Дисципліна
«Безпека інформаційних мереж та систем»

Лектор, науковий ступінь, вчене звання, посада	Пашорін В. І., професор, к. т. н., проф. кафедри інженерії програмного забезпечення та кібербезпеки.
Результати навчання	Формування теоретичних знань та практичних навичок необхідних для безпечного використання інформаційних технологій в інформаційних системах і мережах а також запобігання розголошенню, витоку і неправомірному оволодінню інформацією, протиправним діям щодо знищення, модифікації, копіювання і блокування інформації.
Зміст	Актуальність безпеки інформаційно-телекомунікаційних систем (ІТС). Основні поняття безпеки ІТС. Моделі безпеки ІТС. Кіберпростір і кібербезпека. Ключові питання безпеки ІТС. Кіберзброя і кібервійни. Загрози безпеки ІТС. Класифікація загроз безпеки. Основні навмисні загрози. Сучасні мережеві загрози: інтернет-шахрайство. Сучасні мережеві загрози: крадіжка особистості. Визначення та класифікація атак на ІТС. Мережеві атаки. Застосування бот-мереж. Порушники безпеки ІТС. Сучасні технології захисту інформаційних ресурсів. Основні методи забезпечення безпеки ІТС. Поняття та класифікація шкідливого програмного забезпечення. Поняття і класифікація комп'ютерних вірусів. Коротка характеристика вірусів. Мережні хробаки. «Троянські програми». Спеціальні шкідливі програми. Соціальна інженерія. Методи виявлення шкідливих програм. Типи і характеристики антивірусних програм. Технологія Whitelisting. Законодавство України по кібербезпеці. Нормативні документи системи технічного захисту інформації. Стандарти інформаційної безпеки. Стандарт TCSEC. Класи безпеки комп’ютерних систем. Міжнародний стандарт ISO 27000«Загальні критерії безпеки інформаційних технологій». Організаційний захист. Структура політики безпеки організації. Зразок політики корпоративної безпеки. Програма безпеки. Процедури реалізації політики безпеки. Патчінг та зниження привілеїв – як організаційні заходи безпеки ІТС. Захист приватності і анонімності при роботі в відкритих мережах. Управління ризиками. Загальна характеристика інженерно-технічних засобів безпеки. Фізичний захист. Технічні канали витоку інформації. Технічні засоби промислового шпигунства. Загальна характеристика програмних засобів безпеки ІТС. Ідентифікація, автентифікація та авторизація суб’єктів ІТС. Види автентифікації суб’єктів ІТС. Парольна автентифікація. Апаратна автентифікація. Автентифікація за допомогою біометричних даних. Автентифікація на основі цифрових сертифікатів. Централізовані системи автентифікації. Концепція єдиного логічного входу. Управління доступом. Дискреційна модель розмежування доступу. Мандатна модель розмежування доступу. Рольова модель розмежування доступу. Реєстрація подій і аудит.