



СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кваліфікаційна (магістерська) робота. Атестація

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-12)
Курс, семестр викладання	1 курс, 2 семестр; 2 курс, 1 семестр
Трудовісткість навчальної дисципліни	8 кредитів ЄКТС (240 год.)
Мова викладання	Українська
Кафедра	Кібербезпеки та технічного захисту інформації
Факультет	Інформаційних технологій та кібербезпеки

Викладачі

КІЛЬДІШЕВ Віталій Йосипович,



доцент кафедри кібербезпеки та технічного захисту інформації,
доктор технічних наук, доцент

E-mail: v.y_kildishev@suitt.edu.ua

Консультації: щоп'ятниці з 14²⁰ до 15⁴⁰ год.,
каб. 205 (головний корпус)

Мета дисципліни	– 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	ЗК1 Здатність застосовувати знання у практичних ситуаціях. ЗК2 Здатність проводити дослідження на відповідному рівні. ЗК3 Здатність до абстрактного мислення, аналізу та синтезу. ЗК4 Здатність оцінювати та забезпечувати якість виконуваних робіт. ЗК5 Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності). СК-1. 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. 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-10. 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. СК-12. Здатність ефективно використовувати на практиці різні теорії в області навчання технологіям, засобам та організаційним аспектам безпеки інформаційних і комунікаційних систем та мереж. СК-13. Здатність проводити спеціальні дослідження засобів обробки інформації, технічних засобів та об'єктів інформаційної діяльності.
Програмні результати навчання	ПРН-1. 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. ПРН-2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. ПРН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. ПРН5. 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. ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на

об'єктах інформаційної діяльності та критичної інфраструктури.

ПРН17. 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.

ПРН19. 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.

ПРН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

ПРН22. 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.

ПРН23. 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.

Орієнтовні напрями наукових досліджень

Розробка та оцінка ефективності нових алгоритмів шифрування.

Вивчення та застосування методів квантової криптографії.

Аналіз та оптимізація методів мультифакторної автентифікації.

Розробка та впровадження систем виявлення аномалій в мережах.

Аналіз та захист від атак на блокчейн-технології та криптовалютні системи.

Дослідження та захист від атак на Інтернет речей (IoT).

Створення систем захисту від DDoS-атак.

Розробка та апробація нових алгоритмів цифрового підпису.

Аналіз та вдосконалення методів виявлення і блокування вірусів та шкідливих програм.

Розробка та впровадження методів захисту від атак на хмарні обчислення.

Аналіз та захист від атак на інтегровані системи управління.

Побудова системи захисту від атак на критичну інфраструктуру.

Розробка та впровадження систем захисту від розподілених атак.

Аналіз та оптимізація механізмів ендпоінт-захисту.

Вивчення та захист від атак на мережі Wi-Fi.

Розробка та впровадження методів шифрування електронної пошти.

Дослідження та захист від атак на операційні системи.

Аналіз методів підвищення безпеки мобільних додатків.

Впровадження захисту від атак на системи індустріального управління.

Розробка систем контролю та управління доступом.

Розробка методів підвищення безпеки систем голосового управління.

	Аналіз захисту від атак на блокчейн-протоколи. Дослідження методів захисту від атак на системи електронного голосування. Розробка та апробація нових методів захисту від соціально-інженерних атак. Побудова захисту від атак на системи цифрової медицини.
Форма підсумкового контролю	
Публічний захист кваліфікаційної (магістерської) роботи	
Політика навчальної 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 StrikePlagiarism .
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.
Рекомендовані джерела інформації	
Базові підручники та навчальні посібники	• Тестування на проникнення: навч. посіб. Ч.1 / [Є.О. Живило]; за ред. Є.О. Живило. – П.: ПНТУ “Полтавська політехніка ім. Юрія Кондратюка”, 2024. – 134 с. • Стайкуца С.В., Белова Ю.В., Седов К.С., Севаст'єв Є.О. «Комплексні системи безпеки». Методичні вказівки для виконання лабораторних робіт, Одеса: ДУІТЗ, 2021, 80 с. • Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Васіліу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ФОП Ямчинський О.В., 2020. – 445 с. • Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак – К.: Видавництво НА СБ України, 2020. – 256 с.
Методичні рекомендації та розробки викладачів дисципліни	Методичні вказівки до виконання кваліфікаційних робіт за спеціальністю F5 Кібербезпека та захист інформації [для здобувачів освіти першого (бакалаврського) та другого (магістерського) рівня вищої освіти, ОПП «Кібербезпека та захист інформації»] / Авт.-уклад.: Є.В. Васіліу, В.В. Корчинський, В.Й. Кільдішев. Одеса: ДУІТЗ 2026. 47 с.

Інформаційні ресурси	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.		
Рік введення силабусу – 2026 р.	Затверджено рішенням кафедри кібербезпеки та технічного захисту інформації (Протокол від 22 травня 2026 р. №13)		
	Завідувача кафедри		Володимир КОРЧИНСЬКИЙ
	Гарант освітньої програми		Віталій КІЛЬДІШЕВ