

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРЬСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-21.09- 05.01/291.00.1/Б/ OK12-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 1 / 16

ЗАТВЕРДЖЕНО

Вченою радою факультету
національної безпеки, права та
міжнародних відносин

27 серпня 2024 р., протокол № 8

Голова Вченої ради

Лариса СЕРГІЄНКО



РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Інформаційні технології та безпека у кіберпросторі»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності 291 «Міжнародні відносини, суспільні комунікації
та регіональні студії»

освітньо-професійна програма «Міжнародні відносини і геополітична безпека»
факультет національної безпеки, права та міжнародних відносин
кафедра міжнародних відносин і політичного менеджменту

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

 Завідувач кафедри

Валерій ХОНІК

Гарант освітньої-професійної програми



Андрій ШЕВЧУК

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

Житомир
2024

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-21.09- 05.01/291.00.1/Б/ ОК12-1-2024
	<i>Випуск 1</i>	<i>Зміни 0</i>	<i>Екземпляр № 1</i>	<i>Арк 2 / 16</i>

Робоча програма навчальної дисципліни «Інформаційні технології та безпека у кіберпросторі» для здобувачів вищої освіти освітнього ступеня «бакалавр» спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії» освітньо-професійна програма «Міжнародні відносини і геополітична безпека» затверджена Вченою радою факультету національної безпеки, права та міжнародних відносин від 27 серпня 2024 р., протокол № 8.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-21.09- 05.01/291.00.1/Б/ ОК12-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 3 / 16

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, освітній ступінь	Характеристика навчальної дисципліни денна форма навчання	
		Кількість кредитів – 3	Галузь знань 29 «Міжнародні відносини»
Модулів – 1	Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»	Рік підготовки:	
Змістових модулів – 1		1	-
Загальна кількість годин – 90		Семестр	
		2	-
Тижневих годин для денної форми навчання: аудиторних – 3	Освітній ступінь «бакалавр»	Лекції	
		16 год.	-
		Практичні	
		0 год.	-
		Лабораторні	
		32 год.	-
		Самостійна робота	
42 год.	-		
		Вид контролю: залік	

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

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

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-21.09- 05.01/291.00.1/Б/ OK12-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 4 / 16

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є формування у здобувачів вищої освіти теоретичних знань і практичних навичок використання сучасних інформаційних технологій для аналізу та управління міжнародними процесами, забезпечення безпеки у цифровому середовищі, а також протидії інформаційним загрозам у контексті регіональних і глобальних викликів.

Завданнями вивчення навчальної дисципліни є:

- ознайомлення з теоретичними основами інформаційних технологій;
- розвиток практичних навичок використання цифрових інструментів та управління інформаційними потоками;
- вивчення принципів захисту даних у міждержавних і суспільних комунікаціях та аналіз загроз у кіберпросторі, що впливають на міжнародні процеси;
- ознайомлення із правилами кібергігієни для запобігання інформаційним витокам і кібератакам.
- аналіз ролі соціальних мереж і пошукових систем у формуванні громадської думки та забезпеченні суспільної безпеки;
- вивчення механізмів ведення інформаційних війн і операцій у регіональному та глобальному контекстах.
- розробка стратегій інформаційної протидії та контрпропаганди.

Зміст навчальної дисципліни спрямований на формування наступних **компетентностей** за спеціальністю 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»:

ЗК3. Здатність вчитися і оволодівати сучасними знаннями.

ЗК4. Знання та розуміння предметної області та розуміння професійної діяльності

ЗК9. Здатність використовувати інформаційні та комунікаційні технології

СК2. Здатність аналізувати міжнародні процеси в різних контекстах, зокрема політичному, безпековому, правовому, економічному, суспільному, культурному та інформаційному.

СК12. Здатність до здійснення комунікації та інформаційно-аналітичної діяльності у сфері міжнародних відносин (українською та іноземними мовами).

СК15. Здатність ефективно здійснювати комунікацію в різних суспільно-політичних умовах та на різних рівнях (регіональному, геополітичному, глобальному), використовуючи інформаційно-комунікаційні технології.

Отримані знання з навчальної дисципліни стануть складовими наступних **результатів навчання** за спеціальністю 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»:

РН02. Знати та розуміти природу та динаміку міжнародної безпеки, розуміти особливості її забезпечення на глобальному, регіональному та національному рівні, знати природу та підходи до вирішення міжнародних та інтернаціоналізованих конфліктів.

РН08. Збирати, обробляти та аналізувати великі обсяги інформації про стан міжнародних відносин, зовнішньої політики України та інших держав, регіональних систем, міжнародних комунікацій.

РН14. Використовувати сучасні цифрові технології, спеціалізовані програмне забезпечення, бази даних та інформаційні системи для розв'язання складних спеціалізованих задач у сфері міжнародних відносин, суспільних

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-21.09- 05.01/291.00.1/Б/ OK12-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 5 / 16

комунікацій та/або регіональних студій.

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. Теоретичні та практичні аспекти інформаційних технологій та безпеки у кіберпросторі

Тема 1. Теоретичні основи інформаційних технологій. Системне та програмне забезпечення інформаційних процесів (ЗК 03, ЗК 04, ЗК 09, СК 02, СК12, РН 14)

1. Основні поняття та складові інформаційних технологій
2. Поняття інформації
3. Апаратне забезпечення ПК
4. Структура даних на носіях інформації
5. Програмне забезпечення ПК та його класифікація
6. Призначення та функції операційних систем
7. Автоматизація аналітичних процесів у міжнародних відносинах

Тема 2. Використання програмних продуктів Microsoft Word, Microsoft Excel та Microsoft Powerpoint (ЗК 03, ЗК 09, СК12, РН 08)

1. Текстовий редактор Word, Excel та Powerpoint: функціональні можливості та інтерфейс
2. Робота з таблицями та вбудованими об'єктами
3. Використання формул, графічне представлення даних та сортування інформації в Excel для цілей аналізу
4. Захист документів Microsoft Word, Excel та Powerpoint за допомогою паролів

Тема 3. Захист інформації в інформаційно-телекомунікаційних системах (ЗК 03, ЗК 09, СК 02, СК 15, РН 14)

1. Предмет політики інформаційної системи
2. Принципи політики інформаційної безпеки
3. Види політики інформаційної системи

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-21.09- 05.01/291.00.1/Б/ ОК12-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 6 / 16

4. Протидія несанкціонованому витоку інформації
5. Організація технічного захисту комп'ютерних систем
6. Захист від шкідливого програмного забезпечення

Тема 4. Інформаційні технології у міжнародних відносинах (ЗК 03, ЗК 04, ЗК 09, СК 02, СК12, СК 15, РН 02, РН 08, РН 14)

1. Можливості та виклики цифровізації міжнародних відносин
2. Інформаційні системи в дипломатії та міждержавній комунікації
3. Використання інформаційних технологій в управлінні міжнародними процесами
4. Використання цифрових платформ для управління конфліктами
5. Інформаційні технології як інструмент регіональної дипломатії

Тема 5. Основи побудови та функціонування мережевих технологій (ЗК 03, ЗК 04, ЗК 09, СК 12, РН 08)

1. Основи побудови комп'ютерних мереж, їх класифікація
2. Локальні та глобальні мережі у світовій економіці
3. Загальні принципи побудови глобальних мереж
4. Інформаційні служби та послуги Internet
5. Електронна пошта та корпоративні комунікації для потреб міжнародних відносин
6. Правила безпечної роботи з інформаційними системами в кіберсередовищі

Тема 6. Роль інформаційно-пошукових систем і соціальних мереж у міжнародних відносинах (ЗК 03, ЗК 04, СК 02, СК 15, РН 02, РН 08, РН 14)

1. Загальна характеристика інформаційно-пошукових систем та їх види
2. Використання пошукових систем для збору інформації
3. Використання соціальних мереж у міжнародних відносинах
4. Протидія дезінформації у міжнародних відносинах
5. Аналіз і моніторинг громадської думки в суспільних комунікаціях

Тема 7. Основи кібербезпеки в міжнародних відносинах (ЗК 03, ЗК 04, СК 02, СК 15, РН 02, РН 14)

1. Кіберпростір: термінологія, структура
2. Загрози для дипломатичних установ у кіберпросторі
3. Основні поняття захисту інформації та інформаційної безпеки
4. Принципи захисту інформації у міждержавних комунікаціях
5. Використання кібергігієни для запобігання інформаційним загрозам
6. Методи виявлення та протидії дезінформації у міжнародних відносинах

Тема 8. Протиборство у кіберпросторі (ЗК 03, ЗК 04, СК 02, СК 15, РН 02, РН 14)

1. Види інформаційних прав і свобод та їх зв'язок з іншими правами та свободами людини та громадянина
2. Протиборство в кіберпросторі як складова інформаційного протиборства
3. Інформаційна злочинність та кіберзлочинність
4. Інформаційний тероризм та кібертероризм

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-21.09- 05.01/291.00.1/Б/ OK12-1-2024	
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 7 / 16	

5. Інформаційна безпека та кібербезпека
6. Інформаційна війна її вплив на міжнародну безпеку
7. Інструменти контрпропаганди в умовах інформаційної війни

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин							
	денна форма				заочна форма			
	усього	лекції	лабораторні	самостійна робота	усього	лекції	лабораторні	самостійна робота
МОДУЛЬ 1								
Змістовий модуль 1. Теоретичні та практичні аспекти інформаційних технологій та безпеки у кіберпросторі								
Тема 1. Теоретичні основи інформаційних технологій. Системне та програмне забезпечення інформаційних процесів	14	2	2	10	–	–	–	–
Тема 2. Використання програмних продуктів Microsoft Word, Microsoft Excel та Microsoft Powerpoint	11	2	10	4	–	–	–	–
Тема 3. Захист інформації в інформаційно-телекомунікаційних системах	11	2	2	6	–	–	–	–
Тема 4. Інформаційні технології у міжнародних відносинах	12	2	2	6	–	–	–	–
Тема 5. Основи побудови та функціонування мережевих технологій	8	2	4	4	–	–	–	–
Тема 6. Роль інформаційно-пошукових систем і соціальних мереж у міжнародних відносинах	15	2	4	4	–	–	–	–
Тема 7. Основи кібербезпеки в міжнародних відносинах	11	2	4	4	–	–	–	–
Тема 8. Протиборство у кіберпросторі	8	2	4	4	–	–	–	–
ВСЬОГО	90	16	32	42	–	–	–	–

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-21.09- 05.01/291.00.1/Б/ ОК12-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 8 / 16

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
МОДУЛЬ 1			
Змістовий модуль 1. Теоретичні та практичні аспекти інформаційних технологій та безпеки у кіберпросторі			
1	Тема 1. Теоретичні основи інформаційних технологій. Системне та програмне забезпечення інформаційних процесів	2	–
2	Тема 2. Використання програмних продуктів Microsoft Word, Microsoft Excel та Microsoft Powerpoint	10	–
3	Тема 3. Захист інформації в інформаційно-телекомунікаційних системах	2	–
4	Тема 4. Інформаційні технології у міжнародних відносинах	2	–
5	Тема 5. Основи побудови та функціонування мережевих технологій	4	–
6	Тема 6. Роль інформаційно-пошукових систем і соціальних мереж у міжнародних відносинах	4	–
7	Тема 7. Основи кібербезпеки в міжнародних відносинах	4	–
8	Тема 8. Протиборство у кіберпросторі	4	–
РАЗОМ		32	–

6. Завдання для самостійної роботи

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
МОДУЛЬ 1			
Змістовий модуль 1. Теоретичні та практичні аспекти інформаційних технологій та безпеки у кіберпросторі			
1	Тема 1. Теоретичні основи інформаційних технологій. Системне та програмне забезпечення інформаційних процесів – Основні поняття та складові інформаційних технологій – Поняття інформації	10	–
2	Тема 2. Використання програмних продуктів Microsoft Word, Microsoft Excel та Microsoft Powerpoint – Текстовий редактор Microsoft Word, Microsoft Excel та Microsoft Powerpoint: функціональні можливості та інтерфейс	4	–
3	Тема 3. Захист інформації в інформаційно-телекомунікаційних системах – Предмет політики інформаційної системи – Принципи політики інформаційної безпеки	6	–
4	Тема 4. Інформаційні технології у міжнародних відносинах – Можливості та виклики цифровізації міжнародних відносин	6	–
5	Тема 5. Основи побудови та функціонування мережевих технологій – Правила безпечної роботи з інформаційними системами в кіберсередовищі	4	–
6	Тема 6. Роль інформаційно-пошукових систем і соціальних мереж у міжнародних відносинах – Використання пошукових систем для збору інформації	4	–
7	Тема 7. Основи кібербезпеки в міжнародних відносинах – Використання кібергігієни для запобігання інформаційним загрозам	4	–
8	Тема 8. Протиборство у кіберпросторі – Види інформаційних прав і свобод та їх зв'язок з іншими правами та	4	–

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-21.09- 05.01/291.00.1/Б/ OK12-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 9 / 16
свободами людини та громадянина				
РАЗОМ				42

7. Індивідуальні самостійні завдання

Індивідуальна робота здобувачів вищої освіти з навчальної дисципліни «Інформаційні технології та безпека у кіберпросторі» включає виконання завдань:

Завдання 1: Розгляньте приклади використання цифрових інструментів у роботі ООН, НАТО чи інших міжнародних організацій та підготуйте презентацію на тему: «Вплив інформаційних технологій на сучасну дипломатію та міжнародні відносини»

Завдання 2: Напишіть есе (2-3 сторінки) на тему «Цифрова дипломатія: як технології змінюють міжнародні відносини?». В роботі акцентуйте увагу на соціальних мережах та платформах для взаємодії між державами.

Завдання 3: Напишіть інструкцію для безпечного користування електронною поштою та месенджерами в умовах роботи з конфіденційною інформацією.

Завдання 4: Проаналізуйте використання соціальних мереж під час міжнародних криз (наприклад, війна, пандемія чи політичний конфлікт). Напишіть аналітичну записку про позитивні та негативні аспекти цього явища.

Завдання 5: Розробіть стратегію інформаційної кампанії для просування іміджу країни в соціальних мережах (оберіть країну на свій розсуд).

Завдання 6: Підготуйте звіт (2-3 сторінки) про найбільші кібератаки, які вплинули на міжнародні відносини, і запропонуйте заходи для запобігання подібним інцидентам у майбутньому.

Завдання 7: Розробіть модель моніторингу кіберзагроз для державного органу, який працює у сфері міжнародних відносин.

Завдання 8: Проведіть аналіз одного з кейсів дезінформації у міжнародних відносинах (наприклад, фейкові новини про конфлікти чи економічні угоди). Напишіть звіт про його наслідки та способи протидії.

Завдання 9: Розробіть пам'ятку для громадян про те, як розпізнавати дезінформацію у соціальних мережах.

Завдання 10: Напишіть аналітичний огляд (3-4 сторінки) про роль інформаційних війн у сучасних міждержавних конфліктах. Наведіть приклади та опишіть їхній вплив на політичну ситуацію.

8. Методи навчання

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

Результат навчання	Методи навчання
РН02. Знати та розуміти природу та динаміку міжнародної безпеки, розуміти особливості її забезпечення на глобальному, регіональному та національному рівні, знати природу та підходи до вирішення міжнародних та	– Вербальні методи (лекція, пояснення); – Практичні методи (виконання лабораторних робіт, практичних завдань); – Ситуаційний метод; – Методи самостійної роботи (анотування опрацьованого матеріалу, написання есе, підготовка

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-21.09- 05.01/291.00.1/Б/ ОК12-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 10 / 16
Результат навчання		Методи навчання		
інтернаціоналізованих конфліктів		доповідей, написання наукових статей)		
РН08. Збирати, обробляти та аналізувати великі обсяги інформації про стан міжнародних відносин, зовнішньої політики України та інших держав, регіональних систем, міжнародних комунікацій		– Вербальні методи (лекція, пояснення); – Практичні методи (виконання лабораторних робіт, практичних завдань); – Ситуаційний метод; – Методи самостійної роботи (анотування опрацьованого матеріалу, написання есе, підготовка доповідей, написання наукових статей)		
РН14. Використовувати сучасні цифрові технології, спеціалізовані програмне забезпечення, бази даних та інформаційні системи для розв'язання складних спеціалізованих задач у сфері міжнародних відносин, суспільних комунікацій та/або регіональних студій		– Вербальні методи (лекція, пояснення); – Практичні методи (виконання лабораторних робіт, 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
РН02. Знати та розуміти природу та динаміку міжнародної безпеки, розуміти особливості її забезпечення на глобальному, регіональному та національному рівні, знати природу та підходи до вирішення міжнародних та інтернаціоналізованих конфліктів	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, перевірка виконання лабораторних робіт, залік
РН08. Збирати, обробляти та аналізувати великі обсяги інформації про стан міжнародних відносин, зовнішньої політики України та інших держав, регіональних систем, міжнародних комунікацій	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, перевірка виконання лабораторних робіт, залік
РН14. Використовувати сучасні цифрові технології, спеціалізовані програмне забезпечення, бази даних та інформаційні системи для розв'язання складних спеціалізованих задач у сфері міжнародних відносин, суспільних комунікацій та/або регіональних студій	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, перевірка виконання лабораторних робіт, 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

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-21.09- 05.01/291.00.1/Б/ OK12-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 11 / 16

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	заочна 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):	10	–
1. Підготовка наукових статей, тез доповідей наукових конференцій		
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 лабораторних 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:

$$P_{H3} = \sum(P_i \times BK_i) \times K_{H3}, \quad (1)$$

де P_{H3} – загальна кількість балів, набраних здобувачем за виконання завдань під час навчальних занять за семестр;

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

BK_i – ваговий коефіцієнт за виконання i -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

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-21.09- 05.01/291.00.1/Б/ OK12-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 12 / 16

занять, на сумарну кількість балів за виконання усіх видів робіт під час навчальних занять за семестр;

$K_{НЗ}$ – 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 програми¹.

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».

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-21.09- 05.01/291.00.1/Б/ ОК12-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 13 / 16

Курси неформальної освіти:

1. Кібергігієна для молоді. URL: <https://osvita.diia.gov.ua/courses/cyber-hygiene-for-youth>
2. Базові знання з кібергігієни. URL: <https://osvita.diia.gov.ua/courses/basic-knowledge-of-cyber-hygiene>
3. Кібергігієна: як захиститися від фішингу. URL: <https://osvita.diia.gov.ua/courses/kibergigiena-ak-zahistitisa-vid-fisinguttps://osvita.diia.gov.ua/courses/kibergigiena-ak-zahistitisa-vid-fisingu>
4. Персональна кібергігієна. URL: <https://osvita.diia.gov.ua/courses/personal-cyberhygiene>
5. ChatGPT для підвищення власної ефективності. URL: <https://osvita.diia.gov.ua/courses/chatgpt-for-personal-effectiveness>
6. Датааналітик. Вступ до Excel. URL: <https://osvita.diia.gov.ua/courses/data-analyst-excel>
7. Демократія через дії. Модуль 1. URL: <https://osvita.diia.gov.ua/courses/democrasy-through-actions-module-1>
8. Демократія через дії. Модуль 2. URL: <https://osvita.diia.gov.ua/courses/democrasy-through-actions-module-2>

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

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-21.09- 05.01/291.00.1/Б/ ОК12-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 14 / 16

11. Глосарій

№ з/п	Термін державною мовою	Відповідник англійською мовою
1.	Big Data	Big Data
2.	Апаратне забезпечення	Hardware
3.	Глобалізація	Globalization
4.	Двофакторна автентифікація	Two-factor authentication
5.	Дезінформація	Disinformation
6.	Інформаційна війна	Information warfare
7.	Інформаційна операція	Information operation
8.	Інформаційний вплив	Information influence
9.	Інформаційні технології	Information technology
10.	Кібератака	Cyberattack
11.	Кібербезпека	Cybersecurity
12.	Кібервійна	Cyberwar
13.	Кібергігієна	Cyber hygiene
14.	Кіберпростір	Cyberspace
15.	Кіберсуверенітет	Cyber sovereignty
16.	Контент	Content
17.	Контрпропаганда	Counterpropaganda
18.	Конфіденційність	Privacy
19.	Мережевий протокол	Network protocol
20.	Операційна система	Operating system
21.	Пошукова система	Search engine
22.	Програмне забезпечення	Software
23.	Соціальні мережі	Social media
24.	Фейкові новини	Fake news
25.	Фішинг	Phishing
26.	Цифрова дипломатія	Digital diplomacy
27.	Шифрування	Encryption

12. Рекомендована література

Основна література

1. Дукуї А., Морозов А., Локтікова Т., Ієфремов І., Забродський Р. Constructing an algorithm of quadratic time complexity for finding the maximal matching. Eastern-European Journal of Enterprise Technologies. 2019. Vol 6. No 4 (102). PP. 21-28. (Scopus)
2. Буйницька О.П. Інформаційні технології та технічні засоби навчання. К.: Центр навчальної літератури. 2019. 240 с.
3. Величко О.М., Гордієнко Т.Б. Інтелектуальні інформаційні системи: структура і застосування: підручник. К.: Олді+, 2022. 728 с.
4. Гуржій А. М. Основи інформаційних технологій : навчальний посібник для здобувачів професійної (професійно-технічної) освіти / А.М. Гуржій, Л.І. Возненко, Н.І. Поворознюк, В.В. Самсонов. К.: Літера ЛТД, 2023. 288 с.
5. Дикий А.П. Формування інформаційно-комунікаційної системи запобігання та протидії економічній злочинності. Наукові перспективи. 2021. № 11 (17). С. 486-499.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-21.09- 05.01/291.00.1/Б/ OK12-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 15 / 16

6. 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.

7. Мирошніченко В.О. Використання сучасних інформаційних технологій: формування мультимедійної компетентності. К.: ЦУЛ, 2020. 296 с.

8. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В.М. Богуш, В.В. Богуш, В.Д. Бровко, В.П. Настрадін; під. ред. В.М. Богуша. К.: Видавництво Ліра-К, 2022. 554 с.

9. 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.

10. Ратушняк Т.В., Ніжегородцев В.О., Гладченко О.В. Інформаційні системи і технології: практикум : навчальний посібник. Ірпінь : Університет ДФС України, 2022. 180 с.

Допоміжна література

11. Myroslav Kryshatanovych, Iryna Gorban, Lesia Kornat, Anatolii Dykyi, Nadiia Marushko. Investment Support for the Digitalization of Socio-Economic Systems in the Context of Ensuring Security. 2022. VOL.22. No.6. PP. 733-738 (WOS)

12. Березко Л. О. Інструментальні засоби вебтехнологій : навч. посіб. / Л.О. Березко, І.Ю. Юрчак. Львів : Національний університет «Львівська політехніка», 2020. 242 с.

13. 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.

14. 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. м. Рига (Латвія): ГО «ВАДНД», 07 жовтня 2022 р. 487 с. С. 41-46.

15. Євдокимов В.В., Дикий А.П. Інформаційний механізм формування та реалізації державної політики в сфері правоохоронної діяльності. Матеріали I Міжнародної науково-практичної конференції "Місьцеве самоврядування в Україні: теорія та практика", 7 грудня 2021 року. Полтава : ПДАУ, 2021. С. 372-375.

16. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: спеціальні питання кваліфікації, проведення слідчих (розшукових) дій, призначення комп'ютерно-технічних судових експертиз : наук-практ. посіб. / Б. Б. Теплицький, Л. Г. Шарай, К. М. Ковальов, С. А. Кузьмін. К.: ПАЛИВОДА А. В., 2019. 168 с.

17. 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.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-21.09- 05.01/291.00.1/Б/ OK12-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 16 / 16

18. Кулешник Я. Ф., Магеровська Т. В., Зачек О. І. Застосування хмарних технологій в інформаційному забезпеченні діяльності Національної поліції: методичні вказівки. Львів : ЛьвДУВС, 2021. 64 с.

19. Магеровська Т.В. Електронні таблиці та системи управління базами даних: навчальний посібник / Т.В. Магеровська, Я.М. Пелех, В.В. Сенік, А.В. Кунинець. Львів : Самвидав, 2020. 415 с.

20. Магеровська Т.В., Пелех Я.М., Кунинець А.В., Філь Б.М. Конспект лекцій з дисципліни інформатика для студентів. Львів : НУ «ЛП», 2019. 224 с.

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

13. Інформаційні ресурси в Інтернеті

1. Закон України «Про національну безпеку України»
2. Закон України «Про основні засади забезпечення кібербезпеки України»
3. Free Software Foundation. URL: <http://www.fsf.org/>.
4. <http://galanet.at.ua>
5. <http://www.osvita.info>
6. <https://informatic.org.ua>
7. Linux in Schools project. URL: <http://www.k12os.org>.
8. Open Source Educational Foundation. URL: <http://www.osef.org>.
9. Віртуальна академія Microsoft. URL: <http://www.microsoftvirtualacademy.com>
10. Інтерактивне навчання за програмою Microsoft IT Academy. URL: <http://itacademy.microsoftlearning.com>
11. Офісний пакет LibreOffice. URL: <http://www.libreoffice.org/>
12. Офісний пакет WPS Office 2019. <https://www.wps.com/office-free/> або <http://wps-community.org/downloads>
13. Офіційний сайт linuxmint. URL: <http://linuxmint.com/>