

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015		Ф-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1 Арк 19 / 1

ЗАТВЕРДЖЕНО

Вченою радою факультету
інформаційно-комп'ютерних
технологій

28 серпня 2024 р., 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 122 «Комп'ютерні науки»
освітньо-професійна програма «Комп'ютерна графіка та розробка ігор»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерних наук


Схвалено на засіданні кафедри
комп'ютерної інженерії та
кібербезпеки

26 08 2024 р., протокол № 6

Завідувач кафедри

 Андрій ЄФІМЕНКО

Гарант освітньо-професійної
програми

 Юрій БРОДСЬКИЙ

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.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	<i>Випуск 1</i>	<i>Зміни 0</i>	<i>Екземпляр № 1</i>	<i>Арк 19 / 2</i>

Робоча програма навчальної дисципліни «Інформаційна безпека та захист ПЗ» для здобувачів вищої освіти освітнього ступеня «бакалавр» спеціальності 122 «Комп'ютерні науки» освітньо-професійна програма «Комп'ютерна графіка та розробка ігор» затверджена Вченою радою факультету інформаційно- комп'ютерних технологій від 28 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-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 19 / 3

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, освітній ступінь	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів – 4	Галузь знань 12 «Інформаційні технології»	Обов'язкова	
Модулів – 1	Спеціальність 122 «Комп'ютерні науки»	Рік підготовки:	
Змістових модулів – 2		3-й	–
Загальна кількість годин – 120		Семестр	
		6-й	–
Тижневих годин для денної форми навчання: аудиторних – 4 самостійної роботи – 3,5	Освітній ступінь «бакалавр»	Лекції	
		32 год.	–
		Практичні	
		–	–
		Лабораторні	
		32 год.	–
		Самостійна робота	
56 год.	–		
		Вид контролю: екзамен	

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.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 19 / 4

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 122 «Комп'ютерні науки» та освітньо-професійною програмою «Комп'ютерна графіка та розробка ігор»:

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК2. Здатність застосовувати знання у практичних ситуаціях.

ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК8. Здатність генерувати нові ідеї (креативність).

СК11. Здатність до інтелектуального аналізу даних на основі методів обчислювального інтелекту включно з великими та погано структурованими даними, їхньої оперативної обробки та візуалізації результатів аналізу в процесі розв'язування прикладних задач.

СК15. Здатність до аналізу та функціонального моделювання бізнес-процесів, побудови та практичного застосування функціональних моделей організаційно-економічних і виробничо-технічних систем, методів оцінювання ризиків їх проектування.

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів** навчання за спеціальністю 122 «Комп'ютерні науки» та освітньо-професійною програмою «Комп'ютерна графіка та розробка ігор»:

ПРН13. Володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп'ютерних систем,

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 19 / 5

знати мережні технології, архітектури комп'ютерних мереж, мати практичні навички технології адміністрування комп'ютерних мереж та їх програмного забезпечення.

ПРН16. Розуміти концепцію інформаційної безпеки, принципи безпечного проєктування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

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 (ЗК1, ЗК2, ПРН16)

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 (ЗК1, ЗК2, ПРН16)

Моноалфавітні шифри простої заміни (підстановки), афінні шифри заміни (підстановки). Шифри перестановки. Поліграмні шифри. Поліалфавітні криптосистеми. Методи криптоаналізу класичних шифрів.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 19 / 6

Тема 3. Криптографічна стійкість шифрів (ЗК1, ЗК2, ЗК4, ЗК8, ПРН13, ПРН16)

Поняття криптографічної стійкості. Теоретична та практична стійкість шифрів. Розсіювання та перемішування. Типи атак на криптосистеми. Абсолютно стійкий шифр.

Тема 4. Потоківі симетричні шифри (ЗК4, ЗК8, ПРН13, ПРН16)

Основні властивості алгоритмів поточкового симетричного шифрування даних. Класифікація поточкових алгоритмів. Генератори псевдовипадкових послідовностей. Поточковий шифри RC4.

Тема 5. Алгоритм блокового симетричного шифрування DES (ЗК1, ЗК2, СК11, СК15, ПРН13, ПРН16)

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 (ЗК2, СК11, ПРН16)

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 (ЗК1, ЗК2, СК11, СК15, ПРН13, ПРН16)

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») (ЗК1, ЗК2, ЗК4, ЗК8, СК11, СК15, ПРН13, ПРН16)

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 (ЗК1, ЗК2, ЗК4, ЗК8, СК11, СК15, ПРН13, ПРН16)

Ідея криптосистеми з відкритим ключем. Поняття односторонньої

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 19 / 7

функції. Математичні основи асиметричних шифрів. Алгоритм рюкзака (криптосистема Меркла-Хелмана). Порівняльний аналіз симетричних та асиметричних алгоритмів.

Тема 10. Асиметричні криптосистеми (ЗК1, ЗК2, СК11, ПРН13, ПРН16)

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

Тема 11. Криптографічні хеш-функції (ЗК1, ЗК2, СК11, ПРН16)

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 (ЗК1, ЗК8, СК11, ПРН13, ПРН16)

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

Тема 13. Криптографічні протоколи (ЗК1, ЗК2, ЗК4, СК15, ПРН13, ПРН16)

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

Тема 14. Основи криптографії на еліптичних кривих (ЗК1, ЗК2, ЗК4, ЗК8, СК11, СК15, ПРН13, ПРН16)

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 (ЗК1, ЗК2, ЗК4, ЗК8, СК11, СК15, ПРН13, ПРН16)

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

Тема 16. Нові напрямки в криптографії (ЗК1, ЗК2, СК11, ПРН13, ПРН16)

Основи квантового шифрування. Технологія «блокчейн». Програмні засоби криптографічного захисту даних.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 19 / 8

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин							
	денна форма				заочна форма			
	у с ь о г о	л е к ц і ї	л а б о р а т о р н і	с а м о с т і й н а р о б о т а	у с ь о г о	л е к ц і ї	л а б о р а т о р н і	с а м о с т і й н а р о б о т а
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 криптоаналіз	10	2	4	4	-	-	-	-
Тема 3. Криптографічна стійкість шифрів	8	2	2	4	-	-	-	-
Тема 4. Потоківі 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	5	2	1	2	-	-	-	-

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	<i>Випуск 1</i>	<i>Зміни 0</i>	<i>Екземпляр № 1</i>	<i>Арк 19 / 9</i>

шифрів								
Тема 16. Нові напрямки в криптографії	7	2	1	2	-	-	-	-
Модульний контроль 2	1	-	1	-	-	-	-	-
<i>Разом за змістовий модуль 2</i>	56	16	12	28	-	-	-	-
ВСЬОГО	120	32	32	56	-	-	-	-

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 19 / 10

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	–
	Модульний контроль 1	1	–
Змістовий модуль 2. Криптосистеми з відкритим ключем			
6	Асиметричні шифри RSA та Ель-Гамала. Алгоритм обміну ключами Діффі-Хелмана	4	–
7	Хеш-функції. Цифровий підпис	3	–
8	Криптографічні перетворення в групах точок еліптичних кривих	4	–
	Модульний контроль 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 1. Модель порушника. 2. Методи та види несанкціонованого доступу.	4	–

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 19 / 11

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
4	Тема 4. Поточкові симетричні шифри 1. Порівняльний аналіз генераторів псевдовипадкових послідовностей. 2. Поточковий шифр SNOW 2.0. 3. Поточковий 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	4	–

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 19 / 12

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
	1. Вимоги до протоколів автентифікації. 2. Модель загроз порушення автентичності. 3. Модель взаємної недовіри та взаємного захисту		
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. Силкові 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 13. Володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп'ютерних систем, знати мережні технології, архітектури комп'ютерних мереж, мати практичні навички технології адміністрування комп'ютерних мереж та їх програмного забезпечення.	Вербальні (лекція, пояснення); наочні (демонстрація, ілюстрація); практичні (різні види завдань на лабораторних роботах); метод активного навчання (командна робота).
ПРН 16. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.	Вербальні (лекція, пояснення); наочні (демонстрація, ілюстрація); практичні (різні види завдань на лабораторних роботах);

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 19 / 13

Результат навчання	Методи навчання
	метод активного навчання (командна робота).

9. Методи контролю

Перевірка досягнення програмних результатів навчання здійснюється з використанням наступних методів.

Результат навчання	Методи контролю
ПРН 13. Володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп'ютерних систем, знати мережні технології, архітектури комп'ютерних мереж, мати практичні навички технології адміністрування комп'ютерних мереж та їх програмного забезпечення.	Перевірка виконання та захист лабораторних робіт, експрес-тестування, перевірка виконання завдань модульного контролю, екзамен.
ПРН 16. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.	Перевірка виконання та захист лабораторних робіт, експрес-тестування, перевірка виконання завдань 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)

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 19 / 14

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	0	–
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	–

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 19 / 15

Разом за виконання завдань під час навчальних занять	60	–
-------------------------------------------------------------	-----------	---

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

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

де $P_{\text{в}}$ – 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 занять, на сумарну кількість балів за виконання усіх видів робіт під час навчальних занять за семестр;

$K_{\text{в}}$ – 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	Кількість балів за семестр
	денна форма
Виконання завдань модульного контролю за змістовий модуль 1	20
Виконання завдань модульного контролю за змістовий модуль 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. 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

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 19 / 16

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 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».

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 19 / 17

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

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 19 / 18

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.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01 122.00.1/Б/ ОК29-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 19 / 19

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>