

СИЛАБУС ОСВІТНЬОЇ КОМПОНЕНТИ



СОЦІОТЕХНІЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ

спеціальність	не обмежено	обов'язковість дисципліни	вибіркова
освітня програма	не обмежено	факультет	навчально-науковий інститут «Кіберпорт»
освітній рівень	не обмежено	кафедра	інформаційних технологій, кібернетики та захисту інформації

ВИКЛАДАЧ

ЧАЛИЙ ІГОР ВІЛЬОВИЧ



Вища освіта – спеціальність „Динаміка та міцність машин ”
Науковий ступень - кандидат технічних наук 05.20.01
Вчене звання - доцент кафедри кібернетики та інформаційних технологій
Досвід роботи – більше 40 років
Показники професійної активності з тематики курсу:

- автор більше 10 методичних розробок;
- співавтор 2 навчальних посібників;
- співавтор 2 тематичних публікацій (1 Scopus);
- учасник наукових і методичних конференцій.

телефон	0503032421	електронна пошта	ivchaly@gmail.com	дистанційна підтримка	Moodle
---------	------------	------------------	-------------------	-----------------------	--------

ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ОСВІТНЮ КОМПОНЕНТУ (ДИСЦИПЛІНУ)

Мета	формування розуміння деяких соціотехнічних аспектів кібербезпеки, ознайомлення студентів з основними поняттями інформаційної безпеки та прийомами захисту інформації в соціальних мережах, набуття компетенцій ефективно реалізовувати знання у своїй практичній та професійній діяльності.		
Формат	лекції, практичні заняття, самостійна робота, індивідуальні завдання		
Деталізація результатів навчання і форм їх контролю	<ul style="list-style-type: none"> • ознайомлення з базовими поняттями: кіберпростір, інформаційна безпека, кібербезпека, та деякими іншими / лекції, практичні завдання; • ознайомлення з сучасною інфосферою та особливостями її захисту в умовах стороннього кібернетичного впливу / лекції, практичні завдання; • розгляд основних кіберінцидентів у сфері високих технологій / лекції, практичні завдання; • вивчення основних понять та визначень, особливостей та моніторингу соціальних мереж / лекції, практичні завдання, індивідуальні завдання; • розгляд концепції та принципів соціальної інженерії, її основних понять та методів / індивідуальні, практичні завдання, самостійна робота; • розгляд дезінформації, як елементу кібератак / лекції, практичні завдання; • розгляд пропаганди як інструменту інформаційного впливу / індивідуальні, практичні завдання, самостійна робота; • надання практичних порад щодо безпечного використання соціальних мереж / лекції, практичні завдання. 		
Обсяг і форми контролю	3 кредити ECTS (90 годин): 12 годин лекції, 18 годин лабораторно-практичні; модульний контроль (2 модулі); підсумковий контроль – диференційований залік.		
Вимоги викладача	вчасне виконання завдань, активність, самостійна робота.		
Умови зарахування	вільне зарахування		

ВІДПОВІДНІСТЬ СТАНДАРТУ ОСВІТИ І ОСВІТНІЙ ПРОГРАМІ

Компетенції	Здатність застосовувати основи інформаційної безпеки у фаховій та навчальній діяльності.	Програмні результати навчання	Застосовувати знання з основ інформаційної безпеки у навчанні та повсякденній роботі за фахом.
-------------	--	-------------------------------	--

СТРУКТУРА ОСВІТНЬОЇ КОМПОНЕНТИ (ДИСЦИПЛІНИ)

Модуль 1. Соціотехнічні аспекти кібербезпеки. Соціальні мережі.

Лекція 1.	Предмет та значення дисципліни. Основні визначення та поняття, що відносяться до змісту курсу. Кіберпростір та кібербезпека як основа інформаційної цивілізації.	Лабораторно-практичне заняття 1 (ЛПЗ 1)	Джерела сучасної термінології інформаційної безпеки.	Самостійна робота	Інформаційна безпека держави. Об'єкти і суб'єкти інформаційної безпеки. Етапи розвитку інформаційної безпеки. Загрози кібертероризму. Кібервійна. Кібербезпека в умовах розгортання четвертої промислової революції: виклики та можливості для України. Сучасна інфосфера та особливості її захисту в умовах стороннього кібернетичного впливу. Самостійне доопрацювання матеріалів змістовного модуля 1.
Лекція 2.	Кіберінциденти у сфері високих технологій: ознаки, проблеми та реагування. Сучасна інфосфера та особливості її захисту в умовах стороннього кібернетичного впливу	ЛПЗ 2	Пошук та опрацювання матеріалів щодо кіберінцидентів у сфері високих технологій.		
Лекція 3.	Соціальні мережі: основні поняття та визначення, особливості. Моніторинг соціальних мереж — цілі та способи реалізації. Поняття соціотехнічної системи та її властивостей.	ЛПЗ 3	Дослідження та характеристика найбільш поширених соціальних мереж.		
.		ЛПЗ 4	LinkedIn - соціальна мережа для пошуку і встановлення ділових контактів. Дослідження матеріалів з кібербезпеки у LinkedIn		
		ЛПЗ 5	Вибір онлайн-ресурсів для самостійного вивчення матеріалів з кібербезпеки.		

Модуль 2. МЕТОДИ І ЗАСОБИ СОЦІАЛЬНОГО ІНЖИНІРИНГУ.

Лекція 4.	Концепції та принципи соціальної інженерії. Основні поняття та визначення методів соціальної інженерії. Загальні принципи. Основні етапи моделі атаки на основі методів соціальної інженерії.	ЛПЗ 6	Базові інструменти просування контенту в соціальних мережах.	Самостійна робота	Базові прийоми та інструменти ведення інформаційної війни у соціальних он-лайн мережах. Прийоми захисту від інформаційних атак в он-лайн мережах. Прийоми здійснення інформаційних атак в он-лайн мережах. Інтернет-технології та соціальні он-лайн мережі в структурі гібридної війни. Мережеві он-лайн проекти в гібридній війні: структура та принципи функціонування. Самостійне доопрацювання матеріалів змістовного модуля 2.
Лекція 5.	Дезінформація як елемент кібератак. Сценарії розвитку та методи протидії. Канали поширення дезінформації. Типи неправдивої інформації. Види маніпуляцій. Маніпуляції з медіаданими. Пропаганда як	ЛПЗ 7	Самостійне проходження з отриманням сертифікатів освітніх ресурсів порталу «Дія. Освіта»		

	інструмент інформаційного впливу.		
Лекція 6.	Практичні поради щодо безпечного використання соціальних мереж. Способи протидії неправдивим повідомленням. Інструменти виявлення неправдивих повідомлень.	ЛПЗ 8	Самостійне проходження з отриманням сертифікатів освітніх ресурсів порталу «Prometheus»
		ЛПЗ 9	Кваліфікований електронний підпис, як засіб безпечної передачі даних.

ОСНОВНА ЛІТЕРАТУРА ТА МЕТОДИЧНІ МАТЕРІАЛИ

Література	<ol style="list-style-type: none"> Бурячок В.Л. Інформаційна та кібербезпека : соціотехнічний аспект: підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. – К.: ДУТ, 2016. 449 с. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.. Лажно В.А. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лажно, Є.В. Васіліу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К.:ЦП «Компринт» О.В., 2021. – 4 4 4 с. Сучасні інформаційні війни в мережевому он-лайн просторі [Текст]: навчальний посібник / О.В.Курбан. – Київ: ВІКНУ, 2016. - 286 с. Інформаційно-психологічне протистояння: підручник. Видання друге перекладене, доповнене та перероблене / [В. М. Петрик, В. В. Бедь, М. М. Присяжнюк та ін.]; за заг. ред. В. В. Бедь, В. М. Петрика. — К.: ПАТ «ВІПОЛ», 2018. – 386 с. 	Методичне забезпечення	<ol style="list-style-type: none"> Використання on-line ресурсів Інтернет для самостійного вивчення дисциплін за фахом. Методика вивчення, порядок проходження: метод. вказ. до виконання лабораторних робіт з дисциплін «Вступ до фаху та академічна доброчесність», «Основи кібербезпеки», «Кібербезпека», «Інформаційна безпека держави» / Мегель Ю.Є., Міхнова О.В., Левкін А.В., Чалий І.В., Яковенко Д.М. - Державний біотехнологічний університет, 2023. - 50 с.. Основи інформаційної безпеки. ч.1. Тлумачний словник. / Мегель Ю.Є., Міхнова О.В., Левкін А.В., Чалий І.В., Яковенко Д.М. - Державний біотехнологічний університет, 2023. - 72 с. Навчальна практика (частина 1):методичні вказівки до виконання навчальної практики для здобувачів першого (бакалаврського) рівня вищої освіти денної та заочної форм навчання спеціальності 125 Кібербезпека та захист інформації / Держ. біотехнологічний ун-т; авт.-уклад.: Ю.Є. Мегель, Т.А.Бутенко, А.В. Левкін, О.Д. Міхнова, Ю.В.Синявіна, І.В. Чалий – Харків : [б.-в.], 2024 – 50с. Хмарні технології в кібербезпеці / Мегель Ю.Є., Міхнова О.В., Левкін А.В., Чалий І.В., Яковенко Д.М. - Державний біотехнологічний університет, 2022. - 50 с. Захист інформаційних ресурсів: навчально-методичний посібник до курсу – Захист інформаційних ресурсів / укл. С. О. Троян. – Умань : [б.в.], 2012. –120 с.
------------	--	------------------------	--

СИСТЕМА		БАЛИ	ДІЯЛЬНІСТЬ, ЩО ОЦІНЮЄТЬСЯ
Підсумкове оцінювання	100 бальна ECTS (стандартна)	до 50	50% від усередненої оцінки за модулі
		до 50	підсумкове тестування
Модульне оцінювання	100 бальна сумарна	до 50	відповіді на тестові питання
		до 20	усні відповіді на лабораторно-практичних заняттях
		до 30	результат засвоєння блоку самостійної роботи

НОРМИ АКАДЕМІЧНОЇ ЕТИКИ ТА ДОБРОЧЕСНОСТІ

Всі учасники освітнього процесу (в тому числі здобувачі освіти) повинні дотримуватися кодексу академічної доброчесності та вимог, які прописані у положенні «Про академічну доброчесність учасників освітнього процесу ДБТУ»: виявляти дисциплінованість, вихованість, поважати гідність один одного, проявляти доброзичливість, чесність, відповідальність.