Силабус дисципліни

Назва дисципліни, обсяг у кредитах ЄКТС	Практика використання апаратно-програмних засобів CISCO для кіберзахисту комп'ютерних мереж (8 кредитів ЄКТС)
Загальна інформація про викладачів	Єгоров Олег Йосипович, к.т.н., доцент, доцент кафедри ЕОМ, 373-15-89, egoroffoleg@ukr.net Заєць Олексій Петрович, ст. викладач кафедри ЕОМ, 373-15-89, zaets.evm.diit@gmail.com
Семестр, у якому можливе (планується) вивчення дисципліни	1 курс, 1,2 семестри (магістри)
Факультети/ННЦ, студентам яких пропонується	КТС
Перелік компетентностей та результатів навчання, що забезпечує дисципліна	Здатність до абстрактного мислення, аналізу та синтезу; здатність використання інформаційних і комунікаційних технологій; здатність до пошуку, опрацювання та аналізу інформації з різних джерел; здатність приймати обґрунтовані рішення; здатність працювати в міжнародному контексті; здатність проводити розробку і дослідження теоретичних та експериментальних моделей захисту об'єктів професійної діяльності; здатність аналізувати, оптимізувати та моделювати складність архітектури комп'ютерних систем та мереж із застосуванням сучасних принципів побудови математичного, програмного, лінгвістичного, технічного та інформаційного забезпечення для захисту інформації; знання основних принципів побудови засобів захисту комп'ютерних систем та мереж, принципів побудови та функціонування їх периферійних засобів; здатність до побудови ефективних алгоритмів формального прогнозу, моделей та методів змістовного прогнозування в науці та техніці шляхом використання принципів функціонування та структури технічних засобів, математичних моделей, історії та логіки розвитку галузі у контексті відповідних величин, феноменів, моделей, методів, функцій та структур технічних засобів, формальних та змістовних методів прогнозування функцій, структур, характеристик та параметрів комп'ютерних систем та мереж; здатність проводити розробку і дослідження теоретичних та експериментальних моделей систем захисту об'єктів професійної діяльності; знати і розуміти наукові і математичні положення, що лежать в основі функціонування програмних, і програмно-технічних засобів захисту інформації в комп'ютерних, системах та мережах; знати професійно-орієнтовані дисципліни спеціальності; мати знання та навички щодо проведення експериментів, збору даних та моделювання загроз в комп'ютерних системах; мати знання із новітніх технологій в галузі кібербезпеки; уміння застосовувати знання і розуміння для розв'язання задач синтезу та аналізу захисних засобів в системах, які характерні обраній спеціальності; уміння використовувати сучасні комп'ютерні засоби системного, функціонального, конструкторського та технологічного проектування для створення сучасних захисних систем; уміння виконувати експериментальні дослідження та застосовувати

	дослідницькі навички за професійною тематикою; уміння здійснювати збір, аналіз науково-технічної інформації, вітчизняного і зарубіжного досвіду з тематики дослідження; уміння використовувати набуті знання з спеціальності для знаходження нових, нешаблонних рішень і засобів їх здійснення при проведенні експериментальних досліджень для розв'язку поставлених задач; уміння опрацьовувати отримані результати, аналізувати та осмислювати їх, представляти результати роботи і обґрунтовувати запропоновані рішення на сучасному науково-технічному і професійному рівні.
Опис дисципліни	
Попередні умови, необхідні для вивчення дисципліни	Вивченню цієї дисципліни має передувати такі дисципліни як «Ділове (наукове) спілкування іноземною мовою», «Теорія проектування захищених комп'ютерних мереж», «Практика проектування захищених інформаційних систем», «Проектування захищених WEB-систем»
Основні теми дисципліни	Куб кібербезпеки. Загрози кібербезпеки, уразливості і атаки. Способи захисту секретної інформації. Концепція "П'ять дев'яток". Захист рівнів забезпечення кібербезпеки. Функції фахівців в області кібербезпеки. Операційні системи. Протоколи, інфраструктури і моніторинг мереж. Моніторинг безпеки комп'ютерних мереж та кінцевих пристроїв.
Мова викладання	Англійська, Українська
Список основної та додаткової літератури	1. Kimberly Graves. CEH: Official Certified Ethical Hacker Review Guide [Текст] / USA: ECCouncil, 2007. – 264 с. 2. Jonathan LeBlanc. Identity and Data Security for Web Development: Best Practices [Текст] / UK.: O'Reilly Media, 2016. – 204 с. 3. Гарасимчук О.І., Дудикевич В.Б., Ромака В.А. Комплексні системи санкціонованого доступу: навч. посібник [Текст] / О.І. Гарасимчук, В.Б. Дудикевич, В.А. Ромака – Л. : Вид-во Львів. політехніки, 2010. –212 с. 4. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. НД ТЗІ 2.5-005-99 [Текст] / ДСТСЗІ СБ України. – К., 1999. – 25 с. 5. Основи інформаційної безпеки [Текст]: навч. пос. / Дудикевич В. Б., Хорошко В.О., Яремчук Ю.Є. – Вінниця : ВНТУ, 2018. – 316 с. **Додаткова** 6. Антонюк А.О. Основи захисту інформації в автоматизованих системах: Навч. посібник [Текст] / К. : Видавничий дім "КМ Академія", 2003. - 244 с. 7. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-002-99 [Текст] / ДСТСЗІ СБ України. – К., 1999. – 31 с. 8. Кулаков Ю. А., Омелянский С. В. Компьютерные сети [Текст] / Киев: Юниор, 1999. – 544 с. 9. Забезпечення інформаційної безпеки держави [Текст] : Навчальний посібник / В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. Львів : Видавництво Львівської політехніки, 2017.— 204 с.