СНІГУРОВА Ірина Іванівна, старший викладач кафедри української мови Національного технічного університету «Харківський політехнічний інститут», аспірантка Харківського національного університету внутрішніх справ *(м. Харків, Україна)*
Науковий керівник:
ДАНЧЕНКО Ірина Олексіївна, доктор педагогічних наук, доцент, професор кафедри ЮНЕСКО «Філософія людського спілкування» та соціально-гуманітарних дисциплін, Державний біотехнологічний університет

ВИКОРИСТАННЯ МЕТОДУ МОДЕЛЮВАННЯ ПРОФЕСІЙНИХ СИТУАЦІЙ ЯК ОДИН ЗІ ШЛЯХІВ ФОРМУВАННЯ МОВНО-КОМУНІКАТИВНОЇ КОМПЕТЕНТНОСТІ МАЙБУТНІХ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

Підготовка майбутніх фахівців з кібербезпеки в закладах вищої освіти має певні особливості. Однією з особливостей є велика кількість професій для таких випускників. Держспецзв'язком за підтримки проєкту USAID «Кібербезпека критично важливої інфраструктури України» було розроблено професійні стандарти, якими введено 21 професію, впроваджено професійні кваліфікації згідно з національною рамкою кваліфікацій (НРК). До таких професій відносять, наприклад, аналітик загроз безпеки, аудитор інформаційних технологій (з кібербезпеки), фахівець з реагування на інциденти кібербезпеки, конструктор систем кібербезпеки, фахівець з криптографічного захисту інформації, фахівець з технічного захисту інформації та інші. Кожна з цих професій має свою специфіку відповідно до трудових функцій, компетентностей і результатів навчання.

Мовно-комунікативна компетентність фахівців з кібербезпеки згідно з вимогами професійних стандартів, а також стандартів вищої освіти є важливим чинником успішної професійної діяльності таких фахівців. Наприклад, професійний стандарт фахівця з реагування на інциденти кібербезпеки визначає такі результати навчання в розділі «Комунікація» для різних компетентностей:

- писати й публікувати звіти проведених заходів;
- готувати звіти, що містять індикатори компрометації для аналізу поведінки зловмисника та збору артефактів його роботи;
- комунікувати з керівниками організації різних рівнів, із представниками зацікавлених сторін щодо проведення аналізу інцидентів;
- налаштовувати координацію з аналітиками розвідки для кореляції даних оцінки загроз;

- взаємодіяти з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами й організаціями, які є суб'єктами національної системи кібербезпеки;
- готувати та виголошувати доповідь з оцінки поточного стану кібербезпеки керівництву, персоналу й користувачам;
- аналізувати дані з одного або декількох джерел, готувати оперативні звіти на основі кібердослідних даних і поширення серед зацікавлених сторін;
- організовувати та проводити практичні семінари з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;
- розроблювати вказівки й настанови для працівників, залучених до розроблення стратегій, програм і політик з розвитку кібербезпеки та інші.

Аналіз таких результатів навчання показує, що фахівець цієї професії повинен вміти ефективно взаємодіяти з використанням творчого й аналітичного мислення, глибоких професійних технічних знань, навичок професійної комунікації з представниками різних організацій, керівництвом і персоналом своєї організації. Він повинен готувати документи, доповіді, звіти, керівні документи з обробки кіберінцидентів, уміти проводити заняття для зацікавлених сторін. Аналіз інших професійних стандартів фахівців з кібербезпеки показує аналогічні вимоги щодо урахування специфіки кожної з таких професій.

Одним з інноваційних методів навчання в таких умовах є метод моделювання професійних ситуацій. Існують різні методи й технології для моделювання професійних ситуацій у сфері ІТ. Найпопулярніші з них – віртуальні лабораторії, реальні проєкти, науково-дослідницька діяльність та ігри-симуляції [2].

Для прикладу, викладачами може бути сплановано командне змагання, під час проведення якого кільком командам ставлять проблемне питання щодо кіберінциденту. Командам дають час для розв'язання завдання. При цьому команди знаходяться в різних аудиторіях і не можуть бачити, що відбувається в інших командах. Передбачається обов'язкове обговорення завдання та можливих рішень у вигляді дискусій, мозкових атак. Кінцеві результати виконання завдання студенти доповідають комісії, відпрацьовуючи уміння їх презентувати. Також може передбачатися заповнення документації стосовно процесу обробки кіберінцидентів. Подібні змагання існують в форматі змагань CTF («Capture the Flag» – «перехоплення прапору»), але такі змагання більше спрямовані на набуття технічних умінь. У запропонованому нами форматі командного змагання розвиваються також уміння комунікувати, працювати в команді, уміння висловлювати свої думки професійною технічною мовою.

Список використаних джерел

1. Реформування системи підготовки кадрів у сфері кібербезпеки: Нацагентство кваліфікацій схвалило 8 нових професійних стандартів. Державна служба спеціального зв'язку та захисту інформації України. https://cip.gov.ua/ua/news/reformuvannya-sistemi-pidgotovki-kadriv-u-sferi-kiberbezpeki-nacagentstvo-kvalifikacii-skhvalilo-8-novikh-profesiinikh-standartiv.
2. Кулєшов С., Остапенко А. Моделювання професійних ситуацій для підготовки бакалаврів з інформаційних технологій. Професійна освіта в умовах сталого розвитку суспільства. Монографія, 2024. С. 342–355.