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 освітнього ступеня «доктор філософії»
спеціальності 051 «Економіка»
освітньо-наукова програма «Економіка»
факультет національної безпеки, права та міжнародних відносин
кафедра національної безпеки, публічного управління та адміністрування

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

Завідувач кафедри
_____ Валерій НОНІК

Гарант освітньо-наукової програми
_____ Юлія МОРОЗ

Розробник: д.е.н., доц., доцент кафедри теорії та історії держави і права
ДИКИЙ АНАТОЛІЙ

Житомир
2023 – 2024 н.р.

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, освітньо-науковий ступінь	Характеристика навчальної дисципліни
Кількість кредитів – 3	Галузь знань 05 «Суспільні та поведінкові науки»	Нормативна
Змістових модулів – 2	051 «Економіка»	**Рік підготовки:**
		1-й
Індивідуальне завдання		**Семестр**
		2-й
Загальна кількість годин – 90		
Тижневих годин: аудиторних – 3 самостійної роботи здобувача – 2,6	Освітньо-науковий ступінь: «доктор філософії»	**Лекції**
		16 год.
		Практичні, семінарські
		32 год.
		Лабораторні
		0 год.
		Самостійна робота
		42 год.
		Індивідуальні завдання
		0 год.
		Вид контролю: залік

Частка аудиторних занять і частка самостійної та індивідуальної роботи у загальному обсязі годин з навчальної дисципліни становить – 53 % аудиторних занять, 47 % самостійної та індивідуальної роботи

2. Мета та завдання навчальної дисципліни

Мета дисципліни полягає в отриманні здобувачами теоретичних знань і практичних навичок щодо ефективного використання цифрових технологій, трансферту технологій та забезпечення особистої інформаційної безпеки дослідника при здійсненні наукових досліджень через:

– розкриття основних положень інформаційного простору та рівнів захисту інформації;

– використання інформаційних технологій при здійсненні наукових досліджень на етапах збору, накопичення, обробки та представлення результатів досліджень;

– розуміння технології трансферту наукових розробок;

– обґрунтування актуальності забезпечення інформаційної безпеки наукових установ та дотримання інформаційної гігієни дослідниками.

Завдання дисципліни спрямовані на:

– отримання здобувачами освіти знань та навичок, необхідних для застосування цифрових технологій на етапах передачі та захисту особистої інформації в сучасному інформаційному просторі;

– вивчення сучасних цифрових технологій та їх застосування в економіці;

– аналіз процесу передачі технологій та розуміння того, як результати досліджень можуть бути ефективно реалізовані в економіці;

– вивчення важливості забезпечення безпеки особистої інформації для дослідників, включаючи захист та конфіденційність даних;

– розробку заходів для забезпечення безпеки особистої інформації під час проведення досліджень і співпраці з іншими дослідниками;

– проведення тематичних досліджень, розгляд реальних прикладів та вивчення найкращих практик для розуміння проблем у сфері цифрових технологій, передачі технологій та безпеки особистої інформації.

Результатом вивчення дисципліни є набуття здобувачами загальних та фахових компетентностей, визначених освітньо-науковою програмою «Економіка».

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

ЗК02. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

СК03. Здатність використовувати сучасні методології, методи та інструменти емпіричних і теоретичних досліджень у сфері економіки, методи комп'ютерного моделювання, сучасні цифрові технології, бази даних та інші електронні ресурси, спеціалізоване програмне забезпечення у науковій та науково-педагогічній діяльності.

СК06. Здатність обґрунтовувати та готувати економічні рішення на основі розуміння закономірностей розвитку соціально-економічних систем і процесів із застосуванням математичних методів та моделей

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

РН04. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу великих масивів даних

та/або складної структури, спеціалізоване програмне забезпечення та інформаційні системи.

РН07. Застосовувати інноваційні науково-педагогічні технології, формулювати зміст, цілі навчання, способи їх досягнення, форми контролю, нести відповідальність за ефективність освітнього процесу з дотриманням норм академічної етики та доброчесності.

РН08. Планувати і виконувати емпіричні та/або теоретичні дослідження у сфері економіки та з дотичних міждисциплінарних напрямів, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми

РН09. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, емпіричних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані.

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. Інтернет як основна складова інфраструктури кіберпростору.

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

1. Розмежування доступу до інформації
2. Системи ідентифікації та автентифікації
3. Системи аудиту та моніторингу
4. Системи антивірусного захисту

Тема 3. Захист інформації на рівні апаратного забезпечення

1. Апаратні ключі
2. Системи сигналізації
3. Засоби 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. Комп'ютерні технології у вирішенні задач текстової, графічної, табличної, математичної обробки, накопичення і збереження даних.
4. Прикладне програмне забезпечення для візуалізації, аналізу і публікації даних.
5. Спеціалізовані пакети обробки наукових даних в сфері економіки.

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

1. Критерії достовірності та механізми верифікації джерел інформації
2. Оцінка достовірності інформації в інформаційному просторі
4. Використання месенджерів для передачі інформації про наукові дослідження

Тема 6. Інформаційна гігієна дослідника

1. Безпека збереження даних
2. Безпечне використання інформаційних ресурсів та прикладних програм (спеціалізоване програмне забезпечення та інформаційні системи)
3. Використання інформації з джерел держави-агресора

Тема 7. Трансферт технологій

1. Форми трансферту технологій на комерційній основі
2. Передача технологій: особливості реалізації
3. Експорт наукоємних технологій подвійного призначення

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

1. Сфера застосування політики інформаційної безпеки
2. Документальне забезпечення політики інформаційної безпеки. Політика Due Diligence
3. Ролі та обов'язки політики інформаційної безпеки

4. Структура (тематичний план) навчальної дисципліни

Назви змістових модулів і тем	Кількість годин			
	Усього	Лекція	Практичні	Самостійна робота
ЗМІСТОВИЙ МОДУЛЬ 1. ІНФОРМАЦІЙНИЙ СИСТЕМИ ТА ІНФОРМАЦІЙНА БЕЗПЕКА				
Тема 1. Концептуальні положення інформаційного простору	10	2	4	4
Тема 2. Захист інформації на рівні прикладного та системного програмного забезпечення	10	2	4	4
Тема 3. Захист інформації на рівні апаратного забезпечення	10	2	4	4
Разом за змістовим модулем 1	**30**	**6**	**12**	**12**
ЗМІСТОВИЙ МОДУЛЬ 2. БЕЗПЕКА НАУКОВИХ ДОСЛІДЖЕНЬ				
Тема 4. Інформаційні технології в наукових дослідженнях	12	2	4	6
Тема 5. Достовірність джерел наукової інформації в інформаційному просторі як основа забезпечення доброчесності	12	2	4	6
Тема 6. Інформаційна гігієна дослідника	12	2	4	6
Тема 7. Трансферт технологій	12	2	4	6
Тема 8. Політика інформаційної безпеки для установ, що здійснюють наукову діяльність	12	2	4	6
Разом за змістовим модулем 2	**60**	**10**	**20**	**30**
УСЬОГО	**90**	**16**	**32**	**42**

5. Теми практичних занять

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

6. Завдання для самостійної роботи

№ з/п	Назва теми	К-ть годин
1	Тема 1. Концептуальні положення інформаційного простору 1. Ідентифікація поняття інформаційного простору	4
2	Тема 2. Захист інформації на рівні прикладного та системного програмного забезпечення 4. Системи антивірусного захисту	4
3	Тема 3. Захист інформації на рівні апаратного забезпечення 2. Системи сигналізації	4
4	Тема 4. Інформаційні технології в наукових дослідженнях 1. Види наукової інформації та її обробка	6
5	Тема 5. Достовірність джерел наукової інформації в інформаційному просторі як основа забезпечення доброчесності 4. Використання месенджерів для передачі інформації про наукові дослідження	6
6	Тема 6. Інформаційна гігієна дослідника 2. Безпечне використання інформаційних ресурсів та прикладних програм в он-лайн режимі	6
7	Тема 7. Трансферт технологій 1. Форми трансферту технологій на комерційній основі	6
8	Тема 8. Політика інформаційної безпеки для установ, що здійснюють наукову діяльність 1. Сфера застосування політики інформаційної безпеки	6
ВСЬОГО		42

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.

1. Обрати по одному інциденту кібертероризму, надати загальну характеристику (заповнити таблицю).

Інцидент	**Дата**	**Характеристика цілі**	**Мета**

Країна	**Причини**	**Суб'єкти**

Наслідки		
Інфраструктурні	*Соціальні*	*Фінансові*

Висновок: *зробити короткий висновок*

Завдання 2. Надати характеристику методам протидії інциденту (заповнити таблицю).

Суб'єкти залученні до протидії	
Інструменти протидії	
Притягнення до відповідальності	

Висновок: *зробити короткий висновок про ефективність суб'єктів протидії інциденту кібертероризму*

Завдання 3. 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			

Висновок: *зробити короткий висновок*

Завдання 4. 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 5.

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. Визначне, які форми міжнародного трансферу технологій можуть бути використані в Україні для посилення його впливу на економічне зростання та обороноздатність.

8. Методи навчання

Результат навчання	Методи навчання
1	2
РН04. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу великих масивів даних та/або складної структури, спеціалізоване програмне забезпечення та інформаційні системи	Вербальні (проблемні лекції, лекції-візуалізації, лекції-дискусії, лекції з аналізом конкретних ситуацій), наочні (ілюстрація, демонстрація), практичні (різні види вправ та завдань, тестування), пояснювально-ілюстративний, метод проблемного викладу, дослідницький метод, дискусійний метод

1	2
РН07. Застосовувати інноваційні науково-педагогічні технології, формулювати зміст, цілі навчання, способи їх досягнення, форми контролю, нести відповідальність за ефективність освітнього процесу з дотриманням норм академічної етики та доброчесності	Вербальні (проблемні лекції, лекції-візуалізації, лекції-дискусії, лекції з аналізом конкретних ситуацій), наочні (ілюстрація, демонстрація), практичні (різні види вправ та завдань, тестування), пояснювально-ілюстративний, метод проблемного викладу, дослідницький метод, дискусійний метод
РН08. Планувати і виконувати емпіричні та/або теоретичні дослідження у сфері економіки та з дотичних міждисциплінарних напрямів, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми	Вербальні (проблемні лекції, лекції-візуалізації, лекції-дискусії, лекції з аналізом конкретних ситуацій), наочні (ілюстрація, демонстрація), практичні (різні види вправ та завдань, тестування), пояснювально-ілюстративний, метод проблемного викладу, дослідницький метод, дискусійний метод
РН09. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, емпіричних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані	Вербальні (проблемні лекції, лекції-візуалізації, лекції-дискусії, лекції з аналізом конкретних ситуацій), наочні (ілюстрація, демонстрація), практичні (різні види вправ та завдань, тестування), пояснювально-ілюстративний, метод проблемного викладу, дослідницький метод, дискусійний метод

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
РН04. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу великих масивів даних та/або складної структури, спеціалізоване програмне забезпечення та інформаційні системи	усне опитування, тестові міні-контрольні роботи, модульний контроль, захист індивідуального завдання
РН07. Застосовувати інноваційні науково-педагогічні технології, формулювати зміст, цілі навчання, способи їх досягнення, форми контролю, нести відповідальність за ефективність освітнього процесу з дотриманням норм академічної етики та доброчесності	усне опитування, тестові міні-контрольні роботи, модульний контроль, захист індивідуального завдання
РН08. Планувати і виконувати емпіричні та/або теоретичні дослідження у сфері економіки та з дотичних міждисциплінарних напрямів, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми	усне опитування, тестові міні-контрольні роботи, модульний контроль, захист індивідуального завдання
РН09. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, емпіричних досліджень і математичного та/або комп'ютерного моделювання, наявні літературні дані	усне опитування, тестові міні-контрольні роботи, модульний контроль, захист індивідуального завдання

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.

Нормативна база

1. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР (із змінами).

2. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII.

3. Про схвалення Стратегії розвитку сфери інноваційної діяльності на період до 2030 року. Розпорядження Кабінету Міністрів України; Стратегія від 10.07.2019 № 526-р

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

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

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

7. Закон України «Про державне регулювання діяльності у сфері трансферу технологій». URL: https://zakon.rada.gov.ua/laws/show/143-16#Text.

8. Закон України «Про інноваційну діяльність». 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, se-curity 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-consolidated-list-of-strategic-military-and-dual-use-items-that-require-export-authorisation

12. Інформаційні ресурси

http://www.niss.gov.ua/
https://cyberpolice.gov.ua/
https://cip.gov-ua/ua
https://cert.gov.ua/
https://ssu.gov.ua/

13. Рекомендовані курси

Prometheus. Безпека в інтернеті під час війни: практичний курс. URL: https://prometheus.org.ua/course/course-v1:MINZMIN+ISWT101+2023_T2

Prometheus. Цифрова безпека на персональному рівні. URL: https://prometheus.org.ua/course/course-v1:Prometheus+DSPL101+2023_T1

Prometheus. Інформаційна гігієна під час війни. URL: https://prometheus.org.ua/course/course-v1:Prometheus+IHWAR101+2022_T2

Дія.Освіта. Персональна кібергігієна. URL: https://osvita.diia.gov.ua/simulators/personal-cyberhygiene-simulator

Дія.Освіта. Дата аналітик. SQL та Power BI. URL: https://osvita.diia.gov.ua/simulators/data-analyst-sql-and-power-bi-simulator