Затверджено
завідувач кафедри
СТКБ_____ Г. Гайдур
«31» 08 2026 р.

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«НАУКОВО-ДОСЛІДНА ПРАКТИКА»

Лектор курсу			**Гайдур Галина Іванівна**, доктор технічних наук, професор		**Контактна інформація лектора (e-mail), сторінка курсу**	**e-mail:** g.haidur@duikt.edu.ua **сторінка курсу** https://classroom.google.com/c/ODE5ODIzMDcwODQ5	
Галузь знань			F Інформаційні технології		**Рівень вищої освіти**	Магістр	
Спеціальність			F5 Кібербезпека та захист інформації		**Семестр**	3	
Освітня програма			Інформаційна та кібернетична безпека		**Тип дисципліни**	Основна компонента освітньо-професійної програми	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	6	180		-			180

АНОТАЦІЯ КУРСУ

Взаємозв'язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	Основна
Освітні компоненти для яких є базовою	Технології виявлення уразливостей мережевих ресурсів, Технології забезпечення безпеки мережевої інфраструктури, Наукова комунікація та технічне документування в кібербезпеці, Проведення наукових досліджень в кібербезпеці
Мета курсу:	закріплення і поглиблення теоретичних знань, отриманих під час навчання за освітньо-професійною програмою; набуття досвіду самостійного дослідження актуальної наукової задачі; оволодіння сучасною методологією наукового дослідження, використання методів проведення наукових досліджень; застосування сучасних методів збирання, аналізу й оброблення наукової інформації; формування навичок викладати здобуті дослідницькі результати у наукових публікаціях, доповідях, тезах, звітах; сприяння активізації науково-дослідної діяльності, самоосвіти і самовдосконалення здобувачів.

Компетентності відповідно до освітньої програми

Soft- skills / Загальні компетентності (ЗК)	**Hard-skills / Спеціальні компетентності (СК)**
ІК1. Здатність особи розв'язувати задачі дослідницького та/ або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки. КЗ-1. Здатність застосовувати знання у практичних ситуаціях.	КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і

КЗ-2. Здатність проводити дослідження на відповідному рівні. КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.	спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. КФ2. 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. КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. КФ5. 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. КФ7. Здатність 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. 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.
Програмні результати навчання (ПРН)	
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. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	

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.
РН13. 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.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Дослідницька складова формування графіку проходження студентом науково-дослідної практики; ознайомлення з вітчизняними та іноземними науковими та іншими джерелами літератури з метою формування бібліографічного списку літератури за напрямом дослідження; підбір та обробка статистичних даних за напрямом кваліфікаційної роботи, **Практична складова** виконання індивідуального завдання, завершення роботи над формуванням теми і структури магістерської кваліфікаційної роботи; **Підготовка наукової публікації** підготовка тез доповіді для виступу на науковій конференції за обраним напрямом або наукову статтю за напрямом дослідження з дотриманням встановлених вимог; **Оформлення й захист результатів практики** підготовка звіту про проходження науково-дослідної практики, іншої звітної документації;	Самостійна робота 180	60	Пояснювально-ілюстративний Самостійна підготовка. Удосконалення отриманих знань та умінь Виконання завдань та практичне застосування знань і вмінь

-захист результатів практики. ***Формування компетенцій:*** ІК1, КЗ1, КЗ2, КЗ3, КЗ4, КФ1, КФ2, КФ3, КФ5, КФ7,, КФ8 ***Програмні результати навчання:*** РН2, РН2, РН3, РН4, РН 8, РН 11, РН 12, РН 13,РН17, РН19, РН20, РН21, РН22, РН23 ***Рекомендовані джерела:*** 1-15.			

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Закон України від 26.11.2015 № 848-VIII «Про наукову і науково-технічну діяльність». [Електронний ресурс]. – Доступний https://zakon.rada.gov.ua/laws/show/848-19#Text
2. Закон від 01.07.2014 № 1556-VII «Про вищу освіту» [Електронний ресурс]. – Доступний http://zakon1.rada.gov.ua/laws/show/1556-18
3. Наказ МОН України від 08.04.1994 № 93 «Про затвердження Положення про проведення практики студентів вищих навчальних закладів України» [Електронний ресурс]. – Доступний https://zakon.rada.gov.ua/go/z0035-93
4. Положення про проведення практики студентів у Державному університеті інформаційно-комунікаційних технологій [Електронний ресурс]. – Доступний https://duikt.edu.ua/uploads/p_447_23214805.pdf
5. Положення про організацію освітнього процесу у Державному університеті інформаційно-комунікаційних технологій [Електронний ресурс]. – Доступний https://duikt.edu.ua/uploads/p_447_49109699.pdf
6. Програма науково-дослідної практики для студентів спеціальності 125 Кібербезпека та захист інформації. [Електронний ресурс]. – https://duikt.edu.ua/uploads/p_840_60262109.pdf?file=p_840_60262109.pdf
7. Методичні рекомендації до виконання магістерських робіт на ступінь вищої освіти для здобувачів спеціальності 125 Кібербезпека / Гайдур Г.І., Гахов С.О., Марченко В.В. ,Чумак Н.С. /– К.: ДУІКТ, 2024. 44 с. [Електронний ресурс]. – Доступний https://duikt.edu.ua/uploads/p_1843_46569360.pdf
8. ВР України. – Режим доступу до журн. : http://zakon2.rada.gov.ua/laws/show/z0155-17/print1509912703741 483 (дата звернення: 10.04.2024). Додаткова
9. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” (1994);
10. Закон України “Про захист персональних даних” (2010)
11. СТРАТЕГІЯ національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015).
12. Закон України “Про національну безпеку (2018)
13. ISO/IEC 27001. "Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. "
14. ISO/IEC 27002. "Інформаційні технології. Методи забезпечення безпеки. Правила управління інформаційною безпекою."
15. ISO/IEC 27005. "Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки".

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Мультимедійний проектор;
2. Комп’ютерний клас для проведення захисту.

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, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації аспірант 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	***Робота на заняттях,*** *у т.ч.:*	
	•	
	• Самостійна робота	60 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, отримання міжнародного сертифікату за напрямом.	10 балів за рішенням викладача
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***залік***	Метоюзаліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання науково-дослідної діяльності.	40 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в екзаменаційній відомості*
90-100	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 Студент 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 студента 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.	Відмінно / Зараховано (А)

82-89	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 студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни	Добре / Зараховано (B)
75-81	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 (C)
67-74	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	Задовільно / Зараховано (D)
60-66	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, студент 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 (E)
35-59	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
0-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі заліку.	**Незадовільний** Студент не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з 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.