ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО
«ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ»

МАУП

Інститут безпеки

Кафедра національної безпеки

ЗАТВЕРДЖУЮ:

Директор Інституту безпеки

_____ С.О. Лисенко

"1" серпня 2024 р.

Схвалено на засіданні кафедри національної безпеки
Протокол №1 від 1 серпня 2024 р.
Заст.зав. кафедри

_____ В.В. Ровний

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ»

спеціальності: 256 Національна безпека (за окремими сферами забезпечення і видами діяльності)

освітнього рівня магістр

освітньої програми: Національна безпека (за окремими сферами забезпечення і видами діяльності)

Галузь знань 25 Воєнні науки, національна безпека, безпека державного кордону

Київ МАУП 2024

Розробник (-и) робочої програми навчальної дисципліни:
Сергій Віталійович Кавун доктор економічних наук, професор.

__________ С. В. Кавун

Викладач:
Сергій Віталійович Кавун доктор економічних наук, професор.

__________ С. В. Кавун

Робочу програму розглянуто і затверджено на засіданні кафедри національної безпеки
(протокол № 1 від "1" серпня 2024 р.)

Схвалено Вченою радою Інституту безпеки
(протокол № 1 від "8" серпня 2024 р.)

Заст.зав. кафедри __________ (підпис) К. В. Ровенська (П.І.Б.)

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 256 Національна безпека (за окремими сферами забезпечення і видами діяльності)
___.____.______р.

Гарант освітньої програми __________ (підпис) О.В. Сербовський (П.І.Б.)

Робочу програму перевірено
___.___._____р.

__________ (підпис) О.В. Сербовський (П.І.Б.)

Пролонговано:

На 20__/20__н.р. __________(________________),"___"___20__р., протокол №_
(підпис) (П.І.Б.)

На 20__/20__н.р. __________(________________),"___"___20__р., протокол №_
(підпис) (П.І.Б.)

На 20__/20__н.р. __________(________________),"___"___20__р., протокол №_
(підпис) (П.І.Б.)

На 20__/20__н.р. __________(________________),"___"___20__р., протокол №_
(підпис) (П.І.Б.)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	Денна, денно-дистанційна форми навчання	**Заочна**
Кібербезпека та захист інформаційних систем		
Курс	1	
Семестр	2	
Обсяг кредитів	3	
Обсяг годин, в тому числі:	90	
Аудиторні	34	
Модульний контроль		
Семестровий контроль		
Самостійна робота	56	
Форма семестрового контролю	Залік	

2. Статус дисципліни: *обов'язкова*

3. Мета та завдання дисципліни. Метою курсу «Кібербезпека та захист інформаційних систем» є формування у здобувачів вищої освіти системного розуміння теоретичних засад і практичних методів забезпечення кібербезпеки, розвиток навичок виявлення, оцінювання та нейтралізації кіберзагроз, а також здатності ефективно застосовувати засоби захисту інформаційних систем відповідно до вимог національного законодавства, міжнародних стандартів і сучасних технологій інформаційної безпеки. Завданнями навчальної дисципліни «Кібербезпека та захист інформаційних систем» є: ознайомлення здобувачів із базовими поняттями, принципами та структурою кібербезпеки й інформаційного захисту; формування знань щодо класифікації та аналізу кіберзагроз і вразливостей; вивчення методів і засобів захисту інформації, зокрема криптографічних, програмно-апаратних і організаційних механізмів; опанування навичок розробки політик безпеки, управління доступом та реагування на кіберінциденти; засвоєння нормативно-правових основ у сфері кібербезпеки України та міжнародних стандартів; розвиток компетентностей у сфері проведення аудиту інформаційної безпеки, оцінювання ризиків, а також забезпечення кіберстійкості інформаційних систем у різних галузях.

4. Компетентності та програмні результати навчання за дисципліною

Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у галузі національної безпеки (за окремими сферами забезпечення і видами діяльності).

Здатність до абстрактного мислення, аналізу та синтезу.

Здатність приймати обґрунтовані рішення.

Здатність вчитися і оволодівати сучасними знаннями.

Здатність інтегрувати знання та розв'язувати складні задачі національної безпеки (за окремими сферами забезпечення і видами діяльності) у широких та/або мультидисциплінарних контекстах за наявності неповної або обмеженої інформації

з урахуванням аспектів соціальної та етичної відповідальності.

Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності.

Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (за сферами забезпечення та видами діяльності), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог.

Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів.

Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.

Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності).

Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.

Здатність застосовувати набуті сучасні знання в галузі національної безпеки для збору, систематизації і аналізу отриманої з публічних джерел інформації стосовно загроз безпеці.

Демонструвати та застосовувати навики управління суб'єктами національної безпеки та їх структурними підрозділами.

5. Структура навчальної дисципліни

№	Курс 1 Семестр 1 Всього годин у семестрі 90 Теми	Кількість годин, з них:					
		лекції	семінарські заняття	практ. лаб. зан. (ПЗ, ЛЗ)	інд.конс. роб. (ІКС)	сам. рою. студ. (СРС)	Примітка
	Модуль 1. Теоретичні основи кібербезпеки та інформаційного захисту						
1.	Поняття та структура кіберпростору і кібербезпеки	2	2			5	СР
2.	Законодавча та нормативна база кібербезпеки в Україні та світі	2	2			5	СР
3.	Класифікація та аналіз кіберзагроз і вразливостей	2	2			5	СР
4.	Принципи та компоненти систем захисту інформаційних систем	2	2			5	СР
5.	Політики	2	2			4	СР

	інформаційної безпеки: цілі, розробка, реалізація						
	Модуль 2. Технічні та організаційні засоби забезпечення кібербезпеки						
6.	Криптографічні методи захисту інформації	2	2			4	СР
7.	Мережеві екрани, IDS/IPS-системи та інші засоби технічного захисту	2	2			4	СР
8.	Аутентифікація, керування доступом та контроль дій користувачів	1	2			4	СР
9.	Захист баз даних, серверів та хмарних сервісів	1	2			4	СР
10.	Захист кінцевих точок і мобільних пристроїв	1	1			3	СР
	Модуль 3. Реагування на інциденти, аудит та розвиток кіберзахисту						
11.	Управління інцидентами інформаційної безпеки	3	3			4	СР
12.	Основи кібергігієни та захисту персональних даних	2	3			4	СР
13.	Аудит інформаційної безпеки та оцінювання ризиків	2	3			4	СР

Тематичний план для денної форми навчання

Форми контролю:

-усне опитування - У;

-контрольні роботи - КР;

- перевірка конспектів - ПК;

- перевірка завдань для самостійної роботи - СР;

- тестування - Т;

- колоквіум - К;

інші:

- реферат.

6. Програма навчальної дисципліни

Модуль 1.Теоретичні основи кібербезпеки та інформаційного захисту
Тема 1. Поняття та структура кіберпростору і кібербезпеки

1. Визначення кіберпростору та його складові.
2. Основні елементи структури кібербезпеки.
3. Взаємозв'язок кіберпростору з інформаційною безпекою.

Література: [1; 2; 8]

Тема 2. Законодавча та нормативна база кібербезпеки в Україні та світі

1. Основні закони України у сфері кібербезпеки.
2. Міжнародні нормативні акти та стандарти з кібербезпеки.
3. Роль національних органів у забезпеченні кібербезпеки.

Література: [5; 7; 10]

Тема 3. Класифікація та аналіз кіберзагроз і вразливостей

1. Типи кіберзагроз: зовнішні та внутрішні.
2. Види вразливостей інформаційних систем.
3. Методи оцінки ризиків і впливу кіберзагроз.

Література: [2; 6; 9]

Тема 4. Принципи та компоненти систем захисту інформаційних систем

1. Основні принципи забезпечення інформаційної безпеки.
2. Технічні, організаційні та правові компоненти систем захисту.
3. Механізми контролю доступу та моніторингу безпеки.

Література: [2; 4; 8]

Тема 5. Політики інформаційної безпеки: цілі, розробка, реалізація

1. Основні цілі політик інформаційної безпеки.
2. Етапи розробки політик інформаційної безпеки.
3. Механізми впровадження та контролю виконання політик.

Література: [2; 7; 10]

Модуль 2. Технічні та організаційні засоби забезпечення кібербезпеки
Тема 6. Криптографічні методи захисту інформації

1. Основні види криптографічних алгоритмів.

2. Симетричне та асиметричне шифрування.
3. Використання цифрових підписів і сертифікатів.

Література: [5; 9; 12]

Тема 7. Мережеві екрани, IDS/IPS-системи та інші засоби технічного захисту

1. Принципи роботи мережевих екранів (Firewall).
2. Функції та типи IDS/IPS-систем.
3. Інші апаратні та програмні засоби технічного захисту.

Література: [5; 10; 12]

Тема 8. Аутентифікація, керування доступом та контроль дій користувачів

1. Методи аутентифікації користувачів.
2. Моделі керування доступом (RBAC, DAC, MAC).
3. Системи моніторингу та аудит дій користувачів.

Література: [8; 9; 12]

Тема 9. Захист баз даних, серверів та хмарних сервісів

1. Методи забезпечення безпеки баз даних.
2. Засоби захисту серверної інфраструктури.
3. Особливості безпеки хмарних сервісів.

Література: [9; 11; 3]

Тема 10. Захист кінцевих точок і мобільних пристроїв

1. Засоби антивірусного та антимальварного захисту
2. Техніки контролю доступу на мобільних пристроях
3. Політики безпеки для кінцевих користувачів і пристроїв.

Література: [4; 10; 5]

Модуль 3. Службові розслідування: нормативна база, алгоритми, практика

Тема 11. Управління інцидентами інформаційної безпеки

1. Процес виявлення та класифікації інцидентів.
2. Методи реагування та ліквідації наслідків інцидентів.
3. Ведення журналів і аналіз інцидентів для запобігання повторенню.

Література: [3; 11; 5]

Тема 12. Основи кібергігієни та захисту персональних даних

1. Рекомендації з безпечної поведінки в кіберпросторі.
2. Методи захисту персональних даних від несанкціонованого доступу.
3. Правові норми щодо захисту персональних даних.

Література: [4; 10; 8]

Тема 13. Аудит інформаційної безпеки та оцінювання ризиків

1. Методи проведення аудиту інформаційної безпеки.
2. Інструменти оцінювання кіберризиків.
3. Формування рекомендацій за результатами аудиту.

Література: [6; 11; 7]

7. Система оцінювання навчальних досягнень студентів

Вид діяльності студента	Макс. к-сть балів за одиницею	Модуль 1		Модуль 2		Модуль 3	
		к-сть одиниць	макс. к-сть одиниць	к-сть одиниць	макс. к-сть одиниць	к-сть одиниць	макс. к-сть одиниць
Відвідування лекцій	2	3	6	2	4	2	4
Відвідування сем. занять	2	4	8	3	6	3	6
Робота на сем. занятті	5	4	20	3	15	3	15
Виконання завд. для сам. роботи	4	6	24	4	16	4	16
Виконання модульної роботи	20	1	20	1	20	1	20
Виконання ІНДЗ	50	-		-		-	

Разом			78		61		61
Максимальна кількість балів:							200
200:100=2. Студент набрав Х балів; розрахунок: Х:2=загальна к-сть балів.							100

7.1. Завдання для самостійної роботи та критерії її оцінювання.

1. Визначити поняття кіберпростору та його основні компоненти.
2. Охарактеризувати структуру кібербезпеки.
3. Проаналізувати основні загрози кібербезпеці в сучасному світі.
4. Вивчити законодавчу базу України щодо кібербезпеки.
5. Описати міжнародні стандарти та нормативи у сфері кібербезпеки.
6. Пояснити роль національних органів у забезпеченні кібербезпеки.
7. Класифікувати типи кіберзагроз та приклади їх реалізації.
8. Виявити основні вразливості інформаційних систем.
9. Розглянути методи оцінки ризиків у кібербезпеці.
10. Проаналізувати принципи захисту інформаційних систем.
11. Описати технічні засоби захисту інформації.
12. Розглянути організаційні компоненти систем безпеки.
13. Вивчити правові засади інформаційної безпеки.
14. Проаналізувати політики інформаційної безпеки: цілі та основні вимоги.
15. Розглянути етапи розробки політик безпеки.
16. Визначити механізми реалізації політик безпеки в організації.
17. Охарактеризувати основні криптографічні методи захисту інформації.
18. Порівняти симетричне та асиметричне шифрування.
19. Вивчити принципи роботи цифрових підписів та сертифікатів.
20. Проаналізувати принципи функціонування мережевих екранів (Firewall).
21. Описати типи IDS/IPS-систем та їхнє застосування.
22. Розглянути інші апаратні та програмні засоби захисту.
23. Вивчити методи аутентифікації користувачів.
24. Проаналізувати моделі керування доступом (RBAC, DAC, MAC).
25. Розглянути системи моніторингу дій користувачів.
26. Описати заходи захисту баз даних.
27. Вивчити засоби захисту серверів.
28. Проаналізувати особливості безпеки хмарних сервісів.
29. Охарактеризувати методи захисту кінцевих точок.
30. Розглянути захист мобільних пристроїв у корпоративних мережах.
31. Вивчити принципи кібергігієни для користувачів.
32. Проаналізувати методи захисту персональних даних.
33. Розглянути законодавчі вимоги до захисту персональних даних.
34. Описати процес виявлення кіберінцидентів.
35. Вивчити класифікацію інцидентів інформаційної безпеки.
36. Проаналізувати методи реагування на кіберінциденти.
37. Визначити порядок ліквідації наслідків кіберінцидентів.

38. Розглянути ведення журналів безпеки та їх аналіз.
39. Охарактеризувати методи аудиту інформаційної безпеки.
40. Проаналізувати інструменти оцінювання кіберризиків.
41. Вивчити формування рекомендацій за результатами аудиту.
42. Описати роль навчання персоналу у забезпеченні кібербезпеки.
43. Проаналізувати соціальну інженерію та методи захисту від неї.
44. Вивчити засоби захисту від фішингових атак.
45. Охарактеризувати методи виявлення та запобігання DDoS-атакам.
46. Проаналізувати роль шифрування у захисті бездротових мереж.
47. Вивчити специфіку безпеки IoT-пристроїв.
48. Описати практики захисту веб-додатків.
49. Розглянути питання безпеки при роботі з API.
50. Вивчити особливості забезпечення безпеки у віртуальних середовищах.
51. Проаналізувати роль блокчейн-технологій у кібербезпеці.
52. Описати основи кіберзлочинності та криміналістики.
53. Розглянути способи цифрової ідентифікації та автентифікації.
54. Проаналізувати особливості захисту інформації в державних установах.
55. Вивчити основи кібербезпеки в банківській сфері.
56. Охарактеризувати кіберзагрози в промислових системах (ICS/SCADA).
57. Проаналізувати механізми забезпечення безпеки електронної пошти.
58. Вивчити принципи роботи систем резервного копіювання та відновлення.
59. Розглянути інструменти автоматизації управління безпекою.
60. Проаналізувати перспективи розвитку кібербезпеки у світлі сучасних технологій.

7.2. Форми проведення модульного контролю та критерії оцінювання.

Модульний контроль відбувається в кінці вивчення блоків змістових модулів і здійснюється у вигляді тестування. Студентами пропонуються тестові завдання у кількості 60 запитань. Максимальна кількість балів - 10 балів.

7.3. Форми проведення семестровго котролю та критерії оцінювання.

Залік

7.4. Орієнтований перелік питань для семестрового комплексного контролю.

1. Поняття кіберпростору та його основні складові.
2. Визначення кібербезпеки та її значення в сучасному світі.
3. Класифікація кіберзагроз за типами і джерелами.
4. Основні вразливості інформаційних систем.
5. Законодавча база України у сфері кібербезпеки.
6. Міжнародні стандарти та норми кібербезпеки (ISO, NIST тощо).
7. Роль державних органів у забезпеченні кібербезпеки.
8. Сутність і компоненти систем захисту інформації.
9. Криптографічні методи захисту: симетричне та асиметричне шифрування.
10. Принципи роботи цифрових сертифікатів та електронних підписів.
11. Механізми контролю доступу в інформаційних системах.

12. Політики інформаційної безпеки: розробка і впровадження.
13. Організаційні заходи для забезпечення кібербезпеки в організації.
14. Технічні засоби захисту: мережеві екрани (firewalls).
15. Системи виявлення та запобігання вторгнень (IDS/IPS).
16. Захист баз даних: основні принципи і методи.
17. Безпека серверів і хмарних обчислень.
18. Особливості захисту кінцевих точок та мобільних пристроїв.
19. Основи кібергігієни для користувачів.
20. Захист персональних даних: законодавчі вимоги і практики.
21. Методи ідентифікації кіберінцидентів.
22. Класифікація інцидентів інформаційної безпеки.
23. Процес реагування на кіберінциденти.
24. Аналіз журналів безпеки і аудит інформаційних систем.
25. Оцінка ризиків кібербезпеки: методи і інструменти.
26. Взаємодія між компонентами системи кібербезпеки.
27. Особливості аутентифікації та авторизації користувачів.
28. Керування правами доступу: моделі RBAC, DAC, MAC.
29. Захист від соціальної інженерії.
30. Методи запобігання фішинговим атакам.
31. Аналіз та протидія DDoS-атакам.
32. Захист бездротових мереж: шифрування та аутентифікація.
33. Особливості кібербезпеки в IoT-середовищах.
34. Безпека веб-додатків: основні уразливості та захист.
35. Методи захисту API.
36. Кібербезпека віртуальних середовищ і контейнерів.
37. Роль блокчейн-технологій у забезпеченні безпеки.
38. Поняття кіберзлочинності та її основні види.
39. Основи цифрової криміналістики.
40. Захист інформації в державних органах.
41. Особливості кібербезпеки в фінансовій сфері.
42. Загрози і захист промислових систем (ICS/SCADA).
43. Механізми захисту електронної пошти.
44. Системи резервного копіювання та відновлення даних.
45. Автоматизація управління інформаційною безпекою.
46. Вплив людини на рівень кібербезпеки організації.
47. Навчання та підвищення кваліфікації в сфері кібербезпеки.
48. Етика і правові аспекти кібербезпеки.
49. Роль стандартів ISO 27001, ISO 31000 в кібербезпеці.
50. Поняття інциденту безпеки та його життєвий цикл.
51. Основні загрози цілісності, доступності та конфіденційності інформації.
52. Модель захисту інформації CIA (Confidentiality, Integrity, Availability).
53. Методи шифрування даних у процесі передачі.
54. Поняття багатофакторної аутентифікації та її реалізація.
55. Використання SIEM-систем для моніторингу безпеки.
56. Розробка планів безперервності бізнесу в умовах кіберзагроз.

57. Техніки соціального інжинірингу та методи протидії.
58. Аналіз уразливостей та проведення пенетраційного тестування.
59. Особливості захисту інформації в мобільних додатках.
60. Перспективи розвитку кібербезпеки в контексті новітніх технологій.

7.5. Шкала відповідності оцінок

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою
		для екзамену, курсового проекту (роботи), практики
90-100	A	5 (відмінно)
82-89	B	4 (добре)
75-81	C	
68-74	D	3 (задовільно)
60-67	E	
35-59	FX	2 (незадовільно)
1-34	F	

8. Рекомендовані джерела

Основна література

1. Баранов, О. А. (2014). Про тлумачення та визначення поняття «кібербезпека». Правова інформатика, 2(42), 54-62.
2. Фурашев, В. М. (2012). Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. Інформація і право, (2 (5)), 162-169.
3. Биков, В. Ю., Буров, О. Ю., & Дементієвська, Н. П. (2019). Кібербезпека в цифровому навчальному середовищі. Інформаційні технології і засоби навчання, (70,№ 2), 313-331.
4. Сопілко, І. М. (2021). Інформаційна безпека та кібербезпека: порівняльноправовий аспект (Doctoral dissertation, Національний авіаційний університет).
5. Tkachenko, O., & Tkachenko, K. (2018). Кіберпростір і кібербезпека: проблеми, перспективи, технології. Цифрова платформа: інформаційні технології в соціокультурній сфері, (1), 75-86.
6. Вітер, С. А., Витер, С. А., Світлишин, І. І., & Светлишин, И. И. (2017). Захист облікової інформації та кібербезпека підприємства.
7. Інформаційна безпека організації як фактор посилення бренду роботодавця [Електронний ресурс] Л. В. Мазник, О. І. Драган Київський економічний науковий журнал. 2023. № 1. С. 39-44. Режим доступу: http://nbuv.gov.ua/UJRN/kecscj_2023_1_7
8. Безпека інформаційних систем організацій [Електронний ресурс] / Я. Пахольчук, А. Митко // Міжнародні відносини, суспільні комунікації та регіональні студії. 2017. № 1. С. 89-96. Режим доступу: http://nbuv.gov.ua/UJRN/mvckrc_2017_1_11

9. Трофименко, О. Г., Прокоп, Ю. В., Логінова, Н. І., & Задерейко, О. В. (2019). Кібербезпека України: аналіз сучасного стану. Ukrainian Information Security Research Journal, 21(3), 150-157.
10. Аналіз теоретичних викладок організації та управління соціальноекономічною безпекою [Електронний ресурс] / А. Д. Калько // Інвестиції: практика та досвід. - 2012. - № 23. - С. 118-123. - Режим доступу: http://nbuv.gov.ua/UJRN/ipd_2012_23_30
11. Когут, Ю. (2022). Кібервійни, кібертероризм, кіберзлочинність. Концепції, стратегії, технології. Дакор, Консалтингова компанія Сідкон.
12. Хлапонін, Ю., Козубцова, Л., Козубцов, І., & Штонда, Р. (2022). Функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(15), 124–134. https://doi.org/10.28925/2663-4023.2022.15.1241341
13. Д.В. Ланде. OSINT у кібербезпеці : навч. пос. / Ланде Д.В. – Київ: ТОВ «Інжиніринг», 2024. – 522 с. ISBN 978-966-2344-97-4
14. Президент України. (2021). Указ № 447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". https://www.president.gov.ua/documents/4472021-40013