

Дисципліна

«Методи і засоби захисту інформації в комп'ютерних системах»

Лектор, науковий ступінь, вчене звання, посада	Пашорін В. І., професор, кандидат технічних наук, професор кафедри інженерії програмного забезпечення та кібербезпеки.
Результати навчання	Формування теоретичних знань та практичних навичок необхідних для ефективного захисту інформації в комп'ютерних системах.
Зміст	<p>Засоби керування безпекою в операційних системах. Адміністрування в операційній системі.</p> <p>Шаблони безпеки. Групова та локальні політики безпеки в операційній системі Windows.</p> <p>Засоби захисту в UNIX-подібних операційних системах.</p> <p>Алгоритми шифрування.</p> <p>Блокові і потокові шифри.</p> <p>Мережа Фейштеля.</p> <p>Архітектура блокових шифрів.</p> <p>Хеш-функції і алгоритми хешування.</p> <p>Режими виконання алгоритмів симетричного шифрування.</p> <p>Цифрові сертифікати в Windows. Формати сертифікатів.</p> <p>Стеганографічні методи захисту інформації.</p> <p>Методи вкладення інформації у файли мультимедіа. Підпис і її властивості.</p> <p>Аутифікація електронних документів. Особливості шифрування ЕЦП.</p> <p>Алгоритм цифрового підпису DSA.</p> <p>Стандарт на процедури ЕЦП.</p> <p>Організаційне забезпечення цифрового підпису. Склад ЕЦП.</p> <p>Технологія застосування ЕЦП.</p> <p>Схеми використання ЕЦП.</p> <p>Інфраструктура відкритих ключів.</p> <p>Призначення і функції Засвідчувального Центру.</p> <p>Електронний сертифікат.</p> <p>Правила застосування і зберігання ЕЦП. Принципи генерації, розподілу та збереження ключів.</p> <p>Закон України «Про електронний цифровий підпис».</p> <p>Кріптопровайдери в системі Windows.</p> <p>Використання функцій CRYPTOAPI для шифрування і расшифрування даних.</p> <p>Використання функцій CRYPTOAPI для отримання і перевірки електронного цифрового підпису.</p>