Волинський національний університет імені Лесі Українки
Кафедра математичного аналізу та статистики

СИЛАБУС

вибіркового освітнього компонента

АЛГЕБРАЇЧНІ ОСНОВИ КРИПТОГРАФІЇ

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	Е Природничі науки, математика та статистика
Спеціальність	Е7 Математика
Освітня програма	Математика
Форма здобуття освіти	Денна
Розробник (викладач)	Волошина Тетяна Володимирівна, кандидат фізико-математичних наук, доцент
Контактна інформація	Електронна адреса викладача: tetianavoloshyna@gmail.com Телефон: 050-26-28-392
Семестр, курс	6 семестр, 3 курс
Обсяг освітнього компонента	Загальний обсяг: 5 кредитів ЄКТС / 150 годин. Аудиторних годин: 30; з них: лекцій – 10 год., практичних – 20 год. Самостійної роботи: 110 годин. Консультацій: 10 годин.
Форма контролю	Залік
Мова навчання	Українська
Час занять	Тижневих годин – 2 год. Аудиторні заняття проводяться за розкладом: http://94.130.69.82/cgi-bin/timetable.cgi Консультації викладача відповідно затвердженого графіку.
Анотація курсу	У курсі «Алгебраїчні основи криптографії» вивчаються вибрані питання теорії груп та скінчених полів, теорії чисел, а також їх прикладні застосування у сучасній криптографії. З обчислювальної точки зору задача знаходження дискретного логарифма вважається важкою в тому сенсі, що вимагає дуже великих об'ємів обчислень. На цій обчислювальній складності задачі дискретного логарифмування ґрунтується її застосування у криптографічних протоколах. Розглядаються протокол вироблення спільного секретного ключа, протокол цифрового підпису, протокол підкидання монети по телефону та інші.
Мета і завдання освітнього компонента	Головною метою курсу є формування особистості здобувача, розвиток інтелекту, аналітичного та синтетичного мислення, математичної культури та інтуїції; оволодіння теоретичними основами загальної алгебри; понятійним апаратом та методами теорії груп; набуття знань, умінь для подальшого успішного їх застосування на практиці, при розробці криптографічних протоколів; формування професійних компетентностей математика. Основні завдання курсу полягають у тому, щоб розвинути у здобувачів здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
Soft skills	Вивчення вибіркового курсу «Алгебраїчні основи криптографії» сприяє тому, що здобувачі будуть розвивати у собі: • здатність застосовувати знання у практичних ситуаціях; • здатність генерувати ідеї, проявляти креативність;

	• здатність перевіряти гіпотези, умови виконання математичних тверджень, коректно переносити умови та твердження на нові класи об'єктів; • здатність вести конструктивну дискусію; • здатність формулювати та обґрунтовувати висновки у словесній та формальній формі, приймати обґрунтовані рішення; • здатність до автономної роботи; • здатність працювати у малих групах над розв'язанням професійних задач; • цілеспрямованість та наполегливість у досягненні мети.

Структура освітнього компонента

Назви змістових модулів і тем	Кількість годин					Форма контролю* / бали
	Усього	у тому числі				
		Лекції	Практичні заняття	Консультації	Самостійна робота	
Змістовий модуль 1. Скінченні поля та циклічні групи						
Тема 1. Елементи теорії чисел.	14	1	2	1	10	УО, РЗ / 5 б.
Тема 2. Циклічні групи.	14	1	2	1	10	УО, РЗ / 5 б.
Тема 3. Кільця і поля лишків.	14	1	2	1	10	УО, РЗ / 5 б.
Тема 4. Дискретний логарифм елемента у групі.	14	1	2	1	10	УО, РЗ / 5 б.
Разом за змістовим модулем 1	**56**	**4**	**8**	**4**	**40**	**20 б.**
Змістовий модуль 2. Криптографічні протоколи						
Тема 5. Криптографічні протоколи.	19	1	2	1	15	УО, РЗ / 5 б.
Тема 6. Протокол Діффі-Гелмана.	20	1	2	2	15	УО, РЗ / 5 б.
Тема 7. Протокол цифрового підпису.	27	2	4	1	20	РМГ, РЗ / 10 б.
Тема 8. Протокол підкидання монети по телефону.	28	2	4	2	20	РМГ, РЗ / 10 б.
Разом за змістовим модулем 2	**94**	**6**	**12**	**6**	**70**	**30 б.**
Письмова контрольна робота						**25 б.**
Колоквіум						**25 б.**
Всього годин / балів	**150**	**10**	**20**	**10**	**110**	**100 б.**

* УО – усне опитування; РМГ – робота в малих групах; РЗ – розв'язування задач.

Завдання для самостійного опрацювання

Самостійна робота здобувачів включає в себе:

1. Опрацювання теоретичних основ лекційного матеріалу. 20 год.
   Перевірка здійснюється під час практичних занять і враховується при виставленні поточної оцінки за відповідний змістовий модуль.
2. Підготовка до практичних занять, виконання домашніх завдань. 30 год.

Перевірка здійснюється під час практичних занять. Якість, кількість і терміни виконання враховуються при виставленні поточної оцінки за відповідний змістовий модуль.

3. Систематизація вивченого матеріалу перед контрольними заходами. 30 год.
   Перевірка здійснюється під час контрольної роботи та під час колоквіуму.
4. Вивчення тем, що не розглядаються в курсі лекцій. 30 год.
   Перевірка здійснюється під час контрольних заходів.

Оцінювання

Політика оцінювання та організація контрольних заходів здійснюється згідно з Положенням про поточне та підсумкове оцінювання знань здобувачів освіти Волинського національного університету імені Лесі Українки https://cutt.ly/yrNruzhM.

Оцінювання навчальних досягнень з вибіркового курсу «Теорія груп» здійснюється за 100 бальною шкалою. Оцінка включає в себе поточний контроль (оцінюється робота на парах під час усного опитування та розв'язування задач; вчасне і якісне виконання домашніх завдань, самостійне вивчення окремих тем курсу, виконання індивідуальних завдань – всього 50 балів за усі види робіт) та оцінки за колоквіум (25 балів) та письмову контрольну роботу (25 балів). Максимальна кількість балів, яку може накопичити здобувач за семестр, складає 100 балів. Призери студентської математичної олімпіади можуть отримати додаткові (бонусні) бали за правильне розв'язання задач з алгебри на олімпіаді (не більше 5 балів), які зараховуються як результати поточного контролю.

Письмова контрольна робота містить типові задачі курсу. На колоквіумі здобувачу пропонується письмово розкрити теоретичне питання. Розподіл балів між завданнями у межах письмової роботи та критерії їх оцінювання вказані у відповідній модульній роботі.

При оцінюванні окремого завдання (задачі) викладач керується наступними критеріями оцінювання:

- правильно розв'язана задача із повним обґрунтуванням усіх кроків (повністю та послідовно викладене теоретичне питання з доведенням та прикладами) оцінюється максимальною кількістю балів, передбаченою за це завдання;
- розв'язана задача, у викладках до якої допущено незначні недоліки, наявні прогалини у обґрунтуванні деяких кроків (теоретичне питання з неповним доведенням, без наведених прикладів, викладено непослідовно) оцінюється кількістю балів у межах 75-95% від максимальної кількості балів, передбаченою за це завдання;
- розв'язана задача, проте у її розв'язанні допущено суттєві помилки, висновки необґрунтовані (виклад теоретичного питання непослідовний, неповний, без доведень та прикладів, з неточностями у формулюваннях), оцінюється кількістю балів у межах 50-74% від максимальної кількості балів, передбаченою за це завдання;
- задача розв'язана не до кінця, з суттєвими помилками та прогалинами у розв'язанні, висновки відсутні (частковий виклад теоретичного питання, без доведень та прикладів, з суттєвими помилками), оцінюється кількістю балів у межах 25-49% від максимальної кількості балів, передбаченою за це завдання;
- задача нерозв'язана, проте наведені окремі продуктивні міркування та обчислення, які можуть привести до часткових чи проміжних результатів (поверхневий виклад міркувань щодо теоретичного питання, доведення відсутні, допущено грубі помилки), оцінюється кількістю балів у межах 11-24% від максимальної кількості балів, передбаченою за це завдання;
- задача нерозв'язана, наведені міркування та обчислення не привели до часткових чи проміжних результатів (містяться фрагментарні міркування щодо теоретичного питання, хибні твердження, неправильні формули), оцінюється кількістю балів, що не перевищує 10% від максимальної кількості балів, передбаченою за це завдання.

Якщо за результатами семестру здобувачем накопичено не менше 60 балів, і студент (ка) погоджується із цим результатом, то оцінка за семестр виставляється без складання заліку в день, передбачений графіком заліково-екзаменаційної сесії. Якщо за результатами семестру

накопичено менше 60 балів або студент (ка) не погоджується із результатом, то він (вона) складає залік як ліквідацію академічної заборгованості, при цьому бали накопичені за семестр анулюються. Залік проходить у письмовій формі, здобувачу пропонується набір задач та теоретичних запитань, передбачених програмою курсу.

Перелік питань до заліку

- Властивості простих і складених чисел. Перевірка числа на простоту.
- Взаємно прості числа та їх властивості. Лінійне зображення НСД двох цілих чисел.
- Функція Ейлера, властивості, формули для обчислення її значень.
- Властивості конгруенцій, теореми Ейлера і Ферма.
- Основні алгебраїчні структури: групи, кільця, поля. Приклади.
- Порядок елемента в групі. Циклічні підгрупи.
- Теорема Лагранжа та наслідки з неї.
- Циклічні групи, їх властивості. Твірні елементи циклічних груп.
- Класи лишків за модулем натурального числа.
- Кільця та поля лишків.
- Скінченні поля. Мультиплікативна група скінченного поля.
- Поняття дискретного логарифма елемента.
- Основні поняття криптографії.
- Поняття криптографічного протоколу.
- Протокол вироблення спільного секретного ключа.
- Протокол цифрового підпису.
- Протокол підкидання монети по телефону.

Вирішення конфліктних ситуацій

Будь-яка конфліктна ситуація, що виникає між учасниками освітнього процесу вирішується згідно з Положенням про порядок і процедури вирішення конфліктних ситуацій у ВНУ імені Лесі Українки https://cutt.ly/SteZfYIg .

Політика викладача щодо здобувача

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загально-прийнятих морально-етичних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності. Атмосфера на заняттях повинна бути творчою, відкритою до конструктивної критики. Недопустимі запізнення на заняття без поважних причин; користування мобільним телефоном або іншими мобільними пристроями під час заняття не з навчальною метою, зокрема розмови, переписка, ігри та інші розваги; списування. Очікується, що всі студенти відвідають усі лекції і практичні заняття курсу. У випадку запровадження дистанційної форми навчання, що може бути пов’язано із карантином, надзвичайними ситуаціями, воєнним станом і т. ін., заняття проводитимуться в режимі відео конференції Zoom та / або з використанням платформи Moodle https://moodle-cs.vnu.edu.ua/ . Матеріал пропущених занять здобувач опрацьовує самостійно, звітує про виконання викладачу в індивідуальному порядку. Пропущені заняття не звільняють студента від вчасного виконання контрольних заходів разом із групою.

Перезарахування окремих змістових модулів, контрольних заходів в межах освітнього компонента регламентується Положенням про визнання результатів навчання, отриманих у формальній, неформальній та/або інформальній освіті у Волинському національному університеті імені Лесі Українки https://cutt.ly/erMCERSG .

Політика щодо академічної доброчесності

Під час навчання учасники освітнього процесу зобов’язані дотримуватися академічної доброчесності: етичних принципів та визначених законом правил, якими мають керуватися

учасники освітнього процесу під час навчання, викладання та провадження наукової діяльності https://cutt.ly/VrMCNwQN .

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, тверджень, відомостей; дотримання норм законодавства про авторське право; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

Під час оцінювання результатів навчання студенти не користуються забороненими засобами (мобільний телефон, планшет, конспект, навчальна література, інші джерела інформації, в тому числі Інтернет-ресурси), самостійно виконують запропоновані завдання.

Політика щодо дедлайнів та перескладання

Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, він/вона вивчають теоретичний матеріал самостійно використовуючи навчальні посібники, конспекти лекцій, дистанційний курс, виконують всі завдання для аудиторних занять, всі домашні завдання. Прозвітуватися про виконання завдань можна під час консультацій, одночасно при цьому з'ясувати незрозумілі моменти, задати запитання викладачу.

Перескладання контрольних заходів заборонено. Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку.

Рекомендована література

Методичне забезпечення

Волошина Т.В. Елементи теорії груп: навч. посіб. Луцьк: Вежа-Друк, 2023. 145 с.

Основна література

1. Ганюшкін О. Г., Безущак О. О. Теорія груп: навчальний посібник. К.: Видавничо-поліграфічний центр «Київський університет», 2005. 128 с.
2. Вербіцький О.В. Вступ до криптології. Львів: Видавництво науково-технічної літератури, 1998. 247 с.
3. Глинчук Л.Я. Криптологія: навч. посібник. Луцьк : РВВ «Вежа» Волин. нац. ун-т ім. Лесі Українки, 2011. 132 с.

Додаткова література

1. Волошина Т.В. Групи, кільця, поля (курс лекцій). Луцьк: Вежа-Друк, 2020. 84 с.
2. Блінцов В.С., Гальчевський Ю.Л. Математичні основи криптології + CD : навч. посібник Миколаїв: НУК, 2006. 232 с.
3. Богуш В.М., Мухачов В.А. Криптографічні застосування елементарної теорії чисел: навч. посібник. К.: ДУІКТ, 2006. 126 с.
4. Кузнецов Г.В., Фомичов В.В., Сушко С.О., Фомичова Л.Я. Математичні основи криптографії : навч. посіб. Д. : НГУ, 2004. Ч.1. 392 с.

Затверджено на засіданні кафедри математичного аналізу та статистики

протокол № 8 від 30 січня 2026 р.

Завідувач кафедри _____ Федуник-Яремчук О.В.

Погоджено

Гарант освітньо-професійної програми _____ Волошина Т.В.