МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Харківський національний університет внутрішніх справ
Факультет № 4
Кафедра протидії кіберзлочинності
Факультет № 6
Кафедра кібербезпеки та DATA-технологій

ЗАТВЕРДЖЕНО
на спільному засіданні
кафедри протидії кіберзлочинності
факультету № 4 та
кафедри кібербезпеки та DATA-
технологій факультету № 6
протокол № 3 від 23.06.2023.
Завідувач кафедри
протидії кіберзлочинності
_____**Олександр МАНЖАЙ**
Завідувач кафедри
кібербезпеки та DATA-технологій
_____ **Юрій ГНУСОВ**

ТЕХНІЧНІ ЗАСОБИ ОХОРОНИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ (ВК.03)

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кафедра	Кафедра протидії кіберзлочинності (https://univd.edu.ua/uk/dir/1740/kafedra-protydii-kiberzlochynnosti)
Контактний телефон	+38 057 7398085 (роб.)
E-mail	kaf-itk@univd.edu.ua
ЛЕКТОР (ЛЕКТОРИ)	
	**Світличний Віталій Анатолійович,** доцент кафедри протидії кіберзлочинності факультету № 4, к.т.н., доцент svetlichnii@univd.kharkov.ua **Лекційний потік:** факультет № 5, шифр навчальних груп: Ф5-104м, факультет № 6, шифр навчальних груп: Ф-6-КБдб-22-1м
Назва освітньо-професійної	Кібербезпека та захист інформації (безпека

програми	інформаційних та комунікаційних систем) Cybersecurity and information protection (security of information and communication systems)
Рівень вищої освіти	Другий (магістерський) (НРК України – 7 рівень та другий цикл вищої освіти Рамки кваліфікацій Європейського простору вищої освіти)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Статус дисципліни	Нормативна компонента освітньо-наукової програми, вивчається в 2 семестрі І курсу навчання
Мета вивчення дисципліни	Вивчення 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.
Завдання вивчення дисципліни	Дослідження особливостей предметної області засобів охорони об`єктів. Дослідження структури інформаційних трактів в охорони об`єктів. Дослідження 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.
Обсяг дисципліни в кредитах ECTS/годинах	3 кредита ECTS (загальний обсяг – 90 год.) З них (денна/заочна):
	- аудиторна робота: 40/10 год.
	- самостійна робота: 50/80 год.
Форми та види проведення навчальних занять	Форма навчання –денна Види навчальних занять: - лекції: 20 год.; - семінарські заняття:0 год.; - практичні заняття:20 год; - лабораторні заняття:0 год. Форма навчання –заочна Види навчальних занять: - лекції: 4 год.; - семінарські заняття:0 год.; - практичні заняття: 6 год; - лабораторні заняття: 0 год.
Самостійна робота	Опрацювання рекомендованої літератури, підготовка тез доповідей до конференцій,

	самостійне вирішення практичних завдань.
Індивідуальні завдання	Наукові доповіді, реферати
Необхідне обладнання	Мультимедійне обладнання (ноутбук та проектор), комп'ютерне забезпечення з виходом у мережу Інтернет.
Мова викладання	Українська
Контроль	Поточний та підсумковий контроль Поточний: опитування на практичних заняттях; участь в дискусіях, веб-квестах, обговоренні доповідей, рефератів; підготовка рефератів та доповідей, тестування, виконання самостійних робіт. Критерії оцінки поточного контролю викладач повідомляє на першому занятті та перед кожними оцінюванням. Підсумковий контроль: екзамен.
Інтегральна компетентність, загальні компетентності (ЗК)	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки. КЗ .1. Здатність застосовувати знання у практичних ситуаціях.
Спеціальні компетентності (СК)	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.

ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ТЕМАМИ

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

Поняття комплексного захисту об'єктів. Етапи розвитку інтегрованих систем безпеки. Охоронно-пожежна сигналізація. Класифікація технічних засобів охоронно-пожежної сигналізації. Вимоги до технічного оснащення засобами охоронної сигналізації. Характеристики типових засобів та систем охорони. Технічні засоби протипожежного захисту об'єктів. Класифікація. Основні характеристики пожежних сповіщувачів. Основні принципи вибору пожежних сповіщувачів. Приймально-контрольні прилади та сигнально-спускові пристрої. Технічні системи протипожежного захисту об'єктів.

Тема № 2. Системи контролю та управління доступом.

Технічні системи контролю та управління доступом. Біометричні системи контролю та управління доступом**.** Безконтактні елементи систем контролю й управління доступом. Контактні елементи систем контролю та управління доступом. Біометричні зчитувачі. Управляючі пристрої, що припиняють доступ. Виконуючі пристрої систем контролю та управління доступом. Способи управління систем контролю і управління доступом. Обладнання для КПП і прохідних.

Тема № 3. Будівельні конструкцій та інженерні засоби захисту об'єкта.

Елементи будівельних конструкцій призначені для забезпечення техничного захисту об'єкта. Інженерно-технічні засоби охорони. Технічні характеристики інженерних засобів охорони

Тема № 4. Технічні засоби і системи відеоспостереження.

Конструктивні особливості й характеристики сучасних відеокамер. Комутаційні пристрої. Пристрої відображення. Пристрої документування, лінії передачі відеосигналу. Відеодетектори руху. Тактико-технічні характеристики цифрових відеореєстраторів. Принципи кодування відеозображення у форматах MJPEG, MPEG4, H.264. Побудова системи IP-відеоспостереження. Переваги та недоліки IP-відеоспостереження.

Програмні результати навчання (ПРН)	РН.2. Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах РН.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. РН.7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН.8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. РН.20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН.23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
Критерії оцінювання результатів навчання	Оцінювання навчальної дисципліни проводиться за результатами поточного та підсумкового контролю: - поточний контроль - 50 балів; - підсумковий контроль - 50 балів. Оцінка за поточний контроль складається з оцінювання аудиторної та самостійної роботи здобувача вищої освіти. Оцінка за аудиторну роботу визначається як середнє арифметичне балів, які ним отримані на заняттях

	(здобувач має отримати не менш 5 позитивних оцінок) з коефіцієнтом 5. Оцінка за самостійну роботу визначається як середнє арифметичне балів, які отримані здобувачем за: завдання до самостійної роботи, реферати, тощо (здобувач має підготувати не менш 2 проектів) з коефіцієнтом 5. Підсумкові бали з навчальної дисципліни визначаються як сума балів, які отримані здобувачем протягом семестру, та балів, які набрані на підсумковому контролі (екзамені).

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

Перелік питань, що виносяться на підсумковий контроль

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?

ОСНОВНА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна та наукова література:

1. 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.
2. 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.
3. Бурячок В.Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна і кібербезпека: соціотехнічний аспект: Підручник. – К.: ДУТ, 2015. – 288 с.
4. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. – К.: ДУТ, 2015. – 449 с.
5. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. – Житомир: ЖНАЕУ, 2016. – 636 с.
6. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
7. 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
8. Правове регулювання правоохоронної діяльності: навчальний посібник / М. В. Ковалів, С. С. Єсімов, Ю. Р. Лозинський. – Львів: ЛьвДУВС, 2018. – 323 с
9. 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.
10. 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.

ДОДАТКОВА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна та наукова література:

1. Зубок М.І. Охорона та охоронна діяльність : навчально-методичний посібник. – Київ, 2017. – 246 с.

2. 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.
3. Facial expression recognition using pseudo 3-D hidden Markov models. IEEE Xplore. URL: https://ieeexplore.ieee.org/document/1048229
4. Face recognition using Hidden Markov Models. Apollo Home. URL: https://www.repository.cam.ac.uk/handle/1810/244871
5. Nefian Ara V., Hayes III Monson H. Hidden Markov Models For Face Recognition. URL: http://www.anefian.com/research/nefian98_hidden.pdf

Нормативно-правові акти:

1. 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).
2. 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).
3. 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)
4. 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)
5. 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)
6. 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)
7. ДСТУ 4030-2001. Системи тривожної сигналізації. Системи охоронного призначення.
8. ДСТУ 4030-2001 Системи тривожної сигналізації. Системи охоронної та охоронно-пожежної сигналізації. Терміни та визначення;
9. ДСТУ 4357-3:2004 Системи тривожної сигналізації. Системи охоронної сигналізації. Частина 3. Прилади приймально-контрольні. Технічні умови.
10. ДСТУ EN 50130–4:2006 Системи тривожної сигналізації. електромагнітна сумісність. Вимоги до стійкості складників систем тривожної сигналізації про пожежу, проникнення та суспільну небезпеку.
11. ДСТУ EN 50131-1:2006 Системи тривожної сигналізації. Системи охоронної сигналізації. Частина 1. Загальні вимоги.
12. ДСТУ IEC 60839-1-1-2001 Системи тривожної сигналізації. Частина 1. Загальні вимоги. Розділ 1. Загальні принципи.
13. ДСТУ IEC 60839-1-3-2001 Системи тривожної сигналізації. Частина 1. Загальні вимоги. Розділ 3. Випробування систем тривожної сигналізації на вплив зовнішніх чинників.

14. ДСТУ IEC 60839-1-4-2001 Системи тривожної сигналізації. Частина 1. Загальні вимоги. Розділ 4. Принципи застосування.
15. ДСТУ IEC 60839-2-2-2001 Системи тривожної сигналізації. Частина 2. Вимоги до систем охоронної сигналізації Розділ 2. Вимоги до сповіщувачів. Загальні принципи.
16. ДСТУ IEC 60839-2-6-2001 Системи тривожної сигналізації Частина 2. Вимоги до систем охоронної сигналізації Розділ 6. Пасивні інфрачервоні сповіщувачі для закритих приміщень.
17. ДСТУ IEC 60839-2-2-2001 Системи тривожної сигналізації. Частина 2. Вимоги до систем охоронної сигналізації Розділ 2. Вимоги до сповіщувачів. Загальні принципи.
18. ВБН В. 2.5 – 78.11.01 – 2003 Відомчі будівельні норми України. Інженерне обладнання будинків і споруд. Системи сигналізації охоронного призначення.
19. ДСТУ 2272-93 Пожежна безпека. Терміни та визначення.
20. ДСТУ 3972-2000 Техника пожарная. Установки порошкового пожаротушения. Общие технические требования. Методы испытаний.
21. ДСТУ 4095-2002 Пожежна техніка. Установки газового пожежогасіння. Модулі та батарейне обладнання. Загальні технічні вимоги. Методи випробовування (ISO 14520-1:2000, NEQ).
22. ДСТУ 4466-1:2005 Системи газового пожежогасіння. Проектування, монтаж, випробовування, технічне обслуговування та безпека. Частина 1. Загальні вимоги (ISO 14520-1:2000, MOD).
23. 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).
24. 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).
25. ДСТУ 4469-3:2005 Пожежна техніка. Системи газового пожежогасіння. Частина 3. Пристрої ручного запускання та зупинення. Загальні вимоги (EN 12094-3:2003, MOD).
26. ДСТУ 4490:2005 Установки автоматичні аерозольного пожежогасіння. Проектування, монтування та експлуатування. Технічні вимоги.
27. ДСТУ 4578:2006 Системи пожежогасіння діоксидом вуглецю. Проектування та монтаж. Загальні вимоги.
28. ДСТУ Б А.2.4-3-95 (ГОСТ 21.408-93). Правила виконання робочої документації автоматизації технологічних процесів.
29. ДСТУ Б А.2.4-4-99 (ГОСТ 21.101-97). Основні вимоги до проектної і робочої документації.

Інформаційні ресурси в Інтернеті:

1. Introduction to Biometrics // вебсайт Homeland Security. URL : http://www.biometrics.gov/Documents/biofoundationdocs.pdf
2. Iris authentication // веб-сайт URL : https://www.eyelock.com
3. Використання ДНК в ідентифікації. // веб-сайт Accessexcellence.org. URL : http://www.accessexcellence.org/RC/AB/BA/Use_of_DNA_Identification.php.Use

4. Побудова системи інтеграції. // веб-сайт Building Integration System. Boschsecurity.com. URL : https://www.boschsecurity.com/ru/ru/solutions/managementsoftware/building-integration-system
5. Безпека компанії Bosch. // веб-сайт Bosch Security and Safety - Building Integration System solution. URL : https://www.youtube.com/watch?v=K2tb6cuBCcs
6. «СБ – Системи Безпеки» веб-сайт URL : https://cb.kiev.ua