

Опис освітнього компонента вільного вибору

Освітній компонент	Вибірковий освітній компонент1 «Математичні основи криптографії»
Рівень ВО	Перший (бакалаврський) рівень
Назва спеціальності/освітньо-професійної програми	12 Інформаційні технології, 125 Кібербезпека
Форма навчання	Денна
Курс, семестр, протяжність	2 (3 семестр), 5 кредитів ЄКТС
Семестровий контроль	іспит
Обсяг годин (усього: з них лекції/практичні)	150 год, з них: лекц.- 26 год, лаб. - 28
Мова викладання	Українська
Кафедра, яка забезпечує викладання	Комп'ютерних наук та кібербезпеки
Автор ОК	Старший викладач кафедри комп'ютерних наук та кібербезпеки Жигаревич Оксана Костянтинівна
Короткий опис	
Вимоги до початку вивчення	Вивчення на першому курсі, дисциплін «Програмування», «Алгоритми та структури даних», «Математичний аналіз».
Що буде вивчатися	Дисципліна «Математичні основи криптографії» належить до переліку вибірових навчальних дисциплін програми підготовки бакалавра за спеціальністю 125 «Кібербезпека». Вивчається як окремий розділ криптографії та спрямована на вивчення методів отримання вихідного значення зашифрованої інформації за допомогою математичних методів, не маючи доступу до секретної інформації (ключа), необхідної для цього.
Чому це цікаво/треба вивчати	Математичні методи шифрування інформації, дозволять у майбутньому використовувати набуті знання при шифруванні та розшифруванні інформації.
Чому можна навчитися (результати навчання)	Застосовувати метод Цезаря, таблиці Трісімуса, метод Шенонна-Фано на практиці, для шифрування інформації.
Як можна користуватися набутими знаннями й уміннями (компетентності)	ЗК 2. Здатність до абстрактного мислення, аналізу та синтезу. ЗК 3. Здатність застосовувати знання у практичних ситуаціях. ЗК 4. Здатність планувати та управляти часом. ЗК 5. Знання та розуміння предметної області та розуміння професійної діяльності. ЗК 6. Здатність спілкуватися державною мовою як усно, так і письмово ЗК 7. Навички використання інформаційних і комунікаційних технологій. ЗК 8. Здатність вчитися і оволодівати сучасними знаннями. ЗК 9. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК 10. Вміння виявляти, ставити та вирішувати проблеми.
Інформаційне забезпечення	1. Криптоанализ и криптография: история противостояния. [Електронний ресурс]. – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/kriptoanaliz-i-kriptografiya-istoriya-protivostoyaniya/viewer

	2. Анализ симметричных криптосистем. [Электронный ресурс]. – Режим доступа до ресурсу: https://cyberleninka.ru/article/n/analiz-simmetrichnyh-kriptosistem/viewer 3. Шнайер Б. Прикладная криптография, 2-е издание, Протоколы, алгоритмы и исходные тексты на языке С. – М.: “Триумф”, 2001. – 610 с. 4. Baigneres, T. A Classical Introduction to cryptography Exercise Book [Text] / T. Baigneres, P. Junod, Y. Lu, J. Monneart, S. Vaudenay. – Springer, 2006. – 254 p. 5. Hoffstein, J. An Introduction to Mathematical Cryptography [Text] / J. Hoffstein, J. Pipher, J.H. Silverman. – Springer, 2008. – 523 p.
--	---