

### Опис освітнього компонента вільного вибору

Освітній компонент	Вибірковий освітній компонент 11 «Програмування криптографічних алгоритмів та протоколів»
Рівень ВО	Перший (бакалаврський) рівень
Назва спеціальності/освітньо-професійної програми	125 «Кібербезпека»/ «Інформаційна безпека»
Форма навчання	Денна
Курс, семестр, протяжність	4 (7 семестр), 6,5 кредитів ЄКТС
Семестровий контроль	Залік
Кількість кредитів / Обсяг годин (усього: з них лекції/практичні)	195 год, з них: лекц. - 28 год, лаб. - 28 год
Мова викладання	Українська
Кафедра, яка забезпечує викладання	Комп'ютерних наук та кібербезпеки
Автор ОК	Кандидат фізико-математичних наук, доцент кафедри комп'ютерних наук та кібербезпеки <b>Глинчук Людмила Ярославівна</b>
<b>Короткий опис</b>	
Вимоги до початку вивчення	Теорія ймовірностей, Алгебра, Програмування, Основи криптографічного захисту
Що буде вивчатися	Основні симетричні та асиметричні криптографічні алгоритми та методи, хеш-функції, електронний цифровий підпис, криптопротоколи та ін. Особливості програмування криптографічних алгоритмів та протоколів. Вибір мови програмування для завдань криптографічного захисту.
Чому це цікаво/треба вивчати	Криптографічні алгоритми та протоколи мають певну складність та цікаві за своїм змістом та використанням. Дисципліна дасть можливість не тільки зрозуміти криптографічний захист, а і здобути навички програмування таких методів та протоколів.
Чому можна навчитися (результати навчання)	Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. (ПРН 47) Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. (ПРН 48)
Як можна користуватися набутими знаннями й уміннями (компетентності)	Здатність застосовувати знання у практичних ситуаціях. (ЗК 1). Знання та розуміння предметної області та розуміння професії. (ЗК 2). Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. (ЗК4). Здатність до пошуку, оброблення та аналізу інформації. (ЗК 5). Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. (ФК 10).
Інформаційне	1. Глинчук Л.Я. Криптологія: навч.-метод. посіб. / Людмила

забезпечення	<p>Ярославівна Глинчук. – Луцьк: Вежа-Друк, 2014. – 164 с.</p> <p>2. Технології захисту інформації [Електронний ресурс] : підручник для студ. спеціальності 122 «Комп’ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.</p>
--------------	---