



СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Комплекси технічного захисту інформації

Рівень вищої освіти	Другий (магістерський)
Код та назва спеціальності, галузь знань	F5 Кібербезпека та захист інформації; F Інформаційні технології
Тип та назва освітньої програми	Освітньо-професійна програма «Кібербезпека та захист інформації»
Статус навчальної дисципліни	Обов'язкова компонента (ОК-3)
Курс, семестр викладання	1 курс, 1 семестр
Трудомісткість навчальної дисципліни	4 кредити ЄКТС (120 академічних годин), з них: денна (очна) форма навчання: лекц. – 18 год., лаб.зан. – 12 год., практ. зан. – 14 год., самост. роб. – 76 год.; заочна форма навчання: лекц. – 10 год., лаб.зан. – 6 год., практ. зан. – 8 год., самост. роб. – 96 год.;
Мова викладання	Українська
Кафедра	Кібербезпеки та технічного захисту інформації
Факультет	Інформаційних технологій та кібербезпеки

Викладач

ОНАЦЬКИЙ Олексій Віталійович,



доцент кафедри кібербезпеки та технічного захисту інформації,
кандидат технічних наук, доцент
E-mail: onatsky@meta.ua

Консультації: що понеділка з 14²⁰ до 15⁴⁰ год.,
каб. 205 (головний корпус)

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 проєкту і вибирати способи їх реалізації.
Компетентності, формуванню яких сприяє дисципліна	ЗК-1. Здатність застосовувати знання у практичних ситуаціях. ЗК-2. Здатність проводити дослідження на відповідному рівні. СК-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. СК-3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. СК-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. СК-13. Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності. СК-17. Здатність проводити оцінку відповідності (атестацію) комплексів технічного захисту інформації.
Програмні результати навчання	ПРН-6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. ПРН-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. ПРН-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. ПРН-26. Визначати вимоги до показників (характеристик) апаратних засобів технічного захисту інформації, які необхідні для забезпечення захищеності інформації в системі або на об'єкті інформаційної діяльності. ПРН-28. Здійснювати моніторинг та аудит загроз для інформації, що озвучується. ПРН-32. Скласти програму та методику атестації комплексу технічного захисту інформації (ТЗІ). ПРН-33. Здійснювати перевірку повноти і відповідності реалізованих заходів із захисту інформації вимогам технічного завдання на створення комплексу ТЗІ (або на створення КСЗІ в інформаційно-комунікаційних системах в частині вимог до захисту інформації від витоків технічними каналами), нормативно-правових актів та нормативних документів системи ТЗІ.

Програма навчальної дисципліни	
Тема 1. Вимоги щодо захисту інформації та кіберзахисту	Поняття комплексних систем захисту інформації Поняття 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	Організаційні заходи Заходи з технічного захисту мовної інформації Заходи з технічного захисту інформації, яка обробляється в ІКС
Тема 4. Створення комплексів технічного захисту інформації	Передпроектні роботи щодо систем та комплексів захисту інформації
Тема 5. Створення комплексів технічного захисту інформації	Розроблення та впровадження заходів із захисту інформації Випробування та атестація комплексу технічного захисту інформації
Тема 6. Атестації комплексів технічного захисту інформації	Етапи атестації Порядок організації та проведення атестації Контроль функціонування та керування системою захисту інформації
Тема 7. Система технічних документів щодо систем і комплексів захисту інформації	Нормативні документи системи технічного захисту інформації Порядок виконання робіт створення КТЗІ на ОІД, нормативні документи Етапи створення КСЗІ, нормативні документи
Тема 8. 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
Тема 9. Вимоги до КТЗІ від витоку інформації технічними каналами	Вимоги до комплексної системи захисту інформації в АС в частині захисту від витоку інформації технічними каналами Календарний план робіт із захисту інформації в ІКС

Методи навчання

При вивченні навчальної дисципліни використовуються наступні методи навчання:

Інтерактивні	▪ Наочно-демонстраційні дидактичні комплекси до тем, що вивчаються в межах дисципліни (схеми, таблиці, графіки, діаграми; зображення, картини тощо). ▪ Відповіді на запитання і опитування думок здобувачів освіти (дискусії). ▪ Відпрацювання навичок та робота в групах. Організовується групова робота із конкретними завданнями, що виконуються спільно з взаємодопомогою, після чого результати презентуються в аудиторії для розвитку професійних і командних навичок.
Практичні	▪ Вправи. Різні практичні завдання, які застосовуються на будь-якому етапі навчального процесу і допомагають задіювати інтелектуальні, комунікативні та пошукові здібності здобувачів освіти. Вони можуть включати відповіді на запитання, розв'язання задач, виправлення помилок, складання порівняльних таблиць, графіків і т.п. ▪ Творчі роботи (проекти). Мета таких робіт – розвиток творчого мислення, підвищення технічних навичок роботи з необхідним програмним забезпеченням та обладнанням.
Методи дистанційного навчання	▪ Відеоконференції в форматі лекцій або семінарів. Зв'язок здобувачів освіти з викладачем забезпечують різноманітні сучасні платформи, такі як: Zoom, Google Meet та ін. ▪ Онлайн дискусії; ▪ Індивідуальне і групове консультування (викладач дає додаткові роз'яснення щодо виконання завдань через чати та e-mail-надсилання);

Стратегія оцінювання результатів навчання

Змістовий контент результатів навчання з дисципліни	Результати навчання з даної дисципліни, які здобувач може продемонструвати та які можна ідентифікувати, оцінити і виміряти, розглядаються у вимірах 7 рівня Національної рамки кваліфікацій, що відповідає другому циклу вищої освіти Рамки кваліфікацій Європейського простору вищої освіти, а саме: ▪ Знання – очікується засвоєння базових положень створення комплексів технічного захисту інформації, включаючи нормативну базу та структуру документації для атестації комплексів технічного захисту інформації, етапів реалізації. ▪ Уміння/навички – розробляти та аналізувати ефективність засобів захисту інформації; формулювати вимоги до апаратних засобів ТЗІ; складати програму та методику атестації комплексів ТЗІ; перевіряти відповідність заходів захисту встановленим вимогам, складати документацію (звіти, програми, акти). ▪ Комунікація – здатність ефективно спілкуватися та взаємодіяти з командою проєкту, застосовуючи сучасні методи інформаційно-комунікаційних систем та впровадження засобів захисту. ▪ Відповідальність і автономія – здатність самостійно планувати та виконувати завдання з оцінки захищеності та атестації комплексів; нести відповідальність за обґрунтованість технічних рішень і висновків.
Критерії оцінювання	Академічні успіхи здобувачів освіти в межах даної дисципліни оцінюються за бально-рейтинговою шкалою (максимальна кількість – 100 балів), що прийнята в ДУІТЗ, з обов'язковим переведенням кількості балів в оцінки за національною шкалою та за шкалою ECTS.

	Відмінно (А) – від 90 до 100 балів – здобувач у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов’язкову та додаткову літературу. Правильно вирішив усі або не менше 90% завдань, передбачених програмою навчальної дисципліни. Дуже добре (В) – від 82 до 89 балів – здобувач досить повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов’язкову літературу. Однак під час викладання деяких питань допускаються при цьому окремі несуттєві неточності. Правильно вирішив 80-89% письмових завдань. Добре (С) – від 74 до 81 балів – здобувач достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов’язкову літературу. Однак під час викладання деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив 74-81% письмових завдань. Задовільно (D) – від 64 до 73 балів – здобувач в цілому володіє навчальним матеріалом, викладає його основний зміст під час усних та письмових відповідей, але з не зовсім глибоким та всебічним аналізом, обґрунтуванням та аргументацією, з недостатнім використанням необхідної літератури, допускаючи при цьому окремі неточності та помилки. Правильно вирішив 64-73% письмових завдань. Задовільно (Е) – від 60 до 63 балів – здобувач в цілому володіє навчальним матеріалом, викладає його основний зміст під час усних та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури, допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив 60-63% письмових завдань. Незадовільно з можливістю повторного складання (FX) – від 35 до 59 балів – здобувач не в повному обсязі володіє навчальним матеріалом. Фрагментарно, стисло без аргументації та обґрунтування викладає його під час усних виступів та письмових відповідей, поверхово розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності. Правильно вирішив 35-59% письмових завдань. Незадовільно з обов’язковим повторним вивченням дисципліни (F) – від 0 до 34 балів – Здобувач частково володіє навчальним матеріалом, не у змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив 1-34% письмових завдань.
Форма та методи контролю початкових досягнень	В межах даної дисципліни передбачено три види контролю: поточний, підсумковий та семестровий/академічний. Поточний контроль здійснюється під час проведення практичних занять і має на меті перевірку рівня підготовленості здобувачів до виконання конкретної роботи з теми, що вивчається. При поточному контролі оцінюється: активність роботи здобувача на практичних заняттях, результати виконання ним індивідуальних завдань, контрольних робіт, якість підготовлених завдань, що виконувались під час самостійної роботи. У концепції викладу навчальної дисципліни застосовуються такі форми проведення поточного контролю: тестування, опитування. Підсумковий контроль – це накопичена здобувачем сума балів за результатами вивчення дев’яти тем та виконання завдань самостійної роботи.

	Семестровий (академічний) контроль передбачає проведення екзамену, під час якого здобувачу виставляється остаточна оцінка за навчальну дисципліну, яка виводиться із суми балів за результатами підсумкового контролю та складання екзаменаційного тесту. Оцінювання навчальних досягнень здобувачів здійснюється за 100-бальною шкалою.
Політика навчальної дисципліни	
Відвідування	Здобувачі вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на практичних заняттях та контрольних заходах (залік) є обов'язковою. Важливим є своєчасне виконання індивідуальних завдань в межах самостійної роботи, передбачених програмою дисципліни.
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 різні програмні засоби.
Умови зарахування пропущених занять	Відпрацювання академічної заборгованості з дисципліни можливо до початку екзаменаційної сесії. Процедура узгоджується з викладачем, згідно його розкладу консультацій.

Рекомендовані джерела інформації	
Базові підручники та навчальні посібники	- 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. - 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.
Методичні рекомендації та розробки викладачів дисципліни	- Онацький О.В. Презентації лекцій з дисципліни - НД ТЗІ 3.7-003-2023 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі - НД ТЗІ 3.6-005-21 Порядок категоріювання безпеки інформаційної системи та інформації - НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці - НД ТЗІ 2.7-011-2012 Захист інформації на об'єктах інформаційної діяльності - НД ТЗІ 2.6-001-2011 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах - НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час обробки в автоматизованих системах класу - НД ТЗІ 3.6-003-2016 Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації, затверджений наказом Адміністрації Держспецзв'язку від 07.04.2016 № 41

Інформаційні ресурси	▪ Нормативні документи системи ТЗІ [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi2024 ▪ Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом [Електронний ресурс]. – Режим доступу: https://data.gov.ua
-----------------------------	--

Рік введення си­ла­бу­су – 2026 р.	Затверджено рішенням кафедри Кібербезпеки та технічного захисту інформації (Протокол від 22 травня 2026 р. № 13)	
	Завідувач кафедри д.т.н., проф	 Володимир КОРЧИНСЬКИЙ
	Гарант освітньої програми д.т.н., проф.	 Віталій КІЛЬДІШЕВ
	Викладач к.т.н., доц.	 Олексій ОНАЦЬКИЙ