МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра протидії кіберзлочинності, факультет № 4

РОБОЧА ПРОГРАМА

навчальної дисципліни «*Стандартизація і сертифікація в галузі інформаційної безпеки*»
обов'язкових **компонент**
освітньої програми *другого* рівня вищої освіти

125 Кібербезпека та захист інформації (безпека інформаційних та комунікаційних систем)

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30.08.2023 № 7

СХВАЛЕНО
Вченою радою факультету № 4
Протокол від 16.08.2023 № 8

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 29.08.2023 № 7

Розглянуто на засіданні кафедри протидії кіберзлочинності (*протокол від 15.08.2023 № 19*

Розробник:
Завідувач кафедри протидії кіберзлочинності, к.ю.н., професор Манжай О.В.

Рецензенти:

Тулупов В.В., доцент кафедри кібербезпеки та DATA-технологій факультету № 6 Харківського національного університету внутрішніх справ к.т.н., доцент;

Павликівський В.І., перший проректор Харківського університету, д.ю.н., професор

1. Опис навчальної дисципліни

<table>
<tr><th>Найменування показників</th><th>Шифри та назви галузі знань, код та назва спеціальності, ступінь вищої освіти</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><td>Кількість кредитів ECTS – 6
Загальна кількість годин – 180
Кількість тем – 2</td><td>12 Інформаційні технології
125 Кібербезпека
магістр</td><td>Навчальний курс 1
Семестр 2
Вид підсумкового контрою:
- екзамен.</td></tr>
<tr><td colspan="3">Розподіл навчальної дисципліни за видами занять:</td></tr>
<tr><td colspan="2">денна форма навчання

Лекції – 30;
Практичні заняття – 30;
Самостійна робота – 120;

Індивідуальні завдання:
Реферати – 1</td><td>заочна форма навчання

Лекції – 6;
Практичні заняття – 10;
Самостійна робота – 164;

Індивідуальні завдання:
Реферати – 1</td></tr>
</table>

2. Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни «Стандартизація і сертифікація в галузі інформаційної безпеки» є засвоєння здобувачами вищої освіти встановлених стандартами та іншими документами правил побудови комплексної системи захисту інформації та системи управління інформаційною безпекою.

Міждисциплінарні зв’язки: «Технічні засоби охорони об’єктів», «Державне управління у сфері кібербезпеки», «Сучасні проблеми забезпечення інформаційної безпеки держави».

Завданнями вивчення дисципліни «Стандартизація і сертифікація в галузі інформаційної безпеки» є дослідження чинних стандартів у сфері забезпечення безпеки інформації.

Згідно з освітньою програмою здобувачі вищої освіти повинні:

знати:

- основні правила та порядок побудови комплексної системи захисту інформації;
- основні правила та порядок побудови системи управління інформаційною безпекою;
- особливості дотримання правил кібербезпеки в системі публічної служби;

вміти:

- визначати відповідність стану безпеки інформації встановленим вимогам;
- будувати систему управління інформаційною безпекою згідно зі встановленими вимогами;

- об’єктивно оцінювати ризики для безпеки об’єкта та запобігати їм;
- приймати рішення щодо необхідності застосування того чи іншого способу реагування на загрозу;
- критично оцінювати інформацію;

бути ознайомленими

- з основною нормативно-методичною базою у сфері кібербезпеки та інформаційної безпеки.

Програмні компетентності:

Програмні компетентності, які формуються при вивченні навчальної дисципліни:		
Інтегральна компетентність	Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки	
Загальні компетентності (КЗ)	КЗ.1	Здатність застосовувати знання у практичних ситуаціях
	КЗ.4	Здатність оцінювати та забезпечувати якість виконуваних робіт
	КЗ.5	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Фахові компетентності (КФ)	КФ.1	Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки
	КФ.2	Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки
	КФ.4	Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог
	КФ.9	Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому
Програмні результати навчання (ПРН)	ПРН.1	Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань
	ПРН.3	Провадити дослідницьку та/або інноваційну

		діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі
	ПРН.5	Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення
	ПРН.8	Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури
	ПРН.9	Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки
	ПРН.10	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації

3. Програма навчальної дисципліни

Тема № 1. Нормативно-методична база побудови комплексної системи захисту інформації та системи управління інформаційною безпекою.

Нормативно-правова база кібербезпеки. Нормативно-правова база інформаційної безпеки. Нормативно-методичне забезпечення побудови комплексної системи захисту інформації. Система управління інформаційною безпекою.

Тема № 2. Особливості побудови системи управління інформаційною безпекою.

Терміни та методологічна база забезпечення системи управління безпекою інформації. Політика безпеки. Організація забезпечення безпеки інформації. Безпека людських ресурсів. Управління ресурсами системи управління інформаційною безпекою. Контроль доступу. Криптографія. Фізична безпека та безпека інфраструктури. Безпека експлуатації. Безпека комунікацій. Придбання, розроблення та підтримка інформаційних систем. Взаємовідносини з постачальниками. Управління інцидентами інформаційної безпеки.

4. Структура навчальної дисципліни

4.1.1. Розподіл часу навчальної дисципліни за темами, спеціалізація «безпека інформаційних та комунікаційних систем»

(денна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 2							
Тема № 1 **Нормативно-методична база побудови комплексної системи захисту інформації та системи управління інформаційною безпекою**	**70**	**4**	**0**	**4**	**0**	**62**	**Екзамен**
Тема № 2 **Особливості побудови системи управління інформаційною безпекою**	**110**	**26**	**0**	**26**	**0**	**58**	
Всього за семестр № 2:	**180**	**30**	**0**	**30**	**0**	**120**	

(заочна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 2							
Тема № 1 **Нормативно-методична база побудови комплексної системи захисту інформації та системи управління інформаційною безпекою**	**86**	**2**	**0**	**2**	**0**	**82**	**Екзамен**
Тема № 2 **Особливості побудови системи управління інформаційною безпекою**	**94**	**4**	**0**	**8**	**0**	**82**	
Всього за семестр № 2:	**180**	**6**	**0**	**10**	**0**	**164**	

4.1.3. Питання, що виносяться на самостійне опрацювання

Перелік питань до тем навчальної дисципліни	Література:
Тема № 1. Нормативно-методична база побудови комплексної системи	

		захисту інформації та системи управління інформаційною безпекою	
		Самостійно дослідити нормативно-правові акти, як регламентують правила побудови комплексної системи захисту інформації	**1-46, Інтернет**
		Самостійно дослідити нормативно-правові акти, як регламентують правила побудови системи управління інформаційною безпекою	**1-46, Інтернет**
		Підготувати реферат про досвід впровадження системи управління інформаційною безпекою в одній із зарубіжних країн	**1-46, Інтернет**
		Тема № 2. Особливості побудови системи управління інформаційною безпекою	
		Скласти політику безпеки для типового підрозділу поліції	**1-46, Інтернет**
		Вивчити термінологію, яка використовується для забезпечення функціонування системи управління безпекою інформації	**1-46, Інтернет**
		Підготувати таблицю криптографічних засобів, дозволених для використання під час побудови системи управління інформаційною безпекою	**1-46, Інтернет**
		Вивчити методи організації дистанційної роботи на об’єкті інформаційної діяльності	**1-46, Інтернет**

5. Індивідуальні завдання

5.1.1. Теми рефератів

1. Нормативно-правова база інформаційної безпеки.
2. Нормативно-правова база кібербезпеки.
3. Нормативно-методичне забезпечення побудови комплексної системи захисту інформації.
4. Мандатна політика безпеки.
5. Дискреційна політика безпеки.
6. Рольова політика безпеки.
7. Принципи управління безпекою інформації.
8. Структура політики безпеки.
9. Ролі та повноваження щодо безпеки інформації.
10. Безпека інформації в управлінні проектами

5.1.2. Теми курсових робіт

1. Політика щодо мобільного обладнання.
2. Суб’єкти зовнішньої взаємодії у секторі безпеки.
3. Безпека інформації в управлінні проектами.
4. Маркування та обробка інформації.
5. Політика використання криптографічних засобів.
6. Державні стандарти України з криптографічних алгоритмів і механізмів.
7. Контроль інсталяції програмного забезпечення на комп’ютерній техніці.

5.1.3. Теми наукових робіт

1. Управління безпекою мережі.
2. Процедури реагування на інциденти інформаційної безпеки.
3. Взаємозв’язок комплексної системи захисту інформації та системи управління інформаційною безпекою.

6. Методи навчання

Лекції із застосуванням мультимедійного проектора; практичні заняття: моделювання ситуативних задач, дебати, тренінги, рольові та ігрові заняття, розв'язання задач тощо.

7. Перелік питань та завдань, що виносяться на підсумковий контроль

1. Співвідношення понять «інформаційна безпека» та «кібербезпека».
2. Головні загрози кібербезпеці згідно з українським законодавством.
3. Об'єкти кібербезпеки.
4. Потенціал та стратегічні цілі кібербезпеки.
5. Основні пріоритети державної політики в інформаційній сфері щодо забезпечення інформаційної безпеки.
6. Основні процедурні моменти створення побудови комплексної системи захисту інформації.
7. Послідовність дій власника (розпорядника) інформаційно-телекомунікаційних систем із організації розробки комплексної системи захисту інформації.
8. Порядок організації і проведення державної експертизи комплексної системи захисту інформації.
9. Контроль за функціонуванням комплексної системи захисту інформації.
10. Система управління інформаційною безпекою як альтернатива комплексній системі захисту інформації.
11. Поняття загрози безпеки інформації та їх види.
12. Вразливості та їх види.
13. Послідовність вивчення ризиків.
14. Залишкові ризики.
15. Аудит системи безпеки.
16. Події та інциденти безпеки інформації.
17. Моніторинг інформаційних систем та процесів.
18. Система стандартів щодо побудови системи безпеки інформації.
19. Класифікація стандартів ISO/IEC 27-ї серії.
20. Зміст окремих стандартів щодо побудови системи безпеки інформації.
21. Поняття політики безпеки.
22. Методична основа для створення та розробки політики безпеки.
23. Форма представлення політики безпеки.
24. Види політик безпеки.
25. Формалізація суб'єктно-об'єктної моделі системи.
26. Типові помилки під час розробки політики безпеки.
27. Напрями, за якими можуть бути виписані правила для політики безпеки.
28. Змістовне наповнення політики безпеки згідно зі стандартом ДСТУ ISO/IEC 27002:2015.
29. Структурні елементи політики безпеки.

30. Перегляд політики безпеки.
31. Повноваження працівників у сфері забезпечення безпеки інформації.
32. Розподіл відповідальності окремих працівників за убезпечення інформаційних ресурсів.
33. Розмежування доступу до ресурсів інформаційних систем.
34. Делегування повноважень працівників.
35. Вимоги до осіб, відповідальних за впровадження заходів безпеки.
36. Система допуск-доступ до конкретних видів інформаційних ресурсів.
37. Суб'єкти зовнішньої взаємодії у секторі безпеки.
38. Безпека інформації в управлінні проектами.
39. Політика роботи з мобільним обладнанням.
40. Регламентація віддаленої роботи в організації.
41. Повноваження працівників у сфері забезпечення безпеки інформації.
42. Розподіл відповідальності окремих працівників за убезпечення інформаційних ресурсів.
43. Розмежування доступу до ресурсів інформаційних систем.
44. Делегування повноважень працівників.
45. Вимоги до осіб, відповідальних за впровадження заходів безпеки.
46. Система допуск-доступ до конкретних видів інформаційних ресурсів.
47. Суб'єкти зовнішньої взаємодії у секторі безпеки.
48. Безпека інформації в управлінні проектами.
49. Політика роботи з мобільним обладнанням.
50. Регламентація віддаленої роботи в організації.
51. Зміст політики використання криптографічних засобів.
52. Цілі впровадження криптографічних засобів.
53. Стани життєвого циклу криптографічного ключа.
54. Державні стандарти України з криптографічних алгоритмів і механізмів.
55. Зміст політики використання криптографічних ключів.
56. Державні стандарти України з управління ключами.
57. Яким чином має регламентуватися діяльність щодо засобів оброблення інформації, управління якими здійснюється безпосередньо організація/установа?
58. Як слід кваліфікувати події, які впливають на цілісність, доступність та функціонування журналів аудиту подій (логів)?
59. Чим відрізняються правила та порядок виконання робіт на території організації/установи, які застосовуються до найманого персоналу та третіх осіб?
60. Які вимоги висуваються до фізичного розташування обладнання та ліній комунікації?
61. Яи мають бути врегульовані питання передачі обладнання? Якщо так, що має бути передбачено?
62. Сформулюйте три правила, які описують принцип «чистого столу» та «чистого екрану».
63. Що захищається при убезпеченні комунікацій організації?

64. Заходи управління безпекою мережі.
65. Державні стандарти України з убезпечення комп’ютерної мережі.
66. Що таке послуги комп’ютерної мережі?
67. Як описується безпека послуг комп’ютерної мережі?
68. Якою має бути, в контексті безпеки, взаємодія з постачальником послуг мережі?
69. Характеристики безпеки послуг комп’ютерної мережі.
70. Що потребує сегментації в комп’ютерній мережі?
71. За якими ознаками може бути визначено логічні мережні домени?
72. За допомогою яких рішень здійснюється сегментація та контроль доступу між доменами?
73. Що визначає вимоги безпеки домену комп’ютерної мережі?
74. Політики, процедури та заходи безпеки обміну інформацією.
75. Зміст угод щодо безпечного обміну діловою інформацією.
76. Заходи захисту електронного обміну повідомленнями.
77. Зміст угод щодо конфіденційності або нерозголошення для зовнішніх сторін або працівників організації.
78. Цілі управління інцидентами інформаційної безпеки.
79. Взаємозв’язок понять при виникненні інцидентів інформаційної безпеки.
80. Загальний перелік заходів управління інцидентами інформаційної безпеки та вдосконалення СУІБ.
81. Які процедури мають бути розроблені та поширені всередині організації для управління інцидентами інформаційної безпеки?
82. Що забезпечують процедури реагування на інциденти інформаційної безпеки?
83. Що мають включати процедури звітування в управлінні інцидентами інформаційної безпеки?
84. Які події інформаційної безпеки потребують звітування?
85. Віднесення подій до інцидентів інформаційної безпеки.
86. Реагування на інциденти інформаційної безпеки.
87. Аналіз і зіставлення інцидентів інформаційної безпеки.
88. Питання процедур ідентифікації, збирання, отримання і зберігання цифрових доказів щодо інцидентів інформаційної безпеки.
89. Представлення Державних стандартів України через фази процесу розслідування інцидентів інформаційної безпеки.

8. Критерії та засоби оцінювання результатів навчання здобувачів

Контрольні заходи оцінювання результатів навчання включають в себе поточний та підсумковий контролі.

Засобами оцінювання результатів навчання можуть бути екзамени (комплексні екзамени); тести; наскрізні проекти; командні проекти; аналітичні звіти, реферати, есе; розрахункові та розрахунково-графічні роботи; презентації результатів виконаних завдань та досліджень; завдання на лабораторному обладнанні, тренажерах, реальних об'єктах тощо; інші види

індивідуальних та групових завдань.

Поточний контроль. До форм поточного контролю належить оцінювання:

- рівня знань під час семінарських, практичних, лабораторних занять;
- якості виконання самостійної роботи.

Поточний контроль здійснюється під час проведення семінарських, практичних та лабораторних занять і має на меті перевірку набутих здобувачем вищої освіти (далі – здобувач) знань, умінь та інших компетентностей з навчальної дисципліни.

У ході поточного контролю проводиться систематичний вимір приросту знань, їх корекція. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національної системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Оцінки за самостійну роботу виставляються в журналі обліку роботи академічної групи окремою графою за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Результати цієї роботи враховуються під час виставлення підсумкових оцінок.

При розрахунку успішності здобувачів враховуються такі види робіт: навчальні заняття (семінарські, практичні, лабораторні тощо); самостійна робота (виконання домашніх завдань, ведення конспектів першоджерел та робочих зошитів, виконання розрахункових завдань, підготовка рефератів, наукових робіт, публікацій, розроблення спеціальних технічних пристроїв і приладів, моделей, комп'ютерних програм, виступи на наукових конференціях, семінарах та інше); контрольні роботи (виконання тестів, контрольних робіт у формі, передбаченій в робочою програмою навчальної дисципліни). Вони оцінюються за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Здобувач, який отримав оцінку «незадовільно» за навчальні заняття або самостійну роботу, зобов'язаний перескласти її.

Загальна кількість балів (оцінка), отримана здобувачем за семестр перед підсумковим контролем, розраховується як середньоарифметичне значення з оцінок за навчальні заняття та самостійну роботу, та для переводу до 100-бальної системи помножується на коефіцієнт **10**.

$$\textit{Загальна кількість балів (перед підсумковим контролем)} = (\ (\ \textit{Результат навчальних занять за семестр} + \textit{Результат самостійної роботи за семестр}\ )\ /\ 2\ )\ *10$$

Підсумковий контроль. Підсумковий контроль проводиться з метою оцінки результатів навчання на певному ступені вищої освіти або на окремих його завершених етапах.

Для обліку результатів підсумкового контролю використовується поточно-накопичувальна інформація, яка реєструються в журналах обліку роботи академічної групи. Результати підсумкового контролю з дисциплін відображуються у відомостях обліку успішності, навчальних картках здобувачів, залікових книжках. ***Присутність здобувачів на проведенні***

підсумкового контролю (заліку, екзамену) обов'язкова. Якщо здобувач вищої освіти не з'явився на підсумковий контроль (залік, екзамен), то науково-педагогічний працівник ставить у відомість обліку успішності відмітку «не з'явився».

Підсумковий контроль (екзамен, залік) оцінюється за національною шкалою. Для переводу результатів, набраних на підсумковому контролі, з національної системи оцінювання в 100-бальну вводиться коефіцієнт **10**, таким чином максимальна кількість балів на підсумковому контролі (екзамені, заліку), які використовуються при розрахунку успішності здобувачів, становить **50.**

Підсумкові бали з навчальної дисципліни визначаються як сума балів, отриманих здобувачем протягом семестру, та балів, набраних на підсумковому контролі (екзамені, заліку).

Підсумкові бали навчальної дисципліни = ***Загальна кількість балів (перед підсумковим контролем)*** + ***Кількість балів за підсумковим контролем***

Здобувач вищої освіти, який під час складання підсумкового контролю (екзамен, залік) отримав незадовільну оцінку, складає його повторно. Повторне складання підсумкового екзамену чи заліку допускається не більше двох разів з кожної навчальної дисципліни: один раз – викладачеві, а другий – комісії, до складу якої входить керівник відповідної кафедри та 2-3 науково-педагогічних працівники.

Якщо дисципліна вивчається протягом двох і більше семестрів з семестровим контролем у формі екзамену чи заліку, то результат вивчення дисципліни в поточному семестрі визначається як середньоарифметичне значення балів, набраних у поточному та попередньому семестрах.

Підсумкові бали навчальної дисципліни = ***Підсумкові бали за поточний семестр*** + ***Підсумкові бали за попередній семестр*** : ***2***

У цьому розділі також повинні бути розроблені чіткі критерії оцінювання здобувачів вищої освіти під час поточного контролю *(робота на семінарських, практичних, лабораторних та інших аудиторних заняттях, самостійна робота, виконання індивідуальних творчих завдань)* та підсумкового контролю. Кафедра визначає вимоги до здобувачів стосовно засвоєння змісту навчальної дисципліни, а саме: кількість оцінок, яку він повинен отримати під час аудиторної роботи, самостійної роботи. Наприклад:

Робота під час навчальних занять	**Самостійна робота**	**Підсумковий контроль**
Отримати не менше 4 позитивних оцінок	Підготувати реферат, підготувати конспект за темою самостійної роботи, виконати практичне завдання тощо	Отримати за підсумковий контроль не менше 30 балів

9. Шкала оцінювання: національна та ECTS

Оцінка в балах	**Оцінка за національною шкалою**	**Оцінка**	
		Оцінка	**Пояснення**

12	**97-100**	Відмінно («зараховано»)	A	**«Відмінно»** – теоретичний зміст курсу засвоєний **цілком,** необхідні практичні навички роботи з освоєним матеріалом сформовані, **усі** навчальні завдання, які передбачені програмою навчання, **виконані** в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
11	**94-96**			
10	**90-93**			
9	**85-89**	Добре («зараховано»)	B	**«Дуже добре»** – теоретичний зміст курсу засвоєний **цілком**, необхідні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **усі** навчальні завдання, які передбачені програмою навчання, **виконані**, якість виконання **більшості** з них оцінено числом балів, близьким до **максимального,** робота з двома - трьома незначними помилками.
8	**80-84**			
7	**75 – 79**		C	**«Добре»** – теоретичний зміст курсу засвоєний **цілком**, практичні навички роботи з освоєним матеріалом **в основному** сформовані, **усі** навчальні завдання, які передбачені програмою навчання, **виконані**, якість виконання **жодного** з них **не оцінено мінімальним** числом балів, деякі види завдань виконані **з помилками,** робота з декількома незначними помилками, або з однією – двома значними помилками.
6	**70-74**	Задовільно («зараховано»)	D	**«Задовільно»** – теоретичний зміст курсу засвоєний **частково**, але **прогалини не носять істотного** характеру, необхідні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **більшість** передбачених програмою навчання навчальних завдань **виконано, деякі** з виконаних завдань містять **помилки,** робота з трьома значними помилками.
5	**65-69**			
4	**60-64**		E	**«Достатньо»** – теоретичний зміст курсу засвоєний **частково, деякі** практичні навички роботи **не сформовані, частина** передбачених програмою навчання навчальних завдань **не виконана** або якість виконання деяких з них оцінено числом балів, близьким до **мінімального**, робота, що задовольняє мінімуму критеріїв оцінки.
3	**40–59**	Незадовільно («не зараховано»)	FX	**«Умовно незадовільно»** – теоретичний зміст курсу засвоєний **частково**, необхідні практичні навички роботи **не сформовані, більшість** передбачених програм навчання, навчальних завдань **не виконано**, або якість їхнього виконання оцінено числом балів, близьким до **мінімального**; при **додатковій самостійній** роботі над матеріалом курсу **можливе підвищення якості** виконання навчальних завдань (**з можливістю повторного складання**), робота, що потребує доробки.
2	**21-40**			
1	**1–20**		F	**«Безумовно незадовільно»** – теоретичний зміст курсу **не освоєно**, необхідні практичні навички роботи **не сформовані, всі виконані** навчальні завдання містять грубі **помилки, додаткова самостійна** робота над матеріалом курсу **не приведе** до значного **підвищення якості** виконання навчальних завдань, робота, що потребує повної переробки.

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Манжай О.В., Мелешко Д.Г., Носов В.В., Самойлов С.В. Розробка та впровадження системи управління безпекою інформації. Київ: ВАІТЕ, 2021. 138 с.

2. Манжай О. В., Манжай І. А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків : Промарт, 2020. 162 с. з іл.

3. Науково-практичний коментар Закону України «Про основні засади забезпечення кібербезпеки України». Станом на 1 січня 2019 року / М.В. Гуцалюк та ін.; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.

Допоміжна

1. Про інформацію. Закон України від 02.10.1992, № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

2. Про Державну службу спеціального зв'язку та захисту інформації України. Закон України: від 23.02.2006, № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

3. Про захист інформації в інформаційно-комунікаційних системах. Закон України: від 05.07.1994, № 1170-VII. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

4. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 10.08.2022).

5. Про створення Центру протидії дезінформації: Рішення Ради національної безпеки і оборони України від 11 березня 2021 року, введено в дію Указом Президента України від 19 березня 2021 року № 106/2021. URL: https://zakon.rada.gov.ua/laws/show/106/2021#Text

6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

7. Про захист персональних даних. Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

8. ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів - На заміну ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT).

9. ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT) / Поправка № 2:2019.

10. (ISO/IEC 27001:2013/Cor 2:2015, IDT) Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги.

11. ДСТУ ISO/IEC 27002:2015 (ISO/IEC 27002:2013; Cor 1:2014, IDT) / Поправка № 2:2019 (ISO/IEC 27002:2013/Cor 2:2015, IDT). Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.

12. ДСТУ ISO/IEC 27003:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова (ISO/IEC 27003:2017, IDT).

13. ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання (ISO/IEC 27004:2016, IDT).

14. ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT) Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки - На заміну ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT).

15. ДСТУ ISO/IEC 27006:2015 Інформаційні технології. Методи захисту. Вимоги до органів, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою (ISO/IEC 27006:2015, IDT).

16. ДСТУ ISO/IEC 27007:2018 Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою (ISO/IEC 27007:2017, IDT).

17. ДСТУ ISO/IEC TS 27008:2019 (ISO/IEC TS 27008:2019, IDT) Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки - На заміну ДСТУ ISO/IEC TR 27008:2018 (ISO/IEC TR 27008:2011, IDT).

18. ДСТУ ISO/IEC 27009:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Визначення для сфери застосування ISO/IEC 27001. Вимоги (ISO/IEC 27009:2016, IDT).

19. ДСТУ ISO/IEC 27017:2017 Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002, для хмарних послуг (ISO/IEC 27017:2015, IDT).

20. ДСТУ ISO/IEC 27021:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Вимоги до компетенції для професіоналів з керування інформаційною безпекою (ISO/IEC 27021:2017, IDT).

21. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT).

22. ДСТУ ISO/IEC 27033-1:2017 Інформаційні технології. Методи захисту. Захист мережі. Частина 1. Огляд і поняття (ISO/IEC 27033-1:2015, IDT).

23. ДСТУ ISO/IEC 27033-2:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 2. Настанови щодо проектування та реалізації безпеки мережі (ISO/IEC 27033-2:2012, IDT).

24. ДСТУ ISO/IEC 27033-3:2016 Інформаційні технології. Методи захисту. Безпечність мережі. Частина 3. Еталонні мережеві сценарії. Загрози, методи проектування та проблеми керування (ISO/IEC 27033-3:2010, IDT).

25. ДСТУ ISO/IEC 27033-4:2016 Інформаційні технології. Методи захисту. Безпека мережі. Частина 4. Убезпечення комунікацій між мережами з використанням шлюзів безпеки (ISO/IEC 27033-4:2014, IDT).

26. ДСТУ ISO/IEC 27033-5:2016 Інформаційні технології. Методи захисту. Безпечність мережі. Частина 5. Убезпечення комунікацій уздовж мереж із використанням віртуальних приватних мереж (VPNs) (ISO/IEC 27033-5:2013, IDT).

27. ДСТУ ISO/IEC 27033-6:2018 Інформаційні технології. Методи захисту. Безпека мережі. Частина 6. Забезпечення безпроводового доступу до IP-мережі (ISO/IEC 27033-6:2016, IDT).

28. ДСТУ ISO/IEC 27035-1:2018 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами (ISO/IEC 27035-1:2016, IDT).

29. ДСТУ ISO/IEC 27035-2:2018 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти (ISO/IEC 27035-2:2016, IDT).

30. ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT).

31. ДСТУ ISO/IEC 27038:2018 Інформаційні технології. Методи захисту. Специфікація для цифрового редагування (ISO/IEC 27038:2014, IDT).

32. ДСТУ ISO/IEC 27040:2016 Інформаційні технології. Методи захисту. Безпека зберігання (ISO/IEC 27040:2015, IDT).

33. ДСТУ ISO/IEC 27041:2016 Інформаційні технології. Методи захисту. Настанова щодо забезпечення прийнятності та адекватності методів розслідування (ISO/IEC 27041:2015, IDT).

34. ДСТУ ISO/IEC 27042:2016 Інформаційні технології. Методи захисту. Настанови щодо аналізу та інтерпретації цифрового доказу (ISO/IEC 27042:2015, IDT).

35. ДСТУ ISO/IEC 27043:2016 Інформаційні технології. Методи захисту. Принципи та процеси розслідування інцидентів (ISO/IEC 27043:2015, IDT).

36. ДСТУ ISO/IEC 27050-1:2018 Інформаційні технології. Методи захисту. Електронне виявлення. Частина 1. Огляд та поняття (ISO/IEC 27050-1:2016, IDT).

37. ДСТУ ISO/IEC 27050-3:2018 Інформаційні технології. Методи захисту. Електронне виявлення. Частина 3. Звід правил для електронного виявлення (ISO/IEC 27050-3:2017, IDT).

38. ДСТУ ISO/IEC 18033-1:2017 Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 1. Загальні положення (ISO/IEC 18033-1:2015, IDT).

39. ДСТУ ISO/IEC 9796-3:2015 Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 3. Механізми, що ґрунтуються на дискретному логарифмі (ISO/IEC 9796-3:2006, IDT).

40. ДСТУ ISO/IEC 11770-1:2015 Інформаційні технології. Методи захисту. Керування ключами. Частина 1. Основні положення (ISO/IEC 11770-1:2010).

41. ДСТУ ISO/IEC 11770-2:2015 Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів (ISO/IEC 11770-2:2008; Cor 1:2009, IDT).

42. ДСТУ ISO/IEC 11770-3:2015 Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів (ISO/IEC 11770-3:2008; Cor 1:2009, IDT).

43. ДСТУ ISO/IEC 11770-4:2015 Інформаційні технології. Методи захисту. Керування ключами. Частина 4. Механізми, засновані на нестійких секретах (ISO/IEC 11770-4:2008; Cor 1:2009, IDT).

44. ДСТУ ISO/IEC 11770-5:2015 Інформаційні технології. Методи захисту. Керування ключами. Частина 5. Керування груповими ключами (ISO/IEC 11770-5:2011, IDT).

Інформаційні ресурси в Інтернеті

45. Каталог національних стандартів та кодексів усталеної практики. URL: https://katalog.uas.org.ua.