Міністерство освіти і науки України
Державний вищий навчальний заклад
«Донбаський державний педагогічний університет»

Факультет **фізико-математичний**

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

«ЗАТВЕРДЖУЮ»
Перший проректор _____
_____ О.Г. Набока
«29» червня 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ПРИКЛАДНА КРИПТОЛОГІЯ

підготовки здобувачів
першого (бакалаврського) рівня вищої освіти

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

Дніпро-Слов'янськ – 2023 р.

Розробники:

Турка Т.В. – кандидат фізико-математичних наук, доцент, доцент кафедри методики навчання математики та методики навчання інформатики ДВНЗ «Донбаський державний педагогічний університет»;

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. – доктор педагогічних наук, кандидат фізико-математичних наук, професор, професор 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 «25» травня 2023 року.

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

Погоджено групою забезпечення спеціальності *014 Середня освіта (Інформатика)*

Керівник групи забезпечення _____ **А.В. Стьопкін**

Затверджено та рекомендовано до впровадження вченою радою
Державного вищого навчального закладу
«Донбаський державний педагогічний університет»

29 червня 2023 р., протокол №9

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 – 4
самостійної роботи здобувача – 3,5</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 *«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
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. 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. Потокові 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

Результати навчання здобувачів вищої освіти з навчальної дисципліни визначаються у балах, що виставляються згідно з критеріями оцінювання, затвердженими в ДДПУ, а саме за 100-бальною шкалою та національною п'ятибальною шкалою для заліків «зараховано», «незараховано»).

Навчальна дисципліна оцінюється максимальною оцінкою у 100 балів.

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
89 – 75 балів	добре	
60 – 74 балів	задовільно	
26 – 59 балів	незадовільно	не зараховано
0 – 25 балів	неприйнятно	

Критерії оцінювання заліку:

– на оцінку ***«зараховано» (60-100 балів)*** заслуговує здобувач вищої освіти, який за час відвідування лекційних, 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, лабораторних занять й за виконану самостійну роботу не набрав 60 балів упродовж семестру, він має прогалини в знаннях основного навчально-програмного матеріалу.

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.

Результати поточних контролів рівня знань здобувачів вищої освіти денної та заочної форм навчання (у вигляді певної кількості отриманих балів) обов'язково доводяться викладачем наприкінці кожного заняття до їхнього відома, виставляються в Журнал обліку роботи академічної групи та є підставою для одержання допуску до підсумкового контролю.

Оцінювання результатів навчання у формі семестрового заліку проводиться по закінченні вивчення навчальної дисципліни, зазвичай, на останньому лабораторному занятті або в період до початку екзаменаційної сесії відповідно до графіка освітнього процесу.

На останньому аудиторному занятті викладач зобов'язаний оголосити здобувачам вищої освіти відкрито (у присутності групи) накопичені ними бали поточного оцінювання з навчальної дисципліни, отримані під час лекційних, практичних та/або лабораторних 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 з навчальної дисципліни, де формою контролю є залік, шляхом виконання завдань самостійної роботи, але не пізніше ніж до початку екзаменаційної сесії.

6. Засоби діагностики результатів навчання

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

- лабораторні роботи;
- груповий проєкт;

- індивідуальні завдання;
- залік.

7. Рекомендована література

Основна

1. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
2. Класичні методи криптології: методичні рекомендації для здобувачів спеціальностей «Прикладна математика» та «Системний аналіз» / М.М.Повідайчик, І.Я. Шпонтак. Ужгород: В-во УжНУ «Говерла», 2020. 28 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. 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.Тмєнова; 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. 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://212.3.125.77:9090/moodle/course/view.php?id=1649

Турка Т.В. – кандидат фізико-математичних наук,
доцент, доцент кафедри МНМ та МНІ

РПНД перевірена.
Методист НМВ
Коркішко О.Г.