



**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**  
**Харківський національний університет внутрішніх**  
**справ**

**Факультет № 4**

**Кафедра протидії кіберзлочинності**

**Факультет № 6**

**Кафедра кібербезпеки та DATA-технологій**

**ЗАТВЕРДЖЕНО**

На спільному засіданні кафедри  
протидії кіберзлочинності факультету  
№ 4 та кафедри кібербезпеки та  
DATA-технологій факультету №6  
протокол № 2 від 22 червня 2023 р.

Завідувач кафедри

**Олександр МАНЖАЙ**

**СТАНДАРТИЗАЦІЯ І СЕРТИФІКАЦІЯ**  
**В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (ОК.06)**

**ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

<b>Кафедра</b>	Протидії кіберзлочинності ( <a href="https://univd.edu.ua/uk/dir/1740/kafedra-protydii-kiberzlochynnosti">https://univd.edu.ua/uk/dir/1740/kafedra-protydii-kiberzlochynnosti</a> )
<b>Контактний телефон</b>	+38 057 7398085 (роб.)
<b>E-mail</b>	<a href="mailto:moj@univd.edu.ua">moj@univd.edu.ua</a>
<b>ЛЕКТОР (ЛЕКТОРИ)</b>	
	Манжай Олександр Володимирович, завідувач кафедри протидії кіберзлочинності факультету № 4, к.ю.н., професор <a href="mailto:moj@univd.edu.ua">moj@univd.edu.ua</a>  Лекційний потік: факультет № 4, шифр навчальних груп Ф5-104м  Лекційний потік: факультет № 6, шифр навчальних груп Ф6-_____
<b>Назва освітньо-професійної програми</b>	Кібербезпека та захист інформації (безпека інформаційних та комунікаційних систем) Cybersecurity and information protection (security of information and communication systems)

<b>Рівень вищої освіти</b>	Другий (магістерський) (НРК України – 7 рівень та другий цикл вищої освіти Рамки кваліфікацій Європейського простору вищої освіти)
<b>Галузь знань</b>	12 Інформаційні технології
<b>Спеціальність</b>	125 Кібербезпека та захист інформації
<b>Статус дисципліни</b>	Нормативна компонента освітньо-наукової програми, вивчається в 2 семестрі I курсу навчання
<b>Мета вивчення дисципліни</b>	<p>Навчити здобувачів вищої освіти встановлених стандартами та іншими документами правил побудови комплексної системи захисту інформації та системи управління інформаційною безпекою.</p> <p>Виробити вміння: визначати відповідність стану безпеки інформації встановленим вимогам; будувати систему управління інформаційною безпекою згідно зі встановленими вимогами; об'єктивно оцінювати ризики для безпеки об'єкта та запобігати їм; приймати рішення щодо необхідності застосування того чи іншого способу реагування на загрозу; критично оцінювати інформацію.</p> <p>Сформувати у здобувачів вищої освіти знання, уміння і навички щодо основних правил та порядку побудови комплексної системи захисту інформації, системи управління інформаційною безпекою; дотримання правил кібербезпеки в системі публічної служби.</p>
<b>Завдання вивчення дисципліни</b>	Дослідження чинних стандартів у сфері забезпечення безпеки інформації.
<b>Обсяг дисципліни в кредитах ECTS/годинах</b>	5 кредитів ECTS (загальний обсяг - 150 год.)
	- аудиторна робота (денна/заочна): 60/16 год., з них:
	лекції: 30/6 год.
	лабораторні заняття: 0 год.
	практичні заняття: 30/10 год.
	семінарські заняття: 0 год.
<b>Форми та види проведення навчальних занять</b>	самостійна робота: 90/134 год.
	<p>Форма навчання – денна, заочна.</p> <p>Види навчальних занять: лекції, практичні,</p>

	самостійна робота.
<b>Самостійна робота</b>	Опрацювання рекомендованої літератури, підготовка тез доповідей до конференцій
<b>Індивідуальні завдання</b>	Наукові доповіді, реферати
<b>Необхідне обладнання</b>	Мультимедійне обладнання (ноутбук та проектор), комп'ютерне забезпечення з виходом у мережу Інтернет.
<b>Мова викладання</b>	Українська
<b>Контроль</b>	Поточний та підсумковий контроль Поточний: опитування на практичних заняттях; участь в дискусіях, веб-квестах, обговоренні доповідей, рефератів; підготовка рефератів та доповідей, тестування, виконання самостійних робіт, захист лабораторних робіт. Критерії оцінки поточного контролю викладач повідомляє на першому занятті та перед кожними оцінюванням. Підсумковий контроль: залік.
<b>Інтегральна компетентність, загальні компетентності, спеціальні (фахові) компетентності</b>	Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки КЗ.4 Здатність оцінювати та забезпечувати якість виконуваних робіт КФ.2 Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки КФ.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.
<b>ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ТЕМАМИ</b>	
<b>ТЕМА № 1. Нормативно-методична база побудови комплексної системи захисту інформації та системи управління інформаційною безпекою.</b>	
Нормативно-правова база кібербезпеки. Нормативно-правова база інформаційної безпеки. Нормативно-методичне забезпечення побудови	

комплексної системи захисту інформації. Система управління інформаційною безпекою.

## **ТЕМА № 2. Особливості побудови системи управління інформаційною безпекою.**

Терміни та методологічна база забезпечення системи управління безпекою інформації. Політика безпеки. Організація забезпечення безпеки інформації. Безпека людських ресурсів. Управління ресурсами системи управління інформаційною безпекою. Контроль доступу. Криптографія. Фізична безпека та безпека інфраструктури. Безпека експлуатації. Безпека комунікацій. Придбання, розроблення та підтримка інформаційних систем. Взаємовідносини з постачальниками. Управління інцидентами інформаційної безпеки.

### **Програмні результати навчання (ПРН)**

ПРН.2 Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах

ПРН.4 Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки

ПРН.6 Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення

ПРН.7 Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки

ПРН.8 Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури

ПРН.9 Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки

ПРН.10 Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки

	<p>організації</p> <p>РН.11 Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації</p> <p>РН.12 Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому</p> <p>РН.13 Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури</p> <p>РН.14 Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому</p> <p>РН.15 Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб</p> <p>РН.16 Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень</p> <p>РН.18 Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки</p> <p>РН.19 Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту,</p>
--	--

	<p>розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності</p> <p>РН.20 Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик</p> <p>РН.21 Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки</p> <p>РН.22 Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки</p> <p>РН.23 Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації</p>
<p><b>Критерії оцінювання результатів навчання</b></p>	<p>Оцінювання навчальної дисципліни проводиться за результатами поточного та підсумкового контролю:</p> <ul style="list-style-type: none"> <li>- поточний контроль - 50 балів;</li> <li>- підсумковий контроль - 50 балів.</li> </ul> <p>Оцінка за поточний контроль складається з оцінювання аудиторної та самостійної роботи здобувача вищої освіти. Оцінка за аудиторну роботу визначається як середнє арифметичне балів, які ним отримані на семінарських заняттях (здобувач має отримати не менш 5 позитивних оцінок) з коефіцієнтом 5. Оцінка за самостійну роботу визначається як середнє арифметичне балів, які отримані здобувачем за: реферати, програми (здобувач має підготувати не менш 2 проектів) з коефіцієнтом 5.</p> <p>Підсумкові бали з навчальної дисципліни</p>

		визначаються як сума балів, які отримані здобувачем протягом семестру, та балів, які набрані на підсумковому контролі (екзамені).	
ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS			
Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
97-100	Відмінно ("зараховано")	A	„Відмінно” – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом сформовані, всі навчальні завдання, які передбачені програмою навчання виконані в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
94-96			
90-93			
85-89	Добре ("зараховано")	B	„Дуже добре” – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання більшості з них оцінено числом балів, близьким до максимального, робота з двома – трьома незначними помилками.
80-84			
75-79	Задовільно ("зараховано")	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			
65-69	Задовільно ("зараховано")	D	„Задовільно” – теоретичний зміст курсу освоєний не повністю, але прогалини не мають 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.

60-64		Е	„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
<p><b>Перелік питань, що виносяться на підсумковий контроль</b></p> <ol style="list-style-type: none"><li>1. Співвідношення понять «інформаційна безпека» та «кібербезпека».</li><li>2. Головні загрози кібербезпеці згідно з українським законодавством.</li><li>3. Об’єкти кібербезпеки.</li><li>4. Потенціал та стратегічні цілі кібербезпеки.</li><li>5. Основні пріоритети державної політики в інформаційній сфері щодо забезпечення інформаційної безпеки.</li><li>6. Основні процедурні моменти створення побудови комплексної системи захисту інформації.</li><li>7. Послідовність дій власника (розпорядника) інформаційно-телекомунікаційних систем із організації розробки комплексної системи захисту інформації.</li><li>8. Порядок організації і проведення державної експертизи комплексної системи захисту інформації.</li><li>9. Контроль за функціонуванням комплексної системи захисту інформації.</li><li>10. Система управління інформаційною безпекою як альтернатива комплексній системі захисту інформації.</li><li>11.Поняття загрози безпеки інформації та їх види.</li></ol>			



12. Вразливості та їх види.
13. Послідовність вивчення ризиків.
14. Залишкові ризики.
15. Аудит системи безпеки.
16. Події та інциденти безпеки інформації.
17. Моніторинг інформаційних систем та процесів.
18. Система стандартів щодо побудови системи безпеки інформації.
19. Класифікація стандартів ISO/IEC 27-ї серії.
20. Зміст окремих стандартів щодо побудови системи безпеки інформації.
21. Поняття політики безпеки.
22. Методична основа для створення та розробки політики безпеки.
23. Форма представлення політики безпеки.
24. Види політик безпеки.
25. Формалізація суб'єктно-об'єктної моделі системи.
26. Типові помилки під час розробки політики безпеки.
27. Напрями, за якими можуть бути виписані правила для політики безпеки.
28. Змістовне наповнення політики безпеки згідно зі стандартом ДСТУ ISO/IEC 27002:2015.
29. Структурні елементи політики безпеки.
30. Перегляд політики безпеки.
31. Повноваження працівників у сфері забезпечення безпеки інформації.
32. Розподіл відповідальності окремих працівників за убезпечення інформаційних ресурсів.
33. Розмежування доступу до ресурсів інформаційних систем.
34. Делегування повноважень працівників.
35. Вимоги до осіб, відповідальних за впровадження заходів безпеки.
36. Система допуск-доступ до конкретних видів інформаційних ресурсів.
37. Суб'єкти зовнішньої взаємодії у секторі безпеки.
38. Безпека інформації в управлінні проектами.
39. Політика роботи з мобільним обладнанням.
40. Регламентація віддаленої роботи в організації.
41. Повноваження працівників у сфері забезпечення безпеки інформації.
42. Розподіл відповідальності окремих працівників за убезпечення інформаційних ресурсів.
43. Розмежування доступу до ресурсів інформаційних систем.
44. Делегування повноважень працівників.
45. Вимоги до осіб, відповідальних за впровадження заходів безпеки.
46. Система допуск-доступ до конкретних видів інформаційних ресурсів.
47. Суб'єкти зовнішньої взаємодії у секторі безпеки.
48. Безпека інформації в управлінні проектами.
49. Політика роботи з мобільним обладнанням.
50. Регламентація віддаленої роботи в організації.
51. Зміст політики використання криптографічних засобів.
52. Цілі впровадження криптографічних засобів.
53. Стани життєвого циклу криптографічного ключа.

54.Державні стандарти України з криптографічних алгоритмів і механізмів.

55.Зміст політики використання криптографічних ключів.

56.Державні стандарти України з управління ключами.

57.Яким чином має регламентуватися діяльність щодо засобів оброблення інформації, управління якими здійснюється безпосередньо організація/установа?

58.Як слід кваліфікувати події, які впливають на цілісність, доступність та функціонування журналів аудиту подій (логів)?

59.Правила та порядок виконання робіт на території організації/установи, які застосовуються до найманого персоналу та третіх осіб.

60.Вимоги до фізичного розташування обладнання та ліній комунікації.

61.Питання передачі обладнання.

62.Три правила, які описують принцип «чистого столу» та «чистого екрану».

63.Об'єкти захисту комунікацій організації.

64.Заходи управління безпекою мережі.

65.Державні стандарти України з убезпечення комп'ютерної мережі.

66.Послуги комп'ютерної мережі.

67.Безпека послуг комп'ютерної мережі.

68.Якою має бути, в контексті безпеки, взаємодія з постачальником послуг мережі?

69.Характеристики безпеки послуг комп'ютерної мережі.

70.Об'єкти сегментації в комп'ютерній мережі.

71.За якими ознаками може бути визначено логічні мережні домени?

72.За допомогою яких рішень здійснюється сегментація та контроль доступу між доменами?

73.Що визначає вимоги безпеки домену комп'ютерної мережі?

74.Політики, процедури та заходи безпеки обміну інформацією.

75.Зміст угод щодо безпечного обміну діловою інформацією.

76.Заходи захисту електронного обміну повідомленнями.

77.Зміст угод щодо конфіденційності або нерозголошення для зовнішніх сторін або працівників організації.

78.Цілі управління інцидентами інформаційної безпеки.

79.Взаємозв'язок понять при виникненні інцидентів інформаційної безпеки.

80.Загальний перелік заходів управління інцидентами інформаційної безпеки та вдосконалення СУІБ.

81.Які процедури мають бути розроблені та поширені всередині організації для управління інцидентами інформаційної безпеки?

82.Що забезпечують процедури реагування на інциденти інформаційної безпеки?

83.Що мають включати процедури звітування в управлінні інцидентами інформаційної безпеки?

84.Які події інформаційної безпеки потребують звітування?

<p>85.Віднесення подій до інцидентів інформаційної безпеки.</p> <p>86.Реагування на інциденти інформаційної безпеки.</p> <p>87.Аналіз і зіставлення інцидентів інформаційної безпеки.</p> <p>88.Питання процедур ідентифікації, збирання, отримання і зберігання цифрових доказів щодо інцидентів інформаційної безпеки.</p> <p>89.Представлення Державних стандартів України через фази процесу розслідування інцидентів інформаційної безпеки.</p>	
Рекомендована література	<p><b>Нормативно-правові акти:</b></p> <p>1. Про інформацію. Закон України від 02.10.1992, № 2657-XII. URL: <a href="https://zakon.rada.gov.ua/laws/show/2657-12#Text">https://zakon.rada.gov.ua/laws/show/2657-12#Text</a>.</p> <p>2. Про Державну службу спеціального зв'язку та захисту інформації України. Закон України: від 23.02.2006, № 3475-IV. URL: <a href="https://zakon.rada.gov.ua/laws/show/3475-15#Text">https://zakon.rada.gov.ua/laws/show/3475-15#Text</a>.</p> <p>3. Про захист інформації в інформаційно-комунікаційних системах. Закон України: від 05.07.1994, № 1170-VII. URL: <a href="https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text">https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text</a>.</p> <p>4. Про електронні комунікації: Закон України від 16.12.2020 : [із змінами і доповненнями]. <i>Офіційний вісник України</i>. 2021. № 6 (21.01.2021). Ст. 306.</p> <p>5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: <a href="https://zakon.rada.gov.ua/laws/show/2163-19#Text">https://zakon.rada.gov.ua/laws/show/2163-19#Text</a>.</p> <p>6. Про захист персональних даних. Закон України від 01.06.2010 р. № 2297-VI. URL: <a href="https://zakon.rada.gov.ua/laws/show/2297-17#Text">https://zakon.rada.gov.ua/laws/show/2297-17#Text</a>.</p> <p>7. Про критичну інфраструктуру: Закон України від 16.11.2021 р. № 1882-IX. URL: <a href="https://zakon.rada.gov.ua/laws/show/1882-20#Text">https://zakon.rada.gov.ua/laws/show/1882-20#Text</a>.</p> <p>8. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: <a href="https://zakon.rada.gov.ua/laws/show/447/2021#Text">https://zakon.rada.gov.ua/laws/show/447/2021#Text</a> (дата звернення: 10.05.2023).</p> <p>9. Стратегія інформаційної безпеки України, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: <a href="https://zakon.rada.gov.ua/laws/show/685/2021#Text">https://zakon.rada.gov.ua/laws/show/685/2021#Text</a> (дата звернення: 10.05.2023).</p> <p>10. Про створення Центру протидії</p>
Основна	

	<p>дезінформації: Рішення Ради національної безпеки і оборони України від 11 березня 2021 року, введено в дію Указом Президента України від 19 березня 2021 року № 106/2021. URL: <a href="https://zakon.rada.gov.ua/laws/show/106/2021#Text">https://zakon.rada.gov.ua/laws/show/106/2021#Text</a>.</p> <p><b>Основна література:</b></p> <p>11. Манжай О.В., Мелешко Д.Г., Носов В.В., Самойлов С.В. Розробка та впровадження системи управління безпекою інформації. Київ: ВАІТЕ, 2021. 138 с.</p> <p>12. Манжай О. В., Манжай І. А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків : Промарт, 2020. 162 с. з іл.</p> <p>13. Науково-практичний коментар Закону України «Про основні засади забезпечення кібербезпеки України». Станом на 1 січня 2019 року / М.В. Гуцалюк та ін.; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.</p>
<b>Інформаційні ресурси в Інтернеті</b>	<p>1. Каталог національних стандартів та кодексів усталеної практики. URL: <a href="https://katalog.uas.org.ua">https://katalog.uas.org.ua</a>.</p>