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	Перший (бакалаврський)
Факультет	Інформаційних технологій і кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	ОК-28 Практика (виробнича) ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладачі

Бєлова Юлія Володимирівна
bilovaulia@gmail.com

Викладач кафедри Кібербезпеки та технічного захисту інформації

Загальна інформація

Анотація	Практика є обов'язковою компонентною ОПП «Кібербезпека та захист інформації», в межах якої передбачено набуття та удосконалення професійних практичних умінь/навичок зі спеціальності 125 Кібербезпека та захист інформації. На практиці діяльність здобувача вищої освіти спрямована на опанування сучасних технологій, методів, інструментів, робота з обладнанням та програмним забезпеченням.
Мета дисципліни	– систематизація, закріплення і розширення теоретичних і практичних знань здобувача зі спеціальності 125 Кібербезпека та захист інформації, формування у здобувачів професійних умінь і навичок для прийняття самостійних рішень у процесі їхньої професійної діяльності.

Компетентності, формуванню яких сприяє дисципліна	**Загальні компетентності:** ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК 2. Знання та розуміння предметної області та розуміння професії. ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. ЗК5. Здатність до пошуку, оброблення та аналізу інформації. ЗК7. 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. **Спеціальні компетентності:** СК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки. СК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. СК4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки. СК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки. СК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. СК8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. СК9. Здатність здійснювати професійну діяльність на основі впровадження системи управління інформаційною та/або кібербезпекою. СК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності. СК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. СК12. 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 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.
Обсяг дисципліни	Загальний обсяг дисципліни: 4 кредити ЄКТС (120 год.).
Форма підсумкового контролю	екзамен
Терміни викладання дисципліни	Дисципліна викладається: у 6-му семестрі 4 кредити ЄКТС;

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.	**Техніка безпеки і охорона праці на об'єкті.** Знайомство з правилами внутрішнього розпорядку підприємства, інструктаж з техніки безпеки та охорони праці. Техніка безпеки і охорона праці у підрозділі. Техніка безпеки і охорона праці на робочих місцях.
Тема 2.	**Аналіз об'єкту захисту.** Аналіз рівня комп'ютерного забезпечення об'єкту. Аналіз периферійного та мережевого обладнання, локальної комп'ютерної мережі бази практики та ін. Технічна, нормативна документація.
Тема 3.	**Аналіз і оцінка ризиків інформаційної безпеки.** Аналіз вразливостей комп'ютерних систем та мереж. Оцінка вразливостей в комп'ютерних системах та мережах.
Тема 4.	**Організації комплексної безпеки об'єктів.** Структура та рівні мережевої взаємодії при побудові КСБ. Програмно-апаратні рішення в комплексних систем безпеки.

Список рекомендованих джерел

1. Державний стандарт України Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
2. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
3. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.
4. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення.
5. НД ТЗІ 1.6-002-03. Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації.
6. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.
7. НД ТЗІ 2.1-002-07 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення.
8. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.
9. НД ТЗІ 2.6-001-11 Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.
10. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.
11. НД ТЗІ 2.7-011-12 Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв.
12. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Перед проектні роботи.
13. НД ТЗІ 3.3-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.
14. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.
15. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
16. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В.Р – Київ.: ООО "Д.В.К.", 2004. – 508 с.

Інформація про консультації

Щоп’ятниці з 13^{00} до 14^{30} год., ауд. 107 або zoom – викл. Бєлова Ю.В.

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.