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

"Організаційне забезпечення захисту інформації"
зі спеціальності 125 – «Кібербезпека»
(шифр і назва напряму підготовки)
Освітня програма «Кібербезпека»

факультет інформаційних технологій
(назва факультету)

Київ – 2023 рік

1. Опис навчальної дисципліни «Організаційне забезпечення захисту інформації»

(назва)

Галузь знань, напрям підготовки, спеціальність, освітньо-кваліфікаційний рівень		
Галузь знань	Інформаційні технології	
Спеціальність	125 – «Кібербезпека»	
другий (магістерський) рівень	Бакалавр	
Характеристика навчальної дисципліни		
Вид	Обов'язкова	
Загальна кількість годин	150	
Кількість кредитів ECTS	5	
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	2023-2024	
Семестр	3	
Лекційні заняття	30 год.	
Практичні, семінарські заняття		
Лабораторні заняття	30 год.	
Самостійна робота	90 год.	
Індивідуальні завдання		
Кількість тижневих годин для денної форми навчання: аудиторних	4 год.	

2. Мета, завдання та компетентності навчальної дисципліни

Мета: вивчення організаційних методів захисту, організаційно-технічних та організаційно-правових заходів, наукового підходу до організації захисту інформації; планування захисту; керування системою захисту; безперервності процесу захисту інформації; мінімальної достатності організації захисту; системного підходу до організації та проектування систем та методів захисту інформації; комплексного підходу до організації захисту інформації; відповідності рівня захисту цінності інформації; гнучкість захисту; багатозональності захисту, що передбачає розміщення джерел інформації в зонах з контрольованим рівнем її безпеки; обмеження числа осіб, які допускаються до захищеної інформації; особиста відповідальність персоналу за збереження довіреної інформації.

Місце і роль дисципліни в системі підготовки фахівців відповідно до навчального плану. Дана навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в галузі з питань інформаційної безпеки держави, а також сприяє здачі єдиного державного кваліфікаційного іспиту зі спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти.

Вимоги щодо знань і вмінь, набутих внаслідок вивчення дисципліни

Внаслідок вивчення дисципліни студенти повинні:

- знати: систему національного законодавства України та міжнародного законодавства у сфері кібербезпеки; систему управління інформаційною безпекою; основні принципи побудови СУІБ; основи управління інформаційними ризиками; напрямки побудови СУІБ; політику ІБ організації; фізичну безпеку організації та устаткування; управління комп'ютерами та мережами; управління доступом; вимоги до інформаційних систем; управління інцидентами в СУІБ; питання безперервності функціонування організації; організацію внутрішнього аудиту СУІБ; методику впровадження СУІБ; методи розробки політики інформаційної безпеки та цілей СУІБ; методи управління інформаційними активами; порядок впровадження системи управління інформаційними ризиками, розробки та обґрунтування заходів з обробки та зниження інформаційних ризиків; структуру документації СУІБ та порядок її розробки; порядок розробки управлінських процедур, плану безперервності функціонування організації, процедур реагування на надзвичайні ситуації, процедур переходу на аварійний режим; порядок введення в дію СУІБ.

- вміти:

діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки; готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки; 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; здійснювати оцінювання ризиків інформаційної безпеки та управління такими ризиками; застосовувати законодавчу та нормативно-правову базу для побудови СУІБ; розробляти політику ІБ організації; забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки; здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку; аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно з встановленою політикою інформаційної та\або кібербезпеки; впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки; розробляти політики інформаційної безпеки та цілей СУІБ; здійснювати управління інформаційними активами; застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; розробляти та обґрунтовувати заходів з обробки та зниження інформаційних ризиків; застосовувати законодавчу та нормативно-правову базу для розробки документації СУІБ та управлінських процедур; вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.

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):

СК 1. 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.

СК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

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

СК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

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

СК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

СК9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

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

ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній 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 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.

ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної, і/або кібербезпеки.

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 «Організаційне забезпечення захисту інформації» є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма дисципліни «Організаційне забезпечення 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 «Організаційне забезпечення захисту інформації» є курси «Навчальна практика з програмування та інформаційних технологій» та «Інформаційна безпека держави».

Курс «Організаційне забезпечення захисту інформації» є базовим для вивчення наступних дисциплін: «Безпека безпровідних, мобільних та хмарних технологій», «Ризики інформаційної безпеки» та «Комплексні системи захист інформації».

4. Програма та структура навчальної дисципліни

– повного терміну денної (заочної) форми навчання;

Назви змістових модулів і тем	Кількість годин												
	денна форма							Заочна форма					
	тижні	всього	у тому числі					Всього	у тому числі				
			л	п	лр	інд	с.р.		л	п	лр	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Змістовий модуль 1. Системи управління інформаційною безпекою.													
Тема 1. Система національного законодавства України та міжнародного законодавства у сфері кібербезпеки.	1	10	2		2		6						
Тема 2. Системи управління інформаційною безпекою. Основні принципи побудови СУІБ.	2	10	2		2		6						
Тема 3. Основи управління інформаційними ризиками (Ч1).	3	10	2		2		6						
Тема 4. Основи управління інформаційними ризиками (Ч2).	4	10	2		2		6						
Тема 5. Напрямки побудови СУІБ. Політика ІБ організації.	5	10	2		2		6						
Тема 6. Фізична безпека організації та устаткування. Управління комп'ютерами та мережами. Управління доступом. Вимоги до інформаційних систем.	6	10	2		2		6						
Тема 7. Управління інцидентами в СУІБ. Питання безперервності функціонування організації.	7	10	2		2		6						
Тема 8. Внутрішній аудит СУІБ.	8	10	2		2		6						
Разом за змістовим модулем 1		**80**	**16**		**16**		**48**						
Змістовий модуль 2. Впровадження системи управління інформаційною безпекою.													
Тема 1. Методика впровадження СУІБ.	9	10	2		2		6						
Тема 2. Розробка документа політики інформаційної безпеки та цілей СУІБ. Управління інформаційними активами (Ч1).	10	10	2		2		6						
Тема 3. Розробка документа політики інформаційної безпеки та цілей СУІБ. Управління інформаційними активами (Ч2).	11	10	2		2		6						
Тема 4. Впровадження системи управління інформаційними ризиками.	12	10	2		2		6						
Тема 5. Розробка та обґрунтування заходів з	13	10	2		2		6						

обробки та зниженню інформаційних ризиків.													
Тема 6. Структура документації СУІБ та порядок її розробки. Розробка управлінських процедур.	14	10	2		2		6						
Тема 7. Розробка плану безперервності функціонування організації. Розробка процедур реагування на надзвичайні ситуації. Розробка процедур переходу на аварійний режим. Введення в дію СУІБ.	15	10	2		2		6						
Разом за змістовим модулем 2		**70**	**14**		**14**		**42**						
Всього годин		**150**	**30**		**30**		**90**						

5. Теми практичних занять

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

6. Теми семінарських занять

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

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Аналіз нормативно-методичного забезпечення. Підготовка пропозицій до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.	2
2	Застосовування законодавчої та нормативно-правової бази, державних та міжнародних вимог, практик і стандартів з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.	2
3	Оцінювання ризиків інформаційної безпеки підприємства АПК.	2
4	Управління ризиками інформаційної безпеки підприємства АПК.	2
5	Розроблення політики ІБ організації.	2
6	Забезпечення захисту інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах.	2
7	Процедури управління інцидентами, проведення розслідувань.	2
8	Аналізування та оцінка ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.	2
9	Впровадження процесів, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.	2
10	Розроблення політики інформаційної безпеки та цілей СУІБ.	2
11	Здійснення управління інформаційними активами на прикладі підприємств АПК.	2
12	Застосування різних класів політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів на прикладі підприємств АПК.	2
13	Розроблення та обґрунтування заходів з обробки та зниження інформаційних ризиків.	2
14	Застосування законодавчої та нормативно-правової бази для розробки документації СУІБ та управлінських процедур.	2
15	Забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.	2
	Всього	30

Курсове проектування - Не передбачено робочим навчальним планом

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1.	Поняття системи управління інформаційною безпекою. Сутність політики інформаційної безпеки.	6
2.	Основні принципи побудови системи управління інформаційною безпекою. Напрямки побудови системи управління інформаційною безпекою.	6
3.	Заходи щодо організації захисту інформації.	6
4.	Класифікація інформації. Маркування інформації.	6
5.	Поводження з інформаційними ресурсами.	6
6.	Політика контролю доступу. Доступ до мереж та послуг мережі.	6
7.	Управління доступом користувача. Поняття контрольованої зони.	6
8.	Поняття інформаційних ризиків. Поняття оцінки ризиків інформаційної безпеки.	6
9.	Сутність оброблення ризиків інформаційної безпеки. Організаційні ролі, відповідальності та повноваження.	6
10.	Цілі інформаційної безпеки та планування їх досягнення. Поняття створення та оновлення документованої інформації.	6
11.	Контроль документованої інформації. Робоче планування та контроль.	6
12.	Оцінювання результативності інформаційної безпеки.	6
13.	Внутрішній аудит інформаційної безпеки. Перегляд системи управління інформаційною безпекою.	6
14.	Корегувальні дії по відношенню до системи управління інформаційною безпекою. Дії вищого керівництва організації з управління по відношенню до систем управління інформаційною безпекою.	6
15.	Зобов'язання вищого керівництва організації по відношенню до систем управління інформаційною безпекою.	6
	Разом	**90**

9. Індивідуальне завдання

Індивідуальна 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.

Контрольні питання для визначення рівня засвоєння знань студентами

1. Поняття «захист інформації».
2. Сутність та визначення «конфіденційність інформації».
3. Сутність та визначення «цілісність інформації».
4. Сутність та визначення «доступність інформації».
5. Поняття системи управління інформаційною безпекою.
6. Основні принципи побудови системи управління інформаційною безпекою.
7. Напрямки побудови системи управління інформаційною безпекою.
8. Заходи щодо організації захисту інформації.
9. Сутність політики інформаційної безпеки.

10. Класифікація інформації.
11. Маркування інформації.
12. Поводження з інформаційними ресурсами.
13. Поводження з носіями інформації.
14. Політика контролю доступу.
15. Доступ до мереж та послуг мережі.
16. Управління доступом користувача.
17. Поняття контрольованої зони.
18. Поняття інформаційних ризиків.
19. Поняття оцінки ризиків інформаційної безпеки.
20. Сутність оброблення ризиків інформаційної безпеки.
21. Організаційні ролі, відповідальності та повноваження.
22. Цілі інформаційної безпеки та планування їх досягнення.
23. Поняття створення та оновлення документованої інформації.
24. Контроль документованої інформації.
25. Робоче планування та контроль.
26. Оцінювання результативності інформаційної безпеки.
27. Внутрішній аудит інформаційної безпеки.
28. Перегляд системи управління інформаційною безпекою.
29. Корегувальні дії по відношенню до системи управління інформаційною безпекою.
30. Дії вищого керівництва організації з управління по відношенню до систем управління інформаційною безпекою.
31. Зобов'язання вищого керівництва організації по відношенню до систем управління інформаційною безпекою.
32. Визначення сфери застосування системи управління інформаційною безпекою.
33. Забезпечення фізичної безпеки організації та устаткування.
34. Управління комп'ютерами та мережами.
35. Управління доступом.
36. Вимоги до інформаційних систем.
37. Управління інцидентами в системі управління інформаційною безпекою.

10. Методи навчання

Пояснювально-ілюстративний метод – застосовується в ході лекцій та у процесі самостійної роботи студентів для передачі великих масивів навчальної інформації в опрацьованому вигляді.

Репродуктивний метод – застосовується в ході практичних занять і процесі самостійної роботи, передбачає набуття студентами навичок використання визначених алгоритмів вирішення навчальних та професійних завдань.

Метод проблематизації та евристичний метод – застосовуються в ході лекційних, лабораторних занять, самостійної та індивідуальної роботи.

11. Форми контролю

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

Підсумкова атестація – Екзамен.

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 лабораторних робіт за кожний модуль здійснюється у наступній відповідності:

№ лабораторної роботи	Кількість балів	Загальна кількість балів
	1 модуль -	**100**
Лабораторна робота № 1	6	70
Лабораторна робота № 2	8	
Лабораторна робота № 3	8	
Лабораторна робота № 4	8	
Лабораторна робота № 5	6	
Лабораторна робота № 6	8	
Лабораторна робота № 7	8	
Лабораторна робота № 8	8	
Самостійна робота	10	
Модульна контрольна		30
	2 модуль -	**100**
Лабораторна робота № 10	5	70
Лабораторна робота № 11	10	
Лабораторна робота № 12	10	
Лабораторна робота № 13	10	
Лабораторна робота № 14	5	
Лабораторна робота № 15	10	
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 лабораторних робіт, глосарій термінів тощо. Режим доступу: https://elearn.nubip.edu.ua/course/view.php?id=3831

2. Лахно В.А., Дрейс Ю.В., Касаткін Д.Ю. «Організаційне забезпечення захисту інформації» методичні рекомендації до виконання лабораторних робіт / В.А. Лахно, Ю.В. Дрейс, Д.Ю. Касаткін // – К.: НУБіП України, ВЦ Компрінт, 2021 р., - 89 с.

14. Рекомендовані джерела інформації

Основні:

1. Мужанова Т. М. Організаційне забезпечення інформаційної безпеки підприємства: основні засад / Т. М. Мужанова // Сучасний захист інформації. – 2016. №2. - с.78-82. - Режим доступу: http://nbuv.gov.ua/UJRN/szi_2016_2_13.

2. Правовий захист інформації: Навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса: Фенікс, 2015. – 264 с., іл.

3. Національний стандарт, який відповідає ISO/IEC 27001; Cor 1:2014, IDT) Information technology — Security techniques — Information security management systems — Requirements (Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги).

4. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.

5. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2017. – 120 с.

Додаткові:

1. M. E. Whitman, H. J. Mattord. Management of Information Security. [Електронний ресурс]. Режим доступу: https://ru.scribd.com/doc/102088851/Management-of-Information-Security

2. Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools. [Електронний ресурс]. Режим доступу: https://www.enisa.europa.eu.

Інформаційні ресурси

1. ISO [Електронний ресурс] – Режим доступу: https://www.iso.org/isoiec-27001-information-security.html

2. Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості [Електронний ресурс] – Режим доступу: http://uas.org.ua/ua/

3. 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

4. Закон «Про інформацію»: Прийнятий 2 жовтня 1992 р. №2657-XII // Відомості Верховної Ради України, 1992. – № 48. – С. 650.

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

6. Закон України «Про державну таємницю» // Відомості ВРУ, 1999. - № 49. – С. 428.

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

8. ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements.