СИЛАБУС
навчальної дисципліни

ЗАХИСТ ТА БЕЗПЕКА КОМП'ЮТЕРНИХ СИСТЕМ

Код та назва дисципліни	М1002 Захист та безпека комп'ютерних систем
Рівень вищої освіти	Другий (магістерський)
Статус дисципліни	Вибіркова дисципліна загально-університетського каталогу
Обсяг дисципліни	4 кредити ЄКТС (120 академічних годин)
Терміни вивчення дисципліни	2 семестр (півсеместр 2.1)
Назва кафедри, яка викладає дисципліну	Інформаційних технологій і систем (ІТС)
Провідний викладач (лектор)	Старший викладач Кліщ Сергій Михайлович E-mail: klishch@metal.nmetau.edu.ua пр. Гагаріна, 4, кімн. 508
Мова викладання	Українська
Передумови вивчення дисципліни	Базові знання роботи з ПК
Мета навчальної дисципліни	Формування знань з безпеки комп'ютерних систем, алгоритмів захисту інформації від несанкціонованого втручання, організації технології захисту комп'ютерних систем.
Очікувані результати навчання	ОРН1. Знати основні інструменти для забезпечення кіберзахисту інфраструктури
	ОРН2. Знати основні фреймворки необхідні для підвищення рівня захищеності об'єкта інфраструктури
	ОРН3. Вміти проводити базову конфігурацію відповідно до політик безпеки для підвищення рівня захищеності
	ОРН4. Вміти проводити базовий аудит безпеки за допомогою автоматизованих інструментів та створювати відповідні репорти

Види та обсяг навчальної діяльності в академічних годинах

Денна форма навчання

Види навчальної діяльності	Усього	Семестри	
		2	
		2.1	2.2
Усього годин за навчальним планом	120	120	
у тому числі: Аудиторні заняття	32	32	
– лекції	16	16	
– лабораторні роботи	16	16	
– практичні заняття	0	0	
– семінарські заняття	0	0	
Самостійна робота	88	88	
– підготовка до аудиторних занять	16	16	
– виконання та захист курсової роботи	–	–	
– виконання та захист індивідуальних завдань	–	–	
– підготовка та складання екзаменів			
– підготовка до інших контрольних заходів	30	30	
– опрацювання розділів, які не викладаються на лекціях	42	42	
Форма семестрового контролю		Диф. залік	

Заочна форма навчання

Види навчальної діяльності	Усього	Семестри	
		5	6
Усього годин за навчальним планом	120		120
у тому числі: Аудиторні заняття	16		16
– лекції	8		8
– лабораторні роботи	8		8
– практичні заняття	–		–
– семінарські заняття	–		–
Самостійна робота	104		104
– підготовка до аудиторних занять	8		8
– виконання та захист курсової роботи	–		–
– виконання та захист індивідуальних завдань	24		24
– опрацювання навчального матеріалу	42		42
– підготовка та складання екзаменів			
– підготовка та складання інших контрольних заходів	30		30
Форма семестрового контролю			Диф. залік

Зміст навчальної дисципліни	Розділ 1. Кар'єра в кібербезпеці, основні напрямки розвитку, стандарти та фреймворки в кібербезпеці, сертифікація Розділ 2. Налаштування віртуального оточення та SOC інфраструктура Розділ 3. Посада секюріті інженера. Основні обов'язки Розділ 4. Підготовка результатів оцінки поточного стану захисту інфраструктури для клієнта
Заходи та критерії оцінювання	За дисципліною передбачені методи поточного оцінювання розділів, а саме: опитування; перевірка та оцінювання виконання лабораторних робіт за розділами 1–4 (Р1, Р2, Р3, Р4). Оцінки розділів 1, 2, 3, 4 (відповідно Р1, Р2, Р3 та Р4) визначаються за 12-бальною шкалою за результатами лабораторних робіт. Семестровий контроль з дисципліни проводиться у формі диференційованого заліку. Оцінка диференційованого заліку визначається як середнє арифметичне визначених за 12-бальною шкалою оцінок розділів дисципліни з подальшим переведенням до 100-бальної шкали за визначеною методикою. Підсумкова оцінка з навчальної дисципліни співпадає з семестровою оцінкою дисципліни (КЗ). Необхідною умовою допуску до семестрового контролю є відпрацювання усіх лабораторних робіт відповідного розділу дисципліни (для заочної форми навчання – виконання та захист індивідуального завдання (ІЗ)).
Політика викладання	Отримання незадовільної (нижче 4 балів за 12-бальною шкалою) оцінки з розділу або її відсутність через відсутність здобувача на контрольному заході не створює підстав для недопущення здобувача до наступного контрольного заходу. Студент не допускається до семестрового контролю за відсутності позитивної оцінки (не нижче 4 балів за 12-бальною шкалою) хоча б з одного із розділів. Оскарження процедури та результатів оцінювання розділів та семестрового оцінювання з боку здобувачів освіти здійснюється у порядку, передбаченому «Положенням про організацію освітнього процесу в УДУНТ». Порушення академічної доброчесності з боку здобувачів освіти, які, зокрема, можуть полягати у користуванні сторонніми джерелами інформації на контрольних заходах, фальсифікації або фабрикації результатів, що були отримані на лабораторних заняттях, тягнуть відповідальність у вигляді повторного виконання сфальсифікованої роботи та повторного проходження процедури оцінювання.
Специфічні засоби навчання	Навчальний процес передбачає використання інструментів для віртуалізації, встановлення різноманітних дистрибутивів операційних систем.

Навчально-методичне забезпечення	**Основна література** 1. Інформаційна безпека : навч. посіб. / Ю. Я. Бобало та ін.;Львів : Вид-во Львів. політехніки, 2019. 573,с. 2. Веселова Л.Ю. Кібербезпека в умовах гібридної війни: адміністративно-правові засади: монографія. Одеса: Гельветика, 2020. 486 с. 3. Інформаційна безпека держави: навч. посіб. / В. М. Рудницький та ін. Харків: ДІСА ПЛЮС, 2018. 358 с. 4. Кавун С.В. Інформаційна безпека: навч. посіб. Харків: Харківський національний економічний ун-т, 2008. 352 с. 5. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб./В. Д. Козюра [та ін.]. Ніжин: Орхідея, 2019. 144 с. **Інформаційні ресурси Інтернет** 1. OWASP Top Ten [Електронний ресурс]. Режим доступу: https://owasp.org/www-project-top-ten/ 2. Web Vulnerability scanner [Електронний ресурс]. Режим доступу: https://portswigger.net/ 3. Penetration testing distribution [Електронний ресурс]. Режим доступу: https://www.kali.org/ 4. SANS [Електронний ресурс]. Режим доступу: https://www.sans.org/ 5. MITRE [Електронний ресурс]. Режим доступу: https://attack.mitre.org/ 6. Reports [Електронний ресурс]. Режим доступу: https://pentestreports.com/