Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Навчально-науковий інститут
«Каразінський інститут міжнародних відносин та туристичного бізнесу»

Кафедра міжнародних відносин

«ЗАТВЕРДЖУЮ»
Директор ННІ «Каразінський інститут міжнародних відносин та туристичного бізнесу»

_____ Микола ПИСАРЕВСЬКИЙ

«28» серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

СУЧАСНІ ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ В ЗАДАЧАХ ІТ-БЕЗПЕКИ

рівень вищої освіти другий (магістерський)

галузь знань 29 «Міжнародні відносини»

спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»

освітня програма «Міжнародна інформаційна безпека»

вид дисципліни За вибором

навчально-науковий інститут «Каразінський інститут міжнародних відносин та туристичного бізнесу»

2025 / 2026 навчальний рік

Програму рекомендовано до затвердження Вченою радою ННІ «Каразінський інститут міжнародних відносин та туристичного бізнесу»

«28» серпня 2025 року, протокол №1

РОЗРОБНИК ПРОГРАМИ: Сергій ЛУБЕНЕЦЬ, канд. техн. наук, доцент, доцент закладу вищої освіти кафедри міжнародних відносин.

Програму схвалено на засіданні кафедри міжнародних відносин

Протокол № 1 від «25» серпня 2025 року

Завідувач кафедри міжнародних відносин

_____ Наталія ВІННИКОВА
(підпис) (ім'я та прізвище)

Програму погоджено з гарантом освітньо-професійної програми «Міжнародна інформаційна безпека»

Гарант освітньо-професійної програми «Міжнародна інформаційна безпека» (магістерського рівня)

_____ Віталій СОЛОВИХ
(підпис) (ім'я та прізвище)

Програму погоджено науково-методичною комісією ННІ «Каразінський інститут міжнародних відносин та туристичного бізнесу»

Протокол № 1 від «27» серпня 2025 року

Голова науково-методичної комісії ННІ «Каразінський інститут міжнародних відносин та туристичного бізнесу»

_____ Ганна ПАНАСЕНКО
(підпис) (ім'я та прізвище)

ВСТУП

Програма навчальної дисципліни «Сучасні технології штучного інтелекту в задачах ІТ-безпеки» складена відповідно до освітньо-професійної програми

«Міжнародна інформаційна безпека»

підготовки магістра

спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії».

1. Опис навчальної дисципліни

1.1. Метою викладання навчальної дисципліни є формування у здобувачів знань та вмінь з основ штучного інтелекту та його використання в інформаційній ІТ-безпеці держави в умовах зовнішніх та внутрішніх загроз.

1.2. Основні завдання вивчення дисципліни:

– формування у здобувачів вищої освіти теоретичних знань з основ штучного інтелекту та інформаційної безпеки; із сучасних технологій штучного інтелекту та їх ролі в задачах ІТ-безпеки; з основних інструментів штучного інтелекту в забезпеченні ІТ-безпеки;

– формування практичних навичок визначати, аналізувати та оцінювати загрози інформаційній безпеці; використовувати технології штучного інтелекту в забезпеченні ІТ-безпеки; застосовувати інструменти штучного інтелекту в кіберзахисті.

1.3. Кількість кредитів – 4.

1.4. Загальна кількість годин – 120.

1.5. Характеристика навчальної дисципліни	
За вибором	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
2-й	-й
Семестр	
3-й	-й
Лекції	
18 год.	год.
Практичні, семінарські заняття	
4 год. (практ.), 5 год. (сем.)	год.
Лабораторні заняття	
год.	год.
Самостійна робота	
93 год.	год.
Індивідуальні завдання	

1.6. Перелік компетентностей, що формує дана дисципліна

Вивчення навчальної дисципліни передбачає формування та розвиток у здобувачів вищої освіти наступних компетентностей:

- загальні компетентності:

ЗК6. Здатність працювати в міжнародному контексті;

ЗК10. Здатність до абстрактного мислення, аналізу та синтезу;

ЗК12. Здатність до пошуку, оброблення та аналізу інформації з різних джерел;

- спеціальні (фахові) компетентності:

СК6. Здатність використовувати для дослідження міжнародних відносин, суспільних комунікацій та для регіональних студій теоретичні та методологічні підходи політології, економічної та правової науки, міждисциплінарних досліджень;

СК14. Здатність оцінювати зміст та основні напрями діяльності міжнародних організацій в сфері безпеки та сучасних стратегій забезпечення міжнародної інформаційної безпеки;

СК16. Здатність аналізувати основи та особливості захисту національного інформаційного простору та забезпечення інформаційної безпеки держави.

1.7. Перелік результатів навчання, що формує дана дисципліна

Вивчення навчальної дисципліни передбачає формування та розвиток у здобувачів вищої освіти наступних програмних результатів навчання відповідно до ОПП:

РН3. Знати та розуміти основи та особливості захисту національного інформаційного простору та забезпечення інформаційної безпеки держави;

РН16. Аналізувати та оцінювати сучасні стратегії забезпечення міжнародної інформаційної безпеки;

РН22. Демонструвати здатність до подальшого навчання з високим рівнем автономності.

1.8. Пререквізити

Вивчення дисципліни передбачає засвоєння кредитів з дисциплін «Глобальна безпека та міжнародні конфлікти», «Захист національного інформаційного простору», «Міжнародна інформаційна безпека».

2. Тематичний план навчальної дисципліни

Розділ 1. Теоретичні аспекти штучного інтелекту та інформаційної безпеки

Тема 1. Основи штучного інтелекту та цифрової інформаційної безпеки

Поняття та основи штучного інтелекту (ШІ). Ключові аспекти ШІ. Штучний інтелект і нейронні мережі. Системи, засоби та типи ШІ. Формування ефективних запитів у системах ШІ. Напрями застосування та перспективи розвитку ШІ.

Основи цифрової інформаційної безпеки. Сучасні загрози інформаційній безпеці. Поширені форми кібератак. Методи захисту інформації в інформаційно-комунікаційних системах і мережах. Криптографічні методи та технічні засоби захисту інформації в ІТ-безпеці. Програмне забезпечення для захисту інформації в мережах. Засоби мережевої безпеки та їх класифікація. Шифрування каналу передачі даних в ІТ-безпеці. Міжмережеві екрани (брандмауери) та їх застосування в ІТ-безпеці. Антивірусні системи та їх застосування в ІТ-безпеці. Системи захисту від мережевих атак (IDS) в ІТ-безпеці. Віртуальні приватні мережі (VPN) та їх застосування при захисті мережевого трафіка. Системи запобігання мережевих атак (IPS) в ІТ-безпеці.

Тема 2. Загальна характеристика методів штучного інтелекту в ІТ-безпеці

Основні аспекти застосування штучного інтелекту в ІТ-безпеці. Роль штучного інтелекту в кібербезпеці. Еволюція ШІ в кібербезпеці. Переваги застосування ШІ в ІТ-безпеці. Технологія інтегрування ШІ в інформаційну безпеку. Сценарії використання ШІ в ІТ-безпеці. Виявлення та передбачення кіберзагроз на основі штучного інтелекту. Запобігання кібератакам за допомогою ШІ. Перспективи застосування ШІ в ІТ-безпеці.

Розділ 2. Технології застосування штучного інтелекту в задачах ІТ-безпеки

Тема 3. Технології штучного інтелекту та їх застосування в ІТ-безпеці

Основні типи технологій штучного інтелекту в системі інформаційної безпеки. Платформи EDR з виявлення атак на робочих станціях та серверах. Аналітичні платформи NDR для виявляють кібератак на мережевому рівні. Технологія UEBA з поведінкового аналізу користувачів та інформаційних сутностей. Платформи TIP з попереднього детектування кіберзагроз та реагування на них. Технологія SIEM з моніторингу інформаційних систем в режимі реального часу. Технологія SOAR з виявлення загроз інформаційній безпеці та автоматизованого реагування на інциденти. Технологія визначення загроз безпеці прикладних додатків (Application Security). Технологія виявлення загроз в бізнес-процесах та попередження шахрайських операцій в режимі реального часу (Antifraud).

Тема 4. Інструменти штучного інтелекту в задачах ІТ-безпеки

Загальна характеристика інструментів ШІ в реалізації шахрайських кібератак. Автоматизація процесів зламу, пошук вразливостей, подолання засобів захисту за допомогою ШІ. Автоматизація цільового фішингу для викрадення особистих даних за допомогою ШІ. Виготовлення дипфейків для шахрайства та соціальної інженерії за допомогою ШІ. «Отруєння» даних для виведення з ладу ШІ-моделей. Підвищення ефективності розробки шкідливого програмного забезпечення за допомогою ШІ.

Загальна характеристика інструментів ШІ в реалізації кіберзахисту. Автоматична обробка та аналіз звітів з ІТ-безпеки за допомогою ШІ. Детектування вторгнень у ІТ-систему за допомогою ШІ. Моніторинг і аналіз трафіку за допомогою ШІ. Боротьба із «хибною тривогою» за допомогою ШІ. Оновлення ІТ-інфраструктури за допомогою ШІ. Прогнозування кіберзагроз за допомогою ШІ.

3. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин								
	Денна форма					Заочна форма			
	усього	у тому числі				усього	у тому числі		
		л	пз	сем	с.р.		л	пз	с.р
Розділ 1. Теоретичні аспекти штучного інтелекту та інформаційної безпеки									
Тема 1. Основи штучного інтелекту та цифрової інформаційної безпеки	30	6	1	2	21				
Тема 2. Загальна характеристика методів штучного інтелекту в ІТ-безпеці	30	4		1	25				
Разом за розділом 1	60	10	1	3	46				
Розділ 2. Технології застосування штучного інтелекту в задачах ІТ-безпеки									
Тема 3. Технології штучного інтелекту та їх застосування в ІТ-безпеці	30	4	1	1	24				
Тема 4. Інструменти штучного інтелекту в задачах ІТ-безпеки	30	4	2	1	23				
Разом за розділом 2	60	8	3	2	47				
Усього годин	**120**	**18**	**4**	**5**	**93**				

4. Теми семінарських, практичних занять

4.1. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
1	Основи штучного інтелекту та цифрової інформаційної безпеки	2
2	Загальна характеристика методів штучного інтелекту в ІТ-безпеці	1
	Технології штучного інтелекту та їх застосування в ІТ-безпеці	1
3	Інструменти штучного інтелекту в задачах ІТ-безпеки	1
	Разом	**5**

4.2. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Основи штучного інтелекту. Криптографічні методи захисту інформації	1
	Технології штучного інтелекту в ІТ-безпеці. Формування запитів до ШІ	1
2	Інструменти штучного інтелекту в ІТ-безпеці	2
	Разом	**4**

5. Завдання для самостійної роботи

№ з/п	Види, зміст самостійної роботи	Кількість годин
1	Тема 1. Основи штучного інтелекту та інформаційної безпеки. *Завдання:* опрацювання інформаційних джерел за темою, конспектування тез, підготовка доповіді, опрацювання навчального матеріалу дистанційного курсу в Moodle «Сучасні технології штучного інтелекту в задачах ІТ-безпеки»; підготовка до семінарських занять	21
2	Тема 2. Загальна характеристика методів штучного інтелекту в ІТ-безпеці. *Завдання:* опрацювання інформаційних джерел за темою, конспектування тез, підготовка доповіді, опрацювання навчального матеріалу дистанційного курсу в Moodle «Сучасні технології штучного інтелекту в задачах ІТ-безпеки»; підготовка до семінарських занять	25
3	Тема 3. Технології штучного інтелекту та їх застосування в ІТ-безпеці. *Завдання:* опрацювання інформаційних джерел за темою, конспектування тез, підготовка доповіді, опрацювання навчального матеріалу дистанційного курсу в Moodle «Сучасні технології штучного інтелекту в задачах ІТ-безпеки»; підготовка до практичних та семінарських занять, виконання контрольних завдань практичної роботи	24
4	Тема 4. Інструменти штучного інтелекту в задачах ІТ-безпеки. *Завдання:* опрацювання інформаційних джерел за темою, конспектування тез, підготовка доповіді, опрацювання навчального матеріалу дистанційного курсу в Moodle «Сучасні технології штучного інтелекту в задачах ІТ-безпеки»; підготовка до практичних та семінарських занять, виконання контрольних завдань практичної роботи	23
	Разом	**93**

6. Індивідуальні завдання

Індивідуальні завдання не передбачено навчальним планом.

7. Методи навчання

Згідно з вимогами освітньо-професійної програми матриця відповідності освітнього компоненту «Сучасні технології штучного інтелекту в задачах ІТ-безпеки», методів навчання та засобів діагностики (форм оцінювання), які використовуються, програмним результатам навчання, визначеним освітньо-професійною програмою «Міжнародна інформаційна безпека»:

Шифр ПРН (відповідно до ОПП)	Результати навчання (відповідно до ОПП)	Методи навчання	Засоби діагностики /форми оцінювання
РН3	Знати та розуміти основи та особливості захисту національного інформаційного простору та забезпечення інформаційної безпеки держави	Пояснювально-ілюстративний, проблемно-орієнтований, інтерактивний, інформаційно-комп'ютеризований, інформаційно-рецептивний методи – для викладення нового матеріалу (лекційні та практичні форми навчання)	Усне опитування або письмовий (тестовий) контроль на лекціях та практичних заняттях; оцінювання: усних виступів з доповідями, виконання письмових (тестових) завдань, виконання аналітичних завдань, письмової (тестової) залікової роботи
РН16	Аналізувати та оцінювати сучасні стратегії забезпечення міжнародної інформаційної безпеки	Репродуктивний метод – для формування у здобувачів знань, навичок і вмінь та основних розумових операцій (практичні та семінарські заняття, самостійна робота та контрольні завдання)	Виконання практичних та контрольних завдань; оформлення та захист результатів практичних робіт; залікова робота, залікові тестові завдання
РН22	Демонструвати здатність до подальшого навчання з високим рівнем автономності	Репродуктивний метод – для формування у здобувачів знань, навичок і вмінь та основних розумових операцій (практичні та семінарські заняття, самостійна робота та контрольні завдання). Метод самоконтролю за ефективністю навчально-пізнавальної діяльності	Виконання практичних та контрольних завдань; оформлення та захист результатів практичних робіт; залікова робота, залікові тестові завдання

8. Методи контролю

Оцінювання знань здобувачів з дисципліни «Сучасні технології штучного інтелекту в задачах ІТ-безпеки» здійснюється шляхом проведення контрольних заходів, які передбачають поточний та підсумковий семестровий види контролю.

Поточний контроль здійснюється під час проведення практичних та семінарських занять з дисципліни протягом навчального семестру у формі усного опитування та навчальної дискусії з перевіркою знань здобувачів з окремих тем та рівня їх підготовленості до виконання практичних робіт; контролю виконання завдань для самостійної роботи, а також перевірки рівня виконання, оформлення і захисту результатів практичних та контрольних завдань.

Підсумковий семестровий контроль проводиться під час семестрового заліку у формі розгорнутих відповідей на теоретичні питання за темами дисципліни. Заліковий білет містить два теоретичні питання, здобувач одержує до 20 балів за відповідь на кожне питання. Загальна кількість балів за успішне виконання залікових завдань – 40.

За бажанням здобувач має можливість обрати тестову форму залікових завдань, яка містить 40 тестових завдань. Здобувач одержує 1 бал за кожну правильну відповідь.

9. Схема нарахування балів

Розподіл максимально можливих балів успішності здобувачів за результатами поточного та підсумкового семестрового контролю наступний:

Поточний контроль, самостійна робота					Підсумковий контроль	Сума
Розділ 1		Розділ 2		Разом	Залік	
Т1	Т2	Т5	Т6			
15	15	15	15	60	40	100

Т1-Т4 – теми розділів.

Для допуску до складання підсумкового контролю (заліку) здобувач вищої освіти повинен набрати не менше 10 балів з навчальної дисципліни під час поточного контролю, самостійної роботи, індивідуального завдання.

Наявні результати поточного та підсумкового контролю знань здобувачів оцінюються за наступними методами та критеріями:

Критерії та методи оцінювання навчальних досягнень

Методи	Критерії оцінювання	Система оцінювання, бали
Участь у навчальній дискусії, виконання та оформлення практичних робіт	Здобувач бере активну участь у дискусії, добре засвоїв навчальний матеріал за темою, вміє використовувати теоретичні знання при виконанні самостійної роботи та практичних завдань, можливо з незначними неточностями. Оформлення практичних результатів є логічним, послідовним та охайним, згідно вимог	12-15
	Здобувач бере активну участь у дискусії, добре засвоїв навчальний матеріал за темою, вміє застосовувати теоретичні знання при виконанні самостійної роботи та практичних завдань з наявністю незначних помилок та неповних висновків. Оформлення практичних результатів є послідовним та охайним, згідно вимог	8-11

	Здобувач бере участь у дискусії, в основному опанував навчальний матеріал за темою, вміє застосовувати теоретичні знання при виконанні самостійної роботи та практичних завдань з наявністю суттєвих помилок у результатах та висновках. Оформлення результатів є охайним, мають місце незначні відхилення від вимог	4-7
	Здобувач не бере участі в дискусії, поверхово або взагалі не опанував навчальний матеріал за темою, мають місце значні труднощі у виконанні самостійної роботи та практичних завдань, які не виконані загалом або виконані частково з грубими помилками та не правильними висновками. Оформлення результатів не охайне, не відповідає вимогам	0-3
Залікові завдання (за одне питання залікового білету)	Здобувач добре засвоїв теоретичний матеріал, логічно мислить і будує відповідь, грамотно висловлює свої міркування, впевнено та у достатній мірі відповідає на додаткові питання. Вміє використовувати теоретичні знання при розв'язанні конкретних проблемних ситуацій, можливо з незначними неточностями	16-20
	Здобувач добре засвоїв теоретичний матеріал, аргументовано будує відповідь, але припускається певних похибок у логіці викладу, не в повній мірі відповідає на додаткові питання. При вирішенні проблемних ситуацій допускає незначні помилки, робить не зовсім повні висновки	11-15
	Здобувач в основному опанував теоретичний матеріал, але не переконливо відповідає та плутає поняття, додаткові питання викликають невпевненість і демонструють відсутність стабільних знань. При вирішенні проблемних ситуацій здобувач без достатнього розуміння застосовує навчальний матеріал, припускається суттєвих помилок	6-10
	Здобувач поверхово або взагалі не опанував теоретичний матеріал, не знає наукових фактів та визначень, проявляє слабкість або відсутність наукового мислення, стикається зі складнощами при відповіді на додаткові питання. Мають місце значні труднощі у вирішенні конкретних проблемних ситуацій	0-5

Додатково до балів за виконання завдань (вивчення тем) дисципліни здобувач може отримати до 10 балів за такі види активностей:

– проходження тренінг-курсів чи дистанційних курсів за тематикою дисципліни на платформах Google, Coursera, Prometheus тощо (за наявності відповідного документу про їх закінчення, надання копії викладачу);

– участь в майстер-класах, форумах, конференціях, семінарах, зустрічах за тематикою дисципліни (з підготовкою есе, прес-релізу, інформаційного повідомлення тощо, що підтверджено програмою заходу чи відповідним сертифікатом);

– участь у науково-дослідних та прикладних дослідженнях за тематикою дисципліни, що підтверджується відповідними матеріалами.

Підсумкова кількість балів з дисципліни «Сучасні технології штучного інтелекту в задачах ІТ-безпеки» розраховується як сума балів, отриманих за результатами поточного контролю та балів, отриманих за результатами підсумкового контролю (заліку). Максимальна сума балів складає 100 балів.

Набрана кількість балів є основою для оцінки за національною шкалою згідно наступної шкали оцінювання:

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка
	для дворівневої шкали оцінювання
90-100	зараховано
70-89	
50-69	
0-49	не зараховано

10. Рекомендована література

Основна література

1. Гбур З.В. Використання штучного інтелекту в інформаційній безпеці України. *Державне управління: удосконалення та розвиток*. 2022. №1. DOI: 10.32702/2307-2156-2022.1.2

2. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посібник. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 144 с.

3. Гуржій С.В. Особливості використання штучного інтелекту у питаннях забезпечення кібербезпеки. *Інформація і право*. 2023. № 4(47). С. 207-216.

4. Звенігородський О.С., Зінченко О.В., Чичкарьов Є.А., Кисіль Т.М.. Штучний інтелект. Вступний курс. Київ: ДУТ, 2022. 193 с.

5. Когут Ю.І., Довгополий А.С. Штучний інтелект і безпека. Київ: SIDCON. 2024. 294с.

6. Лубенець С.В. Дистанційний курс «Сучасні технології штучного інтелекту в задачах ІТ-безпеки». *Moodle*. URL: https://moodle.karazin.ua/course/view.php?id=14925

7. Лубенець С.В., Харченко І.М., Павленко Є.П. Актуальні проблеми міжнародної інформаційної безпеки. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Міжнародні відносини. Економіка. Країнознавство. Туризм»*. 2023. Вип. 17. С. 42-48.

8. Неретін О., Харченко В. Забезпечення кібербезпеки систем штучного інтелекту: аналіз вразливостей, атак і контрзаходів. *Information Systems And Networks.* 2022. № 12. С. 7-20.

9. Основи кібербезпеки (курс індивідуальної підготовки). 2025. 48 с.

10. Пістунов І.М. Штучний інтелект. Прикладні аспекти: посібник. Дніпро: НТУ «ДП», 2025. 249 с.

11. Сілін Є.С., Кадубовський О.А. Основи кібербезпеки: навчальний посібник. Дніпро, 2023. 200 с.

12. Фратавчан В.Г., Фратавчан Т.М., Лукашів Т.О., Літвінчук Ю.А. Методи та системи штучного інтелекту: навчальний посібник. Чернівці: ЧНУ, 2023. 114 с.

13. Цифрова та інформаційна безпека: Рекомендований перелік онлайн-курсів / КЗ «ЗОУНБ» ЗОР, Регіон. консультаційно-тренінг. центр / уклад. Г. Мацієвська. Запоріжжя: [ЗОУНБ], 2023. 15 с.

14. Шаров С.В. Сучасний стан розвитку штучного інтелекту та напрямки його використання*:* зб. наук. пр. *Інноваційні обрії України*. 2023. № 6. С.136-144.

15. Шелестова А.М., Лубенець С.В. Інтеграція технологій штучного інтелекту в системи кіберзахисту підприємств. *Наукові інновації та передові технології (Серія «Управління та адміністрування», Серія «Право», Серія «Економіка», Серія «Психологія», Серія «Педагогіка»): журнал.* 2025. № 4(44). С. 1020-1033. https://doi.org/10.52058/2786-5274-2025-4(44)-1020-1033.

16. Tuomo Sipola, Tero Kokknen, Mika Karjalainen Artificial Intelligence and Cybersecurity: Theory and Applications. JAMK University of Applied Sciences. Publisher: Springer; 1st ed. 2023 edition (December 8, 2022). 311 p. DOI 10.1007/978-3-031-15030-2

Допоміжна література

17. Бурячок В.Л., Киричок Р.В., Складанний П.М. Основи інформаційної та кібернетичної безпеки. К. Київський університет імені Бориса Грінченка, 2019. 320 с.

18. Лубенець С.В., Харченко І.М., Новікова Л.В. Проблеми побудови консолідованих стратегій управління корпоративною інформаційною безпекою в регіоні ЕМЕА. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Міжнародні відносини. Економіка. Країнознавство. Туризм».* 2021. Вип. 14. С. 24-34.

19. Лубенець С.В., Харченко І.М., Шедякова Т.Є. Тенденції, виклики та рішення цифрової інформаційної безпеки в Центральній та Східній Європі. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Міжнародні відносини. Економіка. Країнознавство. Туризм».* 2024. Вип. 19. С. 16-24.

20. Лубенець С.В., Шелестова А.М., Чернишова Л.О. Напрями підвищення ефективності цифрової інформаційної безпеки в країнах островів Південно-Східної Азії. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Міжнародні відносини. Економіка. Країнознавство. Туризм».* 2025. Вип. 21. Подано до друку (довідка №11 від 29.05.2025 р.).

21. Методи та системи штучного інтелекту: навч. посіб. / укл. Д.В. Лубко, С.В. Шаров. Мелітополь: ФОП Однорог Т.В., 2019. 264 с.

11. Посилання на інформаційні ресурси в Інтернеті, відеолекції, інше методичне забезпечення

22. Застосування ШІ у кібербезпеці: роль та переваги. URL: https://wezom.com.ua/ua/blog/zastosuvannya-shi-u-kiberbezpetsi-rol-ta-perevagi

23. Захист від фішингу. URL: https://youtube.com/live/DmVw1voVBV4?feature=share

24. Захист конфіденційності в онлайн сервісах. URL: https://youtube.com/live/Ut4JVFzZt38?feature=share

25. Захист Wi-Fi мереж. URL: https://youtube.com/live/EOUoy_RVf-Q?feature=share

26. Штучний інтелект у кібербезпеці. URL: https://cutt.ly/3rJAdsdn

27. Що таке штучний інтелект? Вступ, історія та типи ШІ. URL: https://www.guru99.com/uk/artificial-intelligence-tutorial.html

28. Coursera. Професійний сертифікат Google Cybersecurity. URL: https://www.coursera.org/google-certificates/cybersecurity-certificate?utm_source=google&utm_medium=institutions&utm_campaign=sou--google__med--organicsearch__cam--gwgsite__con--null__ter--null

29. Google. Отримайте сертифікат зі штучного інтелекту. URL: https://grow.google/intl/ua/google-career-certificates/

12. Особливості навчання за денною формою в умовах подовження дії обставин непереборної сили

В умовах дії **обставин непереборної сили** освітній процес в університеті здійснюється відповідно до наказів/ розпоряджень ректора/ проректора або за змішаною формою навчання, або повністю дистанційно в синхронному режимі.

Складання підсумкового семестрового контролю: в разі запровадження жорстких обмежень з забороною відвідування ЗВО студентам денної форми навчання надається можливість скласти залік дистанційно на платформі Moodle в дистанційному курсі «Сучасні технології штучного інтелекту в задачах ІТ-безпеки».

Додаток 1

Додаток до робочої програми навчальної дисципліни «Сучасні технології штучного інтелекту в задачах ІТ-безпеки»

Дію робочої програми продовжено: на 20_____/20_____ н. р.

Заступник директора ННІ «Каразінський інститут міжнародних відносин та туристичного бізнесу» з навчальної роботи

_____ _____
(підпис) (прізвище, ініціали)

«____» _____ 20___ р.

Голова науково-методичної комісії ННІ «Каразінський інститут міжнародних відносин та туристичного бізнесу»

_____ _____
(підпис) (прізвище, ініціали)

«____» _____ 20___ р.