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

_____

ПРАВОВІ ЗАСАДИ КІБЕРБЕЗПЕКИ (ВКВС.12)

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кафедра	Кібербезпеки та DATA-технологій (http://univd.edu.ua/uk/dir/2826/kafedra-kiberbezpeky-ta-data-tekhnologiy)
Контактний телефон	+38 057 7398085 (роб.)
E-mail	kaf-itk@univd.edu.ua
ЛЕКТОР (ЛЕКТОРИ)	
	**Манжай Олександр Володимирович,** доцент кібербезпеки та DATA-технологій факультету №6, к.ю.н., професор moj@univd.edu.ua **Лекційний потік:** факультет № 6, шифр навчальних груп Ф6-КБдср-20-1, Ф6-КБзср-20-1
Назва освітньо-професійної програми	Кібербезпека та захист інформації (безпека інформаційних та комунікаційних систем) Cybersecurity and information protection (security of information and communication systems)
Рівень вищої освіти	Перший (бакалаврський) (НРК України – 6 рівень

	та перший цикл вищої освіти Рамки кваліфікацій Європейського простору вищої освіти)
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Статус дисципліни	Вибіркова компонента освітньо-наукової програми, вивчається в 7 семестрі IV курсу навчання
Мета вивчення дисципліни	Навчити здобувачів вищої освіти теоретичним основам, принципам, та конкретним нормативно-правовим актам у сфері захисту інформації з метою їх застосування в службовій діяльності. Виробити вміння: систематизувати законодавчу базу відповідно до напрямів захисту; визначати вид інформації і відповідні методи її захисту, спираючись на чинну нормативно-правову базу; складати юридичні документи, щодо стосуються захисту різних видів інформації; оцінювати внутрішні документи в сфері захисту інформації на відповідність діючому законодавству; визначати гриф обмеження доступу для носіїв інформації з обмеженим доступом. Сформувати у здобувачів вищої освіти знання, уміння і навички щодо протидії поширеним методам порушення існуючого законодавства, щодо захисту інформації.
Завдання вивчення дисципліни	Знати основні положення та терміни що закріплені у нормативно-правових актах та стосуються захисту інформації; основну нормативно-правову базу захисту інформації. Розуміти законодавчо закріплені види інформації, та правові засади її захисту; особливості правового захисту інформації в системі Національної поліції Україн. Упевнено застосувати понятійно-категоріальний апарат, юридичну практику для правозастосовної діяльності, в т.ч. правові позиції Європейського суду з прав людини, Верховного Суду України. Готувати необхідні процесуальні документи.
Обсяг дисципліни в кредитах ECTS/годинах	4 кредити ECTS (загальний обсяг - 120 год.)
	аудиторна робота: 60 год., з них:

	лекції: 30 год. для денної форми навчання, 8 год. – для заочної
	семінарські заняття: 30 год. для денної форми навчання, 12 год. – для заочної
	самостійна робота: 60 год. для денної форми навчання, 100 год. – для заочної
Форми та види проведення навчальних занять	Форма навчання – денна, заочна. Види навчальних занять: лекції, семінарські, самостійна робота.
Самостійна робота	Опрацювання рекомендованої літератури, підготовка тез доповідей до конференцій
Необхідне обладнання	Мультимедійне обладнання (ноутбук та проектор), комп'ютерне забезпечення з виходом у мережу Інтернет.
Індивідуальні завдання	Наукові доповіді, реферати
Мова викладання	Українська
Контроль	Поточний та підсумковий контроль Поточний: опитування на практичних заняттях; участь в дискусіях, веб-квестах, обговоренні доповідей, рефератів; підготовка рефератів та доповідей, тестування, виконання самостійних робіт, захист лабораторних робіт. Критерії оцінки поточного контролю викладач повідомляє на першому занятті та перед кожними оцінюванням. Підсумковий контроль: залік.
Інтегральна компетентність, загальні компетентності, спеціальні (фахові) компетентності	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов ЗК.1 Здатність застосовувати знання у практичних ситуаціях ЗК.2 Знання та розуміння предметної області та ґрозуміння професії ЗК.4 Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням ФК.1 Здатність застосовувати нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки ФК.8 Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку

ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ТЕМАМИ	
ТЕМА № 1 Інформація як об'єкт правового захисту Поняття інформації. Класифікація інформації. Право на інформацію.	
ТЕМА № 2 Структура та засади правового забезпечення інформаційної безпеки та кібербезпеки України Поняття інформаційної безпеки. Інформаційна війна. Захист України від негативного інформаційного впливу. Кібергігієна.	
ТЕМА 3 Правові засади захисту інтелектуальної власності Об'єкти інтелектуальної власності. Характеристика окремих об'єктів промислової власності. Авторське та суміжне право.	
ТЕМА № 4 Захист відкритої інформації в Україні Концептуальні питання захисту відкритої інформації. Публічна інформація. Порядок створення комплексної системи захисту відкритої інформації.	
ТЕМА № 5 Правові засади захисту інформації з обмеженим доступом, що не належить до державної таємниці Захист конфіденційної та службової інформації. Захист інформації про особу.	
ТЕМА № 6 Особливості правового регулювання захисту державної таємниці в Україні та за її межами Захист державної таємниці в Україні. Зарубіжний досвід захисту державної таємниці та службової інформації.	
ТЕМА № 7 Захист електронного документообігу в Україні Правове регулювання електронного документообігу в Україні. Організаційна структура забезпечення використання електронного підпису. Загальний порядок накладання та перевірки електронного підпису.	
Програмні результати навчання (ПРН)	ПРН 3 використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел щодо ефективного розв'язання спеціалізованих задач професійної діяльності ПРН 4 аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення ПРН 7 діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки ПРН 8 готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки

	ПРН 9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки ПРН 43 застосовувати національні та міжнародні регулюючі акти у сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів ПРН 44 вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами ПРН 54 усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні ПРН 55 здійснювати поліцейську діяльність із забезпечення охорони прав і свобод людини, підтримання публічної безпеки і порядку
Критерії оцінювання результатів навчання	Оцінювання навчальної дисципліни проводиться за результатами поточного та підсумкового контролю: - поточний контроль - 50 балів; - підсумковий контроль - 50 балів. Оцінка за поточний контроль складається з оцінювання аудиторної та самостійної роботи здобувача вищої освіти. Оцінка за аудиторну роботу визначається як середнє арифметичне балів, які ним отримані на 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. Підсумкові бали з навчальної дисципліни визначаються як сума балів, які отримані здобувачем протягом семестру, та балів,

			які набрані на підсумковому контролі (екзамені).
ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS			
Оцінка в балах	**Оцінка за національною шкалою**	**Оцінка за шкалою ECTS**	
		Оцінка	**Пояснення**
97-100	Відмінно (“зараховано”)	A	**„Відмінно”** – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом сформовані, всі навчальні завдання, які передбачені програмою навчання виконані в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
94-96			
90-93			
85-89	Добре (“зараховано”)	B	**„Дуже добре”** – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання більшості з них оцінено числом балів, близьким до максимального, робота з двома – трьома незначними помилками.
80-84			
75-79		C	**„Добре”** – теоретичний зміст курсу освоєний цілком, практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання жодного з них не оцінено мінімальним числом балів, деякі види завдань виконані з помилками, робота з декількома незначними помилками, або з однією – двома значними помилками.
70-74	Задовільно (“зараховано”)	D	**„Задовільно”** – теоретичний зміст курсу освоєний не повністю, але прогалинине носять істотного характеру, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, більшість передбачених програмою навчання навчальних завдань виконано, деякі з виконаних завдань, містять помилки, робота з трьома значними помилками.
65-69			

60-64		E	**„Достатньо”** – теоретичний зміст курсу освоєний частково, деякі практичні навички роботи не сформовані, частина передбачених програмою навчання навчальних завдань не виконані, або якість виконання деяких з них оцінено числом балів, близьким до мінімального,робота, що задовольняє мінімуму критеріїв оцінки.
40-59	Незадовільно („не зараховано”)	FX	**„Умовно незадовільно”** – теоретичний зміст курсу освоєний частково, необхідні практичні навички роботи не сформовані, більшість передбачених програм навчання, навчальних завдань не виконано, або якість їхнього виконання оцінено числом балів, близьким до мінімального; при додатковій самостійній роботі над матеріалом курсу можливе підвищення якості виконання навчальних завдань (з можливістю повторного складання), робота, що потребує доробки
21-40			
1-20		F	**„Безумовно незадовільно”** – теоретичний зміст курсу не освоєно, необхідні практичні навички роботи не сформовані, всі виконані навчальні завдання містять грубі помилки, додаткова самостійна робота над матеріалом курсу не приведе до значимого підвищення якості виконання навчальних завдань, робота, що потребує повної переробки

Перелік питань, що виносяться на підсумковий контроль

1. Універсальне поняття інформації, інформація як об’єкт правовідносин, інформаційні ресурси та процеси.
2. Юридично значущі ознаки інформації. Поняття «документ».
3. Класифікація носіїв інформації.
4. Нормативно-правова база захисту інформації.
5. Розгорнута класифікація інформації за порядком доступу.
6. Загальні питання права на інформацію.
7. Доступ до правової інформації.
8. Історія становлення системи національної безпеки України.
9. Складові частини національної безпеки України.
10. Дайте визначення поняття «інформаційна безпека».
11. Основні елементи організаційної основи системи забезпечення інформаційної безпеки України.
12. Основні пріоритети державної політики в інформаційній сфері щодо забезпечення інформаційної безпеки.
13. Поняття інформаційної війни.
14. Форми та мета ведення інформаційної війни.

15. Відмінні риси інформаційної війни.
16. Інформаційна безпека індивідуальної, групової і суспільної свідомості в сфері комерційної реклами.
17. Інформаційна безпека індивідуальної, групової і суспільної свідомості від впливу відео-, аудіо- і друкованих творів, комп'ютерних програм та ігор тощо.
18. Інформаційна безпека громадян як суб'єктів політичного процесу.
19. Об'єкти права інтелектуальної власності, визначені міжнародними конвенціями.
20. Об'єкти права інтелектуальної власності, визначені законодавством України.
21. Винахід та корисна модель.
22. Знаки для товарів і послуг, промисловий зразок.
23. Структура особистих немайнових прав автора.
24. Класифікація майнових прав автора.
25. Випадки вільного використання творів.
26. Окремі випадки вільного відтворення твору. Авторські договори.
27. Нормативно-правова база захисту відкритої інформації.
28. Комплексна система захисту відкритої інформації.
29. Види робіт, які здійснюються в межах технічного захисту інформації.
30. Захисту відкритої інформації**,** важливої для особи та суспільства.
31. Послідовність дій власника (розпорядника) інформаційно-телекомунікаційної системи із організації розробки комплексної системи захисту інформації.
32. Обсяг послуг виконавця із розробки комплексної системи захисту інформації.
33. Підтвердження якості створеної комплексної системи захисту інформації.
34. Контроль за функціонуванням комплексної системи захисту інформації.
35. Нормативно-правова база захисту державної таємниці.
36. Компетенція органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці.
37. Спеціальний суб'єкт, який здійснює віднесення інформації до державної таємниці.
38. Звід відомостей, що становлять державну таємницю, та документи, які складаються на його основі.
39. Реквізити матеріальних носіїв інформації, що містять державну таємницю та ступені секретності.
40. Завдання РСО.
41. Допуск до державної таємниці.
42. Доступ до державної таємниці.
43. Обов'язки громадянина, якому надано допуск до державної таємниці.
44. Компенсація за роботу в умовах режимних обмежень.
45. Відповідальність за порушення законодавства про державну таємницю.
46. Досвід США щодо правого регулювання захисту державної таємниці.
47. Досвід Великої Британії та ФРН щодо правого регулювання захисту державної таємниці.

48. Досвід КНР щодо правого регулювання захисту державної таємниці.
49. Електронний документ та електронний документообіг.
50. Цілі державного регулювання у сфері електронного документообігу.
51. Електронний підпис.
52. Види та визначення ключів в сфері застосування електронних підписів.
53. Організаційна структура накладання та перевірки електронного підпису.
54. Взаємодія суб'єктів правових відносин у сфері електронних довірчих послуг.
55. Особливості електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності.
56. Приблизна модель накладання електронного підпису.
57. Приблизна модель перевірки електронного підпису.

ОСНОВНА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Нормативно-правові акти:

1. Про державну таємницю: закон України від 21.01.1994 ; [із змінами і доповненнями]. *Відомості Верховної Ради України*. 1994. № 16 (19.04.1994). стор. 422. ст. 93.
2. Про доступ до публічної інформації: закон України від 13.01.2011; [із змінами і доповненнями]. *Офіційний вісник України*. 2011. № 10 (18.02.2011), стор. 29, стаття 446.
3. Про електронні довірчі послуги: закон України від 05.10.2017. *Офіційний вісник України*. 2017. № 91 (21.11.2017). ст. 2764.
4. Про електронні документи та електронний документообіг: закон України від 22.05.2003 ; [із змінами і доповненнями]. *Офіційний вісник України*. 2003. № 25 (04.07.2003). ст. 1174.
5. Про захист персональних даних: закон України від 01.06.2010; [із змінами і доповненнями]. *Офіційний вісник України*. 2010. № 49 (09.07.2010), стор. 199, стаття 1604.
6. Про інформацію: закон України від 02.10.1992 р.; [із змінами і доповненнями]. *Відомості Верховної Ради України*. 1992. № 48 (01.12.1992). ст. 650.

Основна література:

7. Манжай О. В., Манжай І. А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків : Промарт, 2020. 162 с. з іл. URL: https://univd.edu.ua/science-issue/issue/4315.

Додаткова література:

8. Етапи побудови КСЗІ. URL: http://altersign.com.ua/korysna-informacija/pobudova-kszi/etapy-pobudovy-kszi (дата звернення: 17.03.2023).
9. Носов В .В., Манжай О. В. Окремі аспекти протидії інформаційній війні в Україні. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2015. № 1(29). С. 26-29.
10. Носов В. В., Манжай І. А. Організаційно-практичні аспекти побудови комплексної системи захисту інформації для системи з інформацією, що публікується в глобальній мережі. *Правове, нормативне та метрологічне*

забезпечення системи захисту інформації в Україні. 2017. № 2(34). С. 56-68.

Інформаційні ресурси в Інтернеті

11.rada.gov.ua