МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра ____математичних методів та системного аналізу_____

ЗАТВЕРДЖУЮ
Завідувач кафедри ММСА
_____ Т.В. Шабельник
«__» _____ 2020 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОК.25. НДПП 1.2.13. **Управління інформаційною безпекою**
(шифр і назва навчальної дисципліни)

Освітньо-професійна програма Кібербезпека
(назва освітньо-професійної програми)

Напрям підготовки 125 Кібербезпека
(шифр і назва напряму підготовки)

Спеціальність 125 Кібербезпека
(шифр і назва спеціальності)

Спеціалізація_____
(назва спеціалізації)

Факультет Економіко-правовий
(назва факультету)

2020 - 2021 рік

Робоча програма з дисципліни управління інформаційною безпекою
(назва навчальної дисципліни)

для студентів ОПП Кібербезпека
за спеціальністю 125 Кібербезпека

Розробники:
Лазаревська Ю.А., асистент кафедри математичних методів та системного аналізу

(вказати авторів, їхні посади, наукові ступені та вчені звання)

Робоча програма затверджена на засіданні кафедри математичних методів та системного аналізу

Протокол від № 1 від “27” серпня 2020 року

Завідувач кафедри математичних методів та системногоаналізу

(підпис) (Шабельник Т.В.)
(прізвище та ініціали)

“27” серпня 2020 року

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td rowspan="2">Кількість кредитів – 5</td><td>Галузь знань
12 Інформаційні технології</td><td colspan="2" rowspan="2">Нормативна</td></tr>
<tr><td>125
“Кібербезпека”</td></tr>
<tr><td>Модулів – 2</td><td rowspan="5"></td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів –2</td><td>4-й</td><td></td></tr>
<tr><td>Індивідуальне науково-дослідне завдання - вирішення типових завдань за темами змістових модулів</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин - 150</td><td>8-й</td><td></td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання: самостійної роботи студента –</td><td rowspan="10">Освітньо-кваліфікаційний рівень: бакалавр</td><td>30</td><td>12</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>20</td><td>8</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>99</td><td>129</td></tr>
<tr><td colspan="2">Індивідуальні завдання:
1</td></tr>
<tr><td colspan="2">Вид контролю: екзамен</td></tr>
</table>

Примітка.

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить:

для денної форми навчання 1:4 (25%)

для заочної форми навчання

1. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни – є отримання студентами необхідних знань щодо принципів створення комплексних систем захисту інформації (КСЗІ) в інформаційних, комунікаційних та інформаційно – телекомунікаційних системах (далі – ІТС), здійснення комплексу заходів, спрямованих на розроблення і впровадження інформаційних технологій, які забезпечують обробку інформації в ІТС згідно з вимогами, встановленими нормативно – правовими актами та нормативними документами у сфері захисту інформації, а також принципів проведення експертизи КСЗІ, отримання студентами необхідних базових знань з організації та проведення аудиту інформаційної безпеки в інформаційно-телекомунікаційних системах різного призначення.

Значна увага приділяється засвоєнню принципів, задач системи управління інформаційною безпекою, вивченню нормативної та правової бази з питань організації та проведення аудиту інформаційної безпеки в інформаційно-телекомунікаційних системах різного призначення, методик оцінки інформаційних ризиків.

Завданням навчальної дисципліни є формування у с здобувачами вищої освіти певних знань та вмінь з теорії та практики побудови та аналізу систем управління інформаційною безпекою в ІТС організацій, установ, підприємств.

Місце навчальної дисципліни в освітній програмі: ОК 25. НДПП 1.2.13.

Передумови для вивчення дисципліни: «Управління інформаційною безпекою» є «Нормативно-правове забезпечення інформаційної безпеки», «Основи правознавства», «Українська мова (за професійним спрямуванням)», «Історія української культури».

Після вивчення дисципліни здобувач вищої освіти повинен **знати:**

- національну та міжнародну нормативно правову базу, науково-методичні та технічні принципи організації, впровадження та застосування систем управління захистом інформації в ІТС;
- принципи створення КСЗІ в ІТС;
- організацію та порядок проведення робіт з проектування, впровадження та супроводу комплексних систем захисту інформації в інформаційних, комунікаційних та інформаційно – телекомунікаційних системах;
- організацію та порядок проведення робіт з державної експертизи КСЗІ та засобів захисту інформації;
- вимоги міжнародних стандартів та вітчизняних нормативних документів в сфері захисту інформації щодо управління захистом інформації в інформаційних, комунікаційних та інформаційно – телекомунікаційних системах.
- вимоги міжнародних стандартів в галузі управління інформаційною безпекою;
- методи, методики, програмні засоби оцінки ризиків інформаційної безпеки в ІТС підприємств, установ, організацій.
- Вміти:
- здійснювати заходи щодо проектування, впровадження та супроводу, систем управління захистом інформації в інформаційних, комунікаційних та інформаційно – телекомунікаційних системах;

- застосовувати вимоги міжнародних стандартів та вітчизняних нормативних документів в сфері захисту інформації при проведенні державної експертизи КСЗІ та засобів захисту інформації, аудиту інформаційних систем та інформаційної безпеки.
- складати моделі загроз безпеки інформації та моделі потенційних порушників;
- розробляти технічні та часткові технічні завдання на КСЗІ;

Результати навчання: Організувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. 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. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та /або кібербезпеки. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організаці. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. Забезпечувати безперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод і громадянина в Україні.

2. Програма навчальної дисципліни

Розділ 1. Концепція побудови захищеної інформаційно-телекомунікаційної системи (ІТС).

Тема 1. Безпека корпоративних мереж. Проблематика безпеки IP мереж. Модель протидії загрозам безпеки. Побудова підсистеми інформаційної безпеки. Шляхи рішення проблем захисту інформації.

Тема 2. Концепція захищеної інформаційно-телекомунікаційної системи. Принципи створення захищеної інформаційно-телекомунікаційної системи. Концептуальна модель інформаційної безпеки організації. Структура концепції. Мета та завдання забезпечення безпеки інформації в ІТС організації.

Тема 3. Стратегія, основні напрямки та методи забезпечення безпеки інформації. Організаційна структура системи забезпечення безпеки інформації.

Розділ 2. Методологія управління інформаційною безпекою.

Тема 4. Концепція управління інформаційною безпекою**.** Принципи управління захистом інформації в ІТС. Задачі управління захистом інформації в ІТС. Глобальна і локальні політики управління захистом інформації в ІТС.

Тема 5. Міжнародні та вітчизняні стандарти в галузі управління, оцінки та аудиту інформаційної безпеки. Планування аудиту інформаційної безпеки організації. Управління аудитом інформаційної безпеки. Процесна модель управління інформаційною безпекою.

Тема 6. Технології аудиту інформаційної безпеки. Практичні шаги аудиту інформаційної безпеки. Задачі, що вирішуються при проведенні аудиту. Принципи аналізу і управління інформаційними ризиками. Методологія оцінки ризиків інформаційної безпеки. Перспективні методи оцінки ризиків інформаційної безпеки. Оцінка інформаційних ризиків з використання методів системного аналізу.

Тема 7. Технологія виявлення атак та аналізу захищеності ІТС. Засоби аналізу захищеності. Архітектура систем виявлення атак. Класифікація систем виявлення атак.

3. 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	сем	інд	с.р.
Модуль 1												
Змістовий модуль 1. Концепція побудови захищеної інформаційно-телекомунікаційної системи (ІТС).												
Тема 1. Безпека корпоративних мереж.	**14**	2		2		10	**17**	2				15
Тема 2. Концепція захищеної інформаційно-телекомунікаційної системи.	**20**	4		2		14	**18**	2		2		14
Тема 3. Стратегія, основні напрямки та методи забезпечення безпеки інформації.	**20**	4		2		14	**24**	2		2		20
Разом за змістовим модулем	**54**	**10**		**6**		**38**	**59**	**6**		**4**		**49**
Змістовий модуль 2. Методологія управління інформаційною безпекою												
Тема 4. Концепція управління інформаційною безпекою**.**	**24**	4		4		16	**22**	2				20
Тема 5. Міжнародні та вітчизняні стандарти в галузі управління, оцінки та аудиту інформаційної безпеки.	**26**	6		4		16	**24**	2		2		20

Тема 6. Технології аудиту інформаційної безпеки.	**24**	6		4		14	**24**	2		2		20
Тема 7. Технологія виявлення атак та аналізу захищеності ІТС.	**21**	**4**		2		15	**20**					20
Разом за змістовим модулем	**95**	**20**		**14**		**61**	**90**	**6**		**4**		**80**
Модуль 2												
ІЗ					**1**						**1**	
Усього годин	**150**	**30**		**20**	**1**	**99**	**150**	**12**		**8**	**1**	**129**

1

4. Теми семінарських (практичних) занять

Денна форма навчання

№ з/п	Види, зміст самостійної роботи	Кількість годин
1	Модель загроз. Модель протидії загрозам безпеки. Шляхи рішення проблем захисту інформації.	2
2	Концептуальна модель інформаційної безпеки організації. Побудова підсистеми інформаційної безпеки.	2
3	Організаційна структура системи забезпечення безпеки інформації. Служба захисту інформації (СЗІ). Функції, завдання, відповідальність, штатна структура СЗІ.	4
5	Міжнародні та вітчизняні стандарти в галузі управління, оцінки та аудиту інформаційної безпеки. Процесна модель управління інформаційною безпекою.	4
6	Методи оцінки ризиків інформаційної безпеки. Оцінка інформаційних ризиків з використання методів системного аналізу.	4
7	Засоби аналізу захищеності ІТС. Виявлення атак та управління інформаційними ризиками.	4
	Разом	20

Заочна форма навчання

№ з/п	Види, зміст самостійної роботи	Кількість годин

1	Модель загроз. Модель протидії загрозам безпеки. Шляхи рішення проблем захисту інформації.	2
2	Концептуальна модель інформаційної безпеки організації. Побудова підсистеми інформаційної безпеки.	2
3	Організаційна структура системи забезпечення безпеки інформації. Служба захисту інформації (СЗІ). Функції, завдання, відповідальність, штатна структура СЗІ.	2
5	Міжнародні та вітчизняні стандарти в галузі управління, оцінки та аудиту інформаційної безпеки. Процесна модель управління інформаційною безпекою.	2
6	Методи оцінки ризиків інформаційної безпеки. Оцінка інформаційних ризиків з використання методів системного аналізу.	2
	Разом	12

5. Самостійна робота

Денна форма навчання

№ з/п	Види, зміст самостійної роботи	Кількість годин
1	Підготовка до практичних занять та виконання домашніх завдань	35
2	Підготовка до лекційних занять та виконання завдань	20
3	Підготовка до тесту залишкових знань	30
4	Підготовка до контрольної роботи	14
	Разом (год)	99

Заочна форма навчання

№ з/п	Види, зміст самостійної роботи	Кількість годин
1	Підготовка до практичних занять та виконання домашніх завдань	55
2	Підготовка до лекційних занять та виконання завдань	35
3	Підготовка до тесту залишкових знань	20
4	Підготовка до контрольної роботи	19
	Разом (год)	129

6. Індивідуальні завдання

Підготовка тез доповіді на конференції/статті з обраної теми.

7. Методи контролю

Викладання дисципліни здійснюється через лекційні та практичні (семінарські) заняття, індивідуальні та групові консультації, самостійну роботу здобувачів освіти, тестування.

8. Критерії оцінювання

Критерії поточного оцінювання знань здобувачів освіти**.**

Усний виступ та виконання письмового завдання, тестування	Критерії оцінювання
5	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі тестові завдання.
4	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість тестових завдань.
3	В цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину тестових завдань.
2	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань.
1	Частково володіє навчальним матеріалом не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив окремі тестові завдання.

Доповнення виступу***:***

2 бали – отримують здобувачі освіти, які глибоко володіють матеріалом, чітко визначили його зміст; зробили глибокий системний аналіз змісту виступу, виявили нові ідеї та положення, що не були розглянуті, але суттєво впливають на зміст доповіді, надали власні аргументи щодо основних положень даної теми.

1 бал отримують здобувачі освіти, які виклали матеріал з обговорюваної теми, що доповнює зміст виступу, поглиблює знання з цієї теми та висловили власну думку.

Суттєві запитання до доповідачів***:***

2 бали отримують здобувачі освіти, які своїм запитанням до виступаючого суттєво і конструктивно можуть доповнити хід обговорення теми.

1 бал отримують здобувачі освіти, які у своєму запитанні до виступаючого вимагають додаткової інформації з ключових проблем теми, що розглядається.

Експрес-контроль***:***

2 бали нараховуються здобувачам освіти, які вільно володіють усім навчальним матеріалом, орієнтуються в темі та аргументовано висловлюють свої думки.

1 бал отримують здобувачі освіти, які частково володіють матеріалом та можуть окреслити лише деякі проблеми теми. Складання словника основних термінів**,** що визначені програмою курсу (за темами): Програмою курсу визначено перелік ключових термінів, що розкривають зміст кожної теми.

Здобувачам освіти пропонується скласти словник основних термінів з конкретної теми на останніх сторінках опорного конспекту лекцій.

2 бали нараховуються здобувачам освіти, які не лише склали повний перелік визначених термінів з конкретної теми, а й можуть вільно розтлумачити їх зміст.

1 бал нараховуються здобувачам освіти, які склали неповний перелік визначених термінів з конкретної теми і не можуть їх розтлумачити без конспекту.

Ведення опорного конспекту лекції***:***

2 бали нараховуються здобувачам освіти, які в повному обсязі самостійно і творчо опрацювали всі питання лекції і вільно володіють її змістом.

1 бал нараховується здобувачам освіти, які опрацювали лише окремі питання лекції і не достатньо вільно володіють її змістом.

Підготовка творчих завдань(есе, дайджест):

2 бали отримують здобувачі освіти, які можуть виокремити з різних джерел основні положення, структурно об’єднати їх, коротко проаналізувати кожне з них та зробити ґрунтовні узагальнюючі висновки.

1 бал отримують здобувачі освіти, які в цілому правильно виокремили основні положення кожного з джерел, але не зробили їх відповідного аналізу та узагальнюючих висновків.

Ведення конспекту першоджерел.

2 бали отримують здобувачі освіти, які опрацювали всю необхідну обов’язкову літературу, засвоїли її основні теоретичні положення, вміють їх

пояснити і розтлумачити.

1 бал отримують здобувачі освіти, котрі опрацювали не всю необхідну літературу, не завжди розуміють її вихідні теоретичні положення, поверхово їх пояснюють.

Підсумковий модульний контроль знань здобувачів освіти**.**

Критерії підсумкового модульного оцінювання знань здобувачів освіти

Письмова контрольна робота або тестування	Критерії оцінювання
21-25	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі тестові завдання.
17-21	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість тестових завдань.
14-17	В цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину тестових завдань.
10-14	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань.
10	Частково володіє навчальним матеріалом не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, и допускаючи при цьому суттєві помилки. Правильно вирішив окремі тестові завдання.

0	Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань. Не вирішив жодного тестового завдання.

9. Засоби оцінювання

Поточний контроль знань ЗВО здійснюється за допомогою тестів, опитувань по темам, захисту практичних (семінарських) робіт. Модульний контроль здійснюється із застосуванням тестів або письмової контрольної роботи. Підсумковий контроль здійснюється у формі екзамену.

Завданням поточного контролю знань ЗВО є перевірка розуміння та запам'ятовування певного теоретичного матеріалу, умінь самостійної роботи зі спеціальною літературою, набуття практичних навичок роботи з ПК і окремими програмними засобами, вміння пояснити і захистити свою роботу.

10. Розподіл балів, які отримують здобувачі освіти

Поточний контроль, самостійна робота, індивідуальні завдання			Разом	Екзамен	Сума
Змістовий модуль №1	Змістовий модуль №2	Контрольна робота, передбачена навчальним планом			
20	20	10	50	50	100

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 - 100	**A**	відмінно	зараховано
82 - 89	**B**	добре	
74 - 81	**C**		
70 - 74	**D**	задовільно	
64 - 73	**E**		
35 - 59	**F X**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0 - 34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

11. Інструменти, обладнання та програмне забезпечення:

Під час викладання дисципліни для занять використовується база комп'ютерних класів МДУ, які обладнано мережею комп'ютерів IBM Pentium.

12. Рекомендована література:

Основна література

1. Замула О.А., Горбенко Ю.І., Шумов А.І. Нормативно-правове забезпечення інформаційної безпеки. Комплексні системи захисту інформації»: Навч. посібник. - Харків: ХНУРЕ, 2010 - 158 с.
2. Замула О.А. Захист держаних секретів. Навчальний посібник. ХНУРЕ – 2004.– 206 с.
3. За редакцією Горбенко І.Д. Горбенко Ю.І. «Побудування та аналіз систем, протоколів та засобів криптографічного захисту інформації». . Монографія. Харків. Форт. 2016 , 902с.
4. За редакцією Горбенко І.Д. Горбенко Ю.І. «Побудування та аналіз систем, протоколів та засобів криптографічного захисту інформації». *Електронна версія*. Монографія. Харків. Форт. 2016 , 902с.
5. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Монографія. Харків. Форт. 2010 , 593с.
6. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків. Форт. 2013р. , 878с.

Допоміжна література

7. Конституція України. Закони України, т. 10, к. 1997
8. Закон України "Про інформацію" від 02.10.1992 року.
9. Закон України "Про державну таємницю" від 21.09.1999 року.
10. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31.05.2005 року, №2594- IV, К., 2005.
11. Положення про порядок здійснення криптографічного захисту інформації в Україні. Затверджено Указом Президенту України № 505 від 22.05. 1998 року
12. Про заходи щодо захисту інформаційних ресурсів держави. Затверджено Указом Президенту України №582 від 10.04 2000 року
13. Петренко С.А., Петренко А.А. Аудит інформаційної безпеки Internet. – М. ДМК Пресс, 2002-416 с.
14. Постанова КМУ від 29.03.2006р. № 373 « Правила забеспечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах ».
15. Порядок проведення робіт із створення комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. НД ТЗІ 3.1-003-2005.

Інформаційні ресурси

16. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп′ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ України від 24.04.1999 р. № 22 Чинний від 01.07.1999 р.

17. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ України від 28.04.1999 р. № 22 Чинний від 01.07.1999 р.

18. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТЗІ СБ України від 04.12.2000 р. № 53 Чинний від 15.12.2000 р.

19. Закон України "Про основи національної безпеки України", м. Київ, 19 червня 2003 р. №964-IV.

20. Марущак А.І. Правові основи захисту інформації з обмеженим доступом: курс лекцій. - К.: КНТ, 2007.-208 с.

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

22. Ліцензійні умови інформації. провадження господарської діяльності з розроблення, виробництва, впровадження, обслуговування, дослідження ефективності систем і засобів технічного захисту інформації, надання послуг у галузі технічного захисту інформації. Затверджено Наказом Державного комітету України з питань регуляторної політики та підприємництва та Адміністрації Державної служби спеціального зв'язку та захисту інформації України №5/9. Зареєстровано в Міністерстві юстиції України 11.02.2009 за № 130/16146.

23. Про затвердження переліку документів, які додаються до заяви про видачу ліцензії для окремого виду господарської діяльності. Постанова КМУ від 04.07.2001р. №756.

24. Порядок проведення робіт із сертифікації засобів забезпечення технічного захисту інформації загального призначення. Введено в дію Наказом ДСТСЗІ СБ України та Держстандарту України від 09.07.2001 р. №329/32.

25. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 № 2594-IV.

26. Правила посиленої сертифікації, затверджених наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України № 3 від 3.01.2005, зареєстрованих в Міністерстві юстиції України 27.01.2005 за № 104/10384 (у редакції наказу Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 10.05.2006 № 50).