



**Силабус навчальної дисципліни
«Спеціальні розділи математики»**

**Спеціальність: 125 «Кібербезпека»
Галузь знань: 12 «Інформаційні технології»**

Рівень вищої освіти	Перший (бакалаврський)
Статус дисципліни	Навчальна дисципліна вибіркового компонента фахового переліку
Семестр	Осінній семестр
Обсяг дисципліни, кредити ЄКТС/загальна кількість годин	3 кредити /90 годин
Мова викладання	Українська
Що буде вивчатися (предмет навчання)	<ul style="list-style-type: none"> – Елементи теорії чисел; – конгруенції; – алгебраїчні структури; – раціональні точки на еліптичних кривих.
Чому це цікаво/потрібно вивчати (мета)	Курс спрямований на пояснення студентам, основних понять та моделей теорії чисел, алгебри, полів Гауа та групових операцій на еліптичних кривих.
Чому можна навчитися (результати навчання)	<p>Інтенсивний розвиток методів прикладної криптології привів до створення широкого спектра систем та засобів криптографічного захисту інформації та інформаційних ресурсів, які ґрунтуються на теорії чисел, методах алгебри, проєктивної геометрії та дискретної математики.</p> <p>Курс “Спецрозділи математики” – складова частина математики, в якій вивчають математичні засоби дослідження дискретних процесів і систем для їх подальшого використання в процедурах криптографічного захисту інформації.</p>
Як можна користуватися набутими знаннями і вміннями (компетентності)	<ul style="list-style-type: none"> – здатність вирішувати прикладні задачі захисту інформації, з використанням теоретико-числових базисів та теорії чисел, груп, кілець і полів та міння застосовувати теорію чисел, теорію груп, кілець і полів – здатність проводити дослідження, обробляти та аналізувати отримані експериментальні дані з метою забезпечення необхідного рівня захисту інформації; – здатність вирішувати завдання теоретичного і прикладного характеру з різних розділів сучасної математики, доведенням тверджень, побудовою моделей об’єктів і понять; – здатність до професійного використання математичних методів для їх подальшого використання в процедурах криптографічного захисту інформації.

<p>Навчальна логістика</p>	<p>Зміст дисципліни: Прості числа, основна теорема арифметики, алгоритм Евкліда, лінійні діофантові рівняння, арифметичні функції, розподіл простих чисел. Конгруенції за модулем n, кільця лишків, китайська теорема про лишки, теореми Ферма, Ейлера, Вілсона, сума двох квадратів, піфагорійські трійки. Квадратичні лишки, символ Лежандра, квадратичний закон взаємності. Ланцюгові дроби, раціональна апроксимація, рівняння Пелля. Діофантові рівняння. Подільність в областях цілісності, подільність в термінах ідеалів, НСД, нерозкладні та прості елементи. Евклідові кільця, алгоритм Евкліда, кільця головних ідеалів, факторіальні кільця, застосування в теорії чисел.</p> <p>Поля, характеристика поля, прості поля. Розширення полів, скінченні та алгебраїчні розширення, прості розширення, алгебраїчні та трансцендентні елементи, алгебраїчно замкнені поля. Поля розкладу многочленів. Раціональні точки на еліптичних кривих. Алгебраїчні структури .</p> <p>Види занять: лекції, лабораторні роботи.</p> <p>Методи навчання: Лекції проводяться з використанням наочних засобів навчання, а саме мультимедійних презентацій.</p> <p>Форми навчання: денна, заочна.</p>
<p>Пререквізити</p>	<p>Вивчення курсу „Спецрозділи математики” передбачає наявність систематичних та ґрунтовних знань із суміжних та шкільних курсів, зокрема «Математичний аналіз», «Теорія ймовірності», «Лінійна алгебра та аналітична геометрія», а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи студентів.</p>
<p>Пореквізити</p>	<p>Знання та вміння, можуть бути використані під час написання курсових та бакалаврської робіт та є базовими для вивчення навчальних дисциплін: «Прикладна криптологія», «Безпека інформаційних і комунікаційних систем».</p>
<p>Інформаційне забезпечення з фонду та репозитарію НТБ НАУ</p>	<p>Науково-технічна бібліотека НАУ:</p> <ol style="list-style-type: none"> 1. Безущак О.О, Ганюшкин О.Г. Елементи теорії чисел. Навчальний посібник. – К.: Видавничо-поліграфічний центр «Київський Університет», 2013. – 202 с. 2. Авдеева Т.В. Загальна алгебра і теорія чисел. Навчально-методичний посібник. М. Академия, 2014. – 272 с. 3. Нестеренко Ю.В. Теория чисел М. Академия, 2015. – 272 с. 4. Барковський В.В. Теорія ймовірностей та математична статистика : навч. посіб для студ. екон. спец. вищ. навч. закл. / В.В. Барковський. – 3-тє вид., переробл. і допов. – Київ : Центр навч. літ., 2016. – 447 с. 5. Николайчук Я.М. Теорія джерел інформації / Я.М. Николайчук // Видання друге, виправлене, – Тернопіль: ТзОВ “Терно-граф”, 2010. – 536 с.. 6. Андерсон Д.А. Дискретная математика и комбинаторика: Пер. с англ. – М.: Изд. дом «Вильямс», 2003. – 960 с 7. Грэхем Р., Кнут Д., Паташник О., Конкретная математика. Основание информатики: Пер. с англ. – М.: Мир, 1998. – 703 с. 8. Новиков Ф.А. Дискретная математика для программистов: Учебник для вузов. 3-е изд. – Спб.: Питер, 2008. – 384 с. <p>Репозитарій НАУ: https://er.nau.edu.ua/handle/NAU/9161</p>

Локація та матеріально-технічне забезпечення	Навчальні та мультимедійні аудиторії, проектор
Семестровий контроль, екзаменаційна методика	Диф. залік, тестування
Кафедра	Комп'ютеризованих систем захисту інформації
Факультет	Кібербезпеки, комп'ютерної та програмної інженерії
Викладач(і)	 <p> Ільєнко Анна Вадимівна Посада: Доцент Науковий ступінь: к.т.н. Вчене звання: доцент Профайл викладача: http://kszi.nau.edu.ua/ru/pro-kafedru/kadrovij-sklad/39-vukladachi/87-ilenkoav Тел.: 044 4061809 E-mail: anna.ilienko@npp.nau.edu.ua Робоче місце: 11.118 </p>
Оригінальність навчальної дисципліни	Авторський курс
Лінк на дисципліну	