

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ**

Кафедра протидії кіберзлочинності, факультет № 4

МЕТОДИЧНІ МАТЕРІАЛИ

ДО ЛАБОРАТОРНИХ ЗАНЯТЬ

**навчальної дисципліни «Технічні засоби охорони об'єктів критичної
інфраструктури»
обов'язкових компонент
освітньої програми другого рівня вищої освіти
"Кібербезпека (безпека інформаційних та комунікаційних систем)"**

Кам'янець-Подільський 2023

01^æ^â/â^ Å ææ^!•ā } Å -Å[&^æ^!:

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

Розробники:

1. доцент кафедри протидії кіберзлочинності, к.т.н., доцент
Світличний В.А.
2. завідувач кафедри кібербезпеки та DATA-технологій, к.т.н., доцент
Гнусов Ю.В.

Рецензенти:

1. завідувач кафедри інформаційних управляючих систем ХНУРЕ, д.т.н.,
професор Петров К.Е.,
2. доцент кафедри кібербезпеки та DATA-технологій факультету №6
ХНУВС, к.т.н., доцент Тулупов В.В.

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	екз.
Тема №2. Системи контролю та управління доступом	60	10	4	6	40	
Тема №3. Будівельні конструкції та інженерні засоби захисту об'єкта	58	10	2	6	40	
Тема №4. Технічні засоби і системи відеоспостереження	58	10	2	6	40	
Всього за семестр	240	40	12	28	160	

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	екз.
Тема №2. Системи контролю та управління доступом	60	2	2	2	54	
Тема №3. Будівельні конструкції та інженерні засоби захисту об'єкта	62	4	2	2	54	
Тема №4. Технічні засоби і системи відеоспостереження	58	2		2	54	
Всього за семестр	240	10	6	8	216	

2. Методичні вказівки до лабораторних занять

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

Лабораторне заняття до теми №1

Тема заняття: Системи безпеки об'єкта, поняття, класифікація, вимоги.

Навчальна мета заняття: Аналіз структури технічних засобів охорони об'єктів.

Кількість годин 10.

Місце проведення: згідно з розкладом.

Навчальні питання:

Вступ.

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

Висновки

Література: [1-3, 21-44]

План проведення заняття:

I. Порядок проведення вступу до заняття.

Перевірка наявності здобувачів вищої освіти на занятті та їх готовності до заняття. Нагадати основні терміни і визначення.

II. Порядок проведення основної частини заняття.

Детально розглянути матеріали відповідних лекцій. Обговорити питання, розібрати матеріал лекції що викликає складність в засвоєнні питання. Навести практичні приклади застосування. Здобувачі надають розгорнуті відповіді на наступні 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 сигналізації?
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 ємності?
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 проводний 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 "ПК"?
34. Призначення та принцип дії сповіщувача поверхневого п'єзоелектричного "Грань-2", "Гюрза-50ПЗ".
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".

III. Порядок проведення заключної частини заняття. Викладач оцінює відповіді. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Після закінчення заняття підбиваються підсумки.

Тема №2. Системи контролю та управління доступом

Лабораторне заняття №2

Тема заняття: Системи контролю та управління доступом

Навчальна мета заняття: Аналіз технічної реалізації засобів і систем контролю та управління доступом

Кількість годин 6.

Місце проведення: згідно з розкладом.

Навчальні питання:

Вступ.

1. Технічні системи контролю та управління доступом. Біометричні системи контролю та управління доступом.
2. Безконтактні елементи систем контролю та управління доступом. Контактні елементи систем контролю та управління доступом. Біометричні читувачі.
3. Управляючі пристрої, що припиняють доступ. Виконуючі пристрої систем контролю та управління доступом. Способи управління систем контролю і управління доступом. Обладнання для КПП і прохідних.

Висновки.

Література: [4, 11-12, 46-50, ресурси Internet]

План проведення заняття:

I. Порядок проведення вступу до заняття.

Перевірка наявності здобувачів вищої освіти на занятті та їх готовності до заняття. Нагадати основні терміни і визначення.

II. Порядок проведення основної частини заняття.

Детально розглянути матеріали відповідних лекцій. Обговорити питання, розібрати матеріал лекції що викликає складність в засвоєнні питання. Навести практичні приклади застосування. Здобувачі надають розгорнуті відповіді на наступні питання:

1. Для чого призначені системи керування та контролю доступу?
2. Що розуміють під процесом ідентифікації?
3. На чому заснована біометрична ідентифікація?
4. Основні функції СКУД?
5. Які існують електронні системи ідентифікації?
6. Переваги та недоліки мережних СКУД.
7. Переваги та недоліки автономних СКУД.

8. Відмінні риси СКУД з розподіленою архітектурою.
9. Тактико-технічні можливості контролера N-750.
10. Технічні можливості програмного забезпечення та контролерів СКУД компанії APPOLO.
11. Які Вам відомі технології біометричної ідентифікації?
12. Конструктивні особливості та принцип дії карти Віганда.
13. Переваги та недоліки зчитувачів і карт Віганда.
14. Принцип дії PROX ідентифікації.
15. Особливості активної та пасивної PROX-ідентифікації.
16. Переваги та недоліки PROX і карт.
17. Переваги та недоліки інфрачервоних зчитувачів і брелоків.
18. Переваги та недоліки LOGO і HICO магнітних карт.
19. Принцип дії Smart-технології.
20. Переваги та недоліки Smart-карт.
21. Застосування клавіатурного введення для ідентифікації.
22. Що означає коефіцієнт надійності, помилка першого та другого роду?
23. Способи біометричної ідентифікації.
24. Особливості та функціональна структура програмного забезпечення СКУД.
25. Вибір програмного забезпечення СКУД.
26. Конструктивні особливості електромагнітного, електромоторного та соленоїдного замків.
27. Які технічні засоби можуть застосовуватися для регулювання руху автотранспортом?
28. Як класифікуються приводи для воріт?
29. Основні технологічні способи керування приводами для воріт?
30. Особливості керування за допомогою PROX-карт і міток фірми Motorola Indiana Corp.
31. Устаткування для КПП і прохідних.
32. Класифікація турнікетів.
33. Призначення та конструкція повнозростового турнікета роторного типу.
34. Технічна реалізація доступу на особливо важливі об'єкти.
35. Характерні особливості шлюзових кабін.

III. Порядок проведення заключної частини заняття. Викладач оцінює відповіді. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національної системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Після закінчення заняття підбиваються підсумки.

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

Лабораторне заняття №3

Тема заняття: Будівельні конструкції та інженерні засоби захисту об'єкта. Інженерні засоби технічного захисту об'єктів

Навчальна мета заняття: Систематизація основних понять за темою, отримання практичних навичок вирішення задач інсталяції та синтезу елементів технічних засобів і систем охорони об'єктів.

Кількість годин: 6

Місце проведення: згідно з розкладом.

Навчальні питання:

Вступ.

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

Висновки.

Література: [8-10, ресурси Internet]

План проведення заняття:

I. Порядок проведення вступу до заняття.

Перевірка наявності здобувачів вищої освіти на занятті та їх готовності до заняття. Нагадати основні терміни і визначення.

II. Порядок проведення основної частини заняття.

Детально розглянути матеріали відповідних лекцій. Обговорити питання, розібрати матеріал лекції що викликає складність в засвоєнні питання. Навести практичні приклади застосування. Здобувачі надають розгорнуті відповіді на наступні питання:

1. Технічна реалізація доступу на особливо важливі об'єкти.
2. У якому випадку дозволяється установка ґрат або сіток із внутрішньої сторони приміщення?
3. Які технічні вимоги висуваються перед елементами будівельних конструкцій призначених для забезпечення захисту об'єкта?

4. Які Ви знаєте види огороження периметра?
 5. Призначення огороження периметра.
 6. Призначення та технічні характеристики огороження периметра та окремих ділянок території об'єкта, що знаходиться під охороною.
 7. Що таке зона відторгнення? Що розміщається в цій зоні?
 8. Призначення та технічні характеристики контрольно-слідової смуги.
 9. Призначення та технічні характеристики воріт і хвірток.
 10. Що включають у себе інженерні засоби захисту об'єкта?
 11. У чому полягає посилення дерев'яної коробки дверей?
 12. Які технічні вимоги висуваються перед вікнами та дверима?
 13. Призначення фарбування металевих поверхонь.
 14. Поняття захисного скляного покриття.
 15. Забезпечення захисту інформації за допомогою багатошарового листового скла.
- III. Порядок проведення заключної частини заняття. Викладач оцінює відповіді. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національної системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Після закінчення заняття підбиваються підсумки.

Тема №4 Технічні засоби і системи відеоспостереження

Лабораторне заняття №4

Тема заняття: Технічні засоби і системи відеоспостереження

Навчальна мета заняття: Систематизація основних понять за темою, отримання практичних навичок вирішення задач інсталяції та синтезу елементів технічних засобів і систем охоронного відеоспостереження.

Кількість годин: 6

Місце проведення: згідно з розкладом.

Навчальні питання:

Вступ.

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

Висновки.

Література: [8-10, ресурси Internet]

План проведення заняття:

I. Порядок проведення вступу до заняття.

Перевірка наявності здобувачів вищої освіти на занятті та їх готовності до заняття. Нагадати основні терміни і визначення.

II. Порядок проведення основної частини заняття.

Детально розглянути матеріали відповідних лекцій. Обговорити питання, розібрати матеріал лекції що викликає складність в засвоєнні питання. Навести практичні приклади застосування. Здобувачі надають розгорнуті відповіді на наступні питання:

1. Загальне призначення та функціональний склад "замкнутих телевізійних систем" (CCTV- Closed Circuit TeleVision).
2. Конструктивні особливості відіконів.
3. Типи світлочутливих матриць, особливості перетворення сигналу.
4. Переваги та недоліки світлочутливих матриць CCD і CMOS типів.
5. Ефективна та повна кількість пікселів світлочутливої матриці.
6. Процес формування кольорового зображення в системах охоронного спостереження.
7. Що означає поняття роздільна здатність відеокамери?
8. Що розуміють під чутливістю відеокамери?
9. Основні характеристики об'єктивів відеокамер.
10. Призначення ND фільтра.
11. Особливості Pin-hole об'єктивів.
12. Яке устаткування відноситься до комутаційних пристроїв передачі відеосигналу?
13. Призначення та особливості квадраторів відеосигналу.
14. Призначення та особливості дуплексних мультиплексорів.

15. Призначення та особливості триплексних мультиплексорів.
 16. Призначення та особливості мережних мультиплексорів, мережних відеореєстраторів і відеореєстраторів.
 17. У яких випадках застосовуються матричні комутатори?
 18. Основні характеристики пристроїв відображення відеосигналу.
 19. Призначення та технічні особливості пристроїв документування відеосигналу.
 20. Способи передачі відеосигналу на відстань.
 21. Особливості та технічна реалізація передачі відеосигналу на відстань до 300 метрів.
 22. Особливості та технічна реалізація передачі відеосигналу на відстань до 1500 метрів.
 23. Особливості та технічна реалізація передачі відеосигналу на відстань більше 1500 метрів.
 24. Які тактико-технічні характеристики цифрових реєстраторів відеосигналу Ви знаєте?
 25. Що прийнято розуміти під критерієм якості відеозапису?
 26. Які формати стиску відеоінформації Вам відомі?
 27. Що необхідно знати для визначення мінімально необхідного дискового простору відеореєстратора?
 28. Для чого призначені відеовиходи BNC і D-Sub у відеореєстраторі?
 29. Які мережні функції відеореєстраторів Вам відомі?
 30. Реалізація керування зовнішніми пристроями (відеокамерами, тривожними виходами, іншими відеореєстраторами).
 31. Програмні особливості використання формату стиску MJPEG у відеореєстраторах.
 32. Програмні особливості використання формату стиску MPEG-4 у відеореєстраторах.
 33. Програмні особливості використання формату стиску H.264/MPEG-4 AVC у відеореєстраторах.
 34. Поняття про кадри відеозображення.
 35. Основні методи стиску відеоданих у форматі H.264.
 36. Які основні відмінності IP-відеокамери від інших типів відеокамер охоронного спостереження?
 37. Історія створення IP-відеокамери?
 38. Які функціональні елементи має у своєму складі IP-відеокамера?
 39. Типові апаратні рішення організації IP-відеоспостереження?
 40. Основні переваги IP-відеокамер і IP-відеоспостереження в порівнянні зі звичайними камерами та системами?
 41. Основні недоліки IP-відеокамер і IP-відеоспостереження в порівнянні зі звичайними камерами та системами?
- III. Порядок проведення заключної частини заняття. Викладач оцінює відповіді. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Після закінчення заняття підбиваються підсумки.

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

1. Світличний В.А. Тексти лекцій з дисципліни «Технічні засоби охорони об'єктів». Харків: ХНУВС, 2016. (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.: ІСЗІ 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. Гришук 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 I 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

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 охоронного призначення.
 24. ДСТУ 4030-2001 Системи тривожної сигналізації. Системи охоронної та охоронно-пожежної сигналізації. Терміни та визначення;
 25. ДСТУ 4357-3:2004 Системи тривожної сигналізації. Системи охоронної сигналізації. Частина 3. Прилади приймально-контрольні. Технічні умови.
 26. ДСТУ EN 50130-4:2006 Системи тривожної сигналізації. електромагнітна сумісність. Вимоги до стійкості складників систем тривожної сигналізації про пожежу, проникнення та суспільну небезпеку.
 27. ДСТУ EN 50131-1:2006 Системи тривожної сигналізації. Системи охоронної сигналізації. Частина 1. Загальні вимоги.
 28. ДСТУ ІЕС 60839-1-1-2001 Системи тривожної сигналізації. Частина 1. Загальні вимоги. Розділ 1. Загальні принципи.
 29. ДСТУ ІЕС 60839-1-3-2001 Системи тривожної сигналізації. Частина 1. Загальні вимоги. Розділ 3. Випробування систем тривожної сигналізації на вплив зовнішніх чинників.
 30. ДСТУ ІЕС 60839-1-4-2001 Системи тривожної сигналізації. Частина 1. Загальні вимоги. Розділ 4. Принципи застосування.
 31. ДСТУ ІЕС 60839-2-2-2001 Системи тривожної сигналізації. Частина 2. Вимоги до систем охоронної сигналізації Розділ 2. Вимоги до сповіщувачів. Загальні принципи.
 32. ДСТУ ІЕС 60839-2-6-2001 Системи тривожної сигналізації Частина 2. Вимоги до систем охоронної сигналізації Розділ 6. Пасивні інфрачервоні сповіщувачі для закритих приміщень.
 33. ДСТУ ІЕС 60839-2-2-2001 Системи тривожної сигналізації. Частина 2.

- Вимоги до систем охоронної сигналізації Розділ 2. Вимоги до сповіщувачів. Загальні принципи.
34. ВБН В. 2.5 – 78.11.01 – 2003 Відомчі будівельні норми України. Інженерне обладнання будинків і споруд. Системи сигналізації охоронного призначення.
 35. [ДСТУ 2272-93](#) Пожежна безпека. Терміни та визначення.
 36. [ДСТУ 3972-2000](#) Техника пожарная. Установки порошкового пожаротушения. Общие технические требования. Методы испытаний.
 37. [ДСТУ 4095-2002](#) Пожежна техніка. Установки газового пожежогасіння. Модулі та батарейне обладнання. Загальні технічні вимоги. Методи випробовування (ISO 14520-1:2000, NEQ).
 38. [ДСТУ 4466-1:2005](#) Системи газового пожежогасіння. Проектування, монтаж, випробовування, технічне обслуговування та безпека. Частина 1. Загальні вимоги (ISO 14520-1:2000, MOD).
 39. [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).
 40. [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).
 41. [ДСТУ 4469-3:2005](#) Пожежна техніка. Системи газового пожежогасіння. Частина 3. Пристрої ручного запускання та зупинення. Загальні вимоги (EN 12094-3:2003, MOD).
 42. [ДСТУ 4490:2005](#) Установки автоматичні аерозольного пожежогасіння. Проектування, монтування та експлуатування. Технічні вимоги.
 43. [ДСТУ 4578:2006](#) Системи пожежогасіння діоксидом вуглецю. Проектування та монтаж. Загальні вимоги.
 44. [ДСТУ Б А.2.4-3-95 \(ГОСТ 21.408-93\)](#). Правила виконання робочої документації автоматизації технологічних процесів.
 45. [ДСТУ Б А.2.4-4-99 \(ГОСТ 21.101-97\)](#). Основні вимоги до проектної і робочої документації.

Інформаційні ресурси в Інтернеті

46. Introduction to Biometrics // вебсайт Homeland Security. URL : <http://www.biometrics.gov/Documents/biofoundationdocs.pdf> (дата звернення: 14.01.2022).
47. Iris authentication // веб-сайт URL : <https://www.eyelock.com/> (дата звернення: 14.01.2022).
48. 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).
49. Побудова системи інтеграції. // веб-сайт Building Integration System. Boschsecurity.com. URL : <https://www.boschsecurity.com/ru/ru/solutions/>

- 50.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).
- 51.«СБ – Системи Безпеки» веб-сайт URL : <https://cb.kiev.ua/> (дата звернення: 14.01.2022).