

Державний вищий навчальний заклад
«Донбаський державний педагогічний університет»
Фізико-математичний факультет

Кафедра методики навчання математики та методики навчання інформатики

«ЗАТВЕРДЖЕНО»

Перший проректор



Набока
С. Набока

«27» червня 2022 р.

**РОБОЧА ПРОГРАМА
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

ПРИКЛАДНА КРИПТОЛОГІЯ

**підготовки здобувачів
першого (бакалаврського) рівня вищої освіти**

спеціальності	014 Середня освіта (Інформатика)
за освітньо-професійною програмою	Середня освіта (Інформатика)
мова навчання	Українська

Розробник:

Кайдан Н.В. кандидат фізико-математичних наук, доцент, доцент кафедри методики навчання математики та методики навчання інформатики ДВНЗ «Донбаський державний педагогічний університет».

Рецензенти:

Величко В.Є. кандидат фізико-математичних наук, доцент, доцент кафедри методики навчання математики та методики навчання інформатики ДВНЗ «Донбаський державний педагогічний університет».

Кадубовський О.А. кандидат фізико-математичних наук, доцент, доцент кафедри математики та інформатики ДВНЗ «Донбаський державний педагогічний університет».

Робоча програма розглянута і схвалена на засіданні кафедри методики навчання математики та методики навчання інформатики.

Протокол № 11 від «23» червня 2022 р.

Завідувач кафедри методики навчання математики та методики навчання інформатики _____ доц. Величко В.Є.

Погоджено групою забезпечення спеціальності 014 Середня освіта (Інформатика)

Керівник групи забезпечення
кандидат фізико-математичних наук



доц. Стьопкін А.В.

Затверджено та рекомендовано до впровадження вченою радою
Державного вищого навчального закладу
«Донбаський державний педагогічний університет»
«27» червня 2022 р., протокол № 9

1. Опис навчальної дисципліни

Найменування показників	Характеристика навчальної дисципліни
	денна форма навчання
Кількість кредитів – 3	Вибіркова
Загальна кількість годин – 90	Рік підготовки:
	3-й
	Семестр
	6-й
Тижневих годин для денної форми навчання: контактних – 3 самостійної роботи здобувача – 2	Лекції
	24 год.
	Лабораторні
	24 год.
	Самостійна робота
	42 год.
	Вид контролю:
залік	

Метою вивчення дисципліни «Прикладна криптологія» є: ознайомлення з основами теорії криптології; придбання навичок в практичному використанні, постановці і вирішенні задач шифрування інформації; розуміння суті інформаційних процесів в криптографічних системах; застосування комп'ютерів для вирішення завдань шифрування і дешифрування; розробка і використання математичних і обчислювальних моделей процесів шифрування інформації, їх оптимізація та вироблення напрямків вдосконалення.

2. Матриця результатів навчання, методів навчання, методів контролю з навчальної дисципліни

«Прикладна криптологія»

Результати навчання	Методи навчання	Методи контролю
<p>Демонструє знання з основних розділів інформатики.</p> <p>Уміє розробляти алгоритми розв'язування задач з інформатики, аналізувати складність й ефективність алгоритмів; реалізовувати алгоритми мовами програмування; обирати та застосовувати програмне забезпечення для розв'язання прикладних задач.</p> <p>Уміє застосовувати інформаційні та телекомунікаційні технології на уроці, у позакласній і позашкільній роботі.</p> <p>Уміє організовувати діяльність учнів на уроці із дотриманням правил і рекомендацій щодо здоров'язбереження школярів; впроваджувати засоби та методи захисту інформації та безпеки в мережі Інтернет.</p>	<p>Поєднання традиційних та інтерактивних методів навчання з використанням інноваційних технологій:</p> <ul style="list-style-type: none">- словесні методи: лекція, диспут, дискусія;- наочні методи: спостереження, демонстрація; <p>практичні методи: обробка довідкової інформації, тезування, рецензування, аналіз.</p>	<p>Спостереження за навчальною діяльністю здобувачів, усне та письмове опитування, практична перевірка, рейтинговий контроль, оцінювання самостійної роботи, доповіді презентації, контрольна робота, залік.</p>

3. Структура навчальної дисципліни

Назви тем	Кількість годин			
	Денна форма			
	усього	зокрема		
л		лб	с.р.	
Тема 1. Відомості з теорії чисел та математичні основи криптології.	14	4	4	6
Тема 2. Основні поняття та визначення криптології. Криптографія та криптоаналіз.	12	3	3	6
Тема 3. Традиційні шифри.	12	3	3	6
Тема 4. Принципи побудови сучасних блокових шифрів.	14	4	4	6
Тема 5. Потоккові шифри.	12	3	3	6
Тема 6. Стандарт симетричного алгоритму блокового шифрування даних DES.	12	3	3	6
Тема 7. Режими виконання алгоритмів блокового симетричного шифрування даних.	14	4	4	6
Усього годин	90	24	24	42

4. Програма навчальної дисципліни

4.1. Теми лекцій

№ з/п	Назва теми	Кількість годин
1.	Відомості з теорії чисел та математичні основи криптології. Складність арифметичних дій. Алгоритм Евкліда. Функція Ейлера.	4
2.	Основні поняття та визначення криптології. Криптографія та криптоаналіз.	3
3.	Традиційні шифри.	3
4.	Принципи побудови сучасних блокових шифрів.	4
5.	Потокові шифри.	3
6.	Стандарт симетричного алгоритму блокового шифрування даних DES.	3
7.	Режими виконання алгоритмів блокового симетричного шифрування даних.	4
Разом		24

4.2. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1.	Алгоритм Евкліда. Функція Ейлера. (Розв'язування типових задач)	4
2.	Криптографія та криптоаналіз. (Розв'язування типових задач)	3
3.	Традиційні шифри. (Розв'язування типових задач, аналіз алгоритмів)	3
4.	Сучасні блокові шифри. (Розв'язування типових задач, аналіз алгоритмів)	4
5.	Потокові шифри. (Розв'язування типових задач). Контрольна робота	3
6.	Симетричний алгоритм блокового шифрування даних DES. (Розв'язування типових задач, аналіз алгоритмів)	3
7.	Алгоритми блокового симетричного шифрування даних. (Розв'язування типових задач)	4
Разом		24

4.3. Самостійна робота

№ з/п	Назва теми	Кількість годин
1.	Відомості з теорії чисел та математичні основи криптології. Складність арифметичних дій. (Опорний конспект, диктант)	6
2.	Криптографія та криптоаналіз. (Опорний конспект, груповий проєкт)	6
3.	Традиційні шифри. (Опорний конспект, нетипові задачі)	6
4.	Принципи побудови сучасних блокових шифрів. (Опорний конспект, написання програм)	6
5.	Потокові шифри. (Опорний конспект, написання програм)	6
6.	Стандарт симетричного алгоритму блокового шифрування даних DES. (Опорний конспект, аналіз алгоритму)	6
7.	Режими виконання алгоритмів блокового симетричного шифрування даних. (Опорний конспект, аналіз алгоритму)	6
Разом		42

5. Критерії оцінювання результатів навчання

Навчальна дисципліна викладається один семестр та оцінюється максимальною оцінкою у 100 балів.

Оцінювання здійснюється у вигляді поточного контролю знань, оцінювання лабораторних та самостійних робіт. Кожен здобувач може ознайомитись з розподілом балів за всі види роботи впродовж семестру (зокрема, в дистанційному курсі).

Результати поточного контролю рівня знань здобувачів (кількість отриманих балів) обов'язково доводяться викладачем наприкінці кожного заняття до відома всіх здобувачів і виставляються в «Журнал обліку поточної успішності та відвідування занять».

Робота під час лабораторного заняття оцінюється за наступними критеріями:

- опитування – повнота та ґрунтовність відповіді на задане запитання з теми заняття;
- виконання ситуаційних вправ і завдань – за запропонований алгоритм виконання завдання; за знання теоретичних основ проблеми, порушеної в завданні; за володіння формулами та математичними методами, необхідними для виконання завдання; за отриманий правильний результат.

У разі відсутності на лабораторному занятті здобувач вищої освіти повинен самостійно виконати роботу та надати для перевірки.

При проведенні форм контролю знань максимально встановлений бал за кожною з тем може бути знижено у наступних випадках:

- за неповний розв'язок завдання;
- за кожну неправильну відповідь;
- за наявність помилок;
- за несвоєчасне виконання завдання;
- за недостовірність поданої інформації;
- за недостатнє розкриття теми;
- за відсутність обґрунтувань та висновків;
- за порушення академічної доброчесності.

Розподіл балів за темами

Тема	Практичні заняття	Самостійна робота	Залік
Тема 1.	7	7	0
Тема 2.	7	7	
Тема 3.	7	7	
Тема 4.	7	7	
Тема 5.	7	7	
Тема 6.	7	7	
Тема 7.	8	8	
Разом	50	50	100

Для визначення критеріїв оцінювання для отримання заліку потрібно зважати на такі загальні положення:

на оцінку «зараховано» (60-100 балів) заслуговує здобувач вищої освіти, який за час відвідування лекційних, практичних та/або лабораторних занять й за виконану самостійну роботу отримав зазначену кількість балів протягом семестру;

оцінка «не зараховано» (0-59 балів) виставляється здобувачеві вищої освіти, який за час відвідування лекційних, практичних та/або лабораторних занять й за виконану самостійну роботу не набрав 60 балів упродовж семестру, він має прогалини в знаннях основного навчально-програмного матеріалу.

Шкала оцінювання результатів навчання здобувачів вищої освіти		
За накопичувальною 100 - бальною шкалою	За національною шкалою	
	<i>для екзаменів, звітів з практики, курсових робіт</i>	<i>для заліків</i>
90 - 100 балів	відмінно	зараховано
75 - 89 балів	добре	
60 - 74 балів	задовільно	
26 - 59 балів	незадовільно	не зараховано
0 - 25 балів	неприйнятно	

6. Засоби діагностики результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни є:

- груповий проєкт;
- індивідуальні завдання;
- залік.

7. Рекомендована література

Основна

1. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Харків. Форт. 2018 , 593с.
2. Дрозденко В.О. Вища математика: необхідний теоретичний мінімум: навч. посіб. В.О. Дрозденко, О.Л. Дрозденко Б.: Пшонківський О.В., 2020. 264 с.
3. Іваночко С.Г. Криптологія. Львів: Національний Університет Львівська Політехніка, 2018. 46 с.
4. Інформаційна безпека: навч. посіб. / Ю. Я. Бобало [та ін.] ; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого ; Нац. ун-т "Львів. політехніка". - Львів : Вид-во Львів. політехніки, 2019. – 573 с.
5. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч.посібник / Г.Л. Козіна. – Запоріжжя : НУ «Запорізька політехніка», 2020. – 192 с
6. Методичні вказівки до виконання лабораторних робіт з дисципліни “Прикладна криптографія” для студентів спеціальності 125 «Кібербезпека» усіх форм

навчання / Укл.: Г.Л.Козіна. – Запоріжжя: НУ «Запорізька політехніка», 2019. – 34 с. <https://cutt.ly/6Yio41f>

7. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.

Додаткова

1. Безущак О.О, Ганюшкін О.Г., Кочубінська Є.А. Навчальний посібник з лінійної алгебри для студентів механіко-математичного факультету. – К. : ВПЦ «Київський університет», 2019. – 224 с.
2. Дискретна математика. Теорія множин і відношень. Комбінаторика. Числення висловлювань: навч. посіб. / Н. П. Тменова ; Київ. нац. ун-т ім. Тараса Шевченка. - Київ : Київський університет, 2018. - 103 с.
3. Когут Ю. І. Корпоративна безпека: практичний посібник. Консалтингова компанія «СІДКОН», 2021. – 460 с.
4. Лісовська Ю. Інформаційна безпека України: навч. посіб., Кондор, 2018. – 172 с.
5. Он-лайн підручник з криптографії. Режим доступу: <https://cutt.ly/vYii7HQ>

8. Інформаційні ресурси в Інтернеті

1. Криптографія на Python: <https://habr.com/en/post/265309/>
2. Математичний партнер. Режим доступу: <http://mathpar.com/>
3. Основи криптології. Режим доступу: <https://cutt.ly/jYiiH7O>
4. Основні поняття кріптології: <https://cutt.ly/zYiiDQ8>
5. Порівняння симетричних та асиметричних криптосистем: <https://cutt.ly/SYiiBKп>
6. Шифрування у Python: <https://python-scripts.com/encryption-cryptography>

9. Посилання на дистанційний курс

Дистанційний курс дисципліни на освітньому контенті в CMS Moodle <http://212.3.125.77:9090/moodle/course/view.php?id=1649>