СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ОРГАНІЗАЦІЯ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ»

Лектор курсу	Котенко Андрій Миколайович, кандидат технічних наук, доцент кафедри технічних систем кіберзахисту	**Контактна інформаціялектора (e-mail), сторінка курсу в Moodle**	a.kotenko@duikt.edu.ua https://classroom.google.com/c/ODI2MjYyMjA3MDEw?cjc=fm67s6us Код доступу fm67s6us
Галузь знань	F Інформаційні технології	**Рівень вищої освіти**	Магістри
Спеціальність	F5 Кібербезпека та захист інформації	**Семестр**	9
Освітня програма	Технічні системи інформаційного та кібернетичного захисту	**Тип дисципліни**	Вибіркова компонента ВК - 4

Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	24	-	18	12	96

АНОТАЦІЯ КУРСУ

Взаємозв'язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	Методи та засоби захисту інформації
Освітні компоненти для яких є базовою	Написання кваліфікаційної роботи магістра

Мета курсу:	Надбання студентами теоретичних знань та практичних навичок для організації захисту конфіденційної інформації

Компетентності відповідно до освітньої програми

Soft- skills / Загальні компетентності (КЗ)	**Hard-skills / Спеціальні компетентності (КФ)**
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	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 3. Здатність досліджувати ,розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури

	КФ 5 Здатність до дослідження системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації КФ6 Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації 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 КФ8 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 КФ11 Здатність створювати методики ліцензування , атестації та сертифікації у сфері захисту інформації на об'єктах інформаційної діяльності КФ12. Здатність розробляти технічну документацію для проведення тестування, налагоджування та допоміжних заходів щодо функціонування та експлуатації систем захисту інформації на об'єктах інформаційної діяльності.
Програмні результати навчання (ПРН)	
РН 7 Обгрунтовувати використання ,впроваджувати впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки РН-8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. РН 10 Забезпечувати безперервність бізнес/операційних процесів , а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації РН-11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. РН 15 Зрозуміло і недвузначно доносити власні висноки з проблем інформаційної безпеки та/або кібербезпеки організації а також знання та пояснення, що їх обгрунтовують до персоналу, партнерів та інших осіб	

РН 22 Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи і експерименти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки РН 25. Розділяти складові, які відносяться до інформаційної безпеки та захисту інформації на об'єктах інформаційної діяльності. РН 28. Виявляти пристрої несанкціонованого зняття інформації на об'єктах інформаційної діяльності			
ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Тема 1. Види інформації за режимом доступу. Правове забезпечення захисту інформаційних ресурсів обмеженого доступу. Загрози втрати інформації з обмеженим доступом. **Знати.** Проблеми захисту інформації в Україні. Розподіл інформації за режимом правового доступу. Закон України про захист інформації в інформаційних, електронних комунікаційних та комунікаційних системах. **Вміти**. Користуватись нормативними документами технічного захисту інформації. Визначати потенційні канали втрати інформації в автоматизованих системах та на ОІД **Формування компетенцій:** КЗ1, КЗ3; КФ2, КФ3, КФ5, КФ6, КФ8 **Результати навчання:** РН7, РН8, РН10, РН11, РН25 **Рекомендовані джерела:** 1-5, 10			
Інформаційний ресурс як об'єкт захисту	Лекція 1 2 год.		Лекція-презентація, експрес-опитування здобувачів
Загрози втрати конфіденційної інформації	Лекція 2 2 год		Лекція-презентація, експрес-опитування здобувачів.
Вимоги до порядку обліку та зберігання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію.	Практичне заняття 1 2 год	2	Оволодіти практичними навичками обліку та зберігання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію.
Технології перехоплення акустичній конфіденційній інформації	Лекція 3 2 год		Лекція-презентація, експрес-опитування здобувачів.
Виявлення витоку конфіденційної акустичної інформації радіоканалом на ОІД	Лабораторна 1 2 год.	2	Оволодіти практичними навичками користування скануючим приймачем
Захист акустичної конфіденційної інформації	Лекція 4 2 год.		Лекція-презентація, експрес-опитування здобувачів.
Вимоги до порядку використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію.	Практичне заняття 2 2 год.	2	Оволодіти практичними навичками використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію

Дослідження генератору акустичного зашумлення для захисту конфіденційної акустичної інформації	Лабораторна 2 2 год.	2	Оволодіти практичними навичками застосування засобів захисту акустичної інформації
Загрози втрати конфіденційної інформації в автоматизованих системах	Лекція 5 2 год		Лекція-презентація, експрес-опитування здобувачів.
Дослідження порядку пошуку детектором нелінійних переходів радіотехнічних приладів	Лабораторна 3	2	Оволодіти практичними навичками пошуку закладних пристроїв на ОІД
Обстеження середовищ функціонування ІКС	Практичне заняття 3		Оволодіти практичними навичками визначення потенційних шляхів втрати інформації в ІКС
Захист конфіденційної інформації від витоку в автоматизованих системах	Лекція 6 2 год.		Лекція-презентація, експрес-опитування здобувачів.
Дослідження генератора просторового зашумлення радіодіапазону	Лабораторна 4 2 год.		Оволодіти практичними навичками створення активної системи захисту інформації від витоку через ПЕМВН
Пасивні засоби захисту інформації в ІКС	Практичне заняття 4 2 год.	2	Оволодіти практичними навичками створення пасивної системи захисту інформації від наведень ПЕМВ
Захист конфіденційної інформації на матеріальних носіях	Лекція 7 2 год		Лекція-презентація, експрес-опитування здобувачів
Дослідження системи захисту конфіденційної інформації від витоку матеріально-речовим каналом	Лабораторна 5 2 год.	2	Оволодіти практичними навичками використання засобів захисту конфіденційної інформації від витоку матеріально-речовим каналом
Тема 1. Види інформації за режимом доступу. Правове забезпечення захисту інформаційних ресурсів обмеженого доступу. Загрози втрати інформації з обмеженим доступом.	Самостійна робота	12	Види інформації за режимом доступу. Вимоги до захисту інформаційних ресурсів в ІКС та на ОІД. Причини втрати акустичної конфіденційної інформації. Причини втрати конфіденційної

			інформації в ІКС. Методи та засоби захисту конфіденційної інформації в ІКС.
Тема 2. Системний підхід до захисту конфіденційної інформації. Побудова системи захисту конфіденційної інформації **Знати**: Склад проектної документації на систему захисту конфіденційної інформації. **Вміти**: Складати проектну документацію системи захисту конфіденційної інформації . **Формування компетентностей:** К31, К32, К33, К34; КФ2, КФ11, КФ 12 **Результати навчання:** РН7, РН8, РН10, РН15, РН20, РН22, РН25, РН 28 **Рекомендовані джерела:** 1-11.			
Система захисту конфіденційної інформації на ОІД	Лекція 8 2 год.		Лекція-презентація, експрес-опитування здобувачів.
Розробка акту обстеження фізичного середовища	Практичне заняття 5 2 год.	2	Оволодіти практичними навичками обстеження ОІД з метою виявлення потенційних шляхів витоку інформації з ОІД
Розроблення та впровадження заходів із захисту акустичної конфіденційної інформації на ОІД	Лекція 9 2 год.		Лекція-презентація, експрес-опитування здобувачів.
Дослідження засобів локалізації місцезнаходження закладних пристроїв на ОІД	Лабораторна 6 2 год.	2	Оволодіти практичними навичками по використанню детекторів електро магнітного поля
Система захисту конфіденційної інформації в інформаційно-комунікаційній системі	Лекція 10 2 год.		Лекція-презентація, експрес-опитування здобувачів
Дослідження принципу виявлення закладних пристроїв багатофункціональним комплексом DJ Scan	Лабораторна 7 2 год.	2	Оволодіти практичними навичками пошуку ЗП на ОІД багатофункціональним комплексом DJ Scan
Розробка моделі загроз інформації в ІКС	Практичне заняття 6	2	Оволодіти практичними навичками розробки моделі загроз інформації в ІКС
Служба захисту конфіденційної інформації в ІКС	Лекція 11 2 год.		Лекція-презентація, експрес-опитування здобувачів

Дослідження принципу виявлення закладних пристроїв в ІЧ діапазоні багатофункціональним комплексом DJ Scan	Лабораторна 8 2 год.	2	Опанувати принцип пошуку ЗП що використовує ІЧ діапазон для передачі сигналу
Організаційні аспекти захисту конфіденційної інформації в Інформаційно-комунікаційній системі	Лекція 12 2 год.		Лекція-презентація, експрес-опитування здобувачів
Дослідження методу оцінки якості захисту акустичної інформації на ОІД приладом ST 032 Піран'я	Лабораторна 9 2 год.	2	Опанувати метод оцінки якості захисту акустичної інформації на ОІД
Тема 2. Системний підхід до захисту конфіденційної інформації. Побудова системи захисту конфіденційної інформації	Самостійна робота	14	Системи захисту конфіденційної інформації на ОІД. Засоби захисту конфіденційної інформації на ОІД. Оцінка якості захисту акустичної

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проектор;
- Навчальна лабораторія пошуку закладних пристроїв
- Програмне забезпечення.Windows 8,10, MicrosoftOffice.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1, Політанський В.С., Шаповал Р.В. Правові основи кібербезпеки та захисту інформації. Підручник. – ISBN 978-617-8574-84-0/ Київ, Видавни
Олді, 2026. – 306 с.

2. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення https://tzi.com.ua/index_ua.html

3. Технічний захист інформації. Навчальний посібник Богуш В.М., Бровко В. Д., КобусО.С., КозюраВ.Д. – Київ: Видавництво Ліра-К, 2022. - 286
https://knushop.com.ua/image/catalog/lira20230617/pdf/13054.pdf

4. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22. https://tzi.com.ua/downloads/2.5-004-99.pdf

5. НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформа
обмеженим доступом, що не становить державної таємниці https://tzi.com.ua/downloads/1.6-005-2013.pdf

6. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. https://tzi.com.ua/downloads/1.4-001-2000.

7. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизов
системі. https://tzi.com.ua/downloads/3.7-001-99.pdf

8. Технології захисту інформації в інформаційно-телекомунікаційних системах [навч. посіб.] / А.В. Жилін, О.М. Шаповал, О.А. Успенський. – КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
9. Котенко А.М., Хлапонін Ю.І. Конспект лекцій для студентів спеціальності 125 “Кібербезпека та захист інформації“ з дисципліни “Програм апаратні засоби захисту“. - К.: КНУБА, 2025 – 154 с.
10. Лаптєв О.А., Савченко В.А., Шуклін Г.В. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльно – К.: ДУТ. – 2020. – 126 с.
11. Богуш В.М., Бровко В. Д., Кобус О.С., Козюра В.Д. Технічний захист інформації. К., ІТ-право, 2022 р., 508 с.

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов’язкове відвідування лекцій і практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, проведення тестових розрахунків рівнів сигналів для їх подальшого аналізу, поглиблене вивчення матеріалу за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо здобувач відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультується з викладачем.

Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації здобувач повинен вказати джерело, використане в ході виконання завдання.

КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є набрання студентом 60 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	• Виконання практичних робіт	12
	• Виконання лабораторних робіт	18
	• Самостійна робота	30
ПІДСУМКОВЕ ОЦІНЮВАННЯ залік	Метою екзамену є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. • Екзамен проходить у письмовій формі.	30 балів
Додаткова оцінка		
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:		

тези доповіді на фаховій конференції;	2 бали
стаття у фаховому виданні України;	6 балів
стаття в іноземному рецензованому виданні.	10 балів

Максимальна кількість додаткових балів, які можуть бути зараховані здобувачу освіти – 10 балів.

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ
Критерії оцінювання
Рівень компетентності

бали	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або аспірант проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції аспіранта в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	**Оцінка /**запис в екзаменаційній відомості
90-100	Студент демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	**Достатній** Забезпечує аспіранту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни	Відмінно / Зараховано (А)

82-89	Студент в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (B)
75-81	Студент засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Добре / Зараховано (C)
67-74	Студент має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, аспірант з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (D)
60-66	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни аспірант виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у аспіранта відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни	Задовільно / Зараховано (E)
35-59	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Аспірант не допущений до здачі заліку.	**Незадовільний** Студент не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
0-34	Здобувач повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними.	**Незадовільний** Здобувач не підготовлений	Незадовільно з

	Здобувач не допущений до здачі екзамену/заліку.	до самостійного вирішення задач, які окреслює мета та завдання дисципліни.	обов’язковим повторним вивченням / Не допущений (F) В залікову книжку не проставляється

ПОЛІТИКА ДОБРОЧЕСНОСТІ

Здобувач вищої освіти виконуючи самостійну або індивідуальну роботу повинен дотримуватись політики доброчесності.

У разі наявності плагіату в будь-яких видах робіт здобувача, він отримує незадовільну оцінку і повинен повторно виконати завдання, які передбачені у Силабусі.