ЗАТВЕРДЖЕНО
Вченою радою факультету
національної безпеки, права та
міжнародних відносин
27 серпня 2024 р., протокол № 8
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 256 «Національна безпека
(за окремими сферами забезпечення і видами діяльності)»
освітньо-наукова програма «Національна безпека
(за окремими сферами забезпечення і видами діяльності)»
факультет національної безпеки, права та міжнародних відносин
кафедра національної безпеки, публічного управління та адміністрування

Схвалено на засіданні кафедри
теорії та історії держави і права
26 серпня 2024 р., протокол № 7

Завідувач кафедри
_____ Валерій НОНІК

Гарант освітньо-наукової програми
_____ Димитрій ГРИЦИШЕН

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

Житомир
2024 р.

Робоча програма навчальної дисципліни «Цифрові технології, трансферт технологій та особиста інформаційна безпека дослідника» для здобувачів вищої освіти освітньо-наукового ступеня «доктор філософії» спеціальності 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» освітньо-наукова програма «Національна безпека (за окремими сферами забезпечення і видами діяльності)» затверджена Вченою радою факультету національної безпеки, права та міжнародних відносин від 27 серпня 2024 р., протокол № 8.

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>Кількість кредитів – 3</td><td>Галузь знань
25 «Воєнні науки, національна безпека,
безпека державного кордону»</td><td colspan="2">нормативна</td></tr>
<tr><td>Модулів – 1</td><td rowspan="5">Спеціальність
256 «Національна безпека
(за окремими сферами забезпечення і видами діяльності)»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td rowspan="2">Змістових модулів – 2</td><td>1</td><td>–</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 90</td><td>2</td><td>–</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:
аудиторних – 3</td><td rowspan="10">Освітньо-науковий ступінь
«доктор філософії»</td><td>16 год.</td><td>– год</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>32 год.</td><td>– год</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>0 год.</td><td>– год</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>42 год.</td><td>– 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 – 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 та технологій подвійного призначення, зокрема;

– 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 у безпековій сфері;

– аналіз процесу передачі технологій та розуміння того, як результати досліджень можуть бути ефективно реалізовані у безпековій сфері;

– 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.

Зміст навчальної дисципліни спрямований на формування наступних **компетентностей** за спеціальністю 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)»:

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

СК 04. Здатність використовувати та удосконалювати сучасні методології, методи та інструменти емпіричних і теоретичних досліджень у сфері національної безпеки (за окремими сферами забезпечення та її видами), методи комп’ютерного моделювання, сучасні цифрові технології, бази даних та інші електронні ресурси, спеціалізоване програмне забезпечення у науковій та науково-педагогічній діяльності.

СК 06. Здатність виявляти, поглиблено аналізувати та вирішувати проблеми дослідницького характеру у сфері національної безпеки (за окремими сферами забезпечення та її видами), оцінювати та забезпечувати якість виконуваних досліджень.

СК 08. Здатність ініціювати, розробляти і реалізовувати комплексні наукові проєкти в сфері національної безпеки (за окремими сферами забезпечення та її видами) та дотичних до неї галузях, проявляти лідерство та відповідальність при їх реалізації, комерціалізувати результати наукових досліджень та забезпечувати дотримання прав інтелектуальної власності.

Отримані знання з навчальної дисципліни стануть складовими наступних **результатів навчання** за спеціальністю 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)»:

ПРН 04. Розробляти, удосконалювати та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем національної безпеки (за окремими видами забезпечення та її видами), ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у сфері національної безпеки та дотичних міждисциплінарних напрямах

ПРН 07. Розробляти та реалізовувати наукові та/або інноваційні проекти, які дають можливість переосмислити наявне та створити нове цілісне знання та/або професійну практику і розв'язувати значущі фундаментальні та прикладні проблеми у сфері національної безпеки (за окремими видами забезпечення та її видами) з врахуванням соціальних, економічних, екологічних, правових аспектів та сучасних безпекових викликів та загроз; забезпечувати комерціалізацію результатів наукових досліджень та дотримання прав інтелектуальної власності.

ПРН 08. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичних та емпіричних досліджень національної безпеки, комп'ютерне моделювання, наявні літературні дані.

ПРН 09. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи.

Під час вивчення навчальної дисципліни здобувачі вищої освіти зможуть отримати наступні Soft skills:

– *комунікативні навички*: письмове, вербальне й невербальне спілкування; уміння грамотно спілкуватися по e-mail; вести дискусію і відстоювати свою позицію; навички працювати в команді;

– *уміння виступати привселюдно*: навички, необхідні для виступів на публіці; навички проведення презентації;

– *керування часом:* уміння справлятися із завданнями вчасно;

– *гнучкість і адаптивність:* гнучкість, адаптивність і здатність змінюватися; уміння аналізувати ситуацію, орієнтування на вирішення проблеми;

– *лідерські якості*: уміння спокійно працювати в напруженому середовищі; уміння ухвалювати рішення; уміння ставити мету, планувати діяльність;

– *особисті якості:* креативне й критичне мислення; етичність, чесність, терпіння, повага до оточуючих.

3. Програма навчальної дисципліни

МОДУЛЬ 1

ЗМІСТОВИЙ МОДУЛЬ 1. ІНФОРМАЦІЙНИЙ СИСТЕМИ ТА ІНФОРМАЦІЙНА БЕЗПЕКА

Тема 1. Концептуальні положення інформаційного простору (СК 04, ПРН 04)

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 (СК 04, ПРН 04)

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 (СК 04, ПРН 04)

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 (ЗК 02, СК 04, СК 06, СК 08, ПРН 04, ПРН 07, ПРН 08, ПРН 09)

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 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 (ЗК 02, СК 04, СК 06, ПРН 04, ПРН 07, ПРН 08, ПРН 09)

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 (ЗК 02, СК 04, СК 06, СК 08, ПРН 04, ПРН 07, ПРН 08, ПРН 09)

1. Безпека збереження даних
2. Захист від витоку даних під час використання хмарних платформ
3. Безпечне використання інформаційних ресурсів та прикладних програм (спеціалізоване програмне забезпечення та інформаційні системи)
4. Використання інформації з джерел держави-агресора
5. Контроль за використанням штучного інтелекту для забезпечення академічної доброчесності

Тема 7. Трансферт наукоємних технологій подвійного призначення (ЗК 02, СК 04, СК 06, СК 08, ПРН 04, ПРН 07)

1. Ліцензування та оцінка наукоємних розробок подвійного призначення, форми їх трансферту
2. Особливості передачі технологій подвійного призначення
3. Державний контроль в експорті технологій подвійного призначення
4. Міжнародні договори, що регулюють експорт технологій подвійного призначення
5. Механізми моніторингу передачі технологій подвійного призначення між державами
6. Ризики, які виникають під час передачі технологій для енергетичних програм
7. Використання цифрових технологій для виявлення нелегального експорту товарів і технологій подвійного призначення

Тема 8. Політика інформаційної безпеки для установ, що здійснюють наукову діяльність (СК 04, СК 08, ПРН 04, ПРН 07, ПРН 09)

1. Сфера застосування політики інформаційної безпеки
2. Документальне забезпечення політики інформаційної безпеки.
3. Політика Due Diligence
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				Заочна форма			
	Усього	Лекційні	Практичні	Самостійна робота	Усього	Лекційні	Практичні	Самостійна робота
МОДУЛЬ 1 **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 наукоємних технологій подвійного призначення	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**	–	–	–	–
ВСЬОГО	**90**	**16**	**32**	**42**	–	–	–	–

5. Теми практичних занять

№ з/п	Назва теми	К-ть годин	
		Денна форма	Заочна форма
МОДУЛЬ 1 **ЗМІСТОВИЙ МОДУЛЬ 1. ІНФОРМАЦІЙНИЙ СИСТЕМИ ТА ІНФОРМАЦІЙНА БЕЗПЕКА**			
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	–
Разом за змістовим модулем 1		**12**	
ЗМІСТОВИЙ МОДУЛЬ 2. БЕЗПЕКА НАУКОВИХ ДОСЛІДЖЕНЬ			
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 наукоємних технологій подвійного призначення	4	–
8	**Тема 8.** Політика інформаційної безпеки для установ, що здійснюють наукову діяльність	4	–
Разом за змістовим модулем 2		**20**	
РАЗОМ		**32**	–

6. Завдання для самостійної роботи

№ з/п	Назва теми	К-ть годин	
		Денна форма	Заочна форма
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	–
Разом за змістовим модулем 1		**12**	
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 3. Безпечне використання інформаційних ресурсів та прикладних програм в он-лайн режимі	6	–
7	**Тема 7.** Трансферт наукоємних технологій подвійного призначення 4. Міжнародні договори, що регулюють експорт технологій подвійного призначення	6	–
8	**Тема 8.** Політика інформаційної безпеки для установ, що здійснюють наукову діяльність 1. Сфера застосування політики інформаційної безпеки	6	–
Разом за змістовим модулем 2		**30**	
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. 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

Під час викладання навчальної дисципліни використовуються методи навчання, що сприяють досягненню відповідних програмних результатів.

Результат навчання	Методи навчання
1	2
ПРН 04. Розробляти, удосконалювати та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем національної безпеки (за окремими видами забезпечення та її видами), ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у сфері національної безпеки та дотичних міждисциплінарних напрямах	– Вербальні методи (лекція, пояснення); – Практичні методи (виконання практичних завдань); – Ситуаційний метод; Методи самостійної роботи (анотування опрацьованого матеріалу, написання есе, підготовка доповідей, написання наукових статей)
ПРН 07. Розробляти та реалізовувати наукові та/або інноваційні проекти, які дають можливість переосмислити наявне та створити нове цілісне знання та/або професійну практику і розв'язувати значущі фундаментальні та прикладні проблеми у сфері національної безпеки (за окремими видами забезпечення та її видами) з врахуванням соціальних, економічних, екологічних, правових аспектів та сучасних безпекових викликів та загроз; забезпечувати комерціалізацію результатів наукових досліджень та дотримання прав інтелектуальної власності	– Вербальні методи (лекція, пояснення); – Практичні методи (виконання практичних завдань); – Ситуаційний метод; Методи самостійної роботи (анотування опрацьованого матеріалу, написання есе, підготовка доповідей, написання наукових статей)

1	2
ПРН 08. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичних та емпіричних досліджень національної безпеки, комп'ютерне моделювання, наявні літературні дані	– Вербальні методи (лекція, пояснення); – Практичні методи (виконання практичних завдань); – Ситуаційний метод; Методи самостійної роботи (анотування опрацьованого матеріалу, написання есе, підготовка доповідей, написання наукових статей)
ПРН 09. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи	– 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

Перевірка досягнення програмних результатів навчання здійснюється з використанням наступних методів.

Результат навчання	Методи контролю
ПРН 04. Розробляти, удосконалювати та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем національної безпеки (за окремими видами забезпечення та її видами), ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у сфері національної безпеки та дотичних міждисциплінарних напрямах	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, залік
ПРН 07. Розробляти та реалізовувати наукові та/або інноваційні проекти, які дають можливість переосмислити наявне та створити нове цілісне знання та/або професійну практику і розв'язувати значущі фундаментальні та прикладні проблеми у сфері національної безпеки (за окремими видами забезпечення та її видами) з врахуванням соціальних, економічних, екологічних, правових аспектів та сучасних безпекових викликів та загроз; забезпечувати комерціалізацію результатів наукових досліджень та дотримання прав інтелектуальної власності	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, залік
ПРН 08. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичних та емпіричних досліджень національної безпеки, комп'ютерне моделювання, наявні літературні дані	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, залік
ПРН 09. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, залік

10. Оцінювання результатів навчання здобувачів вищої освіти

Оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни здійснюється відповідно до Положення про оцінювання результатів навчання здобувачів вищої освіти у Державному університеті «Житомирська політехніка» та розподілу балів, що наведений нижче.

Система оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни включає поточний та підсумковий контроль.

Поточний контроль проводиться для оцінювання рівня засвоєння знань, формування умінь і навичок здобувачів вищої освіти впродовж вивчення ними матеріалу модуля (змістових модулів) навчальної дисципліни. Поточний контроль здійснюється під час проведення навчальних занять.

Підсумковий контроль проводиться для підсумкового оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни. Підсумковий контроль здійснюється після завершення вивчення навчальної дисципліни. Підсумковий контроль проводиться у формі заліку. Процедура складання заліку визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Розподіл балів з навчальної дисципліни

Види робіт здобувача вищої освіти	Кількість балів за семестр
	денна форма
Виконання завдань поточного контролю	100
Підсумкова семестрова оцінка	**100**

Розподіл балів за виконання завдань поточного контролю

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання завдань під час навчальних занять	88	–
Виконання та захист індивідуальних самостійних завдань	12	–
Виконання науково-дослідної роботи та інших видів робіт (**додаткові – заохочувальні бали**): 1. Підготовка наукових статей, тез доповідей наукових конференцій	10	–
Разом за виконання завдань поточного контролю	**100**	–

Розподіл балів за виконання завдань під час навчальних занять

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання практичних робіт	76	–
Виконання тестових завдань	12	–
Разом за виконання завдань під час навчальних занять	**88**	–

З метою застосування цілих чисел для оцінювання результатів роботи здобувачів під час навчальних занять може використовуватися 100-бальна шкала оцінювання щодо кожного окремо виду робіт. Розрахунок загальної кількості балів, які здобувач може набрати за результатами роботи під час навчальних занять протягом семестру, проводиться за формулою:

$$Р_{НЗ} = \sum(Р_і \times ВК_і) \times К_{НЗ}, \qquad (1)$$

де $Р_{НЗ}$ – загальна кількість балів, набраних здобувачем за виконання завдань під час навчальних занять за семестр;

$Р_і$ – кількість набраних здобувачем балів за семестр за виконання і-го виду робіт під час навчальних занять (за 100-бальною шкалою);

$ВК_і$ – ваговий коефіцієнт за виконання і-го виду робіт під час навчальних занять. Значення вагових коефіцієнтів розраховуються шляхом ділення кількості балів, яка передбачена за виконання окремого виду робіт під час навчальних занять, на сумарну кількість балів за виконання усіх видів робіт під час навчальних занять за семестр;

$К_{НЗ}$ – коригувальний коефіцієнт, який визначається шляхом ділення кількості балів, що передбачена за виконання завдань під час навчальних занять за семестр, на 100 балів.

Якщо здобувач вищої освіти набрав за поточний контроль 60 балів або більше, він може погодити дану оцінку в електронному кабінеті і вона стане семестровою оцінкою за вивчення навчальної дисципліни.

Якщо здобувач вищої освіти під час вивчення навчальної дисципліни набрав 60 балів або більше і бажає покращити свій результат успішності, він проходить процедуру підсумкового контролю у формі заліку. За складання заліку здобувач вищої освіти може набрати 100 балів. Семестрова оцінка з навчальної дисципліни формується за результатами підсумкового контролю.

Здобувач вищої освіти допускається до процедури підсумкового контролю у формі заліку, якщо за виконання завдань поточного контролю набрав 50 балів або більше.

Якщо здобувач вищої освіти за результатами поточного контролю набрав 35–49 балів, він отримує право за власною заявою опанувати окремі теми (змістові модулі) навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми. Вивчення окремих складових навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми, здійснюється у вільний від занять здобувача вищої освіти час.

Якщо здобувач вищої освіти за результатами поточного контролю набрав від 0 до 34 балів (включно), він вважається таким, що не виконав вимоги робочої програми навчальної дисципліни та має академічну заборгованість. Здобувач вищої освіти отримує право за власною заявою опанувати навчальну дисципліну у наступному семестрі понад обсяги, встановлені навчальним планом освітньої програми.

Процедура надання додаткових освітніх послуг здобувачу вищої освіти з метою вивчення навчального матеріалу дисципліни понад обсяги, встановлені навчальним планом освітньої програми, визначена у Положенні про надання додаткових освітніх послуг здобувачам вищої освіти в Державному університеті «Житомирська політехніка».

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках окремих тем навчальної дисципліни, здійснюється викладачем за зверненням здобувача вищої освіти та представленням документів, які підтверджують результати навчання (сертифікати, свідоцтва, скріншоти тощо). Рішення про визнання

та оцінка за відповідну частину освітнього компонента приймається викладачем за результатами співбесіди зі здобувачем вищої освіти.

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках цілого освітнього компонента, здійснюється за процедурою, яка визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Курси неформальної освіти:

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

ChatGPT для підвищення власної ефективності. URL: https://osvita.diia.gov.ua/courses/chatgpt-for-personal-effectiveness

Шкала оцінювання

Шкала ЄКТС	Національна шкала	100-бальна шкала
A	Зараховано	90-100
B	Зараховано	82-89
C		74-81
D	Зараховано	64-73
E		60-63
FX	Не зараховано	35-59
F		0-34

11. Глосарій

№ з/п	Термін державною мовою	Відповідник англійською мовою
1.	Due Diligence	Due Diligence
2.	Автентифікація	Authentication
3.	Антивірусний захист	Antivirus protection
4.	Апаратні ключі	Hardware keys
5.	Аудит інформаційної безпеки	Information security audit
6.	Безпечне збереження даних	Secure data storage
7.	Верифікація	Verification
8.	Графічна обробка	Graphic processing
9.	Джерела держави-агресора	Sources of the aggressor state
10.	Документальне забезпечення	Documentation
11.	Експериментальні дані	Experimental data
12.	Експортний контроль	Export control
13.	Засоби блокування	Blocking tools
14.	Засоби інформаційної взаємодії	Information interaction tools
15.	Ідентифікація	Identification
16.	Інтернет	Internet
17.	Інформаційна безпека	Information security

№ з/п	Термін державною мовою	Відповідник англійською мовою
18.	Інформаційна гігієна	Information hygiene
19.	Інформаційна інфраструктура	Information infrastructure
20.	Інформаційний простір	Information space
21.	Інформаційний шум	Information noise
22.	Інформаційні ресурси	Information resources
23.	Кіберпростір	Cyberspace
24.	Критерії достовірності	Authentication criteria
25.	Ліцензування	Licensing
26.	Месенджери	Messengers
27.	Міжнародні договори	International treaties
28.	Моніторинг системи	System monitoring
29.	Наукова інформація	Scientific information
30.	Нелегальний експорт	Illegal export
31.	Пакети обробки даних	Data processing packages
32.	Політика безпеки	Security policy
33.	Розмежування доступу	Access delimitation
34.	Ролі та обов’язки	Roles and responsibilities
35.	Системи сигналізації	Alarm systems
36.	Спеціалізоване програмне забезпечення	Specialized software provision
37.	Текстова обробка даних	Word processing
38.	Технології подвійного призначення	Dual-purpose technologies

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/