

Назва дисципліни	<b>Безпека інформаційних технологій і систем</b>
Викладач	Жуковицький І.В., д.т.н., професор, зав. кафедрою ЕОМ; т. (056)373-15-89; email: ivzhukl@ua.fm
Курс та семестр, у якому можливе (планується) вивчення дисципліни	Аспірантам PhD, 1 курс, 1 семестр
Факультети, студентам яких пропонується вивчити дисципліну	Комп'ютерні технології та системи
Перелік компетентностей та відповідних результатів навчання, що забезпечує дисципліна	<ul style="list-style-type: none"> <li>- Здатність проводити аналіз безпеки інформаційних технологій, систем, мереж.</li> <li>- Здатність розробляти й моделювати безпечні компоненти інформаційних технологій і систем.</li> <li>- Знати основні нормативно-правові акти в області інформаційної безпеки; основні проблеми в області забезпечення інформаційної безпеки; основні принципи використання методів і засобів забезпечення безпеки інформаційних технологій і систем.</li> <li>- Вміти оцінити ступінь інформаційної безпеки інформаційних систем і мереж; розробляти й моделювати безпечні компоненти інформаційних технологій і систем.</li> </ul>
<b>Опис дисципліни</b>	
Попередні умови, необхідні для вивчення дисципліни	Знання з архітектури комп'ютерів, комп'ютерних мереж, локальних мереж, комп'ютерних систем
Максимальна кількість студентів, які можуть одночасно навчатися	5-10 чоловік
Теми аудиторних занять та самостійної роботи	<p>36 години лекцій, 18 годин практичних занять.</p> <p><b>Основні теми лекцій:</b></p> <ul style="list-style-type: none"> <li>– Основні принципи захисту комп'ютерних систем та мереж, розподілення доступу, аутентифікація;</li> <li>- Основні принципи побудови криптографічних систем симетричної та несиметричної криптографії;</li> <li>- Основні принципи побудови електронного цифрового підпису;</li> <li>- Типові мережеві атаки;</li> <li>- Основні принципи побудови захищених віртуальних мереж (IPSec, SSL, TLS та ін.).</li> </ul> <p><b>Основні теми практичних занять :</b></p> <ul style="list-style-type: none"> <li>- Налаштування пакетних фільтрів з використання програми ipfw і спостереження за результатами їх</li> </ul>

	<p>роботи;</p> <ul style="list-style-type: none"> <li>- Використання internet protocol security (ipsec) для захисту конфіденційних даних, які передаються по протоколу tcp / ip;</li> <li>- Віддалений доступ до мережі з використанням віртуального захищеного з'єднання pptp і l2tp;</li> <li>- Використання протоколу ssl для безпечного взаємодії клієнтів з веб-сервером iis.</li> </ul>
Мова викладання	українська
Рекомендована література	<p><b>Основна</b></p> <ol style="list-style-type: none"> <li>1) Столлингс В. Криптография и защита сетей: принципы и практика. М.: Издательский дом «Вильямс», 2001. – 672с</li> <li>2) Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М.: ДМК Пресс, 2008.</li> <li>3) Мамаев М., Петренко С. Технологии защиты информации в Интернете. Специальный справочник. СПб.: Питер, 2002.</li> <li>4) Жуковицький І.В. Прикладна криптографія. Методичні вказівки до лабораторних робіт. Дніпропетровськ, ДІТ, 2007р.</li> <li>5) Безопасность и резильентность систем и сетей. Практикум / И.В. Жуковицкий, Д.А. Остапец, С.А. Разгонов, А.П. Заец – Под ред. Жуковицкого И.В. – Харьков: Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ». – 2017. – 131 с.</li> <li>6) Навчальні матеріали, розроблені в ході виконання міжнародного проекту SEREIN:  <a href="https://serein.eu.org/teaching-materials/">https://serein.eu.org/teaching-materials/</a> </li> </ol> <p><b>Додаткова</b></p> <ol style="list-style-type: none"> <li>1) В.Зима, А.Молдовян, Н.Молдовян. Безопасность глобальных сетевых технологий. СПб.: БХВ-Петербург, 2000.</li> <li>2) Лукацкий А.В. Обнаружение атак. – СПб.: БХВ-Петербург, 2003. – 608.</li> <li>3) Хорошко В.А., Чекатков А.А. Методы и средства защиты информации.– К.: Издательство Юниор, 2003. – 504 с.</li> <li>4) Архипов О.Є., Луценко В.М., Худяков В.О. Захист інформації в телекомунікаційних мережах та</li> </ol>

системах зв'язку: Навч. – метод. посіб. – К.: ІВЦ «Видавництво «Політехніка», 2003. – 40с.

- 5) Лагун А.Е. Криптографічні системи та протоколи: навч. посібник. Львів : Вид-во Львів. політехніки, 2013. - 96 с.
- 6) Замула А.А. Информационная безопасность в каналах телекоммуникаций : Учеб. Пособие для вузов - 2-е изд. Х.: Регион-информ - Транспорт Украины, 2000. - 216 с
- 7) Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ТИД ДС, 2001. - 688 с.
- 8) Вертузаєв М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібник – К. : Вид-во Європ. ун-ту, 2001. - 321 с.
- 9) Антонюк А.О. Основи захисту інформації в автоматизованих системах: Навч. посібник. – К. : Видавничий дім "КМ Академія", 2003. - 244 с.
- 10) Корниенко А.А., Еремеев М.А., Ададунов С.Е.; ред. Корниенко А.А. Средства защиты информации на железнодорожном транспорте (криптографические методы и средства): учеб. пособие для вузов ж.-д. трансп. М. : Маршрут, 2006. - 253 с.