МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра протидії кіберзлочинності, факультет № 4

РОБОЧА ПРОГРАМА

навчальної дисципліни
«Управління кібербезпекою об'єктів критичної інфраструктури»
обов'язкових компонент
освітньої програми другого (магістерського) рівня вищої освіти

125 «Кібербезпека та захист інформації»
(Безпека інформаційних та комунікаційних систем)

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 29.01.2024 № 1

СХВАЛЕНО
Вченою радою
факультету № 4
Протокол від 17.01.2024 № 1

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС
з технічних дисциплін
Протокол від 26.01.2024 № 1

Розглянуто на засіданні кафедри протидії кіберзлочинності факультету № 4 (протокол від 10.01.2024 № 1).

Розробники:
1. Доцент кафедри кібербезпеки та DATA-технологій факультету № 6, кандидат наук з державного управління, доцент Онищенко Ю.М.
2. Доцент кафедри протидії кіберзлочинності факультету № 4, кандидат педагогічних наук, доцент Колісник Т.П.

Рецензенти:
1. Завідувач кафедри інформаційних управляючих систем Харківського національного університету радіоелектроніки, доктор технічних наук, професор Петров К.Е.
2. Професор кафедри кібербезпеки та DATA-технологій факультету № 6 ХНУВС, д.т.н., професор Можаєв О.О.

1. Опис навчальної дисципліни

<table>
<tr><th>Найменування показників</th><th>Шифри та назви галузі знань, код та назва спеціальності, ступінь вищої освіти</th><th>Характеристика навчальної дисципліни</th></tr>
<tr><td>Кількість кредитів ECTS – 6
Загальна кількість годин – 180
Кількість тем – 6</td><td>125 "Кібербезпека та захист інформації";
(Безпека інформаційних та комунікаційних систем),
магістр</td><td>Дисципліна обов’язкової компоненти ОПП.

Навчальний курс 1
Семестр 2

Види підсумкового контролю: - екзамен.</td></tr>
<tr><td colspan="3">Розподіл навчальної дисципліни за видами занять:</td></tr>
<tr><td colspan="2">денна форма навчання

Лекції – 30 ; (години)
Семінарські заняття – ____; (години)
Практичні заняття – 30 ; (години)
Лабораторні заняття – _____; (години)
Самостійна робота – 120 ; (години)

Індивідуальні завдання:

Курсова робота – _____ (кількість; № семестру)
Реферати (тощо) – _____1____ (кількість; № семестру)</td><td>заочна форма навчання

Лекції – 10 ; (години)
Семінарські заняття – _____; (години)
Практичні заняття – 8 ; (години)
Лабораторні заняття – _____; (години)
Самостійна робота – 162 ; (години)

Індивідуальні завдання:

Курсова робота – _____

(кількість; № семестру)
Реферати – _____1_____ (кількість; № семестру)</td></tr>
</table>

2. Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни «Управління кібербезпекою об'єктів критичної інфраструктури» є:

- навчити здобувачів вищої освіти встановлених законодавством України вимог щодо управління кібербезпекою об’єктів критичної інфраструктури та запобігання і протидії кіберзлочинності в Україні в умовах глобалізації світового інформаційного простору;

- виробити вміння: аналізувати державні механізми запобігання і протидії кіберзлочинності в умовах глобалізації; визначати відповідність стану безпеки інформації встановленим вимогам; будувати систему управління інформаційною безпекою згідно зі встановленими вимогами; приймати рішення щодо необхідності застосування того чи іншого способу реагування на загрозу; критично оцінювати інформацію;

- сформувати у здобувачів вищої освіти знання, уміння і навички щодо теоретичних засад запобігання і протидії проявам кіберзлочинності; сучасного стану державного управління у сфері запобігання і протидії кіберзлочинності в Україні; шляхи удосконалення державних механізмів запобігання і протидії кіберзлочинності; системи управління інформаційною безпекою; дотримання правил кібербезпеки в системі публічної служби; державних механізмів управління кібербезпекою об’єктів критичної інфраструктури та запобігання і протидії кіберзлочинності в Україні.

Основними **завданнями** вивчення дисципліни є:

- ознайомлення здобувачів вищої освіти з законодавством України у сфері захисту об’єктів критичної інфраструктури; вивчення основних засад та принципів державної політики у сфері захисту критичної інфраструктури; аналіз нормативно-правової бази з питань правового регулювання кібербезпеки на об’єктах критичної інфраструктури.

- ознайомлення із сучасними підходами забезпечення ефективного державного управління кібербезпекою об’єктів критичної інфраструктури та структурою державного механізму взаємодії у сфері боротьби з кіберзлочинністю в Україні; формування навичок аналізу державних механізмів запобігання і протидії кіберзлочинності в умовах глобалізації.

Міждисциплінарні зв’язки. Навчальна дисципліна спирається на дисципліни: «Розвідувально-аналітична робота у кіберсфері», «Моделі ризик-орієнтованого аналізу в кібербезпеці», «Моніторинг та аудит кібербезпеки»та формує фахові компетентності в галузі кібербезпеки.

Очікувані результати навчання: у результаті вивчення навчальної дисципліни здобувач вищої освіти повинен

знати: теоретичні засади запобігання і протидії проявам кіберзлочинності; сучасний стан державного управління у сфері запобігання і протидії кіберзлочинності в Україні; шляхи удосконалення державних механізмів запобігання і протидії кіберзлочинності;

вміти: аналізувати державні механізми запобігання і протидії кіберзлочинності в умовах глобалізації.

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 (ЗК)	КЗ.4	Здатність оцінювати та забезпечувати якість виконуваних робіт
Спеціальні (фахові, предметні) компетентності (СК)	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.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. Теоретичні засади запобігання і протидії проявам кіберзлочинності

Понятійно-категоріальний апарат: співвідношення основних понять у сфері боротьби з кіберзлочинністю. Взаємозв'язок злочинності та інформаційних технологій. Запобігання та протидія кіберзлочинності як об’єкт державного управління в умовах глобалізації. Зарубіжний досвід реалізації державних механізмів у галузі запобігання та боротьби з кіберзлочинністю.

Тема 2. Державне управління у сфері запобігання і протидії кіберзлочинності в Україні

Особливості організаційних та нормативно-правових засад боротьби з кіберзлочинністю. Проблеми державного управління у сфері запобігання проявам кіберзлочинності. Напрями вирішення проблеми проявів кіберзлочинності.

Тема 3. Державні механізми запобігання і протидії кіберзлочинності в умовах воєнного стану

Підходи і моделі реформування державних механізмів боротьби з кіберзлочинністю. Напрями впорядкування правового підґрунтя діяльності та взаємовідносин в організаційно-функціональній структурі суб'єктів протидії кіберзлочинності. Система запобігання кіберзлочинності в Україні.

Тема 4. Організаційно-правові аспекти забезпечення кібербезпеки об'єктів критичної інфраструктури України

Поняття та визначення у сфері захисту критичної інфраструктури України. Основні цілі, напрями та принципи державної політики у сфері захисту об'єктів критичної інфраструктури. Правові основи забезпечення безпеки об'єктів критичної інфраструктури. Суб'єкти забезпечення безпеки об'єктів критичної інфраструктури. Організаційні засади національної системи захисту критичної інфраструктури.

Тема № 5. Вимоги до кіберзахисту об'єктів критичної інфраструктури

Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури. Базові вимоги із забезпечення кіберзахисту об'єктів критичної інфраструктури. Формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки. Управління доступом користувачів та адміністраторів до об'єктів захисту ОКІІ ОКІ. Ідентифікація та автентифікація користувачів та адміністраторів ОКІІ ОКІ. Реєстрація подій компонентами ОКІІ ОКІ та їх періодичний аудит. Забезпечення мережевого захисту компонентів та інформаційних ресурсів ОКІІ ОКІ. Забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів ОКІІ ОКІ. Визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на ОКІІ ОКІ. Визначення умов використання програмного та апаратного забезпечення ОКІІ ОКІ. Визначення умов розміщення компонентів ОКІІ ОКІ.

Тема 6. Зарубіжний досвід створення національних систем забезпечення безпеки та стійкості критичної інфраструктури

Передовий зарубіжний досвід створення національних систем забезпечення безпеки та стійкості критичної інфраструктури. Система забезпечення безпеки та стійкості критичної інфраструктури в США. Система забезпечення безпеки та стійкості критичної інфраструктури у Великій Британії. Система забезпечення безпеки та стійкості критичної інфраструктури у Польщі. Висновки для України з огляду на зарубіжний досвід щодо державної системи забезпечення безпеки та стійкості критичної інфраструктури. Організація підготовки кадрів і населення на державному рівні та в межах секторів критичної інфраструктури. Особливості Національної системи планування США.

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. Теоретичні засади запобігання і протидії проявам кіберзлочинності	28	4	4		20	екзамен
Тема № 2. Державне управління у сфері запобігання і протидії кіберзлочинності в Україні	32	6	6		20	
Тема № 3. Державні механізми запобігання і протидії кіберзлочинності в умовах воєнного стану	32	6	6		20	
Тема № 4 Організаційно-правові аспекти забезпечення кібербезпеки об’єктів критичної інфраструктури України	32	6	6		20	
Тема № 5. Вимоги до кіберзахисту об’єктів критичної інфраструктури	32	6	6		20	
Тема № 6. Зарубіжний досвід створення національних систем забезпечення безпеки та стійкості критичної інфраструктури	24	2	2		20	
Всього за семестр № 2	**180**	**30**	**30**		**120**	

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. Теоретичні засади запобігання і протидії проявам кіберзлочинності	29	1	1		27	**екзамен**
Тема № 2. Державне управління у сфері запобігання і протидії кіберзлочинності в Україні	30	2	1		27	
Тема № 3. Державні механізми запобігання і протидії кіберзлочинності в умовах воєнного стану	30	2	1		27	
Тема № 4 Організаційно-правові аспекти забезпечення кібербезпеки об’єктів критичної інфраструктури України	31	2	2		27	
Тема № 5. Вимоги до кіберзахисту об’єктів критичної інфраструктури	31	2	2		27	
Тема № 6. Зарубіжний досвід створення національних систем забезпечення безпеки та стійкості критичної інфраструктури	29	1	1		27	
Всього за семестр № 2	**180**	**10**	**8**		**162**	

4.1.3. Питання, що виносяться на самостійне опрацювання

Перелік питань до тем навчальної дисципліни	Література
Тема № 1. Теоретичні засади запобігання і протидії проявам кіберзлочинності	
Користуючись текстом лекції та рекомендованою літературою до теми, сформувати тези відповідей на контрольні запитання до теми. Скласти порівняльну таблицю зарубіжного досвіду реалізації державних механізмів у галузі запобігання та боротьби з кіберзлочинністю.	1-20, 22-30, 32, 33, 35, 43, 47, 48, 52-58, ресурси Internet
Тема № 2. Державне управління у сфері запобігання і протидії кіберзлочинності в Україні	
Користуючись текстом лекції та рекомендованою літературою до теми, сформувати тези відповідей на контрольні запитання до теми. Скласти порівняльну таблицю напрямів вирішення проблеми проявів кіберзлочинності.	1-20, 22-30, 32, 33, 35, 43, 47, 48, 52-58, ресурси Internet
Тема № 3. Державні механізми запобігання і протидії кіберзлочинності в умовах воєнного стану	
Користуючись текстом лекції та рекомендованою літературою до теми, сформувати тези відповідей на контрольні запитання до теми. Скласти порівняльну таблицю складових системи запобігання кіберзлочинності в Україні.	1-20, 22-30, 32, 33, 35, 43, 47, 48, 52-58, ресурси Internet
Тема № 4 Організаційно-правові аспекти забезпечення кібербезпеки об'єктів критичної інфраструктури України	
Користуючись текстом лекції та рекомендованою літературою до теми, сформувати тези відповідей на контрольні запитання до теми. Скласти порівняльну таблицю складових системи запобігання кіберзлочинності в Україні.	1-46, ресурси Internet
Тема № 5. Вимоги до кіберзахисту об'єктів критичної інфраструктури	
Користуючись текстом лекції та рекомендованою літературою до теми, сформувати тези відповідей на контрольні запитання до теми.	1-46, ресурси Internet

Перелік питань до тем навчальної дисципліни	Література
Скласти порівняльну таблицю складових системи запобігання кіберзлочинності в Україні.	
Тема № 6. Зарубіжний досвід створення національних систем забезпечення безпеки та стійкості критичної інфраструктури	
Користуючись текстом лекції та рекомендованою літературою до теми, сформувати тези відповідей на контрольні запитання до теми. Скласти порівняльну таблицю складових системи запобігання кіберзлочинності в Україні та зарубіжних країнах.	4-6, 8, 20, ресурси Internet (69-85)

5. Індивідуальні завдання

5.1.1. Теми рефератів

1. Огляд закордонного нормативно-правового забезпечення державного управління у сфері запобігання і протидії кіберзлочинності.
2. Механізми запобігання і протидії кіберзлочинності США.
3. Механізми запобігання і протидії кіберзлочинності ЄС.
4. Державна політика у сфері захисту об'єктів критичної інфраструктури.
5. Правові основи забезпечення безпеки об'єктів критичної інфраструктури.
6. Організаційні засади національної системи захисту критичної інфраструктури.
7. Формування на об’єкті критичної інфраструктури загальної політики інформаційної безпеки.
8. Управління доступом користувачів та адміністраторів до об’єктів захисту ОКІІ ОКІ.
9. Ідентифікація та автентифікація користувачів та адміністраторів ОКІІ ОКІ.
10. Реєстрація подій компонентами ОКІІ ОКІ та їх періодичний аудит.
11. Забезпечення мережевого захисту компонентів та інформаційних ресурсів ОКІІ ОКІ.
12. Забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів ОКІІ ОКІ.
13. Умови використання змінних (зовнішніх) пристроїв та носіїв інформації на ОКІІ ОКІ.
14. Умови використання програмного та апаратного забезпечення ОКІІ ОКІ.
15. Передовий зарубіжний досвід створення національних систем забезпечення безпеки та стійкості критичної інфраструктури.
16. Система забезпечення безпеки та стійкості критичної інфраструктури в США.
17. Система забезпечення безпеки та стійкості критичної інфраструктури у Великій Британії.
18. Система забезпечення безпеки та стійкості критичної інфраструктури у Польщі.
19. Організація підготовки кадрів і населення на державному рівні та в межах секторів критичної інфраструктури.
20. Особливості Національної системи планування США.

6. Методи навчання

Аудиторні заняття проводяться у формі візуального представлення аналітично-графічного матеріалу дисципліни, на яких здобувачі вищої освіти повинні виконувати відповідні розумові, обчислювальні та практичні дії.

Самостійна робота за кожною темою передбачає вивчення теоретичних питань лекційних занять, опрацювання завдань практичних занять.

Індивідуальна робота передбачає написання рефератів.

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

Тема № 1.

1. Аспекти взаємозв'язку злочинності та інформаційних технологій.
2. Співвідношення глобалізації інформаційних процесів та кіберзлочинності.
3. Позитивні та негативні наслідки поширення комп'ютерних технологій.
4. Темпи розвитку всесвітньої мережі Інтернет.
5. Превентивні можливості глобальних інформаційних мереж.
6. Транснаціональна злочинність: визначення, причини виникнення, тенденції.
7. Що належить до комп'ютерних злочинів згідно з міжнародними класифікаторами
8. Напрями використання кібертерористами глобальної мережі Інтернет.
9. Соціально-психологічний аспект глобальної мережі Інтернет.
10. Незаконний контент у глобальній мережі Інтернет: види, способи розповсюдження.
11. Напрями використання інформаційних технологій органами державної влади.
12. Напрями використання інформаційних технологій правоохоронними органами США.
13. Напрями використання інформаційних технологій правоохоронними органами України.
14. Наведіть характеристику дефініції кіберпростір.
15. Ознаки кіберпростору.
16. Шляхи вирішення питання щодо регулювання мережі Інтернет і, відповідно, визначення повноважень держави в цій сфері.
17. Співвідношення понять “кіберзлочинність” і “комп'ютерні злочини”.
18. Як Конвенція Ради Європи «Про кіберзлочинність» визначає види комп'ютерних злочинів “у чистому вигляді”?
19. Як Конвенція Ради Європи «Про кіберзлочинність» визначає скоювані за допомогою комп'ютера (computer-facilitated) злочини?
20. Характеристика дефініції кіберзлочинність.
21. Наведіть визначення поняття кіберпростір.
22. Наведіть визначення поняття кіберзлочин.

Тема № 2.

23. Що складає правову основу забезпечення кібербезпеки України?
24. Який Закон України визначає засади забезпечення кібербезпеки України?
25. Наведіть визначення поняття кібербезпеки.
26. Що належить до об’єктів кібербезпеки?
27. Наведіть визначення поняття кіберзахисту.
28. Що належить до об’єктів кіберзахисту?
29. Визначення терміну об’єкт критичної інформаційної інфраструктури.
30. Визначення терміну система управління технологічними процесами.
31. Які об’єкти можуть бути віднесені до критичної інфраструктури?

32. Надайте визначення та характеристику поняття кіберпростір.
33. Надайте визначення та характеристику поняття інцидент кібербезпеки (кіберінцидент).
34. Надайте визначення та характеристику поняття кібератака.
35. Надайте визначення та характеристику поняття кіберзагроза.
36. Надайте визначення та характеристику поняття кібероборона.
37. Надайте визначення та характеристику поняття кіберзагроз.
38. Визначення терміну кіберрозвідка.
39. Визначення терміну кібершпигунство.
40. Визначення терміну кібертероризм.
41. Хто здійснює координацію діяльності у сфері кібербезпеки в Україні?
42. Хто забезпечує формування та реалізацію державної політики у сфері кібербезпеки в Україні?
43. Суб'єкти забезпечення кібербезпеки.
44. Завдання суб'єктів національної системи кібербезпеки.
45. Надайте визначення та характеристику поняття Національна телекомунікаційна мережа.
46. Надайте визначення та характеристику поняття Національні електронні інформаційні ресурси.
47. Надайте визначення та характеристику поняття системи електронних комунікацій.
48. Наведіть основні завдання Департаменту кіберполіції.
49. Наведіть основні функції Департаменту кіберполіції.
50. Надайте визначення та характеристику поняття національна система кібербезпеки.
51. Наведіть основні завдання у сфері забезпечення кібербезпеки Державної служби спеціального зв'язку та захисту інформації України.
52. Наведіть основні завдання у сфері забезпечення кібербезпеки Національної поліції України.
53. Наведіть основні завдання у сфері забезпечення кібербезпеки Служби безпеки України.
54. Наведіть основні завдання у сфері забезпечення кібербезпеки Міністерства оборони України, Генерального штабу Збройних Сил України.
55. Наведіть основні завдання у сфері забезпечення кібербезпеки розвідувальних органів України.
56. Наведіть основні завдання у сфері забезпечення кібербезпеки Національного банку України.
57. Проведенням яких заходів забезпечується функціонування національної системи кібербезпеки?
58. У чому полягають застереження, з якими Україна ратифікувала Конвенцію «Про кіберзлочинність»?
59. Наведіть юрисдикцію щодо кіберзлочинів згідно Конвенції «Про кіберзлочинність».

60. Яким чином у Конвенції «Про кіберзлочинність» висвітлено принципи міжнародного співробітництва країн-учасниць у сфері протидії кіберзлочинності?

61. У чому полягає процедура екстрадиції?

62. Наведіть визначення OSINT та ставлення Конвенції «Про кіберзлочинність» до даного методу збору інформації.

Тема № 3.

63. Наведіть основні умови для забезпечення функціонування вільної та безпечної глобальної мережі Інтернет.

64. Наведіть основні пропозиції вирішення проблеми національної кібербезпеки.

65. Наведіть першочергові кроки України на шляху забезпечення кібербезпеки.

66. Наведіть основні складові кібербезпеки та надайте їх характеристику.

67. Що має визначати типова політика кібербезпеки держави?

68. Наведіть основні вимоги до національної політики кібербезпеки держави.

69. Які положення має містити стратегія кібербезпеки держави?

70. Значення CERT у забезпеченні кібербезпеки держави?

71. Завдання CERT-UA.

72. Державно-приватне партнерство у сфері забезпечення кібербезпеки держави: визначення, принципи, першочергові завдання.

73. Співпраця між органами державної влади, які опікуються питаннями кібербезпеки держави: визначення, принципи, першочергові завдання.

74. Що вимагає створення національного потенціалу держави для усунення кіберінцидентів?

75. У чому полягає реалізація механізму координації в системі державного управління?

76. У чому полягає реалізація практики обміну інформацією у сфері забезпечення кібербезпеки між приватним сектором і урядовими органами?

77. Принципи застосування законодавства у сфері кібербезпеки.

78. Принципи забезпечення кібербезпеки.

79. Міжнародне співробітництво у сфері кібербезпеки.

80. Контроль за законністю заходів із забезпечення кібербезпеки України.

81. Запобігання та протидія кіберзлочинності як об’єкт державного управління в умовах глобалізації.

82. Зарубіжний досвід щодо реалізації державних механізмів у галузі запобігання та боротьби з кіберзлочинністю.

83. Особливості організаційних та нормативно-правових засад боротьби з кіберзлочинністю.

84. Проблеми державного управління у сфері запобігання проявам кіберзлочинності.

85. Напрями розв'язання проблеми проявів кіберзлочинності.

86. Моделі державних механізмів боротьби з кіберзлочинністю.

87. Напрями впорядкування правового підґрунтя діяльності та взаємовідносин в організаційно-функціональній структурі суб’єктів протидії кіберзлочинності.

88. Система запобігання кіберзлочинності в Україні.

Тема № 4.

89. Чим фрагментарний підхід відрізняється від застосування цілісного підходу під час розбудови системи захисту ОКІ?

90. Що розуміється під терміном «критична інфраструктура»?

91. Що розуміється під терміном «безпека критичної інфраструктури»?

92. Що розуміється під терміном «життєво важливі функції та/або послуги»?

93. Що розуміється під терміном «захист критичної інфраструктури»?

94. Що розуміється під терміном «ідентифікація об’єкта критичної інфраструктури»?

95. Що розуміється під терміном «інцидент безпеки критичної інфраструктури»?

96. Що розуміється під терміном «категоризація об’єктів інфраструктури»?

97. Що розуміється під терміном «категорія критичності (критерії) об’єкта критичної інфраструктури»?

98. Що розуміється під терміном «кризова ситуація»?

99. Що розуміється під терміном «критична технологічна інформація»?

100. Що розуміється під терміном «національна система захисту критичної інфраструктури»?

101. Що розуміється під терміном «несанкціоноване втручання»?

102. Що розуміється під терміном «об’єкти критичної інфраструктури»?

103. Що розуміється під терміном «оператор критичної інфраструктури»?

104. Що розуміється під терміном «охорона об’єктів критичної інфраструктури»?

105. Що розуміється під терміном «паспорт безпеки»?

106. Що розуміється під терміном «проектна загроза об’єкту критичної інфраструктури»?

107. Що розуміється під терміном «реєстр об’єктів критичної інфраструктури»?

108. Що розуміється під терміном «режим функціонування критичної інфраструктури»?

109. Що розуміється під терміном «рівень критичності об’єкта критичної інфраструктури»?

110. Що розуміється під терміном «сектор критичної інфраструктури»?

111. Що розуміється під терміном «стійкість критичної інфраструктури»?

112. Що розуміється під терміном «стійкість критичної інфраструктури»?

113. Які види об'єктів вважаються критичною інфраструктурою в Україні?

114. Які загрози можуть ставитися перед об'єктами критичної інфраструктури?

115. За сукупністю яких критеріїв відбувається віднесення об’єктів до критичної інфраструктури?

116. З якою метою здійснюється категоризація об’єктів критичної інфраструктури?

117. Наведіть категорії критичності об’єктів критичної інфраструктури.

118. Ким здійснюється категоризація об’єктів критичної інфраструктури?

119. Наведіть які об'єкти можуть вважатися частинами критичної інфраструктури в Україні.

120. Наведіть основні засади державної політики у сфері захисту критичної інфраструктури.

121. Наведіть основні принципи формування захисту критичної інфраструктури в Україні.

122. Що є метою державної політики у сфері захисту критичної інфраструктури?

123. Що належить до основних завдань формування і реалізації державної політики у сфері захисту критичної інфраструктури?

124. У яких режимах функціонування здійснюється забезпечення захисту та стійкості критичної інфраструктури?

125. Ким приймається Рішення про оголошення режимів функціонування критичної інфраструктури?

126. Хто належить до основних суб'єктів забезпечення безпеки об'єктів критичної інфраструктури?

127. Який підзаконний акт регламентує порядок визнання об’єкта критичною інфраструктурою?

128. Окресліть повноваження Верховної Ради України у сфері забезпечення захисту критичної інфраструктури суб’єкти державної системи захисту критичної інфраструктури.

129. Окресліть повноваження Президента України у сфері забезпечення захисту критичної інфраструктури суб’єкти державної системи захисту критичної інфраструктури.

130. Окресліть повноваження Кабінету Міністрів України у сфері забезпечення захисту критичної інфраструктури суб’єкти державної системи захисту критичної інфраструктури.

131. Окресліть повноваження Ради національної безпеки і оборони України у сфері забезпечення захисту критичної інфраструктури суб’єкти державної системи захисту критичної інфраструктури.

132. Хто забезпечує формування та реалізацію державної політики у сфері захисту критичної інфраструктури, координацію діяльності суб’єктів національної системи захисту критичної інфраструктури?

133. Наведіть основні завдання функціональних органів у сфері захисту критичної інфраструктури.

134. Наведіть основні завдання секторальних органів у сфері захисту критичної інфраструктури.

135. Наведіть основні завдання місцевих органів виконавчої влади та військово-цивільні адміністрації у сфері захисту критичної інфраструктури.

136. Наведіть основні права, обов’язки та завдання операторів критичної інфраструктури.

137. Які заходи захисту можуть бути вжиті для об'єктів критичної інфраструктури?

138. Які організації відповідають за захист об'єктів критичної інфраструктури в Україні?

139. Правові основи захисту об'єктів критичної інфраструктури в Україні.

140. Які основні принципи безпеки повинні бути враховані при захисті об'єктів критичної інфраструктури?

141. Які види кіберзагроз можуть становити небезпеку для об'єктів критичної інфраструктури?

142. Які стратегії реагування на інциденти пов'язані з захистом об'єктів критичної інфраструктури?

143. Які основні кроки потрібно здійснити для відновлення роботи об'єкта критичної інфраструктури після інциденту?

144. Які міжнародні стандарти і рекомендації визначають принципи захисту об'єктів критичної інфраструктури?

145. Які основні функції центрів керування кризових ситуацій, пов'язаних з захистом об'єктів критичної інфраструктури?

146. Які вимоги ставляться до персоналу, який займається захистом об'єктів критичної інфраструктури?

147. Які основні принципи фізичного захисту об'єктів критичної інфраструктури?

148. Які види контролю та моніторингу можуть застосовуватися для забезпечення безпеки об'єктів критичної інфраструктури?

149. Які юридичні наслідки проведення моніторингу рівня безпеки ОКІ?

150. Яким шляхом здійснюється взаємодія національної системи захисту критичної інфраструктури з іншими системами захисту у сфері національної безпеки?

151. Яким шляхом здійснюється державно-приватне партнерство у сфері захисту критичної інфраструктури?

152. Хто і як часто здійснює зовнішній аудит діяльності уповноваженого органу у сфері захисту критичної інфраструктури України?

153. Яким чином здійснюється Громадський нагляд у сфері захисту критичної інфраструктури?

Тема № 5.

154. Окресліть основні проблеми у створенні системи захисту критичної інфраструктури, які потребують розв’язання.

155. Надайте визначення терміна критичні бізнес/операційні процеси об’єктів критичної інфраструктури.

156. Надайте визначення терміна система інформаційної безпеки.

157. Мета проведення незалежного аудиту інформаційної безпеки на ОКІ.

158. Хто має організовувати проведення незалежного аудиту інформаційної безпеки на ОКІ згідно з вимогами законодавства в сфері захисту інформації та кібербезпеки?

159. На чому ґрунтується технічне завдання на створення системи інформаційної безпеки?

160. Кого має невідкладно інформувати власник та/або керівник ОКІ у випадку настання комп'ютерної надзвичайної події?

161. Розшифруйте та надайте характеристику КСЗІ.

162. Хто забезпечує створення резервних копій інформаційних ресурсів ОКІІ ОКІ та критичних бізнес/операційних процесів ОКІ?

163. Що повинні забезпечувати організаційні та технічні заходи з кіберзахисту, які впроваджуються на ОКІІ ОКІ?

164. З урахуванням чого розробник КСЗІ ОКІІ ОКІ здійснює формування додаткових заходів із забезпечення кіберзахисту ОКІ?

165. Наведіть основні базові вимоги із забезпечення кіберзахисту об'єктів критичної інфраструктури

166. Основні вимоги до формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки.

167. Як на ОКІ оформлюються права та обов'язки всіх категорій користувачів та адміністраторів ОКІІ ОКІ, обов'язки адміністраторів з обслуговування компонентів ОКІІ ОКІ та забезпечення її інформаційної безпеки?

168. Як часто Власник/керівник ОКІ зобов'язаний організовувати та проводити обстеження своїх ОКІІ ОКІ з метою оновлення даних щодо програмно-апаратного складу ОКІІ ОКІ, технології обробки інформації на ОКІІ ОКІ, переліку критичних інформаційних ресурсів та компонентів ОКІІ ОКІ, які підлягають захисту?

169. Що має відбутися, якщо за результатами обстеження ОКІІ ОКІ виявлено, що на ОКІІ ОКІ змінено технологію обробки інформації, впроваджено нові програмні або апаратні компоненти, змінено перелік критичних інформаційних ресурсів та компонентів об'єкта, які підлягають захисту?

170. Що має здійснюватися у випадку виявлення нових загроз та/або ризиків? здійснюється оновлення технічного завдання на створення КСЗІ (системи інформаційної безпеки) ОКІІ ОКІ, іншої документації та впровадження оновлених вимог на ОКІІ ОКІ.

171. Наведіть приклади інформації, яка розкриває параметри та особливості функціонування компонентів ОКІІ ОКІ, і які в інтересах національної безпеки відносять до інформації з обмеженим доступом.

172. Що визначає політика інформаційної безпеки ОКІ?

173. Наведіть вимоги до провадження програми підвищення обізнаності/навчання працівників з питань інформаційної безпеки на ОКІ.

174. Наведіть вимоги до переліку програмного та апаратного забезпечення, що використовується на ОКІІ ОКІ.

175. Наведіть вимоги до управління доступом користувачів та адміністраторів до об’єктів захисту ОКІІ ОКІ.

176. Що передбачає механізм розподілу прав доступу до ОКІІ ОКІ?

177. Наведіть вимоги до ідентифікації та автентифікації користувачів та адміністраторів ОКІІ ОКІ.

178. Наведіть вимоги до використання багатофакторної автентифікації користувачів та адміністраторів на ОКІ.

179. Наведіть вимоги до використання паролів, зокрема паролів за замовчуванням.

180. Які вимоги висуваються до обладнання, яке підключається до системи управління технологічними процесами ОКІ?

181. Наведіть вимоги до реєстрації подій компонентами ОКІІ ОКІ та їх періодичного аудиту.

182. Яку інформацію мають містити журнали реєстрації подій компонентів об’єкта?

183. Які вимоги до зберігання журналів реєстрації подій?

184. Наведіть вимоги до забезпечення мережевого захисту компонентів та інформаційних ресурсів ОКІІ ОКІ.

185. Наведіть вимоги до засобів мережевого захисту, які повинні бути встановлені у разі неможливості фізичного розділення зовнішньої мережі та ОКІІ ОКІ на межі (периметрі) між зовнішніми мережами, іншими інформаційно-комунікаційними системами, що обслуговують ОКІ.

186. Хто і як часто зобов’язаний проводити перевірку ефективності заходів щодо захисту ОКІІ ОКІ від зовнішнього проникнення шляхом виконання періодичних тестів на проникнення (Penetration test)?

187. Які є обмеження щодо використання на ОКІІ ОКІ технологій Wi-Fi та Bluetooth?

188. Наведіть вимоги до забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів ОКІІ ОКІ.

189. Наведіть вимоги до визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на ОКІІ ОКІ.

190. Наведіть вимоги до визначення умов використання програмного та апаратного забезпечення ОКІІ ОКІ.

191. Хто має право на встановлення або видалення програмного забезпечення на ОКІ?

192. Наведіть вимоги до визначення умов розміщення компонентів ОКІІ ОКІ.

193. Наведіть вимоги до зберігання схем розміщення та підключення обладнання.

Тема № 6.

194. Які основні принципи забезпечення конфіденційності, цілісності та доступності інформації в системах критичної інфраструктури?

195. Які види аварій можуть стати загрозою для об'єктів критичної інфраструктури?

196. Які можливі наслідки для суспільства при недостатньому захисті об'єктів критичної інфраструктури?

197. Які стратегії резервування та відновлення даних використовуються для забезпечення безпеки об'єктів критичної інфраструктури?

198. Основні принципи географічного розташування об'єктів критичної інфраструктури для забезпечення безпеки?

199. Що таке "стійкість до впливу стихійних лих" і як вона враховується при захисті об'єктів критичної інфраструктури?

200. Які основні види тренувань та навчання використовуються для підвищення готовності персоналу до реагування на інциденти?

201. Які методи і технології шифрування використовуються для захисту інформації в системах критичної інфраструктури?

202. Основні принципи забезпечення фізичної безпеки персоналу, що працює на об'єктах критичної інфраструктури.

203. Які загрози можуть становити інсайдери (внутрішні працівники) для об'єктів критичної інфраструктури?

204. Наведіть ланцюг п’яти взаємопов’язаних місій, визначених Національною системою готовності США.

205. Які основні етапи розробки та реалізації планів захисту об'єктів критичної інфраструктури?

206. Згідно з прийнятим у США підходом виконання яких етапів передбачає процес планування?

207. З яких елементів складається Національна система планування США?

208. Наведіть, які рівні планування включає Національна система планування США.

209. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Австралії.

210. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Австрії.

211. Охарактеризуйте організаційну структуру забезпечення кібербезпеки. Бельгії.

212. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Бразилії.

213. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Канаді.

214. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Естонії.

215. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Фінляндії.

216. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Франції.

217. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Німеччині.

218. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Угорщині.

219. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Індії.

220. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Італії.

221. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Японії.

222. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Республіки Корея.

223. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Малайзії.

224. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Нідерландах.

225. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Нової Зеландії.

226. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Норвегії.

227. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Польщі.

228. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Сінгапуру.

229. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Іспанії.

230. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Швеції.

231. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Швейцарії.

232. Охарактеризуйте організаційну структуру забезпечення кібербезпеки Великобританії.

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 слухачем знань, умінь і навичок 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 вищої освіти в Університеті 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»).

Результат навчальних занять за семестр розраховується як середньоарифметичне значення з усіх виставлених оцінок під час навчальних занять протягом семестру та виставляється викладачем в журналі обліку роботи академічної групи окремою графою.

Результат самостійної роботи за семестр розраховується як середньоарифметичне значення з усіх виставлених оцінок з самостійної роботи, отриманих протягом семестру та виставляється викладачем в журналі обліку роботи академічної групи окремою графою.

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**.

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

Підсумковий контроль.

Підсумковий контроль проводиться шляхом усного опитування або письмової контрольної роботи з метою оцінки результатів навчання.

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 слухачів, залікових книжках. ***Присутність здобувачів на проведенні підсумкового контролю (заліку) обов'язкова.*** Якщо здобувач вищої освіти не з'явився на підсумковий контроль (залік), то науково-педагогічний працівник ставить у відомість обліку успішності відмітку «не з'явився».

Підсумковий контроль (залік) оцінюється за національною шкалою. Для переводу результатів, набраних на підсумковому контролі (заліку), з національної системи оцінювання в 100-бальну вводиться коефіцієнт **10**, таким чином максимальна кількість балів на підсумковому контролі (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 (заліку).

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

Здобувач вищої освіти, який під час складання підсумкового контролю отримав оцінку «незадовільно», складає підсумковий контроль (залік) повторно. Повторне складання підсумкового контролю (заліку) допускається не більше двох разів з кожної навчальної дисципліни, у тому числі один раз – викладачеві, а другий – комісії, до складу якої входить керівник відповідної кафедри та 2-3 науково-педагогічних працівники.

Незадовільні оцінки виставляються тільки в відомостях обліку успішності. Здобувачам вищої освіти, які отримали не більше як дві незадовільні оцінки (нижче ніж 60 балів) з навчальної дисципліни, можуть бути встановлені різні строки ліквідації академічної заборгованості, але не пізніше як за день до фактичного початку навчальних занять у наступному семестрі.

Робота під час навчальних занять	**Самостійна та індивідуальна робота**	**Підсумковий контроль**
Отримати не менше 3 позитивних оцінок	Підготувати реферат, підготувати конспект за темами 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 **прогалини не носять істотного** характеру, необхідні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **більшість** передбачених програмою навчання навчальних завдань **виконано, деякі** з виконаних завдань, містять **помилки,** робота з трьома значними помилками.
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

10.1 Основна:

1. Манжай О.В., Мелешко Д.Г., Носов В.В., Самойлов С.В. Розробка та впровадження системи управління безпекою інформації. Київ: ВАІТЕ, 2021. 138 с.
2. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків: Промарт, 2020. 162 с. з іл.
3. Павлов Д., Микитюк М. Правові та організаційні засади забезпечення захисту критичної інфраструктури у контексті формування нової безпекової парадигми України. 2020. URL: http://chiz.nangu.edu.ua/article/view/220748 (дата звернення: 20.06.2023).
4. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналітична доповідь / [Бобро Д.Г., Іванюта С.П., Кондратов С.І., Суходоля О.М.]; за заг. ред. О.М. Суходолі. Київ: НІСД, 2019. 224 с. URL: https://niss.gov.ua/sites/default/files/2019-05/Dopov_Suchodolya_print.pdf (дата звернення: 20.06.2023).
5. Щодо створення державної системи захисту критичної інфраструктури: аналітична записка. 2017. URL: https://niss.gov.ua/sites/default/files/2017-02/infrastrukt-86de2.pdf (дата звернення: 20.06.2023).
6. Державна система захисту критичної інфраструктури України: концептуальні засади адміністративно-правового регулювання. Монографія. 2020. URL: https://jurkniga.ua/derzhavna-sistema-zakhistu-kritichnoi-infrastrukturi-ukraini-kontseptualni-zasadi-administrativno-pravovogo-regulyuvannya/ (дата звернення: 20.06.2023).
7. Актуальні питання нормативно-правового регулювання захисту критичної інфраструктури в умовах воєнного стану в Україні. 2022. URL: https://reicst.com.ua/pmtl/article/view/2022-6-01-09 (дата звернення: 20.06.2023).
8. Онищенко Ю.М. Державні механізми запобігання і протидії кіберзлочинності в умовах глобалізації. дис. канд. наук з держ. управ: 25.00.02. Харків, 2015. 200 с.
9. Кравцова М.О. Запобігання кіберзлочинності в Україні: монографія / М.О. Кравцова, О.М. Литвинов / [За загальною редакцією д-ра юрид. наук, проф. О.М. Литвинова]. – Харків: Панов, 2016. – 212 с.

10.2 Додаткова література з навчальної дисципліни

Навчальна та наукова література:

10. Науково-практичний коментар Закону України «Про основні засади забезпечення кібербезпеки України». / М.В. Гуцалюк та ін.; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.
11. Бірюков Д.С. Захист критичної інфраструктури в Україні: від наукового осмислення до розробки засад політики. Науково-інформаційний вісник Академії національної безпеки. 2015. № 3-4. С. 155-170.

12. Зелена книга з питань захисту критичної інфраструктури в Україні: зб. мат-лів міжнар. експерт. нарад / упоряд. Д.С. Бірюков, С.І. Кондратов; за заг. ред. О.М. Суходолі. К. : НІСД, 2015. 176 с.

13. Суходоля О.М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритет державної політики України / О.М. Суходоля // Стратегічні пріоритети. – 2016. – № (3) 40. – С. 62–76.

14. Адміністративно-правові засади формування переліку об’єктів критичної інфраструктури. 2020. URL: http://www.law.stateandregions.zp.ua/archive/3-2_2020/8.pdf (дата звернення: 20.06.2023).

15. Правові умови захисту об’єктів критичної інфраструктури в Україні: проблеми та перспективи. 2021. URL: http://www.sulj.oduvs.od.ua/archive/2021/2/22.pdf (дата звернення: 20.06.2023).

16. Ткачук Н.А. Організаційно-правові засади формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави. 2018. URL: http://ippi.org.ua/tkachuk-na-organizatsiino-pravovi-zasadi-formuvannya-pereliku-informatsiino-telekomunikatsiinikh-sis (дата звернення: 20.06.2023).

17. Крикун В.В. Стан дослідження проблеми захисту об’єктів критичної інфраструктури в Україні. 2019. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/4ec60c7b-501f-4428-b0dd-e21f0bb83260/content (дата звернення: 20.06.2023).

18. Осипчук І.І Правові засади діяльності служби безпеки України як суб’єкта забезпечення критичної інфраструктури та місце серед них адміністративного законодавства. 2020. URL: http://www.nvppp.in.ua/vip/2020/6/tom_2/28.pdf (дата звернення: 20.06.2023).

Нормативно-правові акти:

19. Конституція України від 28 червня 1996 р. № 254к/96-ВР (із змінами). Відомості Верховної Ради України. 1996. № 30. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 20.06.2023).

20. Про кіберзлочинність: конвенція Ради Європи від 07.09.2005 ратифікована Верховною Радою України 07.09.2005 URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 20.06.2023).

21. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 20.06.2023).

22. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 р. № 96/2016. URL: http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 20.06.2023).

23. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 р. № 447/2021.

URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 20.06.2023).

24. Про Державну службу спеціального зв'язку та захисту інформації України. Закон України: від 23.02.2006, № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 20.06.2023).

25. Про національну безпеку України: Закон України від 21.06.2018 № 2469. Відомості Верховної Ради. 2018. № 31.

26. Про захист інформації в інформаційно-комунікаційних системах. Закон України: від 05.07.1994, № 1170-VII. URL: URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 20.06.2023).

27. Про електронні комунікації: Закон України від 16.12.2020: [із змінами і доповненнями]. Офіційний вісник України. 2021. № 6 (21.01.2021). Ст. 306.

28. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 20.06.2023).

29. Стратегія інформаційної безпеки України, затверджена Указом Президента України від 28 грудня 2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 20.06.2023).

30. Про затвердження Положення про організаційно-технічну модель кіберзахисту: Постанова Кабінету Міністрів України від 29.12.2021 № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text

31. Деякі питання проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури. Постанова Кабінету Міністрів України від 24.03.2023 № 257. URL: https://zakon.rada.gov.ua/laws/show/257-2023-%D0%BF#Text

32. Деякі питання реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. Постанова Кабінету Міністрів України від 04.04.2023 № 299. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text

33. Деякі питання функціонування Національного центру резервування державних інформаційних ресурсів. Постанова Кабінету Міністрів України від 07.04.2023 № 311. URL: https://zakon.rada.gov.ua/laws/show/311-2023-%D0%BF#Text

34. Деякі питання створення та функціонування державних електронних платформ для ведення публічних електронних реєстрів. Постанова Кабінету Міністрів України від 18.04.2023 № 356. URL: https://zakon.rada.gov.ua/laws/show/356-2023-%D0%BF#Text

35. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Постанова

Кабінету Міністрів України від 16.05.2023 № 497. URL: https://zakon.rada.gov.ua/laws/show/497-2023-%D0%BF#Text

36. Постанова Кабінету Міністрів України від 28 квітня 2023 р. № 415 «Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього» URL: https://zakon.rada.gov.ua/laws/show/415-2023-%D0%BF#Text (дата звернення: 20.06.2023).

37. Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 «Деякі питання об'єктів критичної інфраструктури» URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n45 (дата звернення: 20.06.2023).

38. Розпорядження Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р «Про схвалення Концепції створення державної системи захисту критичної інфраструктури». URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80/#Text (дата звернення: 20.06.2023).

39. Закон України 18 жовтня 2022 р. № 2684-IX Про внесення змін до деяких законів України щодо повноважень уповноваженого органу у сфері захисту критичної інфраструктури України URL: https://zakon.rada.gov.ua/laws/show/2684-20#Text (дата звернення: 20.06.2023).

40. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 20.06.2023).

41. Деякі питання об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 9 жовтня 2020 р. № 943 URL: https://zakon.rada.gov.ua/laws/show/943-2020-п#n13 (дата звернення: 20.06.2023).

42. Про рішення Ради національної безпеки і оборони України від 16 травня 2019 року "Про організацію планування в секторі безпеки і оборони України": Указ Президента України від 16.05.2019 № 225/2019. URL: https://www.president.gov.ua/documents/2252019-26835 (дата звернення: 20.06.2023).

43. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України": Указ Президента України від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 20.06.2023).

44. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом: Постанова Кабінету Міністрів України від 11.11.2020 № 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-п#Text (дата звернення: 20.06.2023).

45. Деякі питання проведення зовнішнього аудиту діяльності уповноваженого органу у сфері захисту критичної інфраструктури України: Постанова КМУ від 10 червня 2022 р. № 675. URL: https://zakon.rada.gov.ua/laws/show/675-2022-%D0%BF#Text

46. Про затвердження Порядку проведення моніторингу рівня безпеки об’єктів критичної інфраструктури: Постанова КМУ від 22 липня 2022 р. № 821. URL: https://zakon.rada.gov.ua/laws/show/821-2022-%D0%BF#Text

47. Положення про Департамент кіберполіції Національної поліції України, затверджене наказом Національної поліції України № 85: від 10.11.2015. К.: Національна поліція України, 2015. 9 с.

48. Постанова Правління Національного банку України Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України від 12.08.2022 № 178. URL: https://zakon.rada.gov.ua/laws/show/v0178500-22#Text (дата звернення: 20.06.2023).

49. Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. Наказ Адміністрації Держспецзв'язку від 06.10.2021 № 601, в редакції наказу від 10.07.2022 № 343. URL: https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601

50. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами. Наказ Адміністрації Держспецзв'язку від 29.05.2023 № 463. URL: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-29-05-2023-463-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-zabezpechennya-kiberzakhistu-avtomatizovanikh-sistem-upravlinnya-tekhnologichnimi-procesami

51. Про затвердження Методичних рекомендацій щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. Наказ Адміністрації Держспецзв'язку від 03.07.2023 № 570. URL: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-03-07-2023-570-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-reaguvannya-sub-yektami-zabezpechennya-kiberbezpeki-na-rizni-vidi-podii-u-kiberprostori

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

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

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

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

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

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

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

10.3. Інформаційні ресурси в Інтернеті:

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

60. Економіко-правові засади забезпечення захисту критичної інфраструктури URL: https://ekmair.ukma.edu.ua/items/565dc636-5df4-4840-bf76-0f4b82df0c4a

61. Адміністративно-правове забезпечення безпеки критичної інфраструктури і Україні URL: https://dduvs.in.ua/wp-content/uploads/files/Structure/science/rada/auto/35/a1.pdf

62. Internet Organised Crime Threat Assessment (IOCTA). URL: https://www.europol.europa.eu/ activities-services/main-reports/internet-organised-crime-threat-assessment (дата звернення: 20.06.2023).

63. URL: http://www.niss.gov.ua/

64. URL: https://cyberpolice.gov.ua/

65. URL: https://cip.gov.ua/ua

66. URL: https://cert.gov.ua/

67. URL: https://ssu.gov.ua/

68. URL: https://www.president.gov.ua/

69. Europol. – https://www.europol.europa.eu/content/memberpage/austria-791.

70. Online Investigative Principles for Federal Law Enforcement Agents. – https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf .

71. Canadian Cyber Incident Response Centre (CCIRC). – http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx .

72. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx

73. Action Plan 2010-2015 for Canada's Cyber Security Strategy. – http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-eng.aspx

74. Information security. Finnish communication regulatory authority. – https://www.viestintavirasto.fi/en/informationsecurity.html

75. Le secrétariat général de la défense et de la sécurité nationale (SGDSN). – Organisation http://www.sgdsn.gouv.fr/site_rubrique88.html

76. Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. – http://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire

77. Cyber Security Strategy for Germany. – https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile

78. Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary. – http://2010-2014.kormany.hu/download/4/32/b0000/National%20Security%20Strategy.pdf

79. Discussion draft on National Cyber Security Policy. Department of Information Technology Ministry of Communications and Information Technology Government of India Electronics Niketan, Lodhi Road New Delhi – 110003. – http://deity.gov.in/hindi/sites/upload_files/dithindi/files/ncsp_060411.pdf

80. Cyber Security Policies. – http://www.space-cyber.jp/cyber/

81. National Cyber Security Center. – http://service1.nis.go.kr/eng/intro/NCSCInfo.jsp

82. Government ICT Security Command Centre. – http://www.mampu.gov.my/web/en/prisma

83. National risk analysis – Direktoratet for samfunnssikkerhet. – www.dsb.no/Global/Publikasjoner/2013/Tema/NRB_2013_english.pdf

84. Ellyne Phneah /Singapore to open Cyber Security Lab to train law enforcers // Phneah Ellyne. – http://www.zdnet.com/sg/singapore-to-open-cyber-security-lab-to-train-law-enforcers-7000012392/

85. Sweden's Information Security. – https://msb.se/RibData/Filer/pdf/26419. pdf.