



ШІ-агенти в кібербезпеці

Спеціальності: E2 Екологія, E4 Науки про Землю, F2 Інженерія програмного забезпечення, F3 Комп'ютерні науки, F4 Системний аналіз та наука про дані, F5 Кібербезпека та захист інформації, F6 Інформаційні системи і технології, F7 Комп'ютерна інженерія, G5 Електроніка, електронні комунікації, приладобудування та радіотехніка, G6 Інформаційно-вимірювальні технології, G7 Автоматизація, комп'ютерно-інтегровані технології та робототехніка, G18 Геодезія та землеустрій, G22 Біомедична інженерія

Рівень вищої освіти	другий (магістерський)		
Статус дисципліни	вибіркова (Дисципліна індивідуального вибору 4)		
Обсяг дисципліни	150 годин/ 5 кредитів ЄКТС		
Мова викладання	українська/англійська		
Що буде вивчатися (предмет вивчення)	У межах дисципліни вивчаються теоретичні засади, архітектури, моделі та інструментальні засоби побудови AI-агентів і багатоагентних систем для задач кібербезпеки. Розглядаються підходи до проєктування агентів, їх взаємодії, використання зовнішніх інструментів, пам'яті, правил прийняття рішень, механізмів контролю та оркестрації процесів у різних середовищах, зокрема п8п і програмних фреймворках. Окрему увагу приділено застосуванню агентних систем для моніторингу подій безпеки, аналізу загроз, реагування на інциденти та підтримки рішень		
Чому це цікаво/треба вивчати (мета)	Вивчення курсу є актуальним у зв'язку зі зростанням обсягів даних, складності кіберзагроз і потреби в інтелектуальній оркестрації дій у режимі, наближеному до реального часу. Курс дозволяє поєднати знання з штучного інтелекту, автоматизації та кібербезпеки для створення практично орієнтованих рішень, здатних підвищувати швидкість, обґрунтованість і результативність захисту інформаційних систем. Метою курсу є формування у здобувачів системного розуміння сучасних AI-агентів як нового класу інтелектуальних засобів автоматизації та підтримки кібербезпекових процесів		
Як можна користуватися набутими знаннями і уміннями (компетентності)	Набуті знання та вміння можуть бути використані для проєктування, налаштування, інтеграції та оцінювання AI-агентів і багатоагентних систем у задачах кібербезпеки. Здобувачі зможуть застосовувати їх для автоматизації аналізу подій безпеки, оброблення повідомлень про інциденти, підтримки рішень у SOC, оркестрації дій із використанням п8п та інших середовищ, а також для розроблення дослідницьких і прикладних рішень у сфері захисту інформації. Курс формує компетентності системного мислення, агентного проєктування, інтеграції інструментів ШІ та критичного оцінювання їх безпечності й ефективності		
Пререквізити	«Технології забезпечення якості програмно-технічних комплексів»		
Кореквізити	Матеріал, засвоєний під час вивчення цієї дисципліни, є базою для підготовки кваліфікаційної роботи магістра		
Організація навчання	Види занять: лекції, практичні заняття, самостійна робота. Форми здобуття освіти: денна, заочна. Форми контролю: поточний, модульний та підсумковий (семестровий) контроль (іспит)		
Кафедра	Кафедра кібербезпеки та інтелектуальних інформаційних технологій.		
Факультет	Радіоелектроніки, комп'ютерних систем та інфокомунікацій		
Викладач		ПІБ	Брежнев Євген Віталійович
		Посада	професор
		Вчене звання	професор
		Науковий ступінь	доктор технічних наук
		e-mail	e.brezhnev@csn.khai.edu
Посилання на електронні матеріали курсу	https://mentor.khai.edu/course/		
Посилання на силабус			