Державний вищий навчальний заклад
«Донбаський державний педагогічний університет»

Фізико-математичний факультет
Кафедра методики навчання математики та методики навчання інформатики

СИЛАБУС
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

Слов’янськ – 2022 р.

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».

Силабус розглянуто і схвалено на засіданні кафедри методики навчання математики та методики навчання інформатики ДВНЗ «Донбаський державний педагогічний університет»

Протокол № 11 від «23» червня 2022 р.

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

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

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
ПРИКЛАДНА КРИПТОЛОГІЯ

Кількість кредитів	3
Рік підготовки, семестр	3-й рік, 6-й семестр
Компонент освітньої програми	вибірковий
Викладач	Кайдан, Наталія Володимирівна, доцент кафедри методики навчання математики та методики навчання інформатики, кандидат фізико-математичних наук, доцент
Контактна інформація	kaydannv@gmail.com
Консультації	четвер з 15.00 до 16.00
Анотація навчальної дисципліни	Криптологія – наука про захист інформації, шляхом її перетворення. Криптологія поєднує два напрямки – криптографію й криптоаналіз. Криптографія займається пошуком і дослідженням методів перетворення інформації з метою приховання її змісту. Криптоаналіз - дослідження можливості розшифровування інформації без знання ключів. **Об'єктом** вивчення навчальної дисципліни – є теоретико-прикладні основи криптології. **Предметом** вивчення навчальної дисципліни – є математичні моделі та методи криптології.
Опис навчальної дисципліни	Метою вивчення дисципліни 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. **Ключові слова**: криптологія, криптографія, криптоаналіз, симетричні криптосистеми, асиметричні криптосистеми, цифровий підпис. **Очікувані результати навчання**

	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. **Матеріали та ресурси** ***Навчально-методичні матеріали*** **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.** 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. ***Ресурси*** **1.** Дистанційний курс дисципліни на освітньому контенті в CMS Moodle http://212.3.125.77:9090/moodle/course/view.php?id=1649 **2.** Основи криптології. Режим доступу: https://moodle.znu.edu.ua/course/view.php?id=4199
Теми	**Тема 1.** Відомості з теорії чисел та математичні основи криптології. **Тема 2.** Основні поняття та визначення криптології. Криптографія та криптоаналіз. **Тема 3.** Традиційні шифри. **Тема 4.** Принципи побудови сучасних блокових шифрів. **Тема 5.** Потокові шифри. **Тема 6.** Стандарт симетричного алгоритму блокового шифрування даних DES. **Тема 7.** Режими виконання алгоритмів блокового симетричного шифрування даних.

Методичні поради для викладачів «Як навчати?»	Викладач у своїй навчальній діяльності може використовувати наступні методи навчання: ✓ словесний (лекція, дискусія, співбесіда тощо); ✓ практичний метод (практичні заняття); ✓ робота з навчально-методичною літературою (конспектування, тезування, анотування, складання реферату); ✓ відеометод у сполученні з новітніми інформаційними технологіями та комп'ютерними засобами навчання (дистанційні, мультимедійні, веб-орієнтовані); ✓ самостійна робота (розв'язання завдань); ✓ індивідуальна науково-дослідна робота.
Методичні поради для здобувачів «Як навчатися?»	Здобувачам для досягнення навчальної мети даної дисципліни пропонується: ✓ регулярно засвоювати лекційний матеріал, використовуючи словесний метод та метод роботи з навчально-методичною літературою. Використання матеріалів дистанційного курсу також допоможе в досягненні цієї мети; ✓ на практичних заняттях активно приймати участь у розгляді окремих теоретичних положень навчальної дисципліни та формуванні умінь і навичок їх практичного застосування шляхом виконання практичних завдань; ✓ вчасно виконувати та подавати на перевірку (в тому числі і засобами використання дистанційного курсу) самостійні роботи до кожного практичного заняття та індивідуальні завдання; ✓ аналізувати результати контрольних заходів та усувати виявлені недоліки в знаннях.
Оцінювання	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 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**

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. *Норми етичної поведінки.* Відповідно до діючого в ДВНЗ «ДДПУ» кодексу академічної доброчесності, всі учасники освітнього процесу в університеті повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку університету, загальноприйнятих моральних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності; підвищувати престиж університету досягненнями в навчанні та науково-дослідницькій діяльності; дбайливо ставитися до університетського майна. *Академічна доброчесність.* Очікується, що роботи здобувачів будуть їх оригінальними дослідженнями чи міркуваннями. Здобувачі не видають за свої результати роботи інших людей. При використанні чужих ідей і тверджень у власних роботах обов'язково посилаються на використані джерела інформації. Під час оцінювання результатів навчання не користуються недозволеними засобами, самостійно виконують навчальні

	завдання, завдання поточного та підсумкового контролю результатів навчання. Відвідування занять є обов’язковим. Здобувачі зобов'язані дотримуватися термінів виконання усіх видів робіт, передбачених робочою програмою курсу. Впродовж занять здобувачі вищої освіти повинні виконувати діючі правила охорони праці і безпеки життєдіяльності та можуть користуватися електронними девайсами для обчислень при розв’язуванні задач.
Переваги вивчення навчальної дисципліни «Бонус вивчення»	Курс основи криптології в педагогічних університетах має на меті ознайомити здобувачів першого рівня вищої освіти з основами цієї науки, оскільки вона посідає важливе місце в професійній підготовці майбутніх учителів інформатики. Слід зазначити, що курс має яскраво виражене практичне спрямування. Криптологія розвинулась з практичної потреби передавати важливі відомості найнадійнішим чином. Вона є одним з основних засобів захисту інформацій у комп'ютерних мережах і, я к наслідок є, найактуальніщим напрямком сучасних комп’ютерних технологій.

Викладач Н.В. Кайдан