Освітній компонент	**Вибірковий освітній компонент 5** **«Основи інформаційного захисту та криптографії»**
Рівень ВО	Другий (магістерський)
Назва спеціальності / Освітньо-професійної програми	014 Середня освіта(Математика) / Середня освіта. Математика
Форма навчання	Денна
Курс, семестр, протяжність	2 курс, 3 семестр, 4 кредити ЄКТС
Семестровий контроль	Залік
Обсяг годин (усього: з них лекції / практичні)	Усього: 120 год., з них лекцій – 10 год., практичних – 14 год.
Мова викладання	Українська
Кафедра, яка забезпечує викладання	Кафедра математичного аналізу та статистики
Автор ОК	Канд. фіз.-мат. наук, доц. Соліч Катерина Василівна
Короткий опис	
Вимоги до початку вивчення	Необхідний мінімум для початку вивчення дисципліни – базові знання з алгебри та теорії чисел, обчислювальних методів, інформатики та дискретної математики, комбінаторики; розуміння основ математичних алгоритмів та їх застосування.
Що буде вивчатися	У курсі будуть вивчатися ключові концепції криптографії, такі як симетричні та асиметричні криптосистеми, алгоритми шифрування, методи цифрових підписів, а також принципи створення та управління криптографічними ключами. Особлива увага приділяється питанням захисту інформації в сучасних інформаційних системах, створенню надійних систем зв'язку, забезпеченню безпеки при передачі даних через незахищені канали зв'язку. А також формування у здобувачів вищої освіти знань про: проблеми вразливості інформації в сучасних мережах обміну даними; методологія захисту інформації.
Чому це цікаво / треба вивчати	На сучасному етапі розвитку суспільства однією з найбільших цінностей стала інформація. Тому інформаційні ресурси потребують захисту від різних впливів, які можуть знизити їх цінність. Тому без застосування спеціальних заходів існує дуже висока ймовірність втрати або пошкодження інформації в інформаційно-комунікаційній системі, що завдає значних збитків. Існує декілька напрямків та підходів до захисту інформації, і один із них - це криптографія, тобто захист математичними методами. Це дозволяє поєднувати теоретичні знання з практичними навичкати.

Чому можна навчитися (результати навчання)	• основні криптографічні алгоритми симетричного та асиметричного шифрування, цифрового підпису; • стандартні криптографічні протоколи та порядок їх застосування при захисті інформації; • типові вимоги до систем та засобів управління ключовими даними; • базові стандарти в галузі криптографічного захисту інформації.
Як можна користуватися набутими знаннями й уміннями (компетентності)	Після вивчення даного курсу студенти матимуть необхідні навички для впровадження технологій захисту інформації, вивчення та аналізу сучасних загроз інформаційної безпеки та розробки надійних механізмів для криптографічного забезпечення інформації,