ДИСЦИПЛІНА «МЕТОДИ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ»

Анотація. Належить до переліку дисциплін вільного вибору аспіранта. У ній розглядаються теоретичні засади та практичні аспекти застосування технологій штучного інтелекту (ШІ) та машинного навчання (ML) для захисту інформаційних систем. Програма курсу розкриває роль ШІ як інструменту автоматизації виявлення кіберзагроз у реальному часі; аналізує використання нейронних мереж для детекції аномалій, класифікації шкідливого програмного забезпечення та прогнозування цілеспрямованих атак (APT). Особлива увага приділяється етичним аспектам ШІ, проблемі «отруєння» даних (adversarial machine learning) та створенню інтелектуальних систем прийняття рішень, що підвищують стійкість критичної інфраструктури до сучасних цифрових викликів.

Мета навчальної дисципліни: засвоєння аспірантами фундаментальних знань щодо інтеграції методів штучного інтелекту в архітектуру кібербезпеки, формування професійних компетентностей для розробки та впровадження інтелектуальних алгоритмів захисту даних, а також розвиток навичок критичного оцінювання ефективності ШІ-моделей у протидії кіберзлочинності.

Попередні вимоги:

Аспірант повинен знати: архітектуру комп'ютерних мереж, основи криптографічного захисту інформації, базові принципи вищої математики (лінійна алгебра, теорія ймовірностей) та основи програмування.

Аспірант повинен вміти: працювати з інструментами аналізу мережевого трафіку, володіти базовими навичками обробки даних у середовищі Python, аналізувати вразливості інформаційних систем.

Змістові модулі:

- Концепція інтелектуальної кібербезпеки: від реактивного до проактивного захисту.
- Алгоритми машинного навчання у виявленні вторгнень (IDS/IPS).
- Глибоке навчання (Deep Learning) для аналізу шкідливого коду та спаму.
- Методи інтелектуального аналізу поведінки користувачів та сутностей (UEBA).
- Протидія атакам на моделі ШІ: захист від маніпуляцій з даними навчання.
- Автоматизація реагування на інциденти за допомогою інтелектуальних агентів.
- Перспективи використання генеративного ШІ (LLMs) у Red Teaming та Blue Teaming.

Мова викладання: українська (англійська за потреби).

Рік підготовки, шифр навчальної дисципліни: друге півріччя другого року навчання, ВБ.2.02.01.

Кількість кредитів: 4.

Форма заключного контролю: іспит.

Структура навчальної дисципліни: загальний обсяг 120 годин.

Викладач: Толюпа Сергій Васильович, доктор технічних наук, професор.