ЗАТВЕРДЖЕНО
Вченою радою факультету
національної безпеки, права та
міжнародних відносин
22 грудня 2023 р., протокол № 11
Голова Вченої ради

_____ СЕРГІЄНКО Лариса

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ЦИФРОВІ ТЕХНОЛОГІЇ, ТРАНСФЕРТ ТЕХНОЛОГІЙ ТА ОСОБИСТА ІНФОРМАЦІЙНА БЕЗПЕКА ДОСЛІДНИКА»

для здобувачів вищої освіти освітньо-наукового ступеня «доктор філософії»
спеціальності 081 «Право»
освітньо-наукова програма «Право»
факультет національної безпеки, права та міжнародних відносин
кафедра права та правоохоронної діяльності

Схвалено на засіданні кафедри
теорії та історії держави і права
21 грудня 2023 р., протокол № 12

Завідувач кафедри

_____ Валерій НОНІК

Гарант освітньо-наукової програми

_____ Віталій ЦИМБАЛЮК

Розробник: д.е.н., д.н.держ.упр., проф., професор кафедри права та правоохоронної діяльності
Димитрій ГРИЦИШЕН
д.е.н., доц., доцент кафедри теорії та історії держави і права
Анатолій ДИКИЙ

Житомир
2023 – 2024 н.р.

Робоча програма навчальної дисципліни «Цифрові технології, трансферт технологій та особиста інформаційна безпека дослідника» для здобувачів вищої освіти освітньо-наукового ступеня «доктор філософії» спеціальності 081 «Право розроблена відповідно до освітньо-наукової програми «Право» від 11 серпня 2023 р. (наказ № 399/од) та затверджена Вченою радою факультету національної безпеки, права та міжнародних відносин від 22 грудня 2023 р., протокол № 11.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітньо-науковий ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td rowspan="2">Кількість кредитів – 4</td><td rowspan="2">Галузь знань
08 «Право»</td><td colspan="2">Нормативна</td></tr>
<tr><td colspan="2">Рік підготовки:</td></tr>
<tr><td rowspan="3">Змістових модулів – 2</td><td rowspan="4">081 «Право»</td><td colspan="2">1-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td colspan="2" rowspan="2">2-й</td></tr>
<tr><td>Загальна кількість годин – 120</td></tr>
<tr><td rowspan="12">Тижневих годин:
аудиторних – 4
самостійної роботи здобувача – 3,5</td><td rowspan="12">Освітньо-науковий ступінь:
«доктор філософії»</td><td colspan="2">Лекції</td></tr>
<tr><td>32 год.</td><td>10 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>32 год.</td><td>20</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>–</td><td>–</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>56 год.</td><td>90 год.</td></tr>
<tr><td colspan="2">Індивідуальні завдання</td></tr>
<tr><td colspan="2">0 год.</td></tr>
<tr><td colspan="2">Вид контролю: залік</td></tr>
</table>

Частка аудиторних занять і частка самостійної та індивідуальної роботи у загальному обсязі годин з навчальної дисципліни становить:

для денної форми навчання – 53 % аудиторних занять, 47 % самостійної та індивідуальної роботи;

для заочної форми навчання – 25 % аудиторних занять, 75 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою дисципліни є формування у здобувачів вищої освіти системних знань і практичних навичок використання цифрових технологій у науково-дослідній та освітній діяльності, забезпечення інформаційної та кібербезпеки наукових досліджень, дотримання стандартів академічної доброчесності, а також розуміння організаційних і безпекових аспектів трансферту наукоємних технологій, зокрема технологій подвійного призначення.

Завданнями дисципліни є:

–формування розуміння інформаційного та кіберпростору як об’єкта наукового аналізу;

–набуття здатності застосовувати сучасні цифрові інструменти для пошуку, оброблення, аналізу, збереження та візуалізації наукової інформації у науковихдослідженнях;

–опанування методів захисту інформації на програмному та апаратному рівнях у процесі наукової й освітньої діяльності;

–розвиток навичок критичної оцінки достовірності наукових джерел та верифікації інформації в інформаційному просторі;

–формування культури інформаційної гігієни дослідника та запобігання витокам наукових даних;

–забезпечення дотримання вимог академічної доброчесності, права інтелектуальної власності при використанні цифрових технологій та штучного інтелекту;

–набуття знань щодо трансферту наукоємних технологій, зокрема технологій подвійного призначення, та механізмів державного і міжнародного контролю;

–формування здатності моделювати ризики та прогнозувати наслідки передачі технологій у наукових, освітніх і міжнародних проєктах;

–розвиток умінь презентувати результати наукових досліджень із використанням цифрових технологій українською та іноземними мовами.

Предметом вивчення дисципліни є сукупність правових, організаційних, технологічних і безпекових відносин, що виникають у процесі використання цифрових технологій у наукових дослідженнях і освітній діяльності, забезпечення особистої та інституційної інформаційної безпеки дослідника, а також здійснення трансферту наукоємних технологій, у тому числі технологій подвійного призначення, в умовах сучасного інформаційного та кіберпростору.

Результатом вивчення дисципліни є набуття здобувачами загальних та фахових компетентностей, визначених в освітньо-науковій програмі.

Зміст навчальної дисципліни направлений на формування наступних **компетентностей:**

ЗК04. Здатність усно і письмово презентувати результати власного наукового дослідження українською та іноземною мовами, глибоко розуміти іншомовні наукові та професійні тексти за напрямом досліджень

СК02. Здатність застосовувати методи правового і міждисциплінарного дослідження, виявляти їх евристичні можливості та межі, використовувати релевантний дослідницький інструментарій.

СК04. Здатність виявляти, ставити та вирішувати проблеми дослідницького характеру у сфері права та забезпечувати якість виконуваних досліджень; дотримання права інтелектуальної власності та стандартів академічної доброчесності.

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів** навчання:

РН02. Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми права державною та іноземною мовами, оприлюднювати результати досліджень у наукових публікаціях у провідних наукових виданнях.

РН05. Планувати і виконувати теоретичні та прикладні дослідження з права та дотичних міждисциплінарних напрямів з використанням сучасного наукового інструментарію, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу передових концептуальних і методологічних знань щодо досліджуваної проблеми з дотриманням стандартів академічної та професійної етики.

РН07. Застосовувати сучасні інструменти і технології пошуку, оброблення, аналізу й збереження даних та інформації, статистичні методи аналізу даних великого обсягу та складної структури, спеціалізовані програмне забезпечення, бази даних та інформаційні системи у науковій, викладацькій, правотворчій та правозастосовній діяльності.

3. Програма навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1
ІНФОРМАЦІЙНИЙ СИСТЕМИ ТА ІНФОРМАЦІЙНА БЕЗПЕКА

Тема 1. Концептуальні положення інформаційного простору

1. Ідентифікація поняття інформаційного простору.
2. Основні положення інформаційного простору: інформаційні ресурси, засоби інформаційної взаємодії, інформаційна інфраструктура.
3. Кіберпростір та Інтернет як інфраструктурна основа сучасних наукових комунікацій.

Тема 2. Захист інформації на рівні прикладного та системного програмного забезпечення

1. Доступ до інформації та розмежування повноважень користувачів
2. Системи ідентифікації та автентифікації як інструменти забезпечення інформаційної безпеки досліджень
3. Аудит, моніторинг і логування дій користувачів: значення для доказування та відповідальності
4. Антивірусний та програмний захист у контексті забезпечення цілісності наукових даних

Тема 3. Захист інформації на рівні апаратного забезпечення

1. Апаратні засоби контролю доступу та захисту інформації
2. Системи фізичної безпеки та сигналізації як елемент захисту наукової інфраструктури
3. Обмеження та блокування пристроїв та інтерфейсів вводу-виводу інформації

ЗМІСТОВИЙ МОДУЛЬ 2. БЕЗПЕКА НАУКОВИХ ДОСЛІДЖЕНЬ

Тема 4. Інформаційні технології в наукових дослідженнях

1. Види наукової інформації та її обробка.
2. Типи експериментальних даних, підготовка їх до обробки.
3. Цифрові інструменти текстового, табличного, графічного та математичного аналізу в наукових дослідженнях
4. Прикладне програмне забезпечення для візуалізації, аналізу і публікації даних.
5. Спеціалізовані пакети обробки даних в наукових дослідженнях.
6. Використання штучного інтелекту для автоматизації аналізу великих даних

Тема 5. Достовірність джерел наукової інформації в інформаційному просторі як основа забезпечення доброчесності

1. Критерії достовірності та механізми верифікації джерел інформації
2. Методи верифікації та критичної оцінки інформації у цифровому середовищі
3. Використання месенджерів і цифрових платформ для наукової комунікації: ризики та обмеження

Тема 6. Інформаційна гігієна дослідника та захист наукових даних

1. Безпека зберігання та резервування результатів наукових досліджень
2. Захист даних при використанні хмарних сервісів і міжнародних цифрових платформ
3. Безпечне використання спеціалізованого програмного забезпечення та інформаційних систем
4. Обмеження використання інформації з джерел держави-агресора
5. Контроль застосування штучного інтелекту для забезпечення академічної доброчесності

Тема 7. Трансферт наукоємних технологій подвійного призначення

1. Ліцензування та оцінка наукоємних розробок подвійного призначення
2. Форми та моделі трансферту технологій у науковій і освітній діяльності
3. Державний експортний контроль технологій подвійного призначення
4. Міжнародно-правові договори та режими контролю експорту технологій
5. Моніторинг і виявлення порушень у сфері трансферту технологій
6. Цифрові інструменти виявлення нелегального експорту технологій

Тема 8. Політика інформаційної безпеки для установ, що здійснюють наукову діяльність

1. Сфера застосування та структура політики інформаційної безпеки
2. Документальне забезпечення політики інформаційної безпеки.
3. Due Diligence у наукових проєктах і міжнародній співпраці
4. Політика інформаційної безпеки в наукових установах та закладах вищої освіти

4. Структура (тематичний план) навчальної дисципліни

Назви змістових модулів і тем	Кількість годин Денна форма				Кількість годин Заочна форма			
	Усього	Лекція	Практичні	Самостійна робота	Усього	Лекція	Практичні	Самостійна робота
ЗМІСТОВИЙ МОДУЛЬ 1. ІНФОРМАЦІЙНИЙ СИСТЕМИ ТА ІНФОРМАЦІЙНА БЕЗПЕКА								
Тема 1. Концептуальні положення інформаційного простору	16	4	4	8	13	1	2	10
Тема 2. Захист інформації на рівні прикладного та системного програмного забезпечення	16	4	4	8	13	1	2	10
Тема 3. Захист інформації на рівні апаратного забезпечення	16	4	4	8	13	1	2	10
Разом за змістовим модулем 1	48	12	12	24	39	3	6	30
ЗМІСТОВИЙ МОДУЛЬ 2. БЕЗПЕКА НАУКОВИХ ДОСЛІДЖЕНЬ								
Тема 4. Інформаційні технології в наукових дослідженнях	15	4	4	7	17	1	4	12
Тема 5. Достовірність джерел наукової інформації в інформаційному просторі як основа забезпечення доброчесності	15	4	4	7	15	1	2	12
Тема 6. Інформаційна гігієна дослідника та захист наукових даних	14	4	4	6	18	2	4	12
Тема 7. Трансферт наукоємних технологій подвійного призначення	14	4	4	6	15	1	2	12
Тема 8. Політика інформаційної безпеки для установ, що здійснюють наукову діяльність	14	4	4	6	16	2	2	12
Разом за змістовим модулем 2	72	20	20	32	81	7	14	60
РАЗОМ	**120**	**32**	**32**	**56**	**120**	**10**	**20**	**90**

5. Теми практичних занять

№ з/п	Назва теми	К-ть годин	
		Д.ф.	З.ф.
1	Тема 1. Концептуальні положення інформаційного простору	4	2
2	Тема 2. Захист інформації на рівні прикладного та системного програмного забезпечення	4	2
3	Тема 3. Захист інформації на рівні апаратного забезпечення	4	2
4	Тема 4. Інформаційні технології в наукових дослідженнях	4	4
5	Тема 5. Достовірність джерел наукової інформації в інформаційному просторі як основа забезпечення доброчесності	4	2
6	Тема 6. Інформаційна гігієна дослідника та захист наукових даних	4	4
7	Тема 7. Трансферт наукоємних технологій подвійного призначення	4	2
8	Тема 8. Політика інформаційної безпеки для установ, що здійснюють наукову діяльність	4	2
РАЗОМ		**32**	**20**

6. Завдання для самостійної роботи

№ з/п	Назва теми та перелік питань	К-ть годин	
		Д.ф.	З.ф.
1	Тема 1. Концептуальні положення інформаційного простору 3. Кіберпростір та Інтернет як інфраструктурна основа сучасних наукових комунікацій.	8	10
2	Тема 2. Захист інформації на рівні прикладного та системного програмного забезпечення 4. Антивірусний та програмний захист у контексті забезпечення цілісності наукових даних	8	10
3	Тема 3. Захист інформації на рівні апаратного забезпечення 3. Обмеження та блокування пристроїв та інтерфейсів вводу-виводу інформації	8	10
4	Тема 4. Інформаційні технології в наукових дослідженнях 1. Види наукової інформації та її обробка. 2. Типи експериментальних даних, підготовка їх до обробки.	7	12
5	Тема 5. Достовірність джерел наукової інформації в інформаційному просторі як основа забезпечення доброчесності Критерії достовірності та механізми верифікації джерел інформації	7	12
6	Тема 6. Інформаційна гігієна дослідника та захист наукових даних 4. Обмеження використання інформації з джерел держави-агресора	6	12
7	Тема 7. Трансферт наукоємних технологій подвійного призначення 1. Ліцензування та оцінка наукоємних розробок подвійного призначення	6	12
8	Тема 8. Політика інформаційної безпеки для установ, що здійснюють наукову діяльність 1. Сфера застосування та структура політики інформаційної безпеки	6	12
ВСЬОГО		**56**	**90**

7. Індивідуальні завдання

Завдання 1. Провести дослідження та дати аналітичну характеристику найбільшим кібератакам в галузі наукових досліджень в Україні та світі. Перед заповнення таблиць та формуванням висновків вказати інформаційні джерела та їх достовірність та рівень довіри до них.

Обрати по одному кіберінциденту, надати загальну характеристику (заповнити таблицю).

Інцидент	Дата	Характеристика цілі	Мета

Країна	Причини	Суб'єкти	Наслідки

Наслідки		
Інфраструктурні	Соціальні	Фінансові

Зробити короткий висновок

Завдання 2. Надати характеристику змінам, що відбулися в системі інформаційної безпеки держави на основі досвіду подолання інциденту кібертероризму (заповнити таблицю).

Зміни:			
В діяльності суб'єктів протидії	*В національному законодавстві*	*В міжнародному законодавстві*	*В технічному та технологічному забезпеченні*

Пропозиції для України			

Зробити короткий висновок

Завдання 3. Зробіть порівняльний аналіз джерел інформації: друкованих та електронних. Обов'язково зазначте такі їх характеристики як: приклади, переваги та недоліки для застосування в роботі аналітика.

Завдання 4.

Ситуація 1. Витік даних, які стосуються наукових досліджень (характер даних пропонує здобувач вищої освіти)

Шановні члени комітету з безпеки досліджень! Керівником служби інформаційних технологій було наведено докази, які свідчать про те, що наша наукова установа стала жертвою витоку даних наукових досліджень, які є вкрай важливими не лише для нас, а й країни в цілому. Прошу здійснити аналіз ситуації, яка виникла, та надати пропозиції щодо подальших дій.

Ситуація 2. Некоректна робота мережі для внутрішніх користувачів наукової установи

Служба ІТ-підтримки наукової установи регулярно отримує повідомлення від наукових працівників про те, що їх домашня сторінка веб-порталу несподівано зависає, коли вони намагаються ввійти за допомогою свої даних на наукову платформу. Окрім того, є інформація про те, що домашня сторінка порталу відхиляє актуальні дані для входу від наукових працівників. Варто зауважити, наукова установа керує великим сховищем результатів досліджень, які важливі не лише для нас, але і для всієї країни. Необхідно здійснити аналіз ситуації, яка виникла, та розробити пропозиції щодо подальших дій.

Ситуація 3. Робота вірусу

Служба ІТ-підтримки виявила, що кілька тижнів тому невідомі хакери запустили потужний шкідливий код, який може: змінювати вміст веб-сайтів; маніпулювати мережевим трафіком, що доставляється на комп'ютери всередині зараженої мережі; викрадати конфіденційні дані, що передаються між підключеними точками доступу; стежити чи передаються паролі та інші конфіденційні дані до веб-URL з метою їх копіювання та надсилання на сервери, які зловмисники можуть контролювати навіть через тривалий проміжок часу. Необхідно здійснити аналіз ситуації, яка виникла, та розробити пропозиції щодо подальших дій.

Проаналізувати запропоновані ситуації за наступними критеріями:

– можливість продовження наукової діяльності за раніше обраним напрямом;

– характер впливу ситуації, яка склалась, на подальшу діяльність наукової установи;

– характер та розмір шкоди / збитків, яку може спричинити втрата даних наукових досліджень;

– рекомендації менеджменту наукової установи на майбутнє.

Завдання 6. Проаналізувати яким чином політика безпеки та стратегія кібербезпеки наукової установи впливає на:

– вільний на відкритий обмін знаннями;

– наукову комунікацію з аналогічними установами;

– розвиток проектів міжнародної співпраці.

Завдання 7. Охарактеризуйте приклади вітчизняних технологій, розвиток яких має перспективу для експорту і потребує державної підтримки в якості пріоритетних напрямів розвитку науки і техніки в Україні

Завдання 8. Визначте, які форми міжнародного трансферу наукоємних технологій подвійного призначення можуть бути використані в Україні для посилення його впливу на економічне зростання та обороноздатність, а також протидію фінансування тероризму.

8. Методи навчання

Результат навчання	Методи навчання
РН02. Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми права державною та іноземною мовами, оприлюднювати результати досліджень у наукових публікаціях у провідних наукових виданнях	– Вербальні методи (лекція, пояснення); – Практичні методи (виконання практичних завдань); – Ситуаційний метод; Методи самостійної роботи (анотування опрацьованого матеріалу, написання есе, підготовка доповідей, написання наукових статей)
РН05. Планувати і виконувати теоретичні та прикладні дослідження з права та дотичних міждисциплінарних напрямів з використанням сучасного наукового інструментарію, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу передових концептуальних і методологічних знань щодо досліджуваної проблеми з дотриманням стандартів академічної та професійної етики	– Вербальні методи (лекція, пояснення); – Практичні методи (виконання практичних завдань); – Ситуаційний метод; Методи самостійної роботи (анотування опрацьованого матеріалу, написання есе, підготовка доповідей, написання наукових статей)
РН07. Застосовувати сучасні інструменти і технології пошуку, оброблення, аналізу й збереження даних та інформації, статистичні методи аналізу даних великого обсягу та складної структури, спеціалізовані програмне забезпечення, бази даних та інформаційні системи у науковій, викладацькій, правотворчій та правозастосовній діяльності	– Вербальні методи (лекція, пояснення); – Практичні методи (виконання практичних завдань); – Ситуаційний метод; Методи самостійної роботи (анотування опрацьованого матеріалу, написання есе, підготовка доповідей, написання наукових статей)

9. Методи контролю

В основу системи оцінювання навчальної дисципліни покладено поточний та модульний контроль результатів навчання і принцип накопичення зароблених здобувачем вищої освіти балів.

Контроль складається з поточного контролю виконання здобувачами вищої освіти самостійної роботи та роботи на парах та підсумкового (семестрового) контролю.

Поточний контроль – це оцінювання засвоєння здобувачем вищої освіти навчального матеріалу під час проведення аудиторних занять при виконанні індивідуальної і самостійної роботи.

Контроль виконання самостійної роботи здобувачами вищої освіти здійснюється на практичних заняттях дисципліни.

Модульний контроль проводиться у вигляді презентації робіт за модулями.

Підсумковий (семестровий) контроль (залік):

1. Накопичення рейтингових балів в межах дисципліни проводиться в балах, які у підсумку переводяться у національну шкалу та шкалу ЄКТС.

2. Загальна кількість балів на останньому занятті з навчальної дисципліни оприлюднюється здобувачам вищої освіти та виставляється в відомість обліку успішності академічних груп.

3. У випадку погодження здобувача вищої освіти з оцінкою поточної успішності, вона вважається остаточною, враховується як результат семестрового контролю і вноситься у залікову книжку.

4. У разі незгоди здобувача вищої освіти з результатами поточної успішності, оцінка з дисципліни виставляється за результатами дистанційного складання заліку. До тестування допускаються здобувачі, які отримали 50 і більше балів.

5. У разі, якщо здобувач вищої освіти отримав від 0 до 59 балів, то в відомість за національною шкалою виставляється оцінка “незараховано” (“F” та “FX” відповідно до шкали ЄКТС).

Способи перевірки досягнення програмних результатів навчання

В ході вивчення дисципліни досягнення програмних результатів навчання контролюється шляхом застосуванням наступних видів контролю:

Результат навчання	Методи контролю
РН02. Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми права державною та іноземною мовами, оприлюднювати результати досліджень у наукових публікаціях у провідних наукових виданнях	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, залік
РН05. Планувати і виконувати теоретичні та прикладні дослідження з права та дотичних міждисциплінарних напрямів з використанням сучасного наукового інструментарію, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу передових концептуальних і методологічних знань щодо досліджуваної проблеми з дотриманням стандартів академічної та професійної етики	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, залік
РН07. Застосовувати сучасні інструменти і технології пошуку, оброблення, аналізу й збереження даних та інформації, статистичні методи аналізу даних великого обсягу та складної структури, спеціалізовані програмне забезпечення, бази даних та інформаційні системи у науковій, викладацькій, правотворчій та правозастосовній діяльності	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, залік

10. Розподіл балів

Поточне тестування та самостійна робота								ІЗ	Сума
Змістовий модуль 1			Змістовий модуль 2						
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	20	100
10	10	10	10	10	10	10	10		

ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS

За шкалою ЄКТС	За національною шкалою	За 100-бальною шкалою
	Залік	
A	Зараховано	90 – 100
B		82 – 89
C		74 – 81
D		64 – 73
E		60 – 63
FX	Незараховано	35 – 59
F		0 – 34

11. Рекомендована література

Основна література

1. Dykyi A., Dyka O., Naumchuk K. Analysis of current threats to the information security of the state. Socioworld. Social research & behavioral sciences journal. 2021. Vol. 6. Is. 04 (02). PP. 130-138. URL: https://doi.org/ 10.5281/zenodo.5810442.

2. Бурячок В.Л., Киричок Р В., Складанний П.М. Основи інформаційної та кібернетичної безпеки / Навчальний посібник. К., 2018. 320 с.

3. Величко О.М., Гордієнко Т.Б. Інтелектуальні інформаційні системи: структура і застосування: підручник. К.: Олді+, 2022. 728 с.

4. Дикий А.П. Формування інформаційно-комунікаційної системи запобігання та протидії економічній злочинності. Наукові перспективи. 2021. № 11 (17). С. 486-499.

5. Дикий А.П., Наумчук К.М., Тростенюк Т.М. Аналіз сучасних загроз інформаційній безпеці держави. Економічний простір: збірник наукових праць. 2021. №176. С. 155-158.

6. Дикий А.П. Інформаційно-комунікаційне забезпечення функціонування правоохоронної системи. Криза правоохоронної системи України: колективна монографія. Житомир: Бук-друк. 2023. 584 с. С. 496-577.

7. Дикий А.П. Державна політика запобігання та протидії економічній злочинності в системі гарантування економічної безпеки України: монографія. Житомир : Бук-Друк. 2023. 428 с.

8. Дикий А.П., Дика О.С., Наумчук К.М., Тростенюк Т.М. Понятійно-категоріальний апарат інформаційної безпеки України в забезпеченні національної безпеки. Таврійський науковий вісник. Серія: Публічне управління та адміністрування. 2022. Вип. 4. С. 23-31. URL: https://journals.ksauniv.ks.ua/index.php/public/issue/view/17.

9. Дикий А. П., Наумчук К. М., Тростенюк Т. М. Аналіз сучасних загроз інформаційній безпеці держави. Економічний простір. 2021. № 176. С. 155-158. URL: http://www.prostir.pdaba.dp.ua/index.php/journal/article/view/1044.

10. Дикий А. П., Наумчук К. М., Тростенюк Т. М. Особливості державного управління інформаційною безпекою в умовах воєнного стану. Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку: матеріали XXV Міжнародної науково-практичної конференції / за ред. І.В. Жукової, Є.О. Романенка. Рига (Латвія): ВАДНД, 07 жовтня 2022 р. 487 с. С. 41-46. URL: http://perspectives.pp.ua/public/site/conferency/conf-25.pdf.

11. Журавська Н.С. Методологія та організація наукових досліджень з основами інтелектуальної власності: навчально-методичний посібник Ніжин: Видавець ПП Лисенко М.М., 2017. 512 с.

12. Інформаційні технології : навчальний посібник / О.І. Зачек, В.В. Сеник, Т.В. Магеровська та ін.; за ред. О.І. Зачека. Львів : Львівський державний університет внутрішніх справ, 2022. 432 с.

13. Когут М. В. Міжнародний трансфер технологій як чинник економічного зростання. Дисертація на здобуття наукового ступеня кандидата економічних наук. Львівський національний університет імені Івана ранка. Львів. 2017. 193 с. URL: https://lnu.edu.ua/wpcontent/uploads/2017/05/dis_kohut.pdf.

14. Козик В., Мрихіна О., Жураковська М. Центри трансферу технологій. Еволюція моделей, світовий досвід, шляхи розвитку в Україні. Вид-во «Кондор». 2021. 128 с.

15. Палеха Ю. І., Палеха О.Ю., Горбань Ю.І. Інформаційна культура: навч. посібн. / за заг. ред. проф. Палехи Ю.І. К.: Видавництво Ліра-К, 2020. 400 с.

16. Покотилова В.І., Фомішина В.М., Лугінін О.Є. Використання інформаційних технологій в теорії прийняття рішень. Навч. посіб. К.: Гельветика, 2019. 240 с.

17. Сеник В.В. Основи технологій захисту інформації в комп'ютерних системах: навчально-методичний посібник / В.В. Сеник, Т.В. Рудий, С.В. Сеник, Т.В. Магеровська. Львів : ЛьвДУВС. 2019. 192 с.

18. Теоретико-методологічні засади інформатизації освіти та практична реалізація інформаційно-комунікаційних технологій в освітній сфері України : монографія / наук. ред. В.Ю. Биков, С.Г. Литвинова, В.І. Луговий. К.: ЦП Компринт, 2019. 214 с.

Нормативно-правова база

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (із змінами) № 80/94-ВР від 05.07.1994 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text%D0%97%D0%B0%D0%BA%D0%BE%D0%BD%20%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8%20%C2%AB%D0%9F%D1%80%D0%BE%20%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97%20%D0%B2%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE-%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC%D1%83%D0%BD%D1%96%D0%BA%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D1%85%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0%D1%85%C2%BB

2. Закон України «Про інформацію» № 2657-XII від 02.10.1992 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

3. Розпорядження Кабінету Міністрів України Про схвалення Стратегії розвитку сфери інноваційної діяльності на період до 2030 року. № 526-р від 10.07.2019 р. URL: https://zakon.rada.gov.ua/laws/show/526-2019-%D1%80#Text

4. Міністерство економічного розвитку і торгівлі України. URL: http://www.me.gov.ua/?lang=uk-UA.

5. Міністерство цифрової трансформації. URL: https://thedigital.gov.ua.

6. Аналітичні матеріали у сфері трансферу технологій. URL: https://mon.gov.ua/ua/nauka/innovacijna-diyalnist-ta-transfertehnologij/transfertehnologij/analitichni-materiali-u-sferi-transferu-tehnologij.

7. Закон України «Про державне регулювання діяльності у сфері трансферу технологій» № 143-V від 14.09.2006 р. URL: https://zakon.rada.gov.ua/laws/show/143-16#Text.

8. Закон України «Про інноваційну діяльність» № 40-IV від 04.07.2002 р. URL: https://zakon.rada.gov.ua/laws/show/40-15#Text.

9. Наукова та інноваційна діяльність України. Статистичний збірник. 2019. Київ. Державна служба статистики. URL: https://ukrstat.org/uk/druk/publicat/kat_u/2020/zb/09/zb_nauka_2019.pdf.

10. The European Network and Information Security Agency. URL: http://www.enisa.europa.eu/

11. Communication from the Commission on Critical Information Infrastructure Protection: Pro-tecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. COM (2009)149 URL: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

12. Estonian Cyber Security Strategy URL: http://www.mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf

13. Export Administration Regulations. URL: https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear

14. The Commerce Control List. URL: https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl

15. Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast). URL: https://eur-lex.europa.eu/eli/reg/2021/821/oj

16. The Export Control Act 2002. URL: https://www.legislation.gov.uk/ukpga/2002/28/contents

17. The UK Strategic Export Control Lists. URL: https://www.gov.uk/government/publications/uk-strategic-export-control-lists-the-consolidatedlist-of-strategic-military-and-dual-use-items-that-require-export-authorisation

13. Електронні ресурсиhttps://osvita.diia.gov.ua/simulators/personal-cyberhygiene-simulator

1. Національний інститут стратегічних досліджень. URL: http://www.niss.gov.ua/
2. Кіберполіція. Національна поліція України. URL: https://cyberpolice.gov.ua/
3. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov-ua/ua
4. Служба безпеки України. URL: https://ssu.gov.ua/

14. Курси неформальної освіти

1. Prometheus. Безпека в інтернеті під час війни: практичний курс. URL: https://prometheus.org.ua/course/course-v1:MINZMIN+ISWT101+2023_T2
2. Prometheus. Цифрова безпека на персональному рівні. URL: https://prometheus.org.ua/course/course-v1:Prometheus+DSPL101+2023_T1
3. Prometheus. Інформаційна гігієна під час війни. URL: https://prometheus.org.ua/course/course-v1:Prometheus+IHWAR101+2022_T2
4. Дія. Освіта. Дата аналітик. SQL та Power BI. URL: https://osvita.diia.gov.ua/simulators/data-analyst-sql-and-power-bi-simulator