СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

МОНІТОРИНГ ТА АУДИТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

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 і кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	ОК-10 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 «Моніторинг та аудит інформаційно-комунікаційних систем» має міждисциплінарний характер. Вона інтегрує комплекс знань, умінь та навичок які охоплюють предметну область фахівців як безпосередньо з

	кібербезпеки, так і з технічного захисту інформації та управління інформаційною безпекою з відповідними освітніми компонентами. Навчання спрямовано на формування професійних компетенцій, знань, умінь та навичок на основі професійного стандарту «Фахівець сфери захисту інформації», затвердженого наказом Адміністрації Держспецзв'язку № 715 від 25.11.2022, наприклад:: 1) методи та технології моніторингу та аудиту загроз для конфіденційності, цілісності та доступності інформації; 2) методи, засоби та інформаційні технології виявлення несанкціонованого доступу до інформації на різних ієрархічних рівнях інформаційно-комунікаційної системи; 3) здійснювати моніторинг та аудит загроз для інформації в інформаційних системах та мережах та оцінку ризиків безпеки інформації; 4) здійснювати моніторинг та аудит загроз для інформації, що озвучується.
Мета дисципліни	– формування знань щодо способів сканування та розпізнавання вразливостей у системах безпеки для інформації в інформаційних системах і мережах та компетенції щодо здатності здійснювати постійний моніторинг та аудит загроз для інформації та відповідну модернізацію систем і комплексів захисту інформації.
Компетентності, формуванню яких сприяє дисципліна	КІ-1. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки. КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ2. Здатність проводити дослідження на відповідному рівні. КЗ3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому. КФ14. Здатність здійснювати постійний моніторинг та аудит загроз для інформації та відповідну модернізацію (доробку) систем і комплексів захисту інформації. КФ15. Здатність проводити процедури сканування вразливостей і розпізнавання вразливостей в системах безпеки.
Результати навчання	РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а

	також розвитку технологій створення та використання спеціалізованого програмного забезпечення. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН27. Здійснювати моніторинг та аудит загроз для інформації в інформаційних системах та мережах та оцінку ризиків безпеки інформації. РН28. Здійснювати моніторинг та аудит загроз для інформації, що озвучується. РН29. Використовувати інструменти та технології безперервного моніторингу з метою оцінки ризиків, користуватися прикладними програмами моніторингу та аудиту загроз для інформації в інформаційних системах та мережах РН30. Проводити сканування вразливостей і розпізнання вразливостей в ІКС і системах безпеки.
Обсяг дисципліни	Загальний обсяг дисципліни: 5 кредитів ЄКТС 150 годин. Для денної форми навчання: лекції – 18 годин, практичні заняття –16 години, лабораторні заняття –16 години, самостійна робота – 100 годин.
Форма підсумкового контролю	Екзамен
Терміни викладання дисципліни	Дисципліна викладається у 2-му семестрі (1–18 тижні)

Програма дисципліни

Тема 1.	***Загальні принципи аудиту інформаційної безпеки*** Основні цілі та задачі моніторингу та аудиту інформаційних систем.
Тема 2.	***Цілі та метод проведення зовнішнього аудиту***

	Основи проведення аудиту безпеки інформаційно-комунікаційних систем.
Тема 3.	***Аналіз і оцінка ризиків інформаційної безпеки*** Аналіз ризиків для оцінки реальних загроз порушення інформаційної безпеки.
Тема 4.	***Безперервний внутрішній аудит інформаційної безпеки інформаційно-комунікаційних систем*** Здійснення збирання та попередній аналіз даних, планування заходів з підготовки та проведення аудиту.
Тема 5.	***Відповідність аудиту інформаційної безпеки міжнародним стандартам*** Характеристика сучасної національної та міжнародної нормативної бази у сфері інформаційної безпеки.
Тема 6.	***Тестування вразливостей. Етапи тестування на проникнення*** Оформлення аудиторського звіту, аналіз відповідних ризиків та рекомендації щодо їх усунення.

Список рекомендованих джерел

1. Тардаскіна Т. М. Менеджмент інформаційної безпеки в галузі зв'язку: навч. посібник. / Т. М. Тардаскіна, В. Г. Кононович. – Одеса: ОНАЗ, 2010. – 268 с.
2. Програми та методики державної експертизи інформаційної захищеності телекомунікацій: навч. посіб. / С.М. Горохов, Н. В. Кондратьєва, В.Г. Кононович, С.В. Стайкуца; за ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – 252 с.
3. 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.
4. 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.

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
82-89	B	Добре			
74-81	C				
64-73	D	Задовільно			

60-63	E				40 балів.
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=591