СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БЕЗПЕКА І ЕКСПЛУАТАЦІЯ МЕРЕЖЕВИХ І ХМАРНИХ ТЕХНОЛОГІЙ

Галузь знань	12 Інформаційні технології
Шифр та назва спеціальності	125 Кібербезпека
Назва освітньо-професійної програми	Кібербезпека та захист інформації
Рівень вищої освіти	Перший (бакалаврський)
Факультет	Інформаційних технологій та кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	ОК-23 ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладач

Кільдішев Віталій Йосипович
kildishev@ukr.net

Доцент кафедри Кібербезпеки та технічного захисту інформації,
кандидат технічних наук, доцент

Загальна інформація про дисципліну

Анотація до дисципліни	Дисципліна «Безпека і експлуатація мережевих і хмарних технологій» базується на професійно-орієнтованих дисциплінах. Предметом вивчення навчальної дисципліни є правильні настройки привілеїв і прав доступу користувачів і додатків до тих ресурсів, для роботи з якими вони мають необхідні повноваження, а також виконання запису до журналу подій, моніторингу та аналізу журналів, підготовки необхідної звітності IT систем, безпека IT систем, яка пов'язана з конфігураціями, продуктивністю, стійкістю до відмов, веденням обліку, проведенням перевірок, дотримання діючих операційних стандартів і вимог.

Мета дисципліни	– формування основ знань що забезпечують правильну настройку привілеїв і прав доступу користувачів і додатків до тих ресурсів, для роботи з якими вони мають необхідні повноваження, а також виконання запису до журналу подій, моніторингу та аналізу журналів, підготовки необхідної звітності IT систем.
Компетентності, формуванню яких сприяє дисципліна	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. КФ 9. Здатність здійснювати професійну діяльність на основі впровадження системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
Результати навчання	ПРН 4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого

	доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
Обсяг дисципліни	Загальний обсяг дисципліни: 4 кредиту ЄКТС 120 годин. Для денної форми навчання: лекції – 14 годин, практичні заняття –14 годин, лабораторні заняття –14 годин,самостійна робота – 78 годин.
Форма підсумкового контролю	Екзамен
Терміни викладання дисципліни	Дисципліна викладається у 1-му семестрі (1–14 тижні)

Програма дисципліни

Тема 1.	***Роль департаменту експлуатації.*** Захищена мережева інфраструктура та її основні елементи на різних рівнях.
Тема 2.	***Адміністративне управління.*** Диверсифікованість комп'ютерних систем для підвищення їх надійності й захищеності.
Тема 3.	***Рівень гарантій.*** Організація зберігання ключів.
Тема 4.	***Управління конфігурацією.*** Організація доступу до файлів.
Тема 5.	***Витік даних. Доступність мережі і ресурсів.*** Особливості захисту даних від зміни.
Тема 6.	***Мейнфрейми. Безпека електронної пошти.*** Методи захисту від вразливості "переповнення буфера".
Тема 7.	***Тестування вразливостей.*** Вразливості комп'ютерних систем.

Список рекомендованих джерел

1. Бурячок, В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубко. – К.: ДУТ, 2015. – 288 с.

2. Кібербезпека мереж наступного покоління: навч. посібник / Вараксін О.О., Кільдішев В.Й. Кононович В.Г. За ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – С. 234.
3. Захарченко М.В. Інформаційна безпека інформаційно-комунікаційних систем. Захист інформації від НСД у каналах зв'язку: навч. посіб. / М.В. Захарченко, В.В. Топалов, М.С. Русляченко // За ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2014. – 228 с.
4. Кононович В.Г., Гладиш С.В. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Частина 4: навч. посіб. – Одеса: ОНАЗ ім. О.С. Попова, 2009.

Інформація про консультації

Щопонеділка у вересні-грудні 2023 року з 13^{00} до 14^{30} год., ауд. 250 або zoom – доц. В. Й. Кільдішев

Загальна схема оцінювання

Сума балів за всі види навчальної діяльності	**Шкала ЄКТС**	**Оцінка за національною шкалою**		**Нарахування балів**	**Бали нараховуються таким чином:**
		для іспиту	**для заліку**		
90-100	A	Відмінно	зараховано		***Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою*** і становить: за поточну успішність (участь у практичних заняттях, виконання практичних завдань та контрольних робіт) – до 60 балів, за результати екзамену – до 40 балів.
82-89	B	Добре			
74-81	C				
64-73	D	Задовільно			
60-63	E				
35-59	FX	Незадовільно з можливістю повторного складання	Не зараховано з можливістю повторного складання		
0-34	F	Незадовільно з обов'язковим повторним вивченням дисципліни	Не зараховано з обов'язковим повторним вивченням дисципліни		

Політика опанування дисципліни

Відвідування: Здобувачі вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на практичних заняттях, лабораторних заняттях та контрольних заходах (екзамен/залік) є обов'язковою. При проведенні занять в онлайн режимі, присутність здобувача враховується у разі відкритого вікна.

Дотримання принципів академічної доброчесності: Підготовка усіх завдань, письмових робіт і т. ін., що виконуються в межах дисципліни, здійснюється здобувачем вищої освіти самостійно, на засадах академічної доброчесності. Викладач має право для перевірки робіт застосовувати програму **Unicheck.**

Умови зарахування пропущених занять:

Інші умови: Навчально-методичні матеріали дисципліни розміщені на платформі Moodle, за посиланням https://e-learning.suitt.edu.ua/course/view.php?id=936