СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

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-21 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 «Методи та засоби захисту інформації» базується на професійно-орієнтованих дисциплінах. Предметом вивчення навчальної дисципліни є види, джерела та носії інформації, що підлягає захисту, технічні канали витоку інформації, інженерно-технічний захист інформації, принципи функціонування систем технічного захисту інформації, характеристики існуючих систем технічного захисту інформації, принципи побудови систем технічного захисту

	інформації,контроль ефективності технічного захисту інформації.
Мета дисципліни	– формування базових знань механізмів функціонування сучасних систем технічного захисту інформації, придбання умінь користуватися концептуальними принципами побудови систем технічного захисту інформації, отримання навичок для розв'язування реальних задач, які виникають під час експлуатації та модернізації існуючих систем технічного захисту інформації.
Компетентності, формуванню яких сприяє дисципліна	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

Результати навчання	ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. 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 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та кібербезпеки. ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. ПРН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. ПРН 12. Розробляти моделі загроз та порушника. ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент. ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних. ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки. ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

	ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових). ПРН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту. 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. ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки. ПРН 29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів. ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем. ПРН33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків. ПРН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки. ПРН 36. Виявляти небезпечні сигнали технічних засобів. ПРН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах. ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

	ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах. ПРН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних). ПРН 52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах. ПРН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
Обсяг дисципліни	Загальний обсяг дисципліни: 9 кредитів ЄКТС 270 годин. Для денної форми навчання: лекції – 38 годин, практичні заняття –18 годин, лабораторні заняття –52 години, самостійна робота – 162 години.
Форма підсумкового контролю	Екзамен
Терміни викладання дисципліни	Дисципліна викладається у 6-му та 7-му семестрі

Програма дисципліни

Тема 1.	***Основні властивості інформації з позицій її технічного захисту.*** Види інформації, класифікація засобів шпигунства.
Тема 2.	***Характеристики та способи запису сигналів на носії.*** Основні тактико-технічні параметри засобів інформаційної розвідки.
Тема 3.	***Демаскуючі прикмети об'єктів інформаційної діяльності.*** Технологічна класифікація спеціальних технічних засобів.
Тема 4.	***Джерела та носії конфіденційної інформації.*** Спеціальні технічні засоби негласного одержання акустичної (мовний) інформації.
Тема 5.	***Джерела небезпечних сигналів.***

	Техніка перехоплення телефонних розмов і повідомлень.
Тема 6.	***Загрози безпеці інформації.*** Спеціальні фото, відео й оптичні системи.
Тема 7.	***Способи несанкціонованого доступу до джерел інформації.*** Технічні засоби негласного перехоплення й реєстрації інформації з технічних каналів зв'язку.
Тема 8.	***Способи і засоби добування інформації технічними засобами.*** Спеціальні технічні засоби для негласного дослідження предметів і документів.
Тема 9.	***Способи і засоби перехоплення сигналів.*** Спеціальні технічні засоби для негласного проникнення й обстеження приміщень, транспортних засобів і інших об'єктів.
Тема 10.	***Способи і засоби підслуховування акустичних сигналів.*** Спеціальні технічні засоби для негласного одержання (зміни, знищення) інформації з технічних засобів її зберігання, обробки й передачі.
Тема 11.	***Характеристики каналів витоку інформації.*** Спеціальні технічні засоби для негласної ідентифікації особистості.
Тема 12.	***Оптичні канали витоку інформації.*** Спеціальні технічні засоби для негласного контролю над переміщенням транспортних засобів і інших об'єктів.
Тема 13.	**Радіоелектронні та акустичні канали витоку інформації.** Пристрої та системи технічної розвідки.
Тема 14.	***Концепції інженерно-технічного захисту інформації.*** Протидія комерційній розвідці за допомогою технічних засобів.
Тема 15.	***Способи і засоби захисту інформації від спостереження.*** Соціальний фактор у захисті комп'ютерних систем.
Тема 16.	***Способи і засоби захисту інформації від підслуховування.*** Побудова програмно-апаратних комплексів шифрування.
Тема 17.	***Способи і засоби попередження витоку інформації за допомогою закладних пристроїв.*** Ідентифікація користувачів – суб'єктів доступу до даних.
Тема 18.	***Способи і засоби попередження витоку інформації через побічні електромагнітні випромінювання та наводки.*** Захист систем електронної комерції. Основні уразливості, погрози й варіанти захисту.
Тема 19.	***Способи попередження витоку інформації матеріально-речовинному каналу.*** Основні підходи до захисту даних від НСД.

Список рекомендованих джерел

1. Методи та засоби захисту інформації: Навчальний посібник для студентів вищих навчальних закладів./А.М. Олейніков. –Харків:НТМТ, 2014. –298с.
2. Фізичні основи захисту інформації в радіоелектронній апаратурі: навч. посіб./ Д.В. Євграфов. –К.:НТУУ"КПІ", 2014. –176с.
3. Методики оцінки інформаційної захищеності : навч. посібник / Н.В. Кондратьєва, В.Г. Кононович, О.В. Кочетков За ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2012. – С. 234.
4. Тардаскін М.Ф., Савицький Л.Ю., Кононович В.Г., Технічна експлуатація систем захисту інформації. Частина 1. Захист мовної інформації в каналах зв'язку та на об'єктах інформаційної діяльності: Навч. посібник / за ред. М.В. Захарченко. – Одеса: ОНАЗ, 2004. – С 188.

Інформація про консультації

Щопонеділка у вересні-грудні 2024 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=928