СИЛАБУС
Кваліфікаційна (бакалаврська) робота

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	Перший (бакалаврський)
Факультет	Інформаційних технологій та кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	**ОК-30** ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладачі

Онацький Олексій Віталійович
onatsky@meta.ua

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

Загальна інформація

Анотація	Кваліфікаційна (бакалаврська) 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	– дослідження, аналіз та розробка інноваційних стратегій та технологій для забезпечення ефективності та надійності

	кіберзахисту, визначення вразливостей інформаційних систем, розробка заходів протидії кіберзагрозам, вдосконалення стратегій реагування на інциденти.
Компетентності, формуванню яких сприяє дисципліна	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. 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 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. КФ 9. Здатність здійснювати професійну діяльність на основі впровадження системи управління інформаційною та/або кібербезпекою. КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.
Результати навчання	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 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 12. Розробляти моделі загроз та порушника. ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. 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 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 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 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 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 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем. ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки. ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.

	ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та кібербезпеки відповідно до цілей і завдань організації. 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 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 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. ПРН 50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
Обсяг ОК-30	Загальний обсяг дисципліни: 9 кредитів (ЄКТС 270 год.).
Форма підсумкового контролю	Публічний захист кваліфікаційної (бакалаврської) роботи
Терміни викладання ОК-30	Підготовка кваліфікаційної (бакалаврської) роботи здійснюється у 8-му семестрі (32–40 тижні).

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. Аналіз та вдосконалення механізмів виявлення інтернет-атак.
2. Розробка системи виявлення та відновлення від атак на основі штучного інтелекту.
3. Вивчення ефективності блокчейн-технологій у забезпеченні кібербезпеки.
4. Аналіз і вдосконалення методів автентифікації користувачів.
5. Використання машинного навчання для виявлення аномалій в мережах.
6. Розробка імунних систем для захисту від шкідливих програм.
7. Вивчення інцидентів інформаційної безпеки на об'єктах критичної інфраструктури.
8. Аналіз та вдосконалення заходів захисту від DDoS-атак.
9. Розробка системи моніторингу та аналізу поведінки користувачів.
10. Вивчення та оцінка кіберзагроз для Інтернету речей (IoT).
11. Розробка методів шифрування для захисту конфіденційної інформації.
12. Аналіз та підвищення безпеки мобільних додатків.
13. Використання технологій розпізнавання відбитків пальців для біометричної автентифікації.
14. Розробка системи кібербезпеки для хмарних обчислень.
15. Аналіз та вдосконалення механізмів шифрування електронної пошти.
16. Аналіз методів підвищення безпеки мереж Wi-Fi.
17. Розробка алгоритмів виявлення та блокування фішингових веб-сайтів.
18. Вивчення впливу квантового обчислення на криптографію.
19. Розробка та впровадження системи моніторингу кіберзаходів у реальному часі.
20. Захист від атак з використанням штучних інтелектуальних алгоритмів.
21. Вивчення та вдосконалення систем виявлення та запобігання вторгнень.
22. Аналіз використання блокчейн-технологій для створення безпечних інтернет-платформ.
23. Розробка системи контролю та управління доступом на основі Arduino.
24. Аналіз та вдосконалення захисту від витоку конфіденційної інформації.
25. Моделювання системи безпеки підприємства.

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. Онацкий А. В., Йона Л. Г. Асимметричные методы шифрования. – Модуль 2 Криптографические методы защиты информации в телекоммуникационных системах и сетях: Учеб. пособие / Под ред. Н. В. Захарченко – Одесса: ОНАС им. А. С. Попова, 2010. – 148 с.
3. 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.
4. 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 грудні-червні 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 (бакалаврської) 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 (бакалаврської) 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.