**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 (*за предметними спеціальностями*) |
| **за освітньо-професійною програмою** | Середня освіта (Інформатика) |
| **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».

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

Протокол № 11 від «25» травня 2023 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»
«29» червня 2023 р., протокол № 9

# ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
# ОСНОВИ КРИПТОЛОГІЇ

| | |
|---|---|
| **Кількість кредитів** | 3 кредити ECTS / 90 годин |
| **Рік підготовки, семестр** | 3-й рік, 6-й семестр |
| **Компонент освітньої програми** | вибірковий |
| **Викладач** | Турка Тетяна Вікторівна, кандидат фізико-математичних наук, доцент, доцент кафедри методики навчання математики та методики навчання інформатики |
| **Контактна інформація** | tvturka@gmail.com |
| **Консультації** | кожного четверга з 14.00 до 15.00<br>або за попередньою домовленістю |
| **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.<br>*Об'єктом вивчення навчальної дисципліни* – є теоретико-прикладні основи криптології.<br>*Предметом вивчення навчальної дисципліни* – є математичні моделі та методи криптології. |
| **Опис навчальної дисципліни** | **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.<br>**Ключові слова**: криптологія, криптографія, криптоаналіз, симетричні криптосистеми, асиметричні криптосистеми, цифровий підпис.<br>**Очікувані результати навчання**<br>Демонструє знання з основних розділів інформатики.<br>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.<br>Уміє застосовувати інформаційні та телекомунікаційні технології на уроці, у позакласній і позашкільній роботі.<br>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.<br>**Матеріали та ресурси**<br>***Навчально-методичні матеріали***<br>**1.** Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.<br>**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.<br>**3.** Іваночко С.Г. Криптологія. Львів: Національний Університет Львівська Політехніка, 2018. 46 с.<br>***Ресурси***<br>**4.** Дистанційний курс дисципліни на освітньому контенті в CMS Moodle http://212.3.125.77:9090/moodle/course/view.php?id=1649<br>**5.** 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.<br>**Тема 2.** Основні поняття та визначення криптології. Криптографія та криптоаналіз.<br>**Тема 3.** Традиційні шифри.<br>**Тема 4.** Принципи побудови сучасних блокових шифрів.<br>**Тема 5.** Потокові шифри.<br>**Тема 6.** Стандарт симетричного алгоритму блокового шифрування даних DES.<br>**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:<br>✓ словесний (лекція, дискусія, співбесіда тощо);<br>✓ практичний метод (лабораторні заняття);<br>✓ робота з навчально-методичною літературою (конспектування, тезування, анотування, складання реферату); |

<table>
<tr><td></td><td>✓ відеометод у сполученні з новітніми інформаційними технологіями та комп’ютерними засобами навчання (дистанційні, мультимедійні, веб-орієнтовані);<br>✓ самостійна робота (розв’язання завдань);<br>✓ індивідуальна науково-дослідна робота.</td></tr>
<tr><td>Методичні поради для здобувачів «Як навчатися?»</td><td>Здобувачам для досягнення навчальної мети даної дисципліни пропонується:<br>✓ регулярно засвоювати лекційний матеріал, використовуючи словесний метод та метод роботи з навчально-методичною літературою. Використання матеріалів дистанційного курсу також допоможе в досягненні цієї мети;<br>✓ 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;<br>✓ вчасно виконувати та подавати на перевірку (в тому числі і засобами використання дистанційного курсу) самостійні роботи до кожного практичного заняття та індивідуальні завдання;<br>✓ аналізувати результати контрольних заходів та усувати виявлені недоліки в знаннях.</td></tr>
<tr><td>Оцінювання</td><td>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»).<br>Навчальна дисципліна оцінюється максимальною оцінкою у 100 балів.<br>Шкала оцінювання результатів навчання здобувачів вищої освіти
<table>
<tr><th rowspan="2">За накопичувальною 100 – бальною шкалою</th><th colspan="2">За національною шкалою</th></tr>
<tr><th>для екзаменів, звітів зпрактики, курсових робіт</th><th>для заліків</th></tr>
<tr><td>90 – 100 балів</td><td>відмінно</td><td rowspan="3">зараховано</td></tr>
<tr><td>89 – 75 балів</td><td>добре</td></tr>
<tr><td>60 – 74 балів</td><td>задовільно</td></tr>
<tr><td>26 – 59 балів</td><td>незадовільно</td><td>не зараховано</td></tr>
<tr><td>0 – 25 балів</td><td>неприйнятно</td><td></td></tr>
</table>
Критерії оцінювання заліку:<br>– на оцінку «зараховано» (60-100 балів) заслуговує здобувач вищої освіти, який за час відвідування лекційних,</td></tr>
</table>

| | |
|---|---|
| | практичних та/або лабораторних занять й за виконану самостійну роботу отримав зазначену кількість балів протягом семестру;<br>– 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.<br>Оцінювання результатів навчання здобувачів вищої освіти за лекції здійснюється за такими критеріями: присутність здобувача на лекції, складання її конспекту та активна участь у перебігу лекції.<br>Оцінювання результатів навчання здобувачів вищої освіти, отриманих під час практичного заняття здійснюється за такими критеріями:<br>– під час опитувань – за повну й ґрунтовну відповідь на сформульоване запитання з теми заняття;<br>– під час тестування – за правильні відповіді на запитання тесту з теми заняття;<br>– 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 й математичними методами, необхідними для виконання завдання; за отриманий правильний результат.<br>Оцінювання рефератів, доповідей, есе, презентацій тощо за визначеними темами здійснюється відповідно до таких критеріїв:<br>– за повноту та використання сучасних концепцій і джерел інформації (крім лекційного конспекту, має бути ще не менше трьох джерел інформації);<br>– за оформлення роботи згідно з вимогами і наявність посилань на використану літературу та джерела;<br>– за наявність змістовних висновків;<br>– за глибокі знання навчального матеріалу, що містяться в основних і додаткових рекомендованих літературних джерелах.<br>У разі виявлення невідповідності результатів навчання окремим критеріям із тієї чи тієї форми контролю знань кількість балів, яка виставляється здобувачу, може бути знижена:<br>– за неповну відповідь;<br>– за кожну неправильну відповідь; |

– за невчасне виконання завдання;
– за недостовірність поданої інформації;
– за недостатнє розкриття теми;
– за відсутність посилань на літературні джерела.

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 практичному та/або 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.

*Розподіл балів із дисципліни*

| *Тема* | *Аудиторна робота* | | *Самостійна робота* | |
|---|---|---|---|---|
| | *Max* | *Min* | *Max* | *Min* |
| **Тема 1.** | 4 | 2 | 5 | 2 |
| **Тема 2.** | 6 | 4 | 6 | 4 |
| **Тема 3.** | 8 | 5 | 6 | 4 |
| **Тема 4.** | 10 | 6 | 5 | 2 |
| **Тема 5.** | 12 | 7 | 6 | 4 |
| **Тема 6.** | 10 | 6 | 6 | 4 |
| **Тема 7.** | 10 | 6 | 6 | 4 |
| **Разом** | **60** | **36** | **40** | **24** |

| | |
|---|---|
| | *Політика щодо дедлайнів та перескладань, академічної доброчесності:* перездача та повторне вивчення дисципліни здійснюється відповідно до Положення про організацію освітнього процесу в ДДПУ (http://www.slavdpu.dn.ua/images/stories/news/normativ/025.pdf, Положення про академічну доброчесність педагогічних, науково-педагогічних працівників та здобувачів у ДДПУ (http://www.slavdpu.dn.ua/images/stories/news/normativ/012.pdf)<br>Політика щодо:<br>✓ *дедлайнів*: роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (від -1бала до -5балів).<br>✓ *перескладання*: у разі отримання оцінки «незадовільно» здобувач має право на два перескладання: викладачу та комісії.<br>У разі, якщо здобувач вищої освіти не з'явився в день складання екзамену з поважної причини, підтвердженої документально, у відомість обліку успішності ставиться запис «не з'явився», а здобувач має право перескласти екзамен викладачеві у визначений деканатом день.<br>Здобувач, який протягом семестру не набрав 60 балів з навчальної дисципліни, вважається недопущеним до складання екзамену з цієї дисципліни, й у відомість обліку успішності ставиться запис «не допущений». Здобувач має право допрацювати необхідні бали за погодженням з викладачем та перескласти екзамен викладачеві у визначений деканатом день.<br>*оскарження оцінювання*: Якщо здобувач не згоден з оцінюванням його знань він може звернутися до апеляційної комісії та оскаржити виставлену викладачем оцінку у встановленому порядку.<br>✓ *академічної доброчесності* для здобувачів передбачає:<br>– самостійне виконання навчальних завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);<br>– посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;<br>– дотримання норм законодавства про авторське право і суміжні права;<br>– надання достовірної інформації щодо результатів власної навчальної (наукової, творчої) діяльності, використаних методик досліджень та джерел інформації. |

| | |
|---|---|
| | За порушення академічної доброчесності здобувачі ДДПУ можуть бути притягнуті до такої відповідальності:<br>– повторне проходження оцінювання (контрольна робота, іспит, залік тощо);<br>– повторне проходження відповідного освітнього компонента освітньої програми;<br>– позбавлення академічної стипендії відповідно до норм чинного законодавства;<br>– позбавлення наданих ДДПУ пільг з оплати навчання (за умови їх отримання);<br>– усне зауваження від працівника або уповноваженого представника адміністрації (керівника кафедри, факультету тощо) та попередження про можливість притягнення до академічної відповідальності;<br>– повторне виконання завдання;<br>– зниження оцінки за виконання завдання;<br>– усне чи письмове повідомлення юридичної або фізичної особи, яка здійснює оплату за навчання, про факт порушення;<br>– виключення з рейтингу претендентів на отримання академічної стипендії або нарахування штрафних балів у такому рейтингу;<br>– позбавлення права брати участь у конкурсах на отримання стипендій, грантів тощо;<br>– відрахування. |
| **Переваги вивчення навчальної дисципліни «Бонус вивчення»** | Курс «Прикладна криптологія» 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
Т.В. Турка