СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ПРАКТИКА(ВИРОБНИЧА)

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-12** ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладачі

Стайкуца Сергій Володимирович
s.v_staikutsa@suitt.edu.ua

Доцент кафедри кібербезпеки та технічного захисту інформації (КБ та ТЗІ), кандидат філософських наук, доцент

Загальна інформація

Анотація	Практика є обов'язковою компонентною ОПП «Кібербезпека та захист інформації», в межах якої передбачено набуття та удосконалення професійноважливих практичних умінь/навичок зі спеціальності 125 Кібербезпека та захист інформації. На практиці діяльність здобувача вищої освіти спрямована на опанування сучасними технологіями, методами, інструментами, обладнанням і т. ін. По завершенню практики здобувач буде здатен виконувати професійну роботу фахівця і відповідно до Національного класифікатора України: Класифікатор професій (ДК 003:2010) займати первинну посаду за категоріями:

	• 3439 – фахівець з режиму секретності; • 3439 – фахівець із організації захисту інформації з обмеженим доступом; • 3439 – фахівець із організації інформаційної безпеки.
Мета дисципліни	– застосування, отриманих у результаті навчання, знань за напрямами ІБ та їх трансформація у навички.
Компетентності, формуванню яких сприяє дисципліна	КІ-1. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки. КЗ1. Здатність застосовувати знання у практичних ситуаціях. 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). 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.
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. РН15. 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. 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. 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 дисципліни	Загальний обсяг дисципліни: 12 кредитів
Форма підсумкового контролю	Залік
Терміни викладання дисципліни	Дисципліна викладається: у 3-му семестрі

Нормативні посилання	
1.	Положення Про порядок проведення практичної підготовки здобувачів вищої освіти Державного університету інтелектуальних технологій і зв'язку (Затверджено Вченою радою ДУІТЗ протокол №1 від 10.02.2023 р.) https://suitt.edu.ua/polozennja-duitz;
2.	Закону України «Про вищу освіту», стаття 51 «Практична підготовка осіб, які навчаються у закладах вищої освіти» (Відомості Верховної Ради, 2014, № 37-38).

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.	***Аудит поточного стану безпеки підприємства. Моделювання загроз безпеки підприємства.*** 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.	***Робота з результатами аудиту та розробка пропозицій щодо підвищення рівня безпеки в компанії.*** Основна мета розділу - вибрати оптимальні методи та засоби захисту, дія яких спрямована на підвищення рівня захисту за 5-ма базовими напрямками. За базовими напрямами застосувати низку методів та засобів, спрямованих на мінімізацію ризиків.

Список рекомендованих джерел

1. Голев Д.В., Кільдишев В.Й., Кононович В.Г. Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум Частина 1 – Комплекси засобів захисту інформації від НСД: Навч. посібник / За ред. чл.- кор. МАЗ В.Г. Кононовича.– Одеса: ОНАЗ ім. О.С. Попова, 2010. – С.176.
2. 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.
3. Інформаційна безпека цифрових програмно-керованих АТС : [навч. посіб.] / В.Г. Кононович , С.В. Стайкуца, Т.М. Лемеха, Ю.В. Копитін; за ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – С.

Інформація про консультації

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

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

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.