СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

СПЕЦІАЛЬНІ ВИМІРЮВАННЯ В ГАЛУЗІ ТЗІ

Галузь знань	12 Інформаційні технології
Шифр та назва спеціальності	125 Кібербезпека та захист інформації
Назва освітньо-професійної програми	Кібербезпека та захист інформації
Рівень вищої освіти	Другого (магістерського) рівня
Факультет	Інформаційних технологій та кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	ОК 3 ОПП «Кібербезпека та захист інформації»»
Форма навчання	Денна

Викладач

Онацький Олексій Віталійович
onatsky@meta.ua

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

Загальна інформація про дисципліну

Анотація до дисципліни	У дисципліні розглядається порядок проведення робіт з технічного захисту інформації, а саме: організаційні заходи; заходи з технічного захисту мовної інформації; заходи з технічного захисту інформації, яка обробляється в інформаційно-комунікаційних системах; сутність, шляхи та запобігання утворення технічних каналів витоку інформації: мовної та візуальної інформації, матеріально-речовинні канали витоку інформації, технічні канали витоку інформації, що обробляється основними та допоміжними технічними засобами системи, технічні канали витоку інформації на основі закладних пристроїв. Розглядається порядок розроблення технічного завдання, перелік основних

	робіт етапу формування технічного завдання, зміст технічного завдання, створення комплексу технічного захисту інформації, модель загроз для інформації: ситуаційний та генеральний план об'єкту інформаційної діяльності, схеми розташування та опис ОТЗС та ДТЗС, обґрунтування можливості створення технічних каналів витоку інформації. Розглядається порядок розроблення та оформлення програм і методик випробувань, проведення атестації комплексу технічного захисту інформації, основні технічні характеристики вимірювальної апаратури, приклади оформлення протоколів спецдослідження або перевірки захищеності виділеного приміщення різної категорії від можливого витоку мовної інформації з обмеженим доступом акустичним, віброакустичним та акустоелектричним каналом.
Мета дисципліни	– ознайомлення студентів із методами впровадження систем та комплексів захисту інформації, їх склад і призначення, з застосуванням існуючої нормативної бази в Україні; – розвиток у студентів практичних навичок у послідовності розробки комплексу технічного захисту інформації; – підготовка висококваліфікованих фахівців, здатних ставити завдання на виконання етапів технічного проекту і вибирати способи їх реалізації.
Компетентності, формуванню яких сприяє дисципліна	КЗ-1 Здатність застосовувати знання у практичних ситуаціях. КЗ-2 Здатність проводити дослідження на відповідному рівні. КФ 1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ 2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ 8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
Результати навчання	РН 6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН 7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН 13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
Обсяг дисципліни	Загальний обсяг дисципліни: 4 кредитів ЄКТС 120 годин. Для денної форми навчання: лекції – 14 годин, практичні заняття –12 години, лабораторні заняття – 14 годин, самостійна робота – 80 годин.
Форма підсумкового	

контролю	Екзамен
Терміни викладання дисципліни	Дисципліна викладається у 1-му семестрі (1–18 тижні)

Програма дисципліни

Тема 1.	***Вимоги щодо захисту інформації та кіберзахисту.*** Поняття комплексних систем захисту інформації та комплексів технічного захисту інформації, їх склад і призначення.
Тема 2.	***Класифікація технічних каналів витоку інформації.*** Сутність, шляхи та запобігання утворення технічних каналів витоку інформації.
Тема 3.	***Порядок проведення робіт з технічного захисту інформації.*** Передпроектні роботи щодо систем та комплексів захисту інформації.
Тема 4.	***Створення комплексів технічного захисту інформації.*** Попередні випробування та дослідна експлуатація комплексів технічного захисту інформації.
Тема 5.	***Атестації комплексів технічного захисту інформації.*** Оцінювання ефективності комплексу технічного захисту інформації, що циркулюватиме на об'єкті інформаційної діяльності, на відповідність вимогам нормативних документів з технічного захисту інформації.
Тема 6.	***Система технічних документів щодо систем і комплексів захисту інформації.*** Склад та зміст проектної, експлуатаційної та нормативно-розпорядчої документації. Документація, що розробляється на етапі виконання передпроектних робіт. Нормативно-розпорядча документація.
Тема 7.	***Порядок проведення робіт з державної експертизи комплексної системи захисту інформації.*** Порядок проведення робіт з первинної експертизи засобів технічного захисту інформації від несанкціонованого доступу. Особливості проведення робіт з додаткової та контрольної експертизи засобів технічного захисту інформації.

Список рекомендованих джерел

1. Засоби та системи технічного захисту інформації : навч. посіб. для студентів спеціальності 125 "Кібербезпека" спеціалізації "Системи технічного захисту інформації" / І. Є. Антіпов, А. М. Олейніков, Ю. В. Ликов и др. ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків : ХНУРЕ, 2019. – 216 с.

2. Положення про Державну експертизу в сфері технічного захисту інформації. – Затверджено наказом Адміністрації ДССЗЗІ України № 93 від 16.05.07. – Офіційний вісник України. – 2007. – № 52, ст. 2153. – (Серія видань "Нормативний документ").

3. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. – Затверджено наказом ДСТСЗІ СБ України № 125 від 8.11.2005. – (Серія видань "Нормативний документ").

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.
5. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. – Затверджено наказом Адміністрації ДССЗЗІ України № 65 від 12 березня 2011. – (Серія видань “Нормативний документ”).
6. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В.Р – Київ.: ООО "Д.В.К.", 2004. – 508 с.
7. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22 від 28.04.1999. – (Серія видань “Нормативний документ”).
8. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. – Затверджено наказом ДСТСЗІ СБ України № 22 від 28.04.99. – (Серія видань “Нормативний документ”).

Інформація про консультації

Щопонеділка у вересні-грудні 2023 року з 14^{30} до 15^{00} год., ауд. 248 або зум – доц. О. В. Онацький

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 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=27