

## Дисципліна «Основи кібербезпеки»

<b>Лектор, науковий ступінь, вчене звання, посада</b>	Сашньова М.В., доцент, канд. техн. наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки.
<b>Результати навчання</b>	В результаті вивчення дисципліни у студентів повинно бути сформовано: знання опису характеристики «злочинців і героїв» в сфері кібербезпеки; принципів конфіденційності, цілісності та доступності відносно стану даних та заходів протидії загрозам; знання технологій, процесів та процедури для захисту всіх компонентів мережної інфраструктури; вміння описувати тактику, методи та процедури, які використовуються кіберзлочинцями; навички аналізувати та виявляти загрози інформації, а також проводити реалізацію алгоритмів шифрування та дешифрування даних; навички використання законодавчої та нормативно-правової бази, а також вимог відповідних, в тому числі і міжнародних, стандартів та практик щодо безпечного здійснення професійної діяльності; вміння прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави, суспільству, організації та дестабілізуючі чинники в роботі систем управління; вміння розробляти моделі загроз інформації та моделі порушників інформаційної безпеки; вміння реалізовувати організацію безпеки даних на рівні сумісного використання.
<b>Зміст</b>	<p>Основні положення забезпечення кібербезпеки. Сутність кібербезпеки інформаційного суспільства. Потреба в кібербезпеці.</p> <p>Ідентифікація он-лайн, офлайн та персональні дані. Корпоративні дані, наслідки від порушення безпеки. Поняття «кібервійни».</p> <p>Захист даних та конфіденційності.</p> <p>Поняття «кіберзлочинець» та мотиви кіберзлочинців. Навіщо ставати фахівцем з кібербезпеки.</p> <p>Зміст, класифікація та ознаки кіберзагроз. Розповсюдження загроз кібербезпеки.</p> <p>Сутність, цілі та задачі кібернетичних дій.</p> <p>Основи кіберрозвідки.</p> <p>Напрями забезпечення кібербезпеки України. Проблеми забезпечення кібербезпеки на міжнародному рівні.</p> <p>Сутність та класифікація кібератак на інформаційні системи.</p> <p>Технологічні аспекти захисту інформації.</p> <p>Модель кібербезпеки ISO.</p> <p>Шкідливе програмне забезпечення.</p> <p>Методи і засоби соціального інжинірингу. Характеристика сучасних кібератак на інформаційно-комунікаційні технології.</p> <p>Особливості використання технологій та програмних засобів криптозахисту та криптоаналізу інформації в інформаційних системах.</p> <p>Технологічні рішення щодо ідентифікації, автентифікації та авторизації користувачів інформаційної системи.</p> <p>Приховування даних.</p> <p>Типи засобів контролю цілісності даних.</p> <p>Електронний цифровий підпис.</p> <p>Заходи для поліпшення доступності.</p> <p>Впровадження заходів аварійного відновлення. Захист систем та пристроїв.</p> <p>Практичні аспекти забезпечення кібербезпеки. Розуміння етики роботи у кібербезпеці, цивільний захист та безпека праці.</p>