88-98.

4. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).

5. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. (ISO/IEC 27002:2013; Cor 1:2014, IDT).

15. 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

16. Нормативна література

1. ДСТУ ISO/IEC 11770-3:2002 «Інформаційні технології. Методи захисту».

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

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