МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра кібербезпеки та DATA-технологій, факультет № 6

РОБОЧА ПРОГРАМА

навчальної дисципліни **«Технічні засоби охорони об'єктів критичної інфраструктури»** обов'язкових компонент освітньої програми другого рівня вищої освіти

"Кібербезпека (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 № 6
Протокол від 25.08.2023 № 7

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

Розглянуто на засіданні кафедри кібербезпеки та DATA-технологій факультету №6 *(протокол від 15.08.2023 № 8)*

Розробник:
1. доцент кафедри кібербезпеки та DATA-технологій, к.т.н., доцент Світличний В.А.

Рецензенти:
1. завідувач кафедри інформаційних управляючих систем ХНУРЕ, д.т.н., професор Петров К.Е.,
2. провідний науковий співробітник Науково-дослідної лабораторії з проблем розвитку інформаційних технологій ХНУВС, к.т.н., доцент Мордвинцев М.В.

1. Опис навчальної дисципліни

Найменування показників	Шифри та назви галузі знань, код та назва спеціальності, ступінь вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 8 Загальна кількість годин – 240 Кількість тем – 4	12 Інформаційні технології, 125 Кібербезпека, магистр	Навчальний курс 1 Семестр 2 Вид підсумкового контрою: – екзамен
Розподіл навчальної дисципліни за видами занять:		
денна форма навчання		заочна форма навчання
Лекції – 40 год; Лабораторні заняття – 28 год; Практичні заняття – 12 год. Самостійна робота – 160 год; Індивідуальні завдання: Курсова робота – немає; Реферати (тощо) – немає.		Лекції – 10 год; Лабораторні заняття – 8 год; Практичні заняття – 6 год; Самостійна робота – 216 год; Індивідуальні завдання: Курсова робота – немає; Реферати (тощо) – немає.

2. Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни "Технічні засоби охорони об'єктів" є аналіз структури технічних засобів охорони об`єктів, їх складу та окремих елементів, принципів функціонування та побудови, формування знань та вмінь забезпечення технічної безпеки об’єктів що охороняються.

Основними завданнями вивчення дисципліни "Технічні засоби охорони об'єктів" є:

- вивчення особливостей предметної області засобів охорони об`єктів;
- вивчення структури інформаційних трактів в охорони об`єктів;
- вивчення параметрів та характеристик технічних засобів і систем охорони об`єктів;
- отримання практичних навичок вирішення задач інсталяції та синтезу елементів технічних засобів і систем охорони об`єктів.

Згідно з освітньою програмою здобувачі вищої освіти повинні:

знати:

- сучасну концепцію захисту та охорони об'єкта;
- основні відомості про технічні засобі і системи охорони об`єктів, принципи їхнього функціонування та побудови;
- основні складові та структуру технічних засобів і систем охорони об`єктів;
- рівні фізичної безпеки об'єкта;
- інтегровані системи охорони об'єкта;
- основні характеристики технічних засобів охоронної сигналізації;
- основні характеристики систем збору і обробки інформації;
- основні характеристики систем відеоспостереження;
- основні характеристики систем контролю доступу;
- тенденції розвитку технічні засобі і системи охорони об`єктів.

вміти: аналізувати технічні засоби охорони об`єктів та проводити порівняння з метою вибору найбільш ефективних;

- формувати вимоги до технічних засобів охорони об`єктів;
- розробляти структурні, функціональні схеми елементів технічних засобів охорони;
- застосовувати передовий досвід, що представлений у джерелах літератури та правові акти, що висвітлюють зазначенні питання;
- застосовувати отримані знання при вирішенні практичних завдань організації охорони об'єктів.

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.
Фахові компетентності спеціальності (КФ)	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 3	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
	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 5	Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
	КФ 6	Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

3. Програма навчальної дисципліни

Тема № 1 Системи безпеки об'єкта, поняття, класифікація, вимоги.

Комплексна система безпеки об'єкта, поняття, класифікація, вимоги. Принципи побудови охоронної сигналізації. Засоби та системи охоронної сигналізації. Тактико-технічні характеристики. Засоби та системи пожежної сигналізації. Тактико-технічні характеристики.

Тема № 2. Системи контролю та управління доступом.

Основні поняття і функції систем та засобів контролю і управління доступом. Елементи систем контролю та управління доступом. Управляючі загороджувальні пристрої систем контролю та управління доступом.

Тема № 3. Будівельні конструкції та інженерні засоби захисту об'єктів.

Будівельні конструкції технічного захисту об'єктів. Інженерні засоби технічного захисту об'єктів».

Тема № 4. Технічні засоби і системи відеоспостереження.

Технічні засоби відеоспостереження. Елементи систем відеоспостереження. Формати стиску цифрового зображення. Сучасні засоби і системи відеоспостереження.

4. Структура навчальної дисципліни

4.1.1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни					Вид контролю
	Всього	з них:				
		лекції	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр №2						
Тема №1. Системи безпеки об'єкта, поняття, класифікація, вимоги	64	10	4	10	40	
Тема №2. Системи контролю та управління доступом	60	10	4	6	40	
Тема №3. Будівельні конструкції та інженерні засоби захисту об'єктів	58	10	2	6	40	**екз.**
Тема №4. Технічні засоби і системи відеоспостереження	58	10	2	6	40	
Всього за семестр	**240**	**40**	**12**	**28**	**160**	

4.1.2. Розподіл часу навчальної дисципліни за темами (заочна форма навчання)

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни					Вид контролю
	Всього	з них:				
		лекції	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр №2						
Тема №1. Системи безпеки об'єкта, поняття, класифікація, вимоги	60	2	2	2	54	
Тема №2. Системи контролю та управління доступом	60	2	2	2	54	
Тема №3. Будівельні конструкції та інженерні засоби захисту об'єктів	62	4	2	2	54	**екз.**
Тема №4. Технічні засоби і системи відеоспостереження	58	2		2	54	
Всього за семестр	**240**	**10**	**6**	**8**	**216**	

4.1.3. Питання, що виносяться на самостійне опрацювання

Перелік питань до тем навчальної дисципліни	Література
Тема №1. Системи безпеки об'єкта, поняття, класифікація, вимоги	
Відпрацювати матеріал лекцій за темою. Поглиблено вивчити теоретичні питання лекційних занять, а також опрацювати завдання до практичних, лабораторних занять, що входять до теми №1: – **Лекція № 1. «Комплексна система безпеки об'єкта, поняття, класифікація, вимоги».** Етапи розвитку інтегрованих систем безпеки. – **Лекція № 2. «Принципи побудови охоронної сигналізації».** Вимоги до технічного оснащення засобами охоронної сигналізації. – **Лекція №3. «Засоби та системи охоронної сигналізації. Тактико-технічні характеристики».** Тактико-технічні характеристики типових систем охорони. – **Лекція №4. «Засоби та системи пожежної сигналізації. Тактико-технічні характеристики».** Технічні системи протипожежного захисту об'єктів.	[1-3, 21-44], ресурси мережі Internet
Тема №2. Системи контролю та управління доступом	
Відпрацювати матеріал лекцій за темою. Поглиблено вивчити теоретичні питання лекційних занять, а також опрацювати завдання до практичних, лабораторних занять, що входять до теми №2: – **Лекція №5. «Системи та засоби контролю та управління доступом».** Біометричні засоби контролю та управління доступом. – **Лекція №6. «Елементи систем контролю та управління доступом».** Біометричні зчитувачі. – **Лекція №7. «**Управляючі загороджувальні пристрої систем контролю та управління доступом»**.** Обладнання для КПП і прохідних.	[4, 11-12, 46-50,] ресурси мережі Internet
Тема №3. Будівельні конструкції та інженерні засоби захисту об'єктів	

Перелік питань до тем навчальної дисципліни		Література
	Відпрацювати матеріал лекцій за темою. Поглиблено вивчити теоретичні питання лекційних занять, а також опрацювати завдання до практичних, лабораторних занять, що входять до теми 3: – **Лекція №8. «Елементи будівельних конструкцій захисту об'єкта».** Елементи будівельних конструкцій призначені для забезпечення захисту об'єкта; – **Лекція №9. «Інженерні засоби захисту об'єкта».** Характеристики інженерних засобів охорони.	[8-10], ресурси мережі Internet
	Тема №4. Технічні засоби і системи відеоспостереження	
	Відпрацювати матеріал лекцій за темою. Поглиблено вивчити теоретичні питання лекційних занять, а також опрацювати завдання до практичних, лабораторних занять, що входять до теми 4: – **Лекція №10. «Технічні засоби і системи відеоспостереження».** Пристрої відображення; – **Лекція №11. «Елементи систем відеоспостереження».** Відеодетектори руху; – **Лекція №12. «Формати стиску цифрового зображення».** Принципи кодування відеозображення у форматах MJPEG, MPEG4, H.264; – **Лекція №13. «Сучасні засоби та системи відеоспостереження».** Аналіз переваг та недоліків IP–відеоспостереження.	[1,3,4, 11-15, 45-50], ресурси мережі Internet

5. Індивідуальні навчально-дослідні завдання

5.1.1. Теми наукових доповідей

1. Національні інтереси України в сфері інформаційної безпеки.
2. Стан інформаційної безпеки України.
3. Основні завдання, положення, організаційна структура поліції охорони.
4. Потенційні загрози безпеці та типові завдання захисту.
5. Основні напрями забезпечення безпеки інформації та інформаційних ресурсів за допомогою технічних систем захисту.
6. Міжнародне співробітництво України в сфері систем та технологій управління та контролю фізичного доступу.
7. Аналіз систем технічного спостереження.

8. Становлення та розвиток систем сигналізації інформації в Україні.
9. Види та властивості інформації як предмета захисту.
10. Напрями державної політики України в сфері інформатизації та інформаційної безпеки особистості, суспільства, держави.

6. Методи навчання

Аудиторні заняття проводяться у формі практичних занять, на яких здобувачі вищої освіти другого рівня, повинні вміти розв’язувати типові задачі курсу, проводити фізичне моделювання практичних задач.

Самостійна робота за кожною темою – це засвоєння основних фізичних явищ, методів фізичного дослідження, передбачає поглиблене вивчення теоретичних питань лекційних занять, а також опрацювання завдань практичних і лабораторних занять.

Індивідуальна робота передбачає застосування елементів наукового пізнання сучасного світу при виконанні наукових робіт (доповідей).

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

Контроль проводиться по тестових завданнях на підсумковому контролі - екзамені.

Контрольні тестові питання

1. Що є найважливішим елементом захисту інформації на об'єкті?
2. Для чого призначена система керування та контролю доступу?
3. Для чого призначена система охоронної сигналізація?
4. Для чого призначена система пожежної сигналізації?
5. Для чого призначена система відеоспостереження?
6. Для чого призначена система захисту інформації?
7. Для чого призначена система життєзабезпечення?
8. Яка роль приділяється персоналу служби безпеки?
9. Призначення спец. засобів огляду, відбиття та ліквідації погроз.
10. Що розуміють під процедурними засобами?
11. Для чого призначена система оперативного та гучномовного зв'язку?
12. Що містять у собі елементи будівельних конструкцій?
13. Що належить до інженерних засобів захисту?
14. Які етапи розвитку інтегрованих систем безпеки Вам відомі?
15. Що є об'єктами охоронної сигналізації?
16. Хто є суб'єктами охоронної сигналізації?
17. Як поділяються технічні засоби охоронно-пожежної сигналізації по області застосування та функціональному призначенню?
18. Як розрізняються охоронні сповіщувачі по виду контрольованої зони?
19. Як розрізняються охоронні сповіщувачі за принципом дії?
20. Для охорони яких об'єктів призначені приймально-контрольні прилади малої, середньої та великої інформаційної ємкості?
21. Оповіщувачі: призначення та види повідомлення.
22. Системи передачі тривожних повідомлень: призначення та вид використаного каналу зв'язку.
23. Поняття багаторубіжної охорони об'єктів.
24. Які об'єкти блокуються першим, другим, третім рубежем охорони?

25. Які типи сповіщувачів застосовують для першого, другого, третього рубежу охорони?
26. Основні вимоги пропоновані до точкових датчиків рубежів охорони.
27. Який принцип дії сповіщувача лінійного радіохвильового "Радій-2"?
28. Для чого призначений проводовий засіб охоронної сигналізації "Уран"?
29. Який принцип дії сповіщувача "Біном М"?
30. Призначення та принцип дії оптико-електронного лінійного сповіщувача "Вектор-СПЭК 150".
31. Призначення та принцип дії сповіщувача об'ємного радіохвильового "Шторм-2".
32. Принцип дії сповіщувача магніто-контактного типу.
33. Які об'єкти здатний блокувати сповіщувач поверхневий ємнісний "ПІК"?
34. Призначення та принцип дії сповіщувача поверхневого п'єзоелектричного "Грань-2", "Гюрза-50П3".
35. Які Вам відомі тактико-технічні характеристики приймально-контрольних приладів "Сигнал-20", "Астра-712/4", "Адрес"?
36. Які типові системи експлуатує поліція охорони?
37. Призначення та функціональний склад системи "Фобос".
38. Перспективні напрямки розвитку інтегрованих систем безпеки.
39. Класифікація технічних засобів протипожежного захисту об'єктів.
40. Як поділяються пожежні сповіщувачі відповідно до первинних ознак пожежі?
41. Принцип дії пожежного димового сповіщувача.
42. Принцип дії пожежного теплового сповіщувача.
43. Чим визначається зона виявлення пожежного сповіщувача?
44. Що означає поняття перешкодозахищеність сповіщувача?
45. Чим характеризується чутливість сповіщувача?
46. Що означає поняття інерційності сповіщувача?
47. Які основні принципи вибору пожежних сповіщувачів Вам відомі?
48. Що необхідно враховувати при виборі та монтажі пожежних сповіщувачів залежно від їхньої конструкції та принципу дії?
49. Основні властивості та призначення приймально-контрольних приладів і сигнально-спускових пристроїв пожежної сигналізації?
50. Призначення, конструктивні особливості та технічні характеристики модуля порошкового гасіння "Буран-1".
51. Призначення, конструктивні особливості та технічні характеристики автоматичної системи протипожежного захисту приміщень "АПСЗ-03Ф1".
52. Призначення, конструктивні особливості та технічні характеристики апаратури системи автоматичного пожежегасіння "АСАП-01Ф".
53. Для чого призначені системи керування та контролю доступу?
54. Що розуміють під процесом ідентифікації?
55. На чому заснована біометрична ідентифікація?
56. Основні функції СКУД?
57. Які існують електронні системи ідентифікації?
58. Переваги та недоліки мережних СКУД.
59. Переваги та недоліки автономних СКУД.
60. Відмінні риси СКУД з розподіленою архітектурою.
61. Тактико-технічні можливості контролера N-750.

62. Технічні можливості програмного забезпечення та контролерів СКУД компанії APPOLO.
63. Які Вам відомі технології біометричної ідентифікації?
64. Конструктивні особливості та принцип дії карти Віганда.
65. Переваги та недоліки зчитувачів і карт Віганда.
66. Принцип дії PROX ідентифікації.
67. Особливості активної та пасивної PROX-ідентифікації.
68. Переваги та недоліки PROX і карт.
69. Переваги та недоліки інфрачервоних зчитувачів і брелоків.
70. Переваги та недоліки LOGO і HICO магнітних карт.
71. Принцип дії Smart-технології.
72. Переваги та недоліки Smart-карт.
73. Застосування клавіатурного уведення для ідентифікації.
74. Що означає коефіцієнт надійності, помилка першого та другого роду?
75. Способи біометричної ідентифікації.
76. Особливості та функціональна структура програмного забезпечення СКУД.
77. Вибір програмного забезпечення СКУД.
78. Конструктивні особливості електромагнітного, електромоторного та соленоїдного замків.
79. Які технічні засоби можуть застосовуватися для регулювання руху автотранспортом?
80. Як класифікуються приводи для воріт?
81. Основні технологічні способи керування приводами для воріт?
82. Особливості керування за допомогою PROX-карт і міток фірми Motorola Indiana Corp.
83. Устаткування для КПП і прохідних.
84. Класифікація турнікетів.
85. Призначення та конструкція повнозростового турнікета роторного типу.
86. Технічна реалізація доступу на особливо важливі об'єкти.
87. Характерні особливості шлюзових кабін.
88. У якому випадку дозволяється установка ґрат або сіток із внутрішньої сторони приміщення?
89. Які технічні вимоги висуваються перед елементами будівельних конструкцій призначених для забезпечення захисту об'єкта?
90. Які Ви знаєте види огородження периметра?
91. Призначення огородження периметра.
92. Призначення та технічні характеристики огородження периметра та окремих ділянок території об'єкта, що знаходиться під охороною.
93. Що таке зона відторгнення? Що розміщається в цій зоні?
94. Призначення та технічні характеристики контрольно-слідової смуги.
95. Призначення та технічні характеристики воріт і хвірток.
96. Що включать у себе інженерні засоби захисту об'єкта?
97. У чому полягає посилення дерев'яної коробки дверей?
98. Які технічні вимоги висуваються перед вікнами та дверима?
99. Призначення фарбування металевих поверхонь.
100. Поняття захисного скляного покриття.
101. Забезпечення захисту інформації за допомогою багатошарового листового скла.

102. Загальне призначення та функціональний склад "замкнутих телевізійних систем" (CCTV- Closed Circuit TeleVision).
103. Конструктивні особливості відіконів.
104. Типи світлочутливих матриць, особливості перетворення сигналу.
105. Переваги та недоліки світлочутливих матриць CCD і CMOS типів.
106. Ефективна та повна кількість пікселів світлочутливої матриці.
107. Процес формування кольорового зображення в системах охоронного спостереження.
108. Що означає поняття роздільна здатність відеокамери?
109. Що розуміють під чутливістю відеокамери?
110. Основні характеристики об'єктивів відеокамер.
111. Призначення ND фільтра.
112. Особливості Pin-hole об'єктивів.
113. Яке устаткування відноситься до комутаційних пристроїв передачі відеосигналу?
114. Призначення та особливості квадраторів відеосигналу.
115. Призначення та особливості дуплексних мультиплексорів.
116. Призначення та особливості триплексних мультиплексорів.
117. Призначення та особливості мережних мультиплексорів, мережних відеореєстраторів і відеорекордерів.
118. У яких випадках застосовуються матричні комутатори?
119. Основні характеристики пристроїв відображення відеосигналу.
120. Призначення та технічні особливості пристроїв документування відеосигналу.
121. Способи передачі відеосигналу на відстань.
122. Особливості та технічна реалізація передачі відеосигналу на відстань до 300 метрів.
123. Особливості та технічна реалізація передачі відеосигналу на відстань до 1500 метрів.
124. Особливості та технічна реалізація передачі відеосигналу на відстань більше 1500 метрів.
125. Які тактико-технічні характеристики цифрових реєстраторів відеосигналу Ви знаєте?
126. Що прийнято розуміти під критерієм якості відеозапису?
127. Які формати стиску відеоінформації Вам відомі?
128. Що необхідно знати для визначення мінімально необхідного дискового простору відеореєстратора?
129. Для чого призначені відеовиходи BNC і D- Sub у відеореєстраторі?
130. Які мережні функції відеореєстраторів Вам відомі?
131. Реалізація керування зовнішніми пристроями (відеокамерами, тривожними виходами, іншими відеореєстраторами).
132. Програмні особливості використання формату стиску MJPEG у відеореєстраторах.
133. Програмні особливості використання формату стиску MPEG- 4 у відеореєстраторах.
134. Програмні особливості використання формату стиску H.264/MPEG-4 AVC у відеореєстраторах.
135. Поняття про кадри відеозображення.
136. Основні методи стиску відеоданих у форматі H.264.

137. Які основні відмінності IP-відеокамери від інших типів відеокамер охоронного спостереження?
138. Історія створення IP-відеокамери?
139. Які функціональні елементи має у своєму складі IP-відеокамера?
140. Типові апаратні рішення організації IP-відеоспостереження?
141. Основні переваги IP-відеокамер і IP-відеоспостереження в порівнянні зі звичайними камерами та системами?
142. Основні недоліки IP-відеокамер і IP-відеоспостереження в порівнянні зі звичайними камерами та системами?

8. Критерії та засоби оцінювання результатів навчання здобувачів

Контрольні заходи включають у себе поточний та підсумковий контроль.

Поточний контроль.

До форм поточного контролю належить оцінювання:

- рівня знань під час практичних і лабораторних занять;
- якості виконання індивідуальної та самостійної роботи.

Поточний контроль здійснюється під час проведення практичних та лабораторних занять і має за мету перевірку засвоєння знань, умінь і навичок здобувачем вищої освіти другого рівня (далі – здобувач) 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 та індивідуальну роботи виставляються в журнали 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 (практичні, лабораторні тощо); самостійна та індивідуальна роботи (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 вигляді, передбаченому в робочій програмі 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.

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

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, 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 працівника.

Критерії оцінювання здобувачів вищої освіти під час поточного контролю *(робота на практичних, лабораторних заняттях, самостійна робота, виконання індивідуальних завдань)* та підсумкового контролю.

Робота під час навчальних занять	**Самостійна та індивідуальна робота**	**Підсумковий контроль**
Отримати не менше 4 позитивних оцінок	Підготувати наукову доповідь, підготувати звіт за темою самостійної роботи.	Отримати за підсумковий контроль не менше 30 балів

9. Шкала оцінювання: національна та ECTS

Оцінка в балах	**Оцінка за національною шкалою**	**Оцінка за шкалою ECTS**	
		Оцінка	**Пояснення**
97-100	Відмінно ("зараховано")	A	**„Відмінно"** – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом сформовані, всі навчальні завдання, які передбачені програмою навчання виконані в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
94-96			
90-93			

85-89	Добре (“зараховано”)	B	**„Дуже добре”** – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання більшості з них оцінено числом балів, близьким до максимального, робота з двома – трьома незначними помилками.
80-84			
75-79		C	**„Добре”** – теоретичний зміст курсу освоєний цілком, практичні навички роботи з освоєним матеріалом в основному сформовані, всі 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.
70-74	Задовільно (“зараховано”)	D	**„Задовільно”** – теоретичний зміст курсу освоєний не повністю, але прогалинине 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.
65-69			
60-64		E	**„Достатньо”** – теоретичний зміст курсу освоєний частково, деякі практичні навички роботи не сформовані, частина передбачених програмою навчання навчальних завдань не виконані, або якість виконання деяких з них оцінено числом балів, близьким до мінімального,робота, що задовольняє мінімуму критеріїв оцінки.
40-59	Незадовільно („не зараховано”)	FX	**„Умовно незадовільно”** – теоретичний зміст курсу освоєний 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
21-40			
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 значимого підвищення якості виконання навчальних завдань, робота, що потребує повної переробки

10.Рекомендована література основна, допоміжна, інформаційні ресурси в Інтернеті

Основна література

1. Світличний В.А. Тексти лекцій з дисципліни «Технічні засоби охорони об`єктів». Харків: ХНУВС, 2022. (Електронний варіант).
2. Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник. – К.: ІСЗЗІ НТУУ «КПІ», 2016. – 104 с.
3. Пількевич І.А., Лобанчикова Н.М.,. Молодецька К.В.Захист інформації в автоматизованих системах управління: посібник. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
4. Бурячок В.Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна і кібербезпека: соціотехнічний аспект: Підручник. – К.: ДУТ, 2015. – 288 с.
5. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. – К.: ДУТ, 2015. – 449 с.
6. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. –

Житомир: ЖНАЕУ, 2016. – 636 с.
7. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
8. Поля і хвилі в системах технічного захисту інформації : підручник для студентів вищих навчальних закладів. Ч.1. / В.М. Шокало, В.А.Усін, Д.В.Грецьких, В.О. Хорошко, Л.П. Крючкова ; за заг. ред. В.М. Шокало. – Харків : ХНУРЕ ; Колегіум, 2014. – 456 с
9. Правове регулювання правоохоронної діяльності: навчальний посібник / М. В. Ковалів, С. С. Єсімов, Ю. Р. Лозинський. – Львів: ЛьвДУВС, 2018. – 323 с
10. Організація правоохоронної діяльності Національної поліції України [Електронне видання] : навчально-методичний посібник з навчальної дисципліни «Організація правоохоронної діяльності Національної поліції України» (галузь знань 26 «Цивільна безпека», другий (магістерський) рівень, спеціальність 262 «Правоохоронна діяльність») для студентів І курсу магістратури заочної форми навчання / Н. М. Бакаянова, А. В. Кубаєнко, О. Г. Свида. – Одеса : Фенікс, 2020. – 218 с.
11. Шокало В.М., Правда В.І., Усін В.А., Вунтесмері В.С., Грецьких Д.В. Електродинаміка та поширення радіохвиль. Ч.2. Випромінювання та поширення електромагнітних хвиль: підручник для студентів ВНЗ. – Харків: ХНУРЕ; Колегіум, 2020. – 435 с.
12. Зубок М.І. Охорона та охоронна діяльність : навчально-методичний посібник. – Київ, 2017. – 246 с.
13. Мазепа М. М., Загуменна Ю. О. Охоронна діяльність в Україні : монографія : у 2-х ч. : Ч. 1. Державна служба охорони при МВС України. Харків : ФОП Коваленко, 2018. 112 с.
14. Facial expression recognition using pseudo 3-D hidden Markov models. *IEEE Xplore*. URL: https://ieeexplore.ieee.org/document/1048229 (date of access: 04.12.2022).
15. Face recognition using Hidden Markov Models. *Apollo Home*. URL: https://www.repository.cam.ac.uk/handle/1810/244871 (date of access: 04.12.2022).
16. Nefian Ara V., Hayes III Monson H. Hidden Markov Models For Face Recognition. URL: http://www.anefian.com/research/nefian98_hidden.pdf (дата звернення: 04.12.2022).

Допоміжна література

17. Про Національну поліцію: закон України від 02.07.2015 № 580-VIII // База даних «Законодавство України»/Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/580-19 (дата звернення: 14.01.2022).
18. Про Інформацію: закон України від 05.07.1994 № 80/94-ВР// База даних «Законодавство України»/Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94 (дата звернення: 14.01.2022).
19. Про державну таємницю: закон України від 21.01.1994 № 3855-XII // База даних «Законодавство України»/Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3855-12 (дата звернення: 14.01.2022)
20. Про захист інформації в інформаційно-телекомунікаційних системах: закон України від 05.07.1994 № 80/94-ВР// База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94 (дата звернення: 14.01.2022)
21. Про оперативно-розшукову діяльність: закон України від 18.02.1992 № 2135-XII // База даних «Законодавство України»/Верховна Рада України. URL:

https://zakon.rada.gov.ua/laws/show/2135-12 (дата звернення: 14.02.2022)
22. Про охоронну діяльність закон України від 22.03.2012 № 4616-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4616-vi#Text (дата звернення: 14.01.2022)
23. ДСТУ 4030-2001 Системи тривожної сигналізації. Системи охоронної та охоронно-пожежної сигналізації. Терміни та визначення.
24. ДСТУ 4357-3:2004 Системи тривожної сигналізації. Системи охоронної сигналізації. Частина 3. Прилади приймально-контрольні. Технічні умови.
25. ДСТУ EN 50130–4:2006 Системи тривожної сигналізації. електромагнітна сумісність. Вимоги до стійкості складників систем тривожної сигналізації про пожежу, проникнення та суспільну небезпеку.
26. ДСТУ EN 50131-1:2006 Системи тривожної сигналізації. Системи охоронної сигналізації. Частина 1. Загальні вимоги.
27. ДСТУ IEC 60839-1-1-2001 Системи тривожної сигналізації. Частина 1. Загальні вимоги. Розділ 1. Загальні принципи.
28. ДСТУ IEC 60839-1-3-2001 Системи тривожної сигналізації. Частина 1. Загальні вимоги. Розділ 3. Випробування систем тривожної сигналізації на вплив зовнішніх чинників.
29. ДСТУ IEC 60839-1-4-2001 Системи тривожної сигналізації. Частина 1. Загальні вимоги. Розділ 4. Принципи застосування.
30. ДСТУ IEC 60839-2-2-2001 Системи тривожної сигналізації. Частина 2. Вимоги до систем охоронної сигналізації Розділ 2. Вимоги до сповіщувачів. Загальні принципи.
31. ДСТУ IEC 60839-2-6-2001 Системи тривожної сигналізації Частина 2. Вимоги до систем охоронної сигналізації Розділ 6. Пасивні інфрачервоні сповіщувачі для закритих приміщень.
32. ДСТУ IEC 60839-2-2-2001 Системи тривожної сигналізації. Частина 2. Вимоги до систем охоронної сигналізації Розділ 2. Вимоги до сповіщувачів. Загальні принципи.
33. ВБН В. 2.5 – 78.11.01 – 2003 Відомчі будівельні норми України. Інженерне обладнання будинків і споруд. Системи сигналізації охоронного призначення.
34. ДСТУ 2272-93 Пожежна безпека. Терміни та визначення.
35. ДСТУ 3972-2000 Техника пожарная. Установки порошкового пожаротушения. Общие технические требования. Методы испытаний.
36. ДСТУ 4095-2002 Пожежна техніка. Установки газового пожежогасіння. Модулі та батарейне обладнання. Загальні технічні вимоги. Методи випробовування (ISO 14520-1:2000, NEQ).
37. ДСТУ 4466-1:2005 Системи газового пожежогасіння. Проектування, монтаж, випробовування, технічне обслуговування та безпека. Частина 1. Загальні вимоги (ISO 14520-1:2000, MOD).
38. ДСТУ 4466-8:2005 Системи газового пожежогасіння. Проектування, монтаж, випробовування, технічне обслуговування та безпека. Частина 8. Вогнегасна речовина HCFC 125 (ISO 14520-8:2000, MOD).
39. ДСТУ 4466-9:2005 Системи газового пожежогасіння. Проектування, монтаж, випробовування, технічне обслуговування та безпека. Частина 9. Вогнегасна речовина HFC 227ea (ISO 14520-9:2000, MOD).
40. ДСТУ 4469-3:2005 Пожежна техніка. Системи газового пожежогасіння. Частина 3. Пристрої ручного запускання та зупинення. Загальні вимоги (EN 12094-

3:2003, MOD).
41. ДСТУ 4490:2005 Установки автоматичні аерозольного пожежогасіння. Проектування, монтування та експлуатування. Технічні вимоги.
42. ДСТУ 4578:2006 Системи пожежогасіння діоксидом вуглецю. Проектування та монтаж. Загальні вимоги.
43. ДСТУ Б А.2.4-3-95 (ГОСТ 21.408-93). Правила виконання робочої документації автоматизації технологічних процесів.
44. ДСТУ Б А.2.4-4-99 (ГОСТ 21.101-97). Основні вимоги до проектної і робочої документації.

Інформаційні ресурси в Інтернеті

45. Introduction to Biometrics // вебсайт Homeland Security. URL : http://www.biometrics.gov/Documents/biofoundationdocs.pdf (дата звернення: 14.01.2022).
46. Iris authentication // веб-сайт URL : https://www.eyelock.com/ (дата звернення: 14.01.2022).
47. Використання ДНК в ідентифікації. // веб-сайт Accessexcellence.org. URL : http://www.accessexcellence.org/RC/AB/BA/Use_of_DNA_Identification.php.Use (дата звернення: 14.02.2022).
48. Побудова системи інтеграції. // веб-сайт Building Integration System. Boschsecurity.com. URL : https://www.boschsecurity.com/ru/ru/solutions/managementsoftware/building-integration-system (дата звернення: 14.02.2022).
49. Безпека компанії Bosch. // веб-сайт Bosch Security and Safety - Building Integration System solution. URL : https://www.youtube.com/watch?v=K2tb6cuBCcs. (дата звернення: 14.01.2022).
50. «СБ – Системи Безпеки» веб-сайт URL : https://cb.kiev.ua/ (дата звернення: 14.01.2022).