СИЛАБУС ОСВІТНЬОЇ КОМПОНЕНТИ

Основи промт-інжинірингу

спеціальність	**F5 «Кібербезпека та захист інформації»**	**обов'язковість дисципліни**	**вибіркова**
освітня програма	**Основи промт-інжинірингу**	**факультет**	**менеджменту, адміністрування та права**
освітній рівень	**перший (бакалаврський)**	**кафедра**	**інформаційних технологій, кібернетики та захисту інформації**

ВИКЛАДАЧ

Сотников Юрій Олексійович

Вища освіта – спеціальність «економіст по бухгалтерському обліку у сільському господарстві»
Науковий ступінь - кандидат економічних наук 08.07.02 – «Економіка сільського господарства і АПК
Вчене звання – доцент інформаційних технологій, кібернетики та захисту інформації
Досвід роботи – більше 30 років
Показники професійної активності з тематики курсу:

- автор більше 5 методичних розробок;
- консультування ТОВ «СТАНДАРТАГРО»ХАРКІВСЬКОГО РАЙОНУ ХАРКІВСЬКОЇ ОБЛАСТІ
- співавтор 20 тематичних публікацій;
- учасник наукових і методичних конференцій.

Телефон	**+380505709285**	**електронна пошта**	**0505709285@btu.kharkov.ua**	**дистанційна підтримка**	**https://meet.google.com/sag-acfp-pyu**

ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ОСВІТНЮ КОМПОНЕНТУ (ДИСЦИПЛІНУ)

Мета	**Опанування основ промт-інжинірингу та практичної роботи з генеративним ШІ для задач кібербезпеки.**
Формат	**лекції, практичні заняття, самостійна й командна робота**
Специфічні результати навчання і форми їх контролю	• **Застосування технік промтингу для аналітичних задач кібербезпеки (ЗК1, ЗК5, ЗК9, СК2, РН4, РН10, РН22).** • **Виявлення ризиків генеративного ШІ та дотримання кібергігієни (ЗК1, СК2, СК10, РН10, РН21).** • **Доброчесне використання ШІ, перевірка даних і підготовка технічної документації (ЗК2, ЗК5, ЗК7, ЗК9, РН4, РН6, РН22).**
Обсяг і форми контролю	**3 кредити ECTS: 12 год. лекцій, 18 год. практичних, 60 год. самостійної роботи; модульний контроль; диференційований залік.**
Вимоги викладача	**вчасне виконання завдань, активність**
Умови зарахування	**згідно з навчальним планом**

ВІДПОВІДНІСТЬ СТАНДАРТУ ОСВІТИ І ОСВІТНІЙ ПРОГРАМІ

Компетенції	**ІК.01 Здатність розв’язувати складні спеціалізовані задачі і практичні завдання в галузі кібербезпеки та захисту інформації** **ЗК.01 Здатність застосовувати знання у практичних ситуаціях.** **ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності** **ЗК.05 Здатність вчитися і оволодівати сучасними знаннями.** **ЗК7. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.** **ЗК.09. Здатність до пошуку, оброблення та системному аналізу інформації** **СК.02 Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.** **СК.10 Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою безпеки *(у контексті Prompt Injection, Jailbreak-загроз та витоку даних через LLM)*.**	**Програмні результати навчання**	**РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.** **РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.** **РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.** **РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.** **РН22. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності**

СТРУКТУРА ОСВІТНЬОЇ КОМПОНЕНТИ (ДИСЦИПЛІНИ)					
Модуль 1 Основи промт-інжинірингу та взаємодії з генеративними моделями					
Лекція 1.	**Основи генеративного ШІ та LLM: принципи роботи, токени, контекст, параметри, можливості й обмеження.**	**Практичне заняття1 (ПЗ 1)**	**Ознайомлення з інструментами генеративного ШІ, налаштування середовища, порівняння моделей і правила конфіденційності.**	**Самостійна робота**	**СР1. Формування словника основних термінів промт-інжинірингу**
Лекція 2.	**Структура ефективного промту: роль, контекст, завдання, обмеження, формат відповіді, критерії якості та типові помилки.**	**ПЗ 2**	**Створення базових промтів із роллю, метою, контекстом, обмеженнями та форматом результату.**		**СР2. Порівняльний аналіз можливостей генеративних моделей**
					СР3. Аналіз правил конфіденційності та умов використання генеративних сервісів
		ПЗ 3	**Застосування прикладів у промтах: zero-shot, one-shot, few-shot і порівняння результатів.**		**СР4. Розроблення бібліотеки базових промтів для навчальних завдань**
Лекція 3.	**Методи промт-інжинірингу: декомпозиція, уточнення промтів, шаблони, системні інструкції, змінні та структурований контекст.**	**ПЗ 4**	**Розроблення шаблонів промтів зі змінними, обмеженнями та заданим форматом відповіді.**		**СР5. Розроблення набору тестових промтів для обраної предметної області**
Лекція 4. .	**Оцінювання відповідей LLM: точність, повнота, релевантність, узгодженість, відтворюваність, галюцинації та перевірка фактів.**	**ПЗ 5**	**Декомпозиція складних завдань на етапи, послідовні промти й перевірку проміжних результатів.**		**СР6. Створення промтів для отримання структурованих результатів**
					СР7.Аналіз прикладів галюцинацій і помилкових відповідей мовних моделей
		ПЗ 6	**Тестування промтів: критерії оцінювання, порівняння варіантів і документування результатів.**		**СР 8. Проведення порівняльного тестування промтів та оформлення результатів**
Лекція 5.	**Безпекові ризики LLM: prompt injection, маніпуляції інструкціями, витік даних, небезпечні результати та мінімізація ризиків.**	**ПЗ 7**	**Виявлення небезпечних промтів: аналіз prompt injection і правила захисту інструкцій та даних.**		**СР 9. Розроблення пам’ятки безпечного використання генеративного ШІ**
Лекція 6.	**Промт-інжиніринг у кібербезпеці: аналіз подій і журналів, звіти, навчання користувачів, реагування на інциденти, етика й право.**	**ПЗ 8**	**Промти для оборонної кібербезпеки: аналіз журналів, класифікація подій, рекомендації та звіт.**		**СР 10. Аналіз ризиків використання мовних моделей у кібербезпеці**
		ПЗ 9	**Підсумковий мініпроєкт: система промтів для асистента з кібербезпеки, аналізатора подій або звітів.**		**СР 11. Розроблення мініпроєкту з використанням промт-інжинірингу — 6 год.**
					СР 12. Підготовка звіту та презентації результатів мініпроєкт

ОСНОВНА ЛІТЕРАТУРА ТА МЕТОДИЧНІ МАТЕРІАЛИ

Література

1. **Шульхофф С. Інженерія запитів: вступний курс [Електронний ресурс] // *Learn Prompting*. Оновлено 7 серпня 2024 р. URL: https://learnprompting.org/uk/docs/introduction (дата звернення: 22.07.2026).**
2. **Prompt engineering [Електронний ресурс] // *AI-School: посібник*. URL: https://ai-school-handleiding.web.app/uk/docs/basis/prompt-engineering/ (дата звернення: 22.07.2026).**
3. **Chala H. Що таке ChatGPT і як ним користуватися: інструкція для новачків [Електронний ресурс] // Блог HOSTiQ.ua. 07.08.2024. URL: https://hostiq.ua/blog/ukr/chat-gpt-complete-guide/ (дата звернення: 22.07.2026).**
4. **Przystalski K., Argasiński J. K., Lipp N., Pacholczyk D. Building Personality-Driven Language Models: How Neurotic is ChatGPT [Electronic resource]. Cham : Springer, 2025. XVII, 178 p. DOI: 10.1007/978-3-031-80087-0.**
5. **Srivastava S., Vurukonda N. Prompt Engineering in Action [Електронний ресурс]. Version 4. Manning Publications, 2025. URL: https://www.manning.com/books/prompt-engineering-in-action (дата звернення: 22.07.2026).**

Методичне забезпечення

1. **Сирий В. Сотников Ю. Загальний курс користувача ПК. Методичні вказівки.- Харків, 2019.-56с.**
2. **Сотников Ю., Сирий В. Моделювання технологічних процесів і систем. Навч. посібник.- 2021.-126 с.**

СИСТЕМА ОЦІНЮВАННЯ
(https://biotechuniv.edu.ua/wp-content/uploads/2022/04/norm-b-nm-op-pol6.pdf)

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.