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 в кіберпросторі»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності 256 «Національна безпека
(за окремими сферами забезпечення і видами діяльності»
освітньо-професійна 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 освітньої-професійної програми
_____ Ірина СУПРУНОВА

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

Житомир
2024 р.

Робоча програма навчальної дисципліни «Інформаційні технології та безпека в кіберпросторі» для здобувачів вищої освіти освітнього ступеня «бакалавр» спеціальності 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» за освітньо-професійною програмою «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, освітній 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">Обов’язкова</td></tr>
<tr><td>Модулів – 1</td><td rowspan="4">Спеціальність
256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 1</td><td colspan="2">1</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 90</td><td colspan="2">Семестр</td></tr>
<tr><td colspan="2">2</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:
аудиторних – 3</td><td rowspan="10">Освітній ступінь «бакалавр»</td><td colspan="2">Лекції</td></tr>
<tr><td>16 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>0 год.</td><td>0 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>32 год.</td><td>8 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>42 год.</td><td>76 год.</td></tr>
<tr><td colspan="2">Вид контролю: екзамен</td></tr>
</table>

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

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

для заочної форми навчання – 16 % аудиторних занять, 84 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є формування у здобувачів вищої освіти системних знань про сучасні інформаційні технології, принципи їх функціонування, методи забезпечення інформаційної безпеки та управління ризиками у кіберпросторі, а також розвиток навичок використання цифрових інструментів для аналізу, прогнозування і протидії кіберзагрозам у контексті національної безпеки.

Завданнями вивчення навчальної дисципліни є набуття знань щодо:

–забезпечити теоретичну підготовку студентів щодо основ інформаційних технологій, принципів функціонування системного та програмного забезпечення;

–сформувати практичні навички роботи з офісними програмами (Microsoft Word, Microsoft Excel) для аналізу та візуалізації даних;

–ознайомити із сучасними мережевими технологіями та принципами безпечної роботи в локальних і глобальних мережах;

–розкрити роль інформаційно-пошукових систем і соціальних мереж у зборі даних, аналізі інформації та забезпеченні національної безпеки;

–дослідити структуру кіберпростору та основні загрози, пов’язані з функціонуванням державних систем;

–пояснити природу протиборства у кіберпросторі, зокрема кіберзлочинності, інформаційного тероризму, кібервійни та методів їхнього запобігання;

–сформувати культуру кібергігієни як важливого аспекту забезпечення інформаційної безпеки в державних і приватних установах;

–навчити аналізувати інформаційні операції та інформаційну війну, а також розробляти стратегії їхньої протидії;

–розвинути навички застосування сучасних інформаційних технологій у забезпеченні кібербезпеки, прогнозуванні загроз і побудові стратегій захисту.

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

ЗК 1. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК 2. Здатність застосовувати знання у практичних ситуаціях.

ЗК 4. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК 5. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК 6. Здатність виявляти, ставити та вирішувати проблеми, приймати обґрунтовані рішення.

СК 2. Здатність використовувати категорійно-понятійний апарат теорії національної безпеки, виявляти та аналізувати виклики та загрози національній безпеці, оцінювати особливості функціонування сучасної системи національної безпеки на різних рівнях.

СК 6. Здатність описувати й оцінювати безпекові процеси та явища у різних контекстах, синтезувати інформацію з метою встановлення бачення та цілей стратегії у визначальних сферах національної безпеки (політичній, воєнній, економічній, соціальній, інформаційній, тощо), включаючи запобігання та протидію терористичним загрозам.

СК 13. Здатність виявляти можливі загрози інформаційному простору та протидіяти інформаційно-психологічним впливам шляхом використання інформаційно-комунікаційних технологій, імплементації сучасних методів інформаційної безпеки та захисту інформації.

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

ПРН 4. Обґрунтовано застосовувати знання з основ теорії національної безпеки, зокрема, оцінювати обстановку, рівень небезпек та загроз національній безпеці, вміти використовувати базовий категорійно-понятійний та аналітично-дослідницький апарат сучасної науки в сфері національної безпеки.

ПРН 6. Вміти використовувати інформаційні та комунікаційні технології, сучасні методи інформаційної безпеки та захисту інформації у професійній діяльності, порушення яких може завдати шкоду національним інтересам держави.

ПРН 13. Протидіяти інформаційно-психологічним впливам під час адаптації та дій в умовах мирного часу та в особливий період, критично оцінювати достовірність джерел інформації, виявляти дезінформацію та маніпулятивний контент, що може впливати на національну безпеку, використовуючи методи верифікації та фактчекінгу.

ПРН 14. Демонструвати уміння виявляти та вирішувати складні спеціалізовані завдання та практичні проблеми у сфері національної безпеки, використовувати аналітичний інструментарій, критичне мислення для формування принципово нових ідей та адаптації до нових безпекових викликів та ситуацій.

ПРН 20. Демонструвати розуміння природи тероризму та антитерористичної безпеки, виявляти та прогнозувати ризики терористичних загроз, у межах компетенцій суб'єктів забезпечення національної безпеки приймати участь в організації та здійсненні заходів боротьби з тероризмом.

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
Змістовний модуль 1

Тема 1. Теоретичні основи інформаційних технологій. Системне та програмне забезпечення інформаційних процесів (ЗК 2, ЗК 4, СК 13, ПРН 6)

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

Тема 2. Використання програмних продуктів Microsoft Word, Microsoft Excel та Microsoft Powerpoint (ЗК 1, ЗК 2, ЗК 5, СК 13, ПРН 6)

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. Мережеві технології (ЗК 1, ЗК 4, ЗК 5, СК 13, ПРН 6, ПРН 14)

1. Основи побудови комп’ютерних мереж, їх класифікація
2. Принципи та архітектура локальних мереж
3. Використання ресурсів внутрішньої мережі
4. Загальні принципи побудови глобальних мереж
5. Інформаційні служби та послуги Internet
6. Ведення електронної кореспонденції: створення, відправлення повідомлень, пошук та накопичення адрес
7. Безпечна робота з інформаційними системами в кіберсередовищі

Тема 4. Роль інформаційно-пошукових систем та соціальних мереж у забезпеченні національної безпеки (ЗК 1, ЗК 2, ЗК 4, СК 13, ПРН 6, ПРН 14)

1. Загальна характеристика інформаційно-пошукових систем та їх види
2. Пошукові системи як спосіб збору розвідувальної інформації
3. Поняття та види соціальних мереж
4. Соціальні мережі у виявленні потенційних загроз
5. Ідентифікація та протидія пропаганді та дезінформації в соціальних мережах
6. Значення та використання соціальних мереж з метою забезпечення національної безпеки

Тема 5. Кіберпростір та кібербезпека (ЗК 2, ЗК 4, ЗК 5, ЗК 6, СК 2, СК 6, СК 13, ПРН 4, ПРН 14)

1. Кіберпростір: термінологія, структура.
2. Види загроз у кіберпросторі та їх вплив на функціонування державних інституцій
3. Види атак, спрямованих на державні системи
4. Система моніторингу кіберзагроз
5. Забезпечення суверенітету держави у кіберпросторі

Тема 6. Протиборство у кіберпросторі (ЗК 4, ЗК 6, СК 2, СК 6, СК 13, ПРН 4, ПРН 20)

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. Протидії кіберзлочинам в умовах воєнного стану
4. Інформаційний тероризм
5. Інформаційна війна та кібервійна
6. Інформаційна безпека та кібербезпека

Тема 7. Кібергігієна у сфері національної безпеки (ЗК 2, ЗК 4, СК 2, ПРН 6, ПРН 13, ПРН 14, ПРН 20)

1. Поняття, принципи кібергігієни та її роль у забезпеченні національної безпеки
2. Ідентифікація загроз національній безпеці, викликаних недотриманням правил кібегігієни
3. Популяризація кібергігієни серед працівників у сфері національної безпеки

Тема 8. Інформаційна війна та інформаційні операції (ЗК 1, ЗК 5, ЗК 6, СК 2, СК 13, ПРН 6, ПРН 13, ПРН 14, ПРН 20)

1. Поняття інформаційної війни та її основних інструментів
2. Методи протидії інформаційним атакам
3. Big Data у прийнятті рішень у сфері безпеки

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
Тема 1. Теоретичні основи інформаційних технологій. Системне та програмне забезпечення інформаційних процесів	8	2	2	4	10	1	–	9
Тема 2. Використання програмних продуктів Microsoft Word, Microsoft Excel та Microsoft Powerpoint	14	2	10	2	13	–	4	9
Тема 3. Мережеві технології	12	2	4	6	12	1	1	10
Тема 4. Роль інформаційно-пошукових систем та соціальних мереж у забезпеченні національної безпеки	10	2	2	6	11	1	–	10
Тема 5. Кіберпростір та кібербезпека	12	2	4	6	11	–	1	10
Тема 6. Протиборство у кіберпросторі	12	2	4	6	10	1	–	9
Тема 7. Кібергігієна у сфері національної безпеки	10	2	2	6	11	1	1	9
Тема 8. Інформаційна війна та інформаційні операції	10	2	2	6	12	1	1	10
Модульний контроль	2	–	2	–	–	–	–	–
ВСЬОГО	**90**	**16**	**32**	**42**	**90**	**6**	**8**	**76**

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
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	4
3	**Тема 3.** Мережеві технології	4	1
4	**Тема 4.** Роль інформаційно-пошукових систем та соціальних мереж у забезпеченні національної безпеки	2	–
5	**Тема 5.** Кіберпростір та кібербезпека	4	1
6	**Тема 6.** Протиборство у кіберпросторі	4	–
7	**Тема 7.** Кібергігієна у сфері національної безпеки	2	1
8	**Тема 8.** Інформаційна війна та інформаційні операції	2	1
	Модульний контроль	2	–
РАЗОМ		**32**	**8**

6. Завдання для самостійної роботи

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1.** Теоретичні основи інформаційних технологій. Системне та програмне забезпечення інформаційних процесів Основні поняття та складові інформаційних технологій Поняття інформації	4	9
2	**Тема 2.** Використання програмних продуктів Microsoft Word, Microsoft Excel та Microsoft Powerpoint Текстовий редактор Word, Excel та Powerpoint: функціональні можливості та інтерфейс	2	9
3	**Тема 3.** Мережеві технології Поняття та види соціальних мереж	6	10
4	**Тема 4.** Роль інформаційно-пошукових систем та соціальних мереж у забезпеченні національної безпеки Поняття та види соціальних мереж	6	10
5	**Тема 5.** Кіберпростір та кібербезпека Види загроз у кіберпросторі та їх вплив на функціонування державних інституцій	6	10
6	**Тема 6.** Протиборство у кіберпросторі Види інформаційних прав і свобод та їх зв'язок з іншими правами та свободами людини та громадянина	6	9
7	**Тема 7.** Кібергігієна у сфері національної безпеки Популяризація кібергігієни серед працівників у сфері національної безпеки	6	9
8	**Тема 8.** Інформаційна війна та інформаційні операції Поняття інформаційної війни та її основних інструментів	6	10
РАЗОМ		**42**	**76**

7. Індивідуальні самостійні завдання

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

Завдання 1: Написати короткий звіт (2-3 сторінки) на тему: «Еволюція інформаційних технологій: від першого комп'ютера до хмарних сервісів». При написанні звіту використовувати оформлення різними стилями з використанням списків, таблиць та зображень.

Завдання 2: Розробити в Excel таблицю із показниками щодо кількості кібератак у різних регіонах та візуалізувати дані за допомогою графіків і діаграм.

Завдання 3: Розробити рекомендації щодо безпечного використання загальнодоступних мереж Wi-Fi.

Завдання 4: Провести аналіз пошукової видачі в Google за однією з актуальних політичних тем і скласти звіт із оцінкою якості інформації.

Завдання 5: Створити план моніторингу соціальних мереж для виявлення потенційних загроз (наприклад, поширення фейкової інформації).

Завдання 6: Підготувати доповідь про вплив порушення суверенітету держави в кіберпросторі (з прикладами кейсів).

Завдання 7: Створити карту загроз, пов'язаних із кіберзлочинністю, кібертероризмом і кібервійною, із коротким поясненням кожної загрози.

Завдання 8: Створити пам'ятку з правилами кібергігієни для працівників державних установ.

Завдання 9: Провести аналіз кейсу про наслідки нехтування кібергігієною у великій організації (наприклад, атака через фішинг-листи).

8. Методи навчання

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

Результат навчання	Методи навчання
1	2
ПРН 4. Обґрунтовано застосовувати знання з основ теорії національної безпеки, зокрема, оцінювати обстановку, рівень небезпек та загроз національній безпеці, вміти використовувати базовий категорійно-понятійний та аналітично-дослідницький апарат сучасної науки в сфері національної безпеки.	– 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)
ПРН 6. Вміти використовувати інформаційні та комунікаційні технології, сучасні методи інформаційної безпеки та захисту інформації у професійній діяльності, порушення яких може завдати шкоду національним інтересам держави.	– 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)

Результат навчання	Методи навчання
1	2
ПРН 13. Протидіяти інформаційно-психологічним впливам під час адаптації та дій в умовах мирного часу та в особливий період, критично оцінювати достовірність джерел інформації, виявляти дезінформацію та маніпулятивний контент, що може впливати на національну безпеку, використовуючи методи верифікації та фактчекінгу.	– 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)
ПРН 14. Демонструвати уміння виявляти та вирішувати складні спеціалізовані завдання та практичні проблеми у сфері національної безпеки, використовувати аналітичний інструментарій, критичне мислення для формування принципово нових ідей та адаптації до нових безпекових викликів та ситуацій.	– 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)
ПРН 20. Демонструвати розуміння природи тероризму та антитерористичної безпеки, виявляти та прогнозувати ризики терористичних загроз, у межах компетенцій суб'єктів забезпечення національної безпеки приймати участь в організації та здійсненні заходів боротьби з тероризмом.	– 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
ПРН 4. Обґрунтовано застосовувати знання з основ теорії національної безпеки, зокрема, оцінювати обстановку, рівень небезпек та загроз національній безпеці, вміти використовувати базовий категорійно-понятійний та аналітично-дослідницький апарат сучасної науки в сфері національної безпеки.	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, перевірка виконання лабораторних робіт, екзамен
ПРН 6. Вміти використовувати інформаційні та комунікаційні технології, сучасні методи інформаційної безпеки та захисту інформації у професійній діяльності, порушення яких може завдати шкоду національним інтересам держави.	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, перевірка виконання лабораторних робіт, екзамен
ПРН 13. Протидіяти інформаційно-психологічним впливам під час адаптації та дій в умовах мирного часу та в особливий період, критично оцінювати достовірність джерел інформації, виявляти дезінформацію та маніпулятивний контент, що	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, перевірка виконання лабораторних робіт, екзамен

Результат навчання	Методи контролю
може впливати на національну безпеку, використовуючи методи верифікації та фактчекінгу.	
ПРН 14. Демонструвати уміння виявляти та вирішувати складні спеціалізовані завдання та практичні проблеми у сфері національної безпеки, використовувати аналітичний інструментарій, критичне мислення для формування принципово нових ідей та адаптації до нових безпекових викликів та ситуацій.	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, перевірка виконання лабораторних робіт, екзамен
ПРН 20. Демонструвати розуміння природи тероризму та антитерористичної безпеки, виявляти та прогнозувати ризики терористичних загроз, у межах компетенцій суб'єктів забезпечення національної безпеки приймати участь в організації та здійсненні заходів боротьби з тероризмом.	усне опитування, відповіді на проблемні запитання, перевірка виконання домашніх завдань, тестування, перевірка виконання та захист індивідуальних завдань, перевірка виконання лабораторних робіт, екзамен

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, модульний та підсумковий контроль – для здобувачів денної форми навчання;

– поточний та підсумковий контроль – для здобувачів заочної форми навчання.

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.

Модульний контроль проводиться з метою оцінювання результатів навчання здобувачів вищої освіти за модуль (змістові модулі) навчальної дисципліни. Модульний контроль проводиться під час навчального заняття після завершення вивчення матеріалу модуля (змістових модулів) навчальної дисципліни. Модульний контроль здійснюється у формі написання модульної контрольної роботи.

Підсумковий контроль проводиться для підсумкового оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни. Підсумковий контроль здійснюється після завершення вивчення навчальної дисципліни або наприкінці семестру. Підсумковий контроль проводиться у формі екзамену. Процедура складання екзамену 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
Для здобувача денної форми навчання	
Виконання завдань поточного контролю	60
Виконання завдань модульного або підсумкового контролю	40
Підсумкова семестрова оцінка	**100**
Для здобувача заочної форми навчання	
Виконання завдань поточного контролю	60
Виконання завдань підсумкового контролю	40
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	48	48
Виконання та захист індивідуальних самостійних завдань	12	12
Виконання науково-дослідної роботи та інших видів робіт (**додаткові – заохочувальні бали**):	До 20	До 20

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Підготовка наукових статей, тез доповідей наукових конференцій		
Разом за виконання завдань поточного контролю	**60**	**60**

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	34	34
Виконання тестових завдань	14	14
Разом за виконання завдань під час навчальних занять	**48**	**48**

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:

$$Р_{НЗ} = \sum(Р_i \times ВК_i) \times К_{НЗ}, \quad (1)$$

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

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

$ВК_i$ – 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.

Розподіл балів за виконання завдань модульного контролю

Види робіт здобувача вищої освіти денної форми навчання	Кількість балів за семестр
Виконання завдань модульного контролю 1	40
Разом за виконання завдань модульного контролю	**40**

Якщо здобувач вищої освіти денної форми навчання виконав завдання модульного контролю і з урахуванням отриманих балів за поточний контроль набрав у сумі 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 денної форми навчання під час вивчення навчальної дисципліни набрав 60 балів або більше і бажає покращити свій результат успішності, він проходить процедуру підсумкового контролю у формі екзамену. За складання екзамену здобувач вищої освіти може набрати 40 балів. Набрані бали за виконання завдань підсумкового контролю у формі екзамену, а також бали за поточний контроль сумуються і формується семестрова оцінка з

навчальної дисципліни. Бали, які здобувач вищої освіти набрав за виконання завдань модульного контролю, при цьому не враховуються під час розрахунку семестрової оцінки з навчальної дисципліни.

У здобувача вищої освіти заочної форми навчання семестрова оцінка за вивчення навчальної дисципліни формується як сума кількості балів за поточний контроль і кількості балів за підсумковий контроль.

Здобувач вищої освіти допускається до процедури підсумкового контролю у формі екзамену, якщо за виконання завдань поточного контролю набрав 20 балів або більше.

Якщо здобувач вищої освіти за результатами поточного контролю набрав 15–19 балів, він отримує право за власною заявою повторно опанувати окремі теми (змістові модулі) навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми. Повторне 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 14 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 повторно опанувати навчальну дисципліну у наступному семестрі понад обсяги, встановлені навчальним планом освітньої програми.

Процедура надання додаткових освітніх послуг здобувачу вищої освіти з метою повторного вивчення навчальної дисципліни чи її окремих складових частин 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».

Шкала оцінювання

Шкала ЄКТС	Національна шкала	100-бальна шкала
A	Відмінно	90-100
B	Добре	82-89
C		74-81
D	Задовільно	64-73

E		60-63
FX	Незадовільно	35-59
F		0-34

11. Глосарій

№ з/п	Термін державною мовою	Відповідник англійською мовою
1.	Апаратне забезпечення	Hardware
2.	Глобальна мережа	Global network
3.	Дезінформація	Disinformation
4.	Захист документів	Document protection
5.	Зловмисне програмне забезпечення	Malware
6.	Ідентифікація загроз	Threat identification
7.	Інформаційна безпека	Information security
8.	Інформаційна війна	Information warfare
9.	Інформаційна операція	Information operation
10.	Інформаційне протиборство	Information confrontation
11.	Інформаційні технології	Information technology
12.	Інформація	Information
13.	Кібератака	Cyberattack
14.	Кібербезпека	Cybersecurity
15.	Кібервійна	Cyberwar
16.	Кібергігієна	Cyber hygiene
17.	Кіберзлочинність	Cybercrime
18.	Кіберпростір	Cyberspace
19.	Кібертероризм	Cyberterrorism
20.	Комп'ютерна мережа	Computer network
21.	Контрпропаганда	Counterpropaganda
22.	Локальна мережа	Local area network
23.	Операційна система	Operating system
24.	Пошукова система	Search engine
25.	Програмне забезпечення	Software
26.	Пропаганда	Propaganda
27.	Соціальна мережа	Social network
28.	Таблиця	Table
29.	Фейкові новини	Fake news
30.	Фішинг	Phishing
31.	Формула	Equation

12. Рекомендована література

Основна література

1. Dykyi A., Morozov A., Loktikova T., Iefremov I., Zabrodskyy P. 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.

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. Мирошниченко В.О. Використання сучасних інформаційних технологій: формування мультимедійної компетентності. К.: Центр учбової літератури, 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 Kryshtanovych, 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 І Міжнародної науково-практичної конференції "Місцеве 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.

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. Сеник, 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. 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.

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.microsoftelearning.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/

14. Цифрові інструменти

1. Кібергігієна для молоді. URL: https://osvita.diia.gov.ua/courses/cyber-hygiene-for-youth
2. Базові знання з кіергігієни. 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/democracy-through-actions-module-1

8. Демократія через дії. Модуль 2. URL: https://osvita.diia.gov.ua/courses/democracy-through-actions-module-2