



СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ПРАКТИКА(ВИРОБНИЧА)

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-11)
Курс, семестр викладання	1 курс, 2 семестр; 2 курс, 1 семестр
Трудовісткість навчальної дисципліни	15 кредитів ЄКТС (450 год.)
Мова викладання	Українська
Кафедра	Кібербезпеки та технічного захисту інформації
Факультет	Інформаційних технологій та кібербезпеки
Викладачі	
ІВАХНЕНКО Максим Сергійович	
	викладач кафедри кібербезпеки та технічного захисту інформації E-mail: m.s_ivakhnenko@suitt.edu.ua Консультації: щоп'ятниці з 13⁰⁰ до 14²⁰ год., каб. 205 (головний корпус)
Мета дисципліни	– застосування, отриманих у результаті навчання, знань за напрямками кібербезпеки та захисту інформації та їх трансформація у навички.

Компетентності, формуванню яких сприяє дисципліна	ЗК1 Здатність застосовувати знання у практичних ситуаціях. 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-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-16. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації.
Програмні результати навчання	ПРН-2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. ПРН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб. 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. 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.

Програма ПРАКТИКИ

Тема 1.	Інструктаж з техніки безпеки. Вивчення правил техніки безпеки, інструкцій пожежної безпеки, електробезпеки. Складання іспитів з правил техніки безпеки, пожежної безпеки та охорони праці на підприємстві.
Тема 2.	Знайомство з організацією. Короткий опис підприємства – назва, види діяльності, послуг чи продукції, місце на ринку, цілі та завдання. Організаційна структура організації (розміщення та склад відділів, департаментів і служб, їх взаємозв'язок), кадровий склад (у співробітників і назви посад), правила внутрішнього розпорядку, наявність внутрішніх правил і регламентів. Типові бізнес-процеси у роботі організації. Виділення ключових бізнеспроцесів.

Тема 3.	<i>Аудит поточного стану безпеки підприємства. Моделювання загроз безпеки підприємства.</i> В основі аудиту – 5 базових напрямків у роботі компанії, а саме – кадри, робота з контрагентами, інженерний захист та технічні засоби охорони, інформаційна інфраструктура (інформаційна мережа підприємства), документообіг та персональні дані. Аудит проводиться лише за погодженням з керівництвом компанії, на основі внутрішніх розпоряджень, регламентом та інших документів компанії, що базується на відкритій інформації. Основна мета аудиту – збір первинної інформації для аналізу та підготовки звіту щодо поточного стану рівня безпеки в компанії. Аналіз зовнішніх загроз підприємства. Аналіз внутрішніх загроз підприємства. Розробка моделі фізичного проникнення порушника.
----------------	---

Тема 4.	<i>Робота з результатами аудиту та розробка пропозицій щодо підвищення рівня безпеки в компанії.</i> Основна мета розділу - вибрати оптимальні методи та засоби захисту, дія яких спрямована на підвищення рівня захисту за 5-ма базовими напрямками. За базовими напрямками застосувати низку методів та засобів, спрямованих на мінімізацію ризиків.
----------------	---

Форма підсумкового контролю

Залік

Політика навчальної дисципліни

Відвідування	Здобувачі вищої освіти зобов'язані дотримуватися графіку проходження практики, своєчасно пройти інструктаж з техніки безпеки. Важливим є виконання індивідуальних завдань, правильне заповнення документації практики (щоденник, звіт та ін.).
---------------------	--

Дотримання принципів академічної доброчесності	Підготовка усіх завдань, письмових робіт і т. ін., здійснюється здобувачем вищої освіти самостійно, на засадах академічної доброчесності.
---	---

Інші умови	Здобувач вищої освіти бере участь (особисто та/або в команді з іншими студентами) у підсумковій конференції з практики, де презентує свої досягнення, подає рекомендації щодо удосконалення практичної підготовки в ДУІТЗ.
-------------------	--

Рекомендовані джерела інформації

Базові підручники та навчальні посібники	• Стайкуца С.В., Белова Ю.В., Седов К.С., Севаст'єєв 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	Наскрізна програма практики за ОПП «Кібербезпека та захист інформації» [для здобувачів другого (магістерського) рівня вищої освіти зі спеціальності F5 Кібербезпека та захист інформації] / Авт.-уклад.: В. Кільдішев, С. Стайкуца, М. Івахненко. Одеса : ДУІТЗ, 2026. 11 с.		
Інформаційні ресурси	1. 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 ; 2. 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 ; 3. 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
	Викладач:		Максим ІВАХНЕНКО