СИЛАБУС
КВАЛІФІКАЦІЙНА (МАГІСТЕРСЬКА) РОБОТА. АТЕСТАЦІЯ

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 та кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	**ОК-13** ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладачі

Кільдішев Віталій Йосипович
kildishev@ukr.net

Доцент кафедри Кібербезпеки та технічного захисту інформації,
кандидат технічних наук, доцент

Загальна інформація

Анотація	Кваліфікаційна (магістерська) робота є обов'язковою компонентною ОПП «Кібербезпека та захист інформації», в межах якої передбачено набуття та удосконалення знань, умінь та навичок щодо проведення наукових розвідок у сфері кібербезпеки та захисту інформації.
Мета	– розширення та глибоке вивчення сфери кібербезпеки та захисту інформації, спрямоване на розробку

	новаторських стратегій, технологій та методів для вдосконалення систем кібербезпеки.
Компетентності, формуванню яких сприяє дисципліна	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. КЗ5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності). КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і 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. КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки. КФ12. Здатність ефективно використовувати на практиці різні теорії в області навчання технологіям, засобам та організаційним аспектам безпеки інформаційних і комунікаційних систем та мереж. КФ13. Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об’єктів інформаційної діяльності.
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. 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. 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. 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.
Обсяг ОК-12	Загальний обсяг дисципліни: 9 кредитів ЄКТС (270 год.).
Форма підсумкового контролю	Публічний захист кваліфікаційної (бакалаврської) роботи
Терміни викладання ОК-12	Підготовка кваліфікаційної (бакалаврської) роботи здійснюється у 11-му семестрі .

Нормативні посилання

1.	Положення Про екзаменаційну комісію та атестацію здобувачів вищої освіти в Державному університеті інтелектуальних технологій і зв'язку (Затверджено Вченою радою ДУІТЗ протокол №1 від 10.02.2023 р.) https://suitt.edu.ua/polozennja-duitz;
2.	Порядок організації наукової та інноваційної діяльності в Державному університеті інтелектуальних технологій і зв'язку (Наказ ректора ДУІТЗ від 03.02.2021 р. № 01-02-32) https://suitt.edu.ua/polozennja-duitz;
3.	Положення Про комісію з питань етики та академічної доброчесності в Державному університеті інтелектуальних технологій і зв'язку (Затверджено Вченою радою ДУІТЗ протокол №11 від 13.07.2022 р.) https://suitt.edu.ua/polozennja-duitz;
4.	Положення Про забезпечення академічної доброчесності та етики в Державному університеті інтелектуальних технологій і зв'язку (Затверджено Вченою радою ДУІТЗ протокол №8 від 23.12.2021 р.) https://suitt.edu.ua/polozennja-duitz;

Орієнтовні напрями наукових досліджень

1. Розробка та оцінка ефективності нових алгоритмів шифрування.
2. Вивчення та застосування методів квантової криптографії.
3. Аналіз та оптимізація методів мультифакторної автентифікації.
4. Розробка та впровадження систем виявлення аномалій в мережах.
5. Аналіз та захист від атак на блокчейн-технології та криптовалютні системи.
6. Дослідження та захист від атак на Інтернет речей (IoT).
7. Створення систем захисту від DDoS-атак.
8. Розробка та апробація нових алгоритмів цифрового підпису.
9. Аналіз та вдосконалення методів виявлення і блокування вірусів та шкідливих програм.
10. Розробка та впровадження методів захисту від атак на хмарні обчислення.
11. Аналіз та захист від атак на інтегровані системи управління.
12. Побудова системи захисту від атак на критичну інфраструктуру.
13. Розробка та впровадження систем захисту від розподілених атак.
14. Аналіз та оптимізація механізмів ендпоінт-захисту.
15. Вивчення та захист від атак на мережі Wi-Fi.
16. Розробка та впровадження методів шифрування електронної пошти.
17. Дослідження та захист від атак на операційні системи.
18. Аналіз методів підвищення безпеки мобільних додатків.
19. Впровадження захисту від атак на системи індустріального управління.
20. Розробка систем контролю та управління доступом.
21. Розробка методів підвищення безпеки систем голосового управління.
22. Аналіз захисту від атак на блокчейн-протоколи.
23. Дослідження методів захисту від атак на системи електронного голосування.
24. Розробка та апробація нових методів захисту від соціально-інженерних атак.
25. Побудова захисту від атак на системи цифрової медицини.

Список рекомендованих джерел

1. Захарченко М. В. Асиметричні методи шифрування в телекомунікаціях: навч. посіб. / М. В. Захарченко, О. В. Онацький, Л. Г. Йона, Т. М. Шинкарчук. – Одеса: ОНАЗ ім. О. С. Попова, 2011. – 184 с.
2. Забезпечення інформаційної безпеки цифрових програмно керованих АТС Інформаційна безпека телефонного зв'язку: навч. посібник / [Кононович В.Г., Стайкуца С.В., Тардаскіна Т.М., Шинкарчук Т.М.] За ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2010. – С. 168.
3. Стайкуца С.В., Бєлова Ю.В., Сєдов К.С., Севастєєв Є.О. «Комплексні системи безпеки». Методичні вказівки для виконання лабораторних робіт, Одеса: ДУІТЗ, 2021, 80 с.

Інформація про консультації

Щопонеділка у вересні-грудні 2024 року з 11^{00} до 14^{00} год., 2 лаб.корп. ауд.108

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*** При оформленні документів за екзаменаційну сесію використовується таблиця відповідності оцінювання знань здобувачів вищої освіти за різними системами
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

Дотримання принципів академічної доброчесності: Підготовка кваліфікаційної (магістерської) роботи здійснюється здобувачем вищої освіти самостійно, на засадах академічної доброчесності. Робота проходить перевірку на рівень академічної доброчесності (плагіат) із застосуванням затверджених в ДУІТЗ процедур, зокрема програми **Unicheck.**

Інші умови: Здобувач вищої освіти, під керівництвом наукового керівника кваліфікаційної (магістерської) роботи, бере активну участь у науково-практичних заходах (конференції, круглі столи, кафедральні дискусійні майданчики, форуми тощо), де презентує власні та/або колективні наукові/освітні здобутки з теми дослідження.