ЗАТВЕРДЖЕНО

Вченою радою факультету інформаційно-комп'ютерних технологій

28 08 2024., протокол №8

Голова Вченої ради

_____ Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
ОК29 «Інформаційна безпека та захист ПЗ»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності 126 «Інформаційні системи та технології»
освітньо-професійна програма «Системи бізнес-аналітики»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерних наук

Схвалено на засіданні кафедри комп'ютерної інженерії та кібербезпеки

26 08 2024р., протокол №6

Завідувач кафедри

_____ Андрій ЄФІМЕНКО

Гарант освітньо-професійної програми

_____ Олександра СВІНЦИЦЬКА

Розробники: старший викладач кафедри комп'ютерної інженерії та кібербезпеки Олександра ПОКОТИЛО, старший викладач кафедри комп'ютерної інженерії та кібербезпеки Наталія ЩУР

Житомир
2026 – 2027 н.р.

Робоча програма навчальної дисципліни «Інформаційна безпека та захист ПЗ» для здобувачів вищої освіти освітнього ступеня «бакалавр» спеціальності 126 «Інформаційні системи та технології» освітньо-професійна програма «Системи бізнес-аналітики» затверджена Вченою радою факультету інформаційно-комп’ютерних технологій від 28 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 – 4</td><td>Галузь знань
12 «Інформаційні технології»</td><td colspan="2">Обов’язкова</td></tr>
<tr><td>Модулів – 1</td><td rowspan="5">Спеціальність
126 «Інформаційні системи та технології»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td rowspan="2">Змістових модулів – 2</td><td>3-й</td><td>–</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 120</td><td>6-й</td><td>–</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="11">Тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи – 3,5</td><td rowspan="11">Освітній ступінь «бакалавр»</td><td>32 год.</td><td>–</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>–</td><td>–</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>32 год.</td><td>–</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>56 год.</td><td>–</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">Вид контролю: екзамен</td></tr>
</table>

Частка аудиторних занять і частка самостійної та індивідуальної роботи у загальному обсязі годин з навчальної дисципліни становить:
для денної форми навчання – 53 % аудиторних занять, 47 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою вивчення навчальної дисципліни є вивчення та розуміння сучасних загроз інформаційній безпеці, а також принципів, методів, засобів побудови класичних та сучасних алгоритмів шифрування та методів їх зламу; формування та набуття професійних та предметних компетентностей, практичних знань та вмінь з криптографічного захисту інформаційних ресурсів та криптографічного аналізу.

Завданнями навчальної дисципліни є:
– забезпечення ґрунтовного оволодіння студентами основними поняттями, методами та алгоритмами захисту інформаційних ресурсів;
– формування у студентів предметних та професійних компетентностей, знань та вмінь з теорії та практики криптографічного захисту даних та криптографічного аналізу.

Зміст навчальної дисципліни направлений на формування наступних **компетентностей**, визначених стандартом вищої освіти зі спеціальності 126 «Інформаційні системи та технології»:
КЗ 1. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ 2. Здатність застосовувати знання у практичних ситуаціях.
КЗ 3. Здатність до розуміння предметної області та професійної діяльності.
КЗ 8. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КЗ 10. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
КС 3. Здатність до проектування, розробки, налагодження та вдосконалення системного, комунікаційного та програмно-апаратного забезпечення інформаційних систем та технологій, Інтернету речей (IoT), комп’ютерно-інтегрованих систем та системної мережної структури, управління ними.
КС 4. Здатність проектувати, розробляти та використовувати засоби реалізації інформаційних систем, технологій та інфокомунікацій (методичні, інформаційні, алгоритмічні, технічні, програмні та інші).
КС 5. Здатність оцінювати та враховувати економічні, соціальні, технологічні та екологічні фактори на всіх етапах життєвого циклу інфокомунікаційних систем.

КС 6. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків.
Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів** навчання за спеціальністю 126 «Інформаційні системи та технології»:
ПРН 3. Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій.

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. Криптосистеми із закритим ключем

Тема 1. Основні поняття інформаційної безпеки (КЗ1, КЗ2, КС4, КС5, ПР3)
Загальні відомості про захист інформації в інформаційно-телекомунікаційних системах. Історія розвитку криптології. Цілі, завдання та принципи криптології. Основні поняття та визначення. Класифікація криптографічних систем.

Тема 2. Класичні шифри та їх криптоаналіз (КЗ3, КС4, КС6, ПР3)
Моноалфавітні шифри простої заміни (підстановки), афінні шифри заміни (підстановки). Шифри перестановки. Поліграмні шифри. Поліалфавітні криптосистеми. Методи криптоаналізу класичних шифрів.

Тема 3. Криптографічна стійкість шифрів (КЗ1, КЗ2, КЗ3, КС4, КС5, КС6, ПР3)
Поняття криптографічної стійкості. Теоретична та практична стійкість шифрів. Розсіювання та перемішування. Типи атак на криптосистеми. Абсолютно стійкий шифр.

Тема 4. Потокові симетричні шифри (КЗ1, КЗ2, КЗ3, КС4, КС5, ПР3)
Основні властивості алгоритмів потокового симетричного шифрування даних. Класифікація потокових алгоритмів. Генератори псевдовипадкових послідовностей. Потоковий шифри RC4.

Тема 5. Алгоритм блокового симетричного шифрування DES (КЗ1, КЗ2, КЗ3, КЗ8, КЗ10, КС4, КС5, КС6, ПР3)
Основні властивості алгоритмів блокового симетричного шифрування даних. Мережа Фейстеля. Стандарт блокового симетричного шифрування DES. Безпека DES. Модифікації DES.

Тема 6. Режими шифрування блоків. Шифр IDEA (КЗ1, КЗ2, КЗ3, КЗ8, КЗ10, КС4, КС5, КС6, ПР3)
Режими роботи блокових шифрів: режим простої заміни, режим зв’язування блоків, режим зі зворотнім зв’язком по шифротексту, режим зі зворотнім зв’язком по виходу, режим лічильника. Міжнародний стандарт шифрування IDEA. Порівняльний аналіз DES та IDEA.

Тема 7. Удосконалений стандарт шифрування AES (КЗ1, КЗ2, КЗ3, КЗ8, КЗ10, КС4, КС5, КС6, ПР3)
Математична база алгоритму шифрування даних AES: додавання та множення байтів у полі Галуа. Основні операції при зашифруванні та дешифруванні за алгоритмом AES. Формування раундових ключів.

Тема 8. Національний стандарт шифрування ДСТУ 7624:2014 («Калина») (КЗ1, КЗ2, КЗ3, КЗ8, КЗ10, КС4, КС5, КС6, ПР3)
Етапи шифрування даних за алгоритмом «Калина». Формування допоміжного ключа та раундових (циклових) ключів шифрування. Режими роботи криптографічного алгоритму «Калина». Порівняльний аналіз AES та «Калина».

Змістовий модуль 2. Криптосистеми з відкритим ключем

Тема 9. Основні положення криптографії з відкритим ключем (КЗ1, КЗ2, КС4, КС5, ПР3)

Ідея криптосистеми з відкритим ключем. Поняття односторонньої функції. Математичні основи асиметричних шифрів. Алгоритм рюкзака (криптосистема Меркла-Хелмана). Порівняльний аналіз симетричних та асиметричних алгоритмів.

Тема 10. Асиметричні криптосистеми (КЗ1, КЗ2, КЗ3, КС4, КС5, ПР3)

Алгоритм RSA. Проблема розкладання на множники великих чисел. Алгоритм Ель-Гамаля. Алгоритм обміну ключами Діффі-Хелмана. Проблема дискретного логарифмування.

Тема 11. Криптографічні хеш-функції (КЗ1, КЗ2, КЗ3, КС4, КС5, ПР3)

Поняття хеш-функції та їх основні властивості. Область застосування хеш-функцій. Хеш-функція SHA-256. Хеш-функція «Купина» (ДСТУ 7564:2014). Інші хеш-функції.

Тема 12. Цифровий підпис (КЗ1, КЗ2, КЗ3, КЗ8, КС5, КС6, ПР3)

Принципи забезпечення автентичності даних з використанням цифрового підпису (ЦП). Процедури підписування та перевірки ЦП. Схеми цифрового підпису RSA та Ель-Гамаля. Стандарт цифрового підпису DSS.

Тема 13. Криптографічні протоколи (КЗ1, КЗ2, КЗ3, КС4, КС5, ПР3)

Криптографічні протоколи управління ключами. Криптографічні протоколи автентифікації. Механізми розподілення таємниці. Синтез та аналіз криптографічних протоколів.

Тема 14. Основи криптографії на еліптичних кривих (КЗ1, КЗ2, КЗ3, КС4, КС5, ПР3)

Математичний опис криптографічних еліптичних кривих. Основні операції в групах точок еліптичних кривих. Алгоритм обміну ключами ECDH. Стандарт цифрового підпису ECDSS.

Тема 15. Елементи криптоаналізу сучасних шифрів (КЗ2, КС6, ПР3)

Завдання та принципи криптоаналізу. Диференціальний криптоаналіз. Лінійний криптоаналіз. Інші методи криптоаналізу.

Тема 16. Нові напрямки в криптографії (КЗ1, КЗ2, КЗ3, КС4, КС5, ПР3)

Основи квантового шифрування. Технологія «блокчейн». Програмні засоби

криптографічного захисту даних.

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. Криптосистеми із закритим ключем								
Тема 1. Основні поняття інформаційної безпеки	7	2	1	4	–	–	–	–
Тема 2. Класичні шифри та їх крипоаналіз	10	2	4	4	–	–	–	–
Тема 3. Криптографічна стійкість шифрів	8	2	2	4	–	–	–	–
Тема 4. Потокові симетричні шифри	8	2	2	4	–	–	–	–
Тема 5. Алгоритм блокового симетричного шифрування DES	8	2	2	4	–	–	–	–
Тема 6. Режими шифрування блоків. Шифр IDEA	6	2	2	2	–	–	–	–
Тема 7. Удосконалений стандарт шифрування AES	10	2	4	4	–	–	–	–
Тема 8. Національний стандарт шифрування ДСТУ 7624:2014 («Калина»)	6	2	2	2	–	–	–	–
Модульний контроль 1	1	-	1	-	–	–	–	–
Разом за змістовий модуль 1	64	16	20	28	–	–	–	–
Змістовий модуль 2. Криптосистеми з відкритим ключем								
Тема 9. Основні положення криптографії з відкритим ключем	7	2	1	4	–	–	–	–
Тема 10. Асиметричні криптосистеми	8	2	2	4	–	–	–	–
Тема 11. Криптографічні хеш-функції	5	2	1	4	–	–	–	–
Тема 12. Цифровий підпис	8	2	2	4	–	–	–	–
Тема 13. Криптографічні протоколи	7	2	1	4	–	–	–	–
Тема 14. Основи криптографії на еліптичних кривих	8	2	2	4	–	–	–	–
Тема 15. Елементи криптоаналізу сучасних шифрів	5	2	1	2	–	–	–	–
Тема 16. Нові напрямки в криптографії	7	2	1	2	–	–	–	–
Модульний контроль 2	1	-	1	-	–	–	–	–
Разом за змістовий модуль 2	56	16	12	28	–	–	–	–
ВСЬОГО	120	32	32	56	–	–	–	–

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
Модуль 1			
Змістовий модуль 1. Криптосистеми із закритим ключем			
1	Класичний шифр простої заміни та його криптоаналіз. Біграмний шифр	4	–
2	Класичний шифр поліалфавітної заміни та його криптоаналіз. Криптосистема Хілла	4	–
3	Моделювання процесів шифрування за допомогою шифру одноразового блокноту. Алгоритм DES	4	–
4	Дослідження властивостей блокового симетричного шифру AES	4	–
5	Дослідження основних операцій шифру «Калина» у процесі формування допоміжного ключа	3	–
	Модульна контрольна робота №1	1	
Змістовий модуль 2. Криптосистеми з відкритим ключем			
6	Асиметричні шифри RSA та Ель-Гамаля. Алгоритм обміну ключами Діффі-Хелмана	4	–
7	Хеш-функції. Цифровий підпис	3	–
8	Криптографічні перетворення в групах точок еліптичних кривих	4	–
	Модульна контрольна робота №2	1	
	РАЗОМ	32	–

6. Завдання для самостійної роботи

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
Модуль 1			
Змістовий модуль 1. Криптосистеми із закритим ключем			
1	**Тема 1. Основні поняття інформаційної безпеки** 1. Математична модель шифрів, теорія зв'язку в секретних системах Клода Шенона. 2. Законодавча база України в галузі криптографії.	4	–
2	**Тема 2. Класичні шифри та їх криптоаналіз** 1. Взаємний індекс збігу. 2. Роторні шифрувальні машини та їх криптоаналіз.	4	–
3	**Тема 3. Криптографічна стійкість шифрів**	4	–

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
	1. Модель порушника. 2. Методи та види несанкціонованого доступу.		
4	**Тема 4. Потокові симетричні шифри** 1. Порівняльний аналіз генераторів псевдовипадкових послідовностей. 2. Потоковий шифр SNOW 2.0. 3. Потоковий шифр Salsa 20.	4	–
5	**Тема 5. Алгоритм блокового симетричного шифрування DES** 1. Алгоритм шифрування Lucifer. 2. Способи доповнення блоків (padding).	4	–
6	**Тема 6. Режими шифрування блоків. Шифр IDEA** 1. Режим зв’язування блоків із поширенням (PCBC). 2. Безпека IDEA.	2	–
7	**Тема 7. Удосконалений стандарт шифрування AES** 1. Алгоритми-фіналісти конкурсу AES: MARS, RC6, Serpent, Twofish. 2. Режими шифрування AES.	4	–
8	**Тема 8. Національний стандарт шифрування ДСТУ 7624:2014 («Калина»)** 1. Стандарт криптографічного перетворення даних ДСТУ ГОСТ 28147:2009. 2. Порівняльний аналіз ДСТУ ГОСТ 28147:2009 та ДСТУ 7624:2014 («Калина»).	2	–
Змістовий модуль 2. Криптосистеми з відкритим ключем			
9	**Тема 9. Основні положення криптографії з відкритим ключем** 1. Основи модулярної арифметики. 2. Поняття і властивості алгебраїчних груп. 3. Тестування чисел на простоту.	4	–
10	**Тема 10. Асиметричні криптосистеми** 1. Головоломка Меркла. 2. Криптосистема Рабіна. 3. Джерела ключів асиметричних криптосистем та вимоги до них.	4	–
11	**Тема 11. Криптографічні хеш-функції** 1. Хеш-функції на основі блокових шифрів. MAC-коди. 2. Порівняльний аналіз хеш-функцій MD2, MD4, MD5 та MD6.	4	–
12	**Тема 12. Цифровий підпис** 1. Правове регулювання ЦП в Україні та світі. 2. Алгоритм цифрового підпису Шнорра. 3. Сліпий підпис, незаперечний підпис, груповий підпис.	4	–
13	**Тема 13. Криптографічні протоколи** 1. Вимоги до протоколів автентифікації. 2. Модель загроз порушення автентичності. 3. Модель взаємної недовіри та взаємного захисту	4	–

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
14	**Тема 14. Основи криптографії на еліптичних кривих** 1. Алгоритм обчислення порядку еліптичної кривої. 2. Криптосистема Мессі-Омури над групою точок еліптичної кривої. 3. Аналіз вразливостей криптографічної схеми ЦП ECDSA.	4	–
15	**Тема 15. Елементи криптоаналізу шифрів** 1. Силові методи криптоаналізу. 2. Криптоаналіз по побічним каналам.	2	–
16	**Тема 16. Нові напрямки в криптографії** 1. Стеганографія та її застосування. 2. Квантовий криптоаналіз.	2	–
	РАЗОМ	**56**	–

7. Індивідуальні самостійні завдання

Індивідуальні завдання не передбачені навчальним планом.

8. Методи навчання

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

Результат навчання	Методи навчання
ПРН 3. Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп’ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп’ютерних програм мовами високого рівня із застосуванням об’єктно-орієнтованого програмування для розв’язання задач проектування і використання інформаційних систем та технологій.	Вербальні (лекція, пояснення); наочні (демонстрація, ілюстрація); практичні (різні види завдань на лабораторних роботах); метод активного навчання (командна робота).

9. Методи контролю

Перевірка досягнення програмних результатів навчання здійснюється з використанням наступних методів.

Результат навчання	Методи контролю
ПРН 3. Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп’ютерних мережах, методи	Перевірка виконання та захист лабораторних робіт, експрес-тестування,

Результат навчання	Методи контролю
створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій.	перевірка виконанн модульного контролю, 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.

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 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	
	денна форма	заочна форма
Виконання завдань поточного контролю	60	-
Виконання завдань модульного 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	60	–
Виконання та захист індивідуальних самостійних завдань	-	–
Виконання науково-дослідної роботи та інших видів робіт (**додаткові – заохочувальні бали**): 1. Участь у студентських предметних олімпіадах, Всеукраїнському конкурсі студентських наукових робіт, грантах, науково-дослідних проектах 2. Підготовка наукових статей, тез доповідей наукових конференцій 3. Інші види робіт (наводиться перелік інших видів робіт)	до 20	–
Разом за виконання завдань поточного контролю	**60**	–

Розподіл балів за виконання завдань під час навчальних занять

Види робіт здобувача вищої освіти[1]	Кількість балів за семестр	
	денна форма	заочна форма
Виконання тестових завдань	12	–
Виконання завдань на заняттях	16	–
Виконання та захист лабораторних робіт	32	–
Разом за виконання завдань під час навчальних занять	**60**	–

З метою застосування цілих чисел для оцінювання результатів роботи здобувачів вищої освіти під час навчальних занять протягом семестру використовується 100-бальна шкала оцінювання кожного окремо виду робіт. Розрахунок набраних здобувачем вищої освіти балів за виконання завдань під час навчальних занять за семестр проводиться за формулою:

$$Р_{НЗ} = (Р_{В100} \times ВК_{В} + Р_{УД100} \times ВК_{УД} + Р_{...} \times ВК_{...}) \times К_{НЗ}, \quad (1)$$

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

$Р_{В100}$, $Р_{УД100}$, $Р_{...}$ – кількість набраних здобувачем вищої освіти балів за семестр відповідно за відповіді (виступи) на заняттях, за участь у дискусії, за виконання іншого виду робіт, визначеного викладачем (кожний окремо вид робіт на навчальних заняттях оцінюється за 100-бальною шкалою);

$Р_{ТЗ100}$, $Р_{ЗЗ100}$, $Р_{ЛР100}$ – кількість набраних здобувачем балів за семестр за виконання тестових завдань, завдань на заняттях, виконання та захист лабораторних робіт (за 100-бальною шкалою);

$ВК_{ТЗ}$, $ВК_{ЗЗ}$, $ВК_{ЛР}$ – ваговий коефіцієнт за виконання тестових завдань, завдань на заняттях, виконання та захист лабораторних робіт. Значення вагових коефіцієнтів становить:

$ВК_{ТЗ} = 12 \div 60 = 0,2$;

$ВК_{ЗЗ} = 16 \div 60 = 0,27$;

$ВК_{ЛР} = 32 \div 60 = 0,53$;

$К_{НЗ}$ – коригувальний коефіцієнт. Значення коригувального коефіцієнту для здобувачів денної форми навчання становить: $К_{НЗ} = 60 \div 100 = 0,6$.

Розподіл балів за виконання завдань модульного контролю

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання завдань модульного контролю 1	20	–
Виконання завдань модульного контролю 2	20	–
Разом за виконання завдань модульного контролю	**40**	–

Якщо здобувач вищої освіти 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 під час вивчення навчальної дисципліни набрав 60 балів або більше і бажає покращити свій результат успішності, він проходить процедуру підсумкового контролю у формі екзамену. Набрані бали за виконання завдань підсумкового контролю, 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.

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

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

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках окремих тем навчальної дисципліни, здійснюється викладачем за зверненням здобувача вищої освіти та представленням документів, які підтверджують результати навчання (сертифікати, свідоцтва, скріншоти тощо). Рішення про визнання та оцінка за відповідну частину освітнього компонента приймається викладачем за результатами співбесіди зі здобувачем вищої освіти.
Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках цілого освітнього компонента, здійснюється за процедурою, яка визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

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	Асиметричне шифрування	Asymmetric encryption
2	Атака на криптосистему	Cryptosystem attack
3	Атака на протокол	Protocol attack
4	Аутентифікація	Authentication
5	Багатофакторна аутентифікація	Multi-factor authentication
6	Блоковий шифр	Block cipher
7	Відкритий текст	Plaintext
8	Еліптичні криві	Elliptic curves
9	Електронний підпис	Digital signature
10	Зашифрований текст	Ciphertext
11	Квантова криптографія	Quantum cryptography
12	Конфіденційність	Confidentiality
13	Криптографічний алгоритм	Cryptographic algorithm
14	Криптографічний протокол	Cryptographic protocol
15	Криптографія	Cryptography
16	Криптоаналіз	Cryptanalysis
17	Потоковий шифр	Stream cipher
18	Приватний ключ	Private key
19	Публічний ключ	Public key
20	Розшифрування	Decryption
21	Сертифікат безпеки	Security certificate
22	Симетричне шифрування	Symmetric encryption
23	Стеганографія	Steganography
24	Хешування	Hashing
25	Шифрування	Encryption

12. Рекомендована література

Основна література

1. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч.посібник/ Г. Л. Козіна. – Запоріжжя : НУ «Запорізька політехніка», 2020. – 192 с.
2. Гребенніков В.В.. Історія криптології та секретного зв’язку / В.В. Гребенніков., 2024. – 800 с.
3. Криптологія: навч. посібник / М.Н. Курко, П.М. Лісовський, Ю.П. Лісовська. — К.: Видавничий дім «Кондор», 2020. — 248 с.
4. Євсеєв С.П., Мілов О.В., Король О.Г. Кібербезпека: лабораторний практикум з основ криптографічного захисту. Навчальний посібник. – Львів: «Новий Світ-2000», 2021. – 241 с.

5. Wenliang Du. Computer & Internet Security: A Hands-on Approach 3rd ed. Edition. - Wenliang Du, 2022. - 725 p.
6. Wong D. Real-World Cryptography. - Manning, 2021. - 400 p.
7. Mihailescu M. I. Pro Cryptography and Cryptanalysis: Creating Advanced Algorithms with C# and .NET 1st ed. Edition.- Stefania Loredana Nita, 2020. - 588 p.
8. Katz J., Lindell Y. Introduction to Modern Cryptography, Third Edition (Chapman & Hall/Crc Cryptography and Network Security). - CRC PR INC, 2020. - 650 p.

Допоміжна література

1. ДСТУ 7624:2014. Алгоритм симетричного блокового перетворення.
2. ДСТУ 7564:2014. Функція хешування.
3. ДСТУ 8845:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення.
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
5. Закон України «Про основні засади забезпечення кібербезпеки України».

13. Інформаційні ресурси в Інтернеті

1. The CrypTool Portal [Електронний ресурс]. — Режим доступу : http://www.cryptool.org/en
2. CrypTool-Online [Електронний ресурс]. – Режим доступу: https://www.cryptool.org/en/cto/
3. GnuPG [Електронний ресурс]. – Режим доступу: http://www.gnupg.org