Державний вищий навчальний заклад
«Донбаський державний педагогічний університет»

Факультет **фізико-математичний**

Кафедра **методики навчання математики та методики навчання інформатики**

«ЗАТВЕРДЖУЮ»:
Перший проректор _____
_____ Набока О.Г.
(ПІБ)
«30» квітня 2021 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Математичні основи криптології

підготовки здобувачів
першого (бакалаврського) рівня вищої освіти

спеціальності *014 Середня освіта (Інформатика)*
(шифр і назва спеціальності)
за освітньо-професійною програмою *Середня освіта (Інформатика)*
(назва програми)
мова навчання *українська*

Слов'янськ – 2021 р.

Розробник:

Кайдан Н.В. кандидат фізико-математичних наук, доцент, доцент кафедри методики навчання математики та методики навчання інформатики

Рецензенти:

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

Кадубовський О.А. кандидат фізико-математичних наук, доцент, доцент кафедри математики та інформатики ДВНЗ «ДДПУ»

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

Протокол № 1 від «30» серпня 2021 р.

Завідувач кафедри _____ **В.Є. Величко**

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»

«30» серпня 2021 р.,
протокол № 1

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td></tr>
<tr><td>Кількість кредитів – 3</td><td>Вибіркова</td></tr>
<tr><td rowspan="5">Загальна кількість годин – 90</td><td>Рік підготовки:</td></tr>
<tr><td>3-й</td></tr>
<tr><td>Семестр</td></tr>
<tr><td>6-й</td></tr>
<tr><td>Лекції</td></tr>
<tr><td rowspan="7">Тижневих годин для денної форми навчання:
контактних – 2,8
самостійної роботи здобувача – 2,5</td><td>24 год.</td></tr>
<tr><td>Лабораторні</td></tr>
<tr><td>24 год.</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>42 год.</td></tr>
<tr><td>Вид контролю:</td></tr>
<tr><td>залік</td></tr>
</table>

Метою вивчення дисципліни «Математичні основи криптології» є: ознайомлення з математичними 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

«Математичні основи криптології»

Результати навчання	Методи навчання	Методи контролю
Демонструє знання з основних розділів інформатики. 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. Уміє застосовувати інформаційні та телекомунікаційні технології на уроці, у позакласній і позашкільній роботі. 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.	Поєднання традиційних та інтерактивних методів навчання з використанням інноваційних технологій: - словесні методи: лекція, диспут, дискусія; - наочні методи: спостереження, демонстрація; практичні методи: обробка довідкової інформації, тезування, рецензування, аналіз.	Спостереження за навчальною діяльністю здобувачів, усне та письмове опитування, практична перевірка, рейтинговий контроль, оцінювання самостійної роботи, доповіді презентації, контрольна роботи, залік.

3. Структура навчальної дисципліни

Назви тем	Кількість годин			
	Денна форма			
	усього	зокрема		
		л	лб	с.р.
Тема 1. Модульна арифметика.	14	4	4	6
Тема 2. Матриці.	14	4	4	6
Тема 3. Традиційні шифри з симетричним ключем.	14	4	4	6
Тема 4. Прості числа.	12	3	3	6
Тема 5. Алгебраїчні структури.	12	3	3	6
Тема 6. Перетворення.	12	3	3	6
Тема 7. Сучасні блокові шифри.	12	3	3	6
Усього годин	**90**	**24**	**24**	**42**

4. Програма навчальної дисципліни

4.1. Теми лекцій

№ з/п	Назва теми	Кількість годин
1.	Модульна арифметика: Арифметика цілих чисел. Множина цілих чисел: бінарні операції, розподіл цілих чисел, два обмеження, граф рівняння поділу.	4
2.	Матриці: Операції і рівняння. Складання і віднімання. Множення. Скалярний множення. Детермінант. Інверсії. Матриці відрахувань. Порівняння. Лінійне рівняння.	4
3.	Традиційні шифри з симетричним ключем: Принципи Керкгоффса. Криптоаналіз. Категорії традиційних шифрів. Шифри підстановки. Моноалфавітні шифри. Адитивний шифр. Шифр зсуву. Шифр Цезаря. Багатоалфавітні шифри. Шифр Віженера.	4
4.	Прості числа: Взаємно прості числа. Перевірка на просте число. Решето Ератосфена. Розкладання на множники. Основна теорема арифметики. Найбільший спільний дільник. Найменше спільне кратне. Методи розкладання на множники.	3
5.	Алгебраїчні структури: Группи. Поле. Поля GF(2n). Поліноми. Операції. Модуль. Додавання. Множення. Множення, що використовує комп'ютер. Використання генератора. Інверсії. Адитивні інверсії. Мультиплікативні інверсії. Додавання і віднімання. Множення і ділення.	3
6.	Перетворення: Критерії. Безпека. Вартість. Реалізація. Раунди. Одиниці даних. Біт. Байт. Слово. Блок. Матриця	3

	станів. Структура кожного раунду. Підстановка. SubBytes. InvSubBytes. Перетворення з використанням поля GF. Алгоритм. Нелінійність. Перестановка.	
7.	Сучасні блокові шифри: Підстановка, або транспозиція. Блокові шифри як групові математичні перестановки. Повнорозмірні ключові шифри. Шифри ключа часткового розміру. Шифри без ключа.	3
Разом		**24**

4.2. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1.	Найпростіші шифри.	4
2.	Блочно симетричні шифри.	4
3.	Асиметричні криптосистеми.	4
4.	Алгоритм цифрового підпису	3
5.	Стеганографічні методи захисту інформації.	3
6.	Використання програми PGP для шифрування повідомлень електронної пошти.	3
7.	Статистичні дослідження генераторів випадкових та псевдовипадкових послідовностей за методикою NISTSTS.	3
Разом		**24**

4.3. Самостійна робота

№ з/п	Назва теми	Кількість годин
1.	Модульна арифметика. (Опорний конспект, диктант)	6
2.	Матриці. (Опорний конспект, нетипові задачі)	6
3.	Традиційні шифри з симетричним ключем. (Опорний конспект, написання програм)	6
4.	Прості числа. (Опорний конспект, нетипові задачі)	6
5.	Алгебраїчні структури. (Опорний конспект, математичний диктант)	6
6.	Перетворення. (Опорний конспект, написання програм)	6
7.	Сучасні блокові шифри. (Опорний конспект, нетипові задачі)	6
Разом		**42**

5. Критерії оцінювання результатів навчання

Оцінювання здійснюється у вигляді поточного контролю знань, проміжних контрольних робіт та оцінювання самостійних і індивідуальних робіт. 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» та є підставою для одержання допуску до підсумкового контролю. Кожен здобувач може ознайомитись з розподілом балів за всі види роботи впродовж семестру (в дистанційному курсі, зокрема).

Результати навчання оцінюються у процесі *лабораторного заняття* за такими критеріями:

- ✓ під час опитувань – за повну і ґрунтовну відповідь на задане запитання з теми заняття;
- ✓ у процесі виконання ситуаційних вправ і завдань – за запропонований правильний алгоритм (послідовність) 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.

Самостійна робота до кожного практичного заняття має бути виконана до початку наступного. Індивідуальні завдання виконуються впродовж семестру.

Максимальний бал оцінювання результатів навчання у процесі написання проміжних контрольних робіт виставляється за правильні відповіді на всі питання роботи. Для кожної контрольної роботи надається розподіл балів за кожне завдання, з яким можна ознайомитись завчасно (зокрема, в дистанційному курсі). Роботи, написані на незадовільну оцінку, не зараховуються та мають бути виконані після аналізу помилок в додатковий час.

Унаслідок виявлення невідповідності результатів навчання окремим критеріям із тієї чи іншої форми контролю знань кількість балів, яка виставляється здобувачу вищої освіти, може бути знижена:

- ✓ за неповну відповідь;
- ✓ за кожну неправильну відповідь;
- ✓ за невчасне виконання завдання;
- ✓ за недостовірність поданої інформації;
- ✓ за недостатнє розкриття теми;
- ✓ за відсутність посилань на літературні джерела;
- ✓ за порушення академічної доброчесності.

Підсумковим контролем з даної дисципліни є залік. Оцінювання результатів навчання проводиться по закінченні вивчення навчальної дисципліни, на останньому практичному занятті або в період до початку екзаменаційної сесії відповідно до графіка освітнього процесу. На останньому аудиторному занятті оголошуються здобувачам вищої освіти відкрито (у присутності групи) накопичені

ними бали поточного оцінювання з навчальної дисципліни, отримані під час лекційних, практичних занять та за виконану самостійну роботу. Залік, як форма контролю, передбачає зарахування здобувачеві балів, накопичених за результатами поточного оцінювання з навчальної дисципліни (за наявності у здобувача не менше 60 балів за поточну роботу - без додаткового опитування) й не вимагає обов'язкової присутності здобувача вищої освіти. Здобувач має право (за бажанням) підвищити власний результат оцінювання в балах, шляхом виконання завдань самостійної роботи, але не пізніше ніж до початку екзаменаційної сесії.

Шкала оцінювання результатів навчання здобувачів вищої освіти

За накопичувальною 100 - бальною шкалою	**За національною шкалою**	
	для екзаменів, звітів з практики, курсових робіт	***для заліків***
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. Іваночко С.Г. Криптологія. Львів: Національний Університет Львівська Політехніка, 2018. 46 с.

3. 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.

4. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч.посібник / Г.Л. Козіна. – Запоріжжя : НУ «Запорізька політехніка», 2020. – 192 с

5. 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. Jean-Philippe Aumasson. Serious Cryptography: A Practical Introduction to Modern Encryption Paperback. Kindle Edition, 2017. – 313 pages.

2. Акуленко, Ірина. Шифр віженера та модульна арифметика у навчанні математики на поглибленому рівні [Текст] / І. Акуленко, Н. Красношлик, Ю. Лещенко // Математика в рідній школі : наук.-метод. журн. - 2017. - № 1. - С. 20-24.

3. 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.

4. Дискретна математика. Теорія множин і відношень. Комбінаторика. Числення висловлювань: навч. посіб. / Н. П. Тмєнова ; Київ. нац. ун-т ім. Тараса Шевченка. - Київ : Київський університет, 2018. - 103 с.

5. Дрозденко В.О. Вища математика: необхідний теоретичний мінімум: навч. посіб. В.О. Дрозденко, О.Л. Дрозденко Б.: Пшонківський О.В., 2020. 264 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. 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/SYiiBKn
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://ddpu.edu.ua:9090/moodle/course/view.php?id=1649