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)
«____» _____ 2020 р.

РОБОЧА НАВЧАЛЬНА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
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 – 2020 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 « 27 » серпня 2020 р.

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»

« 28 » серпня 2020 р.,
протокол № 1

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
	Лекції
Тижневих годин для денної форми навчання: контактних – **2** самостійної роботи здобувача – **3**	**24** год.
	Практичні
	24 год.
	Самостійна робота
	42 год.
	Вид контролю:
	залік

Метою вивчення дисципліни «Основи криптології» 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 «Основи криптології»

Результати навчання	Методи навчання	Методи контролю
Знає основні історичні етапи розвитку предметної області. Знає та розуміє фізичні, логічні та математичні основи інформаційних технологій. Знає та розуміє способи двійкового кодування текстової, числової, графічної, звукової та відео інформації. Знає та розуміє етико-правові засади використання інформаційно-комунікаційних технологій; уміє впроваджувати засоби й методи захисту інформації та безпеки в мережі Інтернет. Уміє створювати інформаційні моделі, реалізовувати їх засобами інформаційно- комунікаційних технологій, здійснювати дослідження, інтерпретувати, аналізувати та узагальнювати його результати.	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	п	с.р.
Тема 1. Основні поняття криптології.	7	2	1	3
Тема 2. Історія кодування та шифрування. Використання кодів. Сучасна криптографія.	8	2	1	4
Тема 3. Класичні шифри перестановки.	7	2	2	3
Тема 4. Класичні шифри заміни.	8	2	2	3
Тема 5. Математичні основи криптографії.	7	2	4	4
Тема 6. Шифри аналітичних перетворень.	8	2	2	4
Тема 7. Псевдовипадкові числа.	7	2	2	3
Тема 8. Шифри з використанням гамування.	8	2	2	4
Тема 9. Стандарт шифрування даних DES.	7	2	2	3
Тема 10. Асиметричні криптосистеми.	8	2	2	4
Тема 11. Ідентифікація та аутентифікація.	7	2	2	3
Тема 12. Електронний цифровий підпис.	8	2	2	4
Усього години	**90**	**24**	**24**	**42**

4. Програма навчальної дисципліни

4.1. Теми лекцій

№ з/п	Назва теми	Кількість годин
1.	Основні поняття криптології.	2
2.	Історія кодування та шифрування. Використання кодів. Сучасна криптографія.	2
3.	Класичні шифри перестановки.	2
4.	Класичні шифри заміни.	2
5.	Математичні основи криптографії.	2
6.	Шифри аналітичних перетворень.	2
7.	Псевдовипадкові числа.	2
8.	Шифри з використанням гамування.	2
9.	Стандарт шифрування даних DES.	2
10.	Асиметричні криптосистеми.	2
11.	Ідентифікація та аутентифікація.	2
12.	Електронний цифровий підпис.	2
Разом		**24**

4.2. Теми практичних занять

№ з/п	Назва теми	Кількість годин
	Розділ І. Множини та відношення.	
1.	Основні поняття криптології. (Розв'язування типових задач)	1
2.	Історія кодування та шифрування. Використання кодів. Сучасна криптографія. (Розв'язування типових задач)	1
3.	Класичні шифри перестановки. (Розв'язування типових задач, аналіз алгоритмів)	2
4.	Класичні шифри заміни. (Розв'язування типових задач, аналіз алгоритмів)	2
5.	Математичні основи криптографії. (Розв'язування типових задач). Контрольна робота	4
6.	Шифри аналітичних перетворень. (Розв'язування типових задач, аналіз алгоритмів)	2
7.	Псевдовипадкові числа. (Розв'язування типових задач)	2
8.	Шифри з використанням гамування. (Розв'язування типових задач, аналіз алгоритмів)	2
9.	Стандарт шифрування даних DES. (Розв'язування типових задач)	2
10.	Асиметричні криптосистеми. (Розв'язування типових задач, аналіз алгоритмів)	2
11.	Ідентифікація та аутентифікація. (Розв'язування типових задач)	2
12.	Електронний цифровий підпис. (Розв'язування типових задач, аналіз алгоритмів)	2
Разом		**24**

4.3. Самостійна робота

№ з/п	Назва теми	Кількість годин
	Розділ І. Множини та відношення.	
1.	Основні поняття криптології. (Опорний конспект, диктант)	3
2.	Історія кодування та шифрування. Використання кодів. Сучасна криптографія. (Опорний конспект, груповий проєкт)	4
3.	Класичні шифри перестановки. (Опорний конспект, нетипові задачі)	3
4.	Класичні шифри заміни. (Опорний конспект, написання програм)	3
5.	Математичні основи криптографії. (Опорний конспект, математичний диктант)	4
6.	Шифри аналітичних перетворень. (Опорний конспект, написання програм)	4
7.	Псевдовипадкові числа. (Опорний конспект, нетипові задачі)	3
8.	Шифри з використанням гамування. (Опорний конспект, нетипові задачі)	4
9.	Стандарт шифрування даних DES. (Опорний конспект, нетипові задачі)	3
10.	Асиметричні криптосистеми. (Опорний конспект, нетипові задачі)	4
11.	Ідентифікація та аутентифікація. (Опорний конспект, презентація)	3
12.	Електронний цифровий підпис. (Опорний конспект, порівняння алгоритмів)	4
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 *практичного 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 практичному 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.

Розподіл балів, що можуть здобути студенти за темами та за формами навчальних занять

№ теми	*Аудиторна робота*	*Самостійна робота*	**Підсумковий контроль (залік)**
Т 1.	1	5	
Т 2.	1	5	
Т 3.	2	5	
Т 4.	2	5	
Т 5.	12	5	
Т 6.	2	5	
Т 7.	2	5	4
Т 8.	2	5	
Т 9.	2	5	
Т 10.	2	5	
Т 11.	2	5	
Т 12.	6	5	
Разом	**36**	**60**	

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.

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 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 занять й за виконану самостійну роботу не набрав 60 балів упродовж семестру, він має прогалини в знаннях основного навчально-програмного матеріалу.

6. Засоби діагностики результатів навчання

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

- письмові самостійні роботи;
- контрольні роботи;
- 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. Акуленко І. А., Красношлик Н. О., Лещенко Ю. Ю. Основи криптології: матеріали курсу за вибором для учнів 9-х класів із поглибленим вивченням математики : навч.-метод. пос. у 2-х частиниах; частина 1 / І.А. Акуленко, Н.О. Красношлик, Ю.Ю. Лещенко – Черкаси, 2015. – 112 с. Режим доступу: https://cryptology2015.wordpress.com/

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 С.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 самостійної роботи студентів з кредитного модуля «Технології захисту інформації» для студентів напряму підготовки 6.050101 «Комп'ютерні науки» програм професійного спрямування «Інформаційні технології проектування», «Комп'ютерний еколого-економічний моніторинг»» / Уклад.: Ю.А. Тарнавський – К.: НТУУ «КПІ», 2016. – 17 с.
7. Он-лайн підручник з криптографії. Режим доступу: https://coderlessons.com/tutorials/akademicheskii/izuchite-kriptografiiu/uchebnik-po-kriptografii

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://moodle.znu.edu.ua/course/view.php?id=4199
4. Основні поняття кріптології: http://lib.mdpu.org.ua/e-book/kruptologiya/lect1.html
5. Порівняння симетричних та асиметричних криптосистем: https://sites.google.com/site/sucasnikriptosistemik/home/porivnanna-simetricnih-zasimetricnimi-kriptosistemami
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