УДК 378

DOI 10.18372/2786-823.1.18135

Горошко Олександр Леонідович

аспірант,

Ніжинський державний університет імені Миколи Гоголя,

м. Ніжин, Україна

my.unix.server@gmail.com

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ДАНИХ ЯК КЛЮЧОВІ СКЛАДОВІ ФОРМУВАННЯ ПРОФЕСІЙНОЇ КОМПЕТЕНТНОСТІ ФАХІВЦІВ КОМП'ЮТЕРНИХ НАУК

Анотація. *У статті розглянуто тему кібербезпеки та захист даних як ключові складові формування професійної компетентності фахівців спеціальності комп'ютерних наук. Аналізуються аспекти навчання та педагогічного підходу до формування компетентностей студентів у цій галузі. Висвітлюється важливість інтегрованого підходу, враховуючи аспекти навчання в сфері кібербезпеки та захисту даних.*

Ключові слова: *кібербезпека, захист даних, комп'ютерні науки.*

Annotation. *The article examines the topic of cyber security and data protection as key components of professional competence formation of computer science specialists. Aspects of training and pedagogical approach to the formation of students' competencies in this field are analyzed. The importance of an integrated approach, taking into account aspects of training in the field of cyber security and data protection, is highlighted.*

Key words*: cyber security, data protection, computer science*

Вступ. Галузь комп'ютерних наук повинна постійно бути на вершині технологічного прогресу та інновацій. Забезпечення інформаційної безпеки вже не є лише актуальною проблемою, воно стало критично важливою складовою в умовах стрімкого розвитку технологій, вимагає високого рівня компетентності

в області кібербезпеки та захисту даних. Розуміння нагальних проблем і викликів та готовність до їх подолання стають обов’язковою передумовою для ефективного функціонування та розвитку даного наукового напряму.

Мета статті. Основною метою є розгляд питань кібербезпеки та захисту даних як необхідної складової для підготовки фахівців галузі комп'ютерних наук.

У статті розглядається важливість оновлення педагогічного підходу до формування професійної компетентності, а також необхідність інтегрованого методу, що об'єднує теоретичні знання та практичний досвід.

Методи дослідження. Дослідження включає аналіз наукових праць та публікацій у галузі комп'ютерних наук та кібербезпеки, тематичних виступів на фахових конференціях. Співпраця з фахівцями в області кібербезпеки дозволила визначити актуальні тенденції та прогалини в науковому знанні.

Виклад основного матеріалу. Сучасна галузь комп'ютерних наук потребує фахівців, які мають глибоке розуміння щодо кібербезпеки та захисту даних. Це важливо не лише для безпеки інформаційних систем і мереж, але й для захисту конфіденційності, цілісності та доступності даних.

Актуальність проблем кібербезпеки в сучасному світі та в контексті вищої освіти висвітлюють наукові праці багатьох вчених, серед яких необхідно виокремити Л.А. Арсенович [1], С.Г. Литвинову [6], С.Л. Проскуру [6], В.М. Богуш [5].

Питання, пов'язані з ефективним забезпеченням інформаційної та кібербезпеки, стають все більш актуальними та потребують постійного вдосконалення.

Тема кібербезпеки та захисту даних розглядається як ключові складові формування професійної компетентності фахівців комп'ютерних наук, важливості педагогічного підходу до процесу формування професійної компетентності студентів у цій галузі, а також необхідності інтегрованого методу, який поєднує практичний досвід та теоретичні знання.

До нормативного змісту підготовки бакалавра за спеціальністю «Комп’ютерні науки» включається розуміння концепції інформаційної

безпеки, принципів безпечного проектування програмного забезпечення, забезпечення безпеки комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних [4]. Навчальні програми повинні сприяти розвитку навичок аналізу потенційних загроз, проектування заходів з захисту та вміння швидко реагувати на інциденти. Слід підкреслити важливість педагогічного супроводу студентів у розвитку вищезазначених навичок та вмінь реагувати на складні ситуації.

Забезпечення кібербезпеки та захист даних стали вкрай важливим завданням. У галузі комп'ютерних наук, де студенти готуються до роботи з інформацією та технологіями, навчання їх навичкам кібербезпеки стає нагальною необхідністю. Зловмисники постійно шукають слабкі місця в інформаційних системах і студентам потрібно навчитися бути готовими вміти ефективно захищати дані та інформаційні ресурси. Навчання студентів кібербезпеці є кроком до створення безпечного та надійного цифрового середовища для країни в цілому. Фахівці в цій галузі повинні не лише володіти технічними навичками, але й розуміти загрози, з якими вони можуть зіткнутися, та вміти захищати системи та дані від цих загроз. Формування професійної компетентності базується на ретельному вивчені основ кіберзахисту та оволодіння практичними навичками [5].

Загрози включають в себе масштабні кібератаки, які можуть призвести до втрати величезної кількості даних, порушення конфіденційності, порушення прав осіб, виведення з ладу цілих підприємств або призупинку їхньої діяльності. Існують загрози, пов'язані зі зламом паролів, атаками на мережеві системи та розповсюдженням вірусів, шкідливих програм. У разі невідповідного захисту даних можуть виникнути серйозні фінансові та репутації збитки. Загрози кібербезпеці продовжують зростати, спостерігається збільшення кількості шпигунських програм, загроз поширюваних через електронну пошту, атакуючи не лише державні установи та корпорації, але й малі та середні підприємства.

Компанія ESET — лідер у галузі інформаційної безпеки — представмла рейтинг найбільш поширених кіберзагроз за січень-квітень 2022

року. У цей період загальна кількість виявлених зразків загроз зросла на 20% порівняно з останніми чотирма місяцями 2021 року. Зокрема збільшилась кількість шпигунських програм та загроз, які поширюються через електронну пошту. Також у цей період значно вплинула на поширення загроз у світі війна в Україні. Зокрема ця тема активно використовувалася у спам-повідомленнях та на шкідливих сайтах. Крім цього, з початком повномасштабного вторгнення Україна неодноразово ставала ціллю кіберзлочинців. Зокрема з 23 лютого під час атак на українські організації зловмисники використали ряд шкідливих програм для знищення даних, а також унікальну загрозу Industroyer, націлену на енергетичний сектор [3].

Педагогічна галузь повинна забезпечити студентів, які вивчають комп'ютерні науки, відповідною освітою, що включає в себе технічні навички, вміння аналізу та вживання превентивних заходів, ефективного реагування на виклики в галузі кібербезпеки. Освітні програми повинні бути спрямовані на розвиток у студентів розуміння загроз, що є невід'ємними складовими у підготовці майбутніх фахівців та ключовими елементами професійної компетентності в цій галузі.

Розглянемо методи та підходи до навчання.

Симуляції та імітації кібератак - цей метод надає студентам можливість відчути реальність кібератак та їх наслідки, не завдаючи реальних шкод. Студенти можуть використовувати віртуальні лабораторії та платформи для практичного моделювання кібератак та розробки методів захисту.

Практичні завдання та вправи - проведення практичних завдань дозволяє набути необхідних навичок, це може включати в себе аналіз логів безпеки, розробку та виконання планів відновлення та тестування вразливостей.

Подійні навчання - участь у змаганнях з кібербезпеки дозволяє студентам випробувати свої навички в реальних умовах та отримати новий досвід. Такі змагання як, наприклад захоплення прапора (Capture the Flag - різновид криптоспорту), де студенти розв'язують завдання, пов'язані з кібербезпекою.

Лекції та теоретичні курси - розуміння теоретичних аспектів кібербезпеки є обов'язковим, надають студентам основні знання про загрози, криптографію, мережеву безпеку та інші важливі поняття.

Сценарії - створення реалістичних сценаріїв допомагають студентам відтворюючі реальні ситуації.

Групові проєкти - залучення до групових проєктів у роботі з системами безпеки та аудиту, надають можливість застосовувати теоретичні знання на практиці.

Співпраця зі спеціалістами - співпраця з компаніями та іншими спеціалістами в цій галузі надають студентам знання про реальний стан справ та поточні вимоги.

Освітні ресурси - освітні ресурси та онлайн-курси, що доступні на платформах з відкритим доступом, можуть допомогти студентам розширити свої знання та навички в сфері кібербезпеки.

Ці методи та підходи допомагають студентам комп'ютерних наук розвивати потрібні компетентності в області кібербезпеки та захисту даних, що є важливою складовою професійної підготовки.

Формування компетентностей у сфері кібербезпеки відкриває нові горизонти та можливості для студента. Допомагає розвивати не лише технічні навички, а й критичне мислення та аналітичні здібності.

Важливою складовою професійної компетентності фахівців із кібербезпеки є цифрова компетентність, яка передбачає здатність та вміння логічно та системно використовувати інформаційні технології. Фахівець із кібербезпеки повинен вільно володіти сучасними технологіями та використовувати їх у своїй професійній діяльності, тим самим забезпечувати життєво важливі інтереси громадянина, суспільства та держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1].

Важливість педагогічного супроводу в навчанні студентів та його мета – забезпечити успішне навчання студентів та їх підготовку; допомогти розвивати навички, які потрібні для досягнення професійних цілей. Він також може включати в себе консультацію, менторство, психологічну підтримку та відіграє важливу роль у навчанні студентів, і це можливо пояснити з кількох ключових причин:

- Допомагає студентам отримати не лише теоретичні знання, але й розвивати практичні навички. Викладачі та наставники надають можливість студентам використовувати здобуті знання на практиці, що є надзвичайно важливим, де реальний досвід має велике значення.
- Сфера кібербезпеки постійно змінюється, нові загрози з'являються щодня. Потрібно забезпечити актуальність та оновлення навчальних матеріалів, щоб студенти могли отримувати найсвіжішу інформацію та навички в цій галузі.
- Допомогти студентам визначити свій прогрес та слабкі місця, надаючи зворотний зв'язок та відповідну оцінку. Це допомагає краще розуміти досягнення та працювати над вдосконаленням.
- Навичка розвивати критичне мислення є надзвичайно важливою в сфері кібербезпеки, де потрібно приймати рішення в умовах невизначеності.
- Можливість консультуватися, вирішувати труднощі та стимулюють до досягнень. Це особливо важливо у галузі кібербезпеки, де завдання можуть бути складними та вимагати великих зусиль.

Узагальнюючи, педагогічний супровід гарантує отримання комплексної та ефективної освіти у сфері кібербезпеки [2; 6]. Він сприяє професійному розвитку, готовності до викликів галузі та забезпечує надійні фундаментальні знання і навички, необхідні для успішної кар'єри в цьому напрямку.

Фахівці із кібербезпеки, які ведуть викладацьку діяльність, повинні бути готовими до реалізації нових ідей, використовувати можливості інформаційних технологій, підвищувати якість навчального процесу, готувати молодь до успішного життя. Цифрова компетентність є ключовою у процесі професійного розвитку [1].

До основних результатів дослідження слід віднести виявлення ключових аспектів формування професійної компетентності студентів у галузі комп'ютерних наук, зосереджуючись на важливості збалансованого поєднання теоретичних знань та реального практичного досвіду.

Виділимо наступні основні аспекти:

Актуальність. Дослідження підтверджує, що галузь комп'ютерних наук потребує високого рівня компетентності. Забезпечення інформаційної безпеки стає критично важливою складовою в умовах стрімкого розвитку технологій.

Роль викладачів. Викладачі закладів вищої освіти відіграють ключову роль у підготовці студентів, охоплюючи не лише технічні аспекти комп'ютерних наук, а й розвиток аналітичних та управлінських навичок.

Необхідність інтегрованого підходу. Навчання повинно включати інтегрований підхід, який поєднує теоретичні знання, практичний досвід та сучасні методи навчання, такі як симуляції та групові проекти.

Важливість постійного оновлення. Сфера кібербезпеки постійно змінюється, тому навчальні програми повинні постійно оновлюватися, щоб відповідати актуальним викликам та технологічним тенденціям.

Цифрова компетентність. Цифрова компетентність є ключовою у процесі професійного розвитку, яка проявляється при вирішенні різних завдань із залученням засобів інформаційних технологій

Висновки. Формування професійної компетентності студентів повинно враховувати не лише теоретичні знання, а й практичний досвід. У галузі комп'ютерних наук це може включати навички аналізу потенційних загроз, розробки заходів з підвищення безпеки та реагування на інциденти. Викладачі закладів вищої освіти мають готувати студентів не лише до вивчання технічних аспектів комп'ютерних наук, важливо розвивати здатність швидко та обізнано приймати рішення, оскільки в сучасному цифровому світі це може виявитися вирішальним. Володіння навичками захисту даних та цифрова компетентність є невід'ємними складовими успішної кар'єри фахівця комп'ютерних наук в сучасному світі інформаційних технологій.

Список використаних джерел

1. Арсенович Л.А. Інструментарій підвищення рівня цифрової компетентності фахівців із кібербезпеки в освітньому процесі. *Кібербезпека: освіта, наука, техніка.* 2022. №3(15). URL: https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/338/281 (дата звернення: 29.10.2023).

2. Драч І.І. Педагогічний супровід формування професійної компетентності майбутніх викладачів вищої школи в умовах магістратури. *Педагогіка формування творчої особистості у вищій і загальноосвітній школах:* зб. наук. пр. 2013. Вип. 28 (81). – Запоріжжя: КПУ. С. 473 - 479. URL: http://pedagogy-journal.kpu.zp.ua/archive/2013/28/28_2013.pdf (дата звернення: 29.10.2023).

3. Рейтинг Інтернет-загроз: вплив війни в Україні та найактивніші шкідливі програми. URL: https://www.eset.com/ua/about/newsroom/press-releases/malware/reyting-internet-ugroz-kak-izmenilas-aktivnost-khakerov-vo-vremya-voyny/ (дата звертання: 30.10.2023)

4. Комп’ютерні науки — спеціальність рівня «бакалавр». Сайт «Освіта.UA». URL: https://osvita.ua/consultations/spec-bach/65203/ (дата звернення: 29.10.2023).

5. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під. ред. В. М. Богуша. - Київ: Видавництво Ліра-К, 2020. 554 с. URL: https://jurkniga.ua/contents/osnovi-kiberprostoru-kiberbezpeki-ta-kiberzakhistu.pdf (дата звертання: 30.10.2023).

6. Проскура С.Л., Литвинова С.Г. Формування професійної компетентності майбутніх бакалаврів комп'ютерних наук. *Фізико-математична освіта (ФМО).* 2019. № 2(20). URL: https://repository.sspu.edu.ua/bitstream/123456789/7608/1/Proskura_Lytvynova_Formuvannia_profesiinoi_kompetentnosti.pdf (дата звертання: 15.10.2023).