ОСОБЛИВОСТІ ПРОВЕДЕННЯ ПРАКТИЧНИХ РОБІТ ДЛЯ МАЙБУТНІХ БАКАЛАВРІВ З КІБЕРБЕЗПЕКИ

PECULIARITIES OF PRACTICAL WORK FOR FUTURE BACHELORS IN CYBERSECURITY

УДК 378.016
DOI https://doi.org/10.32782/2663-6085/2024/71.1.35

Самойленко О.О.,
докт. пед. наук, доцент,
доцент кафедри кібербезпеки
Навчально-наукового інституту
інформаційної безпеки та стратегічних
комунікацій

У статті автор розглядає особливості проведення практичних робіт для майбутніх бакалаврів з кібербезпеки. Зазначається важливе значення таких занять у фаховій підготовці здобувачів та їх вплив на практичну компетентність у цій сфері. Актуальність теми дослідження обумовлена тим, що практичні роботи є важливою складовою навчального процесу підготовки фахівців з кібербезпеки. Висвітлені методи, інструменти та підходи, які можна використовувати під час проведення практичних та лабораторних занять з кібербезпеки, наводиться аналіз особливостей проведення практичних робіт. Встановлено, що балансування теоретичних знань і практичних вмінь виступає ключовим елементом навчання майбутніх фахівців з кібербезпеки. Хоча теоретична база є невід'ємною частиною, практичні навички, які здобувачі отримують у процесі роботи з реальними системами та інструментами, допомагають їм зрозуміти, як застосовувати ці знання на практиці. З урахуванням швидких змін у технологіях та загрозах кібербезпеці, фахівці повинні бути готові швидко адаптуватися та використовувати нові інструменти. Практичні навички сприяють розвитку гнучкості та здатності до швидкого навчання, а також допомагають у розвитку аналітичних здібностей, дозволяють розв'язувати складні проблеми та виявляти вразливості в системах кібербезпеки.

Результати проведеного дослідження дають можливість дійти висновку, що практичні заняття відіграють значущу роль у формуванні навичок майбутніх бакалаврів з кібербезпеки, даючи їм можливість набути практичний досвід, необхідний для успішної кар'єри у даній області. Ці заняття дозволяють майбутнім фахівцям експериментувати з різними методами та інструментами, а також отримувати прямий досвід у вирішенні реальних ситуацій в галузі кібербезпеки.

Ключові слова: *кібербезпека, заклади вищої освіти, освітній процес, цифровізація, практичні роботи, методика.*

In the article, the author discusses the peculiarities of practical work for future bachelors in cybersecurity. The author emphasizes the importance of such classes in the professional training of applicants and their impact on practical competence in this area. The relevance of the research topic is due to the fact that practical work is an important component of the educational process of training cybersecurity specialists. The article highlights the methods, tools and approaches that can be used in practical and laboratory classes on cybersecurity, and analyzes the peculiarities of practical work. It has been established that balancing theoretical knowledge and practical skills is a key element in the training of future cybersecurity professionals. Although the theoretical framework is an integral part, the practical skills that students acquire while working with real systems and tools help them understand how to apply this knowledge in practice. Given the rapid changes in technology and cybersecurity threats, professionals must be ready to adapt quickly and use new tools. Practical skills promote flexibility and the ability to learn quickly, as well as help develop analytical skills, solve complex problems and identify vulnerabilities in cybersecurity systems.

The results of the study allow us to conclude that practical classes play a significant role in developing the skills of future bachelors in cybersecurity, giving them the opportunity to gain the practical experience necessary for a successful career in this field. These classes allow future professionals to experiment with different methods and tools, as well as gain direct experience in solving real-life cybersecurity situations.

Key words: *cybersecurity, higher education institutions, educational process, digitalization, practical work, methodology.*

Постановка питання в загальному вигляді. Методика відіграє надзвичайно важливу роль у систематичному та цілеспрямованому засвоєнні професійних знань, навичок і вмінь, в умовах цифровізації освітнього процесу. Проведення практичних робіт для майбутніх бакалаврів з кібербезпеки має свої особливості, адже ця спеціальність потребує великої уваги до деталей, актуальних методів захисту та практичних навичок. В умовах сьогодення, загроза кібератак продовжує зростати зі збільшенням кількості складних і успішних цілеспрямованих кібератак по всьому світу. Щоб вирішити цю проблему, існує гостра потреба в професіоналах з кібербезпеки з відповідною мотивацією та навичками для запобігання, виявлення, реагування або навіть пом'якшення ефекту таких загроз.

Мета дослідження: аналіз особливостей проведення практичних робіт для майбутніх бакалаврів з кібербезпеки

Методологія дослідження ґрунтується на аналітичному методі через аналіз наукової літератури з проблеми дослідження.

Аналіз наукових досліджень. В Україні професійна підготовка бакалаврів з кібербезпеки регулюється законодавчо-нормативними актами, зокрема Законами України «Про освіту», «Про вищу освіту», «Про інформацію», а також Стратегією кібербезпеки України та Законом «Про національну безпеку України». Розвиток нових концепцій у професійній підготовці бакалаврів з кібербезпеки вимагає уваги до результатів наукових досліджень і прогностичних ідей, особливо

в контексті інтеграції України до європейського освітньо-інформаційного простору. Високий рівень розвитку національної системи кібербезпеки в Україні забезпечує міцну стратегічну та законодавчу базу.

Розробка та використання віртуальних навчальних об'єктів у освітньому процесі стає все більш актуальною та обговорюваною темою серед вчених і практиків у сфері освіти. Методичним проблемам визначення, побудови і використання віртуальних лабораторних практикумів присвячені роботи зарубіжних та вітчизняних вчених, зокрема О. Спіріна, Б. Брайко, М. Нагорняка, М. Мазура, Н. Котенко, Л. Харлай, О. Манька, О. Коновалова та ін.

Основна частина дослідження. У контексті дистанційного та змішаного навчання, яке стало нормою для України у зв'язку з пандемією COVID-19 та війною, розпочатою російською федерацією, постає актуальне питання якісного засвоєння освітніх кваліфікацій. Це стає важливою проблемою як для викладачів, так і для здобувачів. Належне збалансування теоретичного знання та практичних навичок є важливим елементом освіти майбутніх фахівців з кібербезпеки. Теоретичні знання є важливими, але навички, отримані в процесі роботи з реальними системами та інструментами, допомагають здобувачам освіти зрозуміти, як застосовувати ці знання на практиці. Швидкі зміни в технологіях та загрозах кібербезпеки означають, що фахівці повинні бути готові швидко адаптуватися та використовувати нові інструменти, а практичні навички допомагають розвивати гнучкість та вміння швидко навчатися, разом з тим практичні завдання сприяють розвитку аналітичних здібностей майбутніх фахівців, допомагаючи їм вирішувати складні проблеми та розпізнавати вразливості в системах. Варто зазначити, що лабораторні та практичні роботи відіграють надзвичайно важливу роль у підготовці технічних фахівців, незалежно від галузі. Вони дозволяють здобувачам освіти отримати практичний досвід, розвивають аналітичні та проблемно-орієнтовані навички, а також сприяють формуванню важливих компетентностей.

Проаналізувавши ряд наукових досліджень [5; 3; 4], зазначимо деякі компетентності:

a) Дослідницька компетентність: практичні роботи стимулюють здобувачів до дослідницької діяльності, вони навчаються встановлювати гіпотези, проводити експерименти та аналізувати результати.

b) Пошукова компетентність: виконання практичних робіт сприяє розвитку навичок пошуку та аналізу інформації, що є важливим у сучасному інформаційному середовищі.

c) Інформаційно-організуюча компетентність: майбутні фахівці навчаються організовувати та обробляти отриману інформацію, вибирати найбільш важливі аспекти та представляти результати своїх досліджень.

d) Оціночно-аналітична компетентність: виконання практичних робіт допомагає здобувачам розвивати вміння аналізувати та оцінювати отримані результати, робити висновки та приймати обґрунтовані рішення.

Як було зазначене вище, практичні роботи (ПР) є важливою складовою освітнього процесу для майбутніх бакалаврів з кібербезпеки. Вони дають можливіть здобувачам можливість набути практичних навичок та знань, необхідних для успішного виконання їхніх професійних обов'язків. Підготовка бакалавра з кібербезпеки – це систематичний і послідовний процес, організований у рамках певної системи, яка сприяє його результативності. Проте, діяльність фахівців з кібербезпеки у вирішенні стратегічних завдань щодо забезпечення кібербезпеки України залишається недостатньо ефективною у виявленні та ліквідації кіберзагроз, як відкритих, так і прихованих.

Зазначимо основні цілі ПР з кібербезпеки:

- Ознайомлення здобувачів з основними інструментами та методами роботи в сфері кібербезпеки.
- Розвиток у здобувачів практичних навичок з захисту інформаційних систем.
- Формування у майбутніх бакалаврів навичок аналітичного та критичного мислення.
- Виховання у майбутніх фахівців відповідальності за інформаційну безпеку.

Основними типами практичних робіт, які використовуються з кібербезпеки можна зазначити наступні:

- Практичні заняття. Передбачають відпрацювання бакалаврами практичних навичок з використанням реальних сценаріїв кібератак. Практичні заняття можуть проводитися як у лабораторних умовах, так і на базі підприємств та організацій.
- Навчальні симуляції. Цей тип ПР передбачає використання здобувачами комп'ютерних симуляторів для відпрацювання навичок роботи в умовах кіберінцидентів. Навчальні симуляції дозволяють отримати досвід роботи з реальними кіберзагрозами без ризику для інформаційних систем.

Тенденція віртуалізації в кібербезпеці стає все більш популярною, особливо в контексті навчання та тренування майбутніх фахівців. Віртуалізовані лабораторні середовища дозволяють здобувачам освіти отримати практичний досвід без необхідності доступу до дорогого обладнання або фізичних лабораторій. Зростання популярності віртуалізації призвело до появи широкого спектра інструментів та обладнання, спеціально розроблених для роботи у віртуальному середовищі [6; 4]. Використання спеціалізованої віртуальної лабораторії кібербезпеки (CVLab) та її впровадження

у освітній процес закладів вищої освіти може значно покращити якість підготовки майбутніх фахівців з кібербезпеки.

При оцінці компетентності випускника ЗВО як майбутнього фахівця, необхідно враховувати його особистісні якості, які виявляються у підході до виконання професійних обов'язків. Ці особистісні риси не лише включають в себе дотримання регламентованих обов'язків, але й охоплюють інноваційне мислення, творчість, комунікативність, організаторські здібності, а також проектні, прогностичні та інші професійні та особистісні навички.

Виконання практичних робіт, незалежно від того, чи це реальна чи віртуальна лабораторія, включає кілька етапів. Переважна більшість цих етапів співпадає як для віртуальних, так і для реальних практичних робіт. Однак основна відмінність полягає в тому, що віртуальні практичні роботи виконуються індивідуально, тоді як реальні практичні роботи виконуються групами зазвичай в складі 2–3 осіб. Робота у групі сприяє формуванню у здобувачів навичок колективної роботи, почуття відповідальності та співпраці, що є важливим аспектом їх майбутньої професійної діяльності. Також варто відзначити різницю в експериментальній частині виконання роботи.

Для проведення практичних робіт у цифровому середовищі використовуються такі засоби, як скрінкасти з прикладами розв'язування завдань, розміщені на відео-порталі, посилання на методичні рекомендації з електронної бібліотеки, а також сервіси колективної роботи, що можуть надаватися як електронні освітні системи навчального закладу, так і зовнішні ресурси. Один з ключових елементів завдань для лабораторних та самостійних робіт бакалаврів з кібербезпеки полягає у забезпеченні доступу до програмних пакетів для виконання завдань [3].

Для проведення практичних робіт для майбутніх бакалаврів з кібербезпеки за допомогою Moodle, варто враховувати наступне: організація матеріалів курсу має бути таким чином, щоб здобувачів легко могли знайти всю необхідну інформацію для практичних занять, включаючи інструкції, приклади, завдання та ресурси; варто створити завдання для майбутніх фахівців таким чином, щоб вони включали в себе практичні вправи з кібербезпеки, зокрема виконання практичних завдань, вирішення кейсів, аналіз вразливостей тощо; варто налагоджувати зворотний зв'язок від здобувачів щодо якості та ефективності практичних та лабораторних занять з кібербезпеки на платформі Moodle та вносити необхідні корективи для поліпшення освітнього процесу. Moodle пропонує різні інструменти для надання персоналізованої зворотної зв'язку, що може допомогти кожному майбутньому фахівцю досягти успіху. Moodle пропонує широкий спектр інструментів для надання та отримання зворотнього зв'язку, таких як коментарі – викладачі можуть залишати листові коментарі до завдань, тестів, форумів та інших навчальних матеріалів; оцінки – викладачі можуть виставляти оцінки за завдання та тести, а також надавати письмові відгуки про оцінювання (рис. 1–2).

Таким чином, практичні заняття відіграють важливу роль в підготовці бакалаврів з кібербезпеки, оскільки дають їм можливість отримати практичні навички, необхідні для успішної роботи у цій сфері. Ці заняття дозволяють здобувачам експериментувати з різними методами та інструментами,

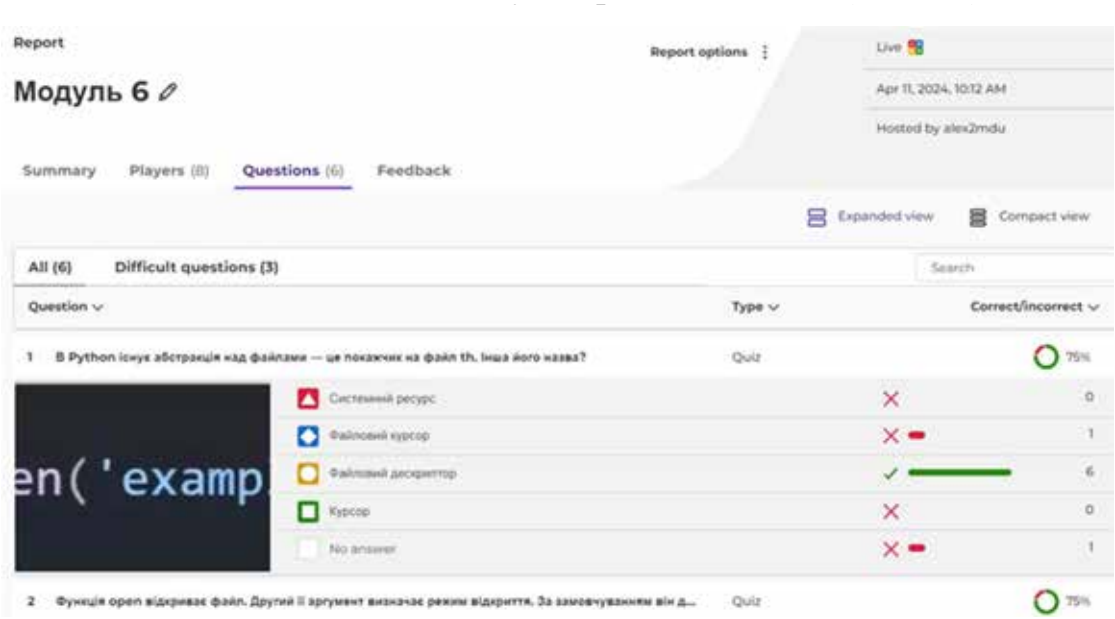

Рис. 1. Організація роботи в Kahoot

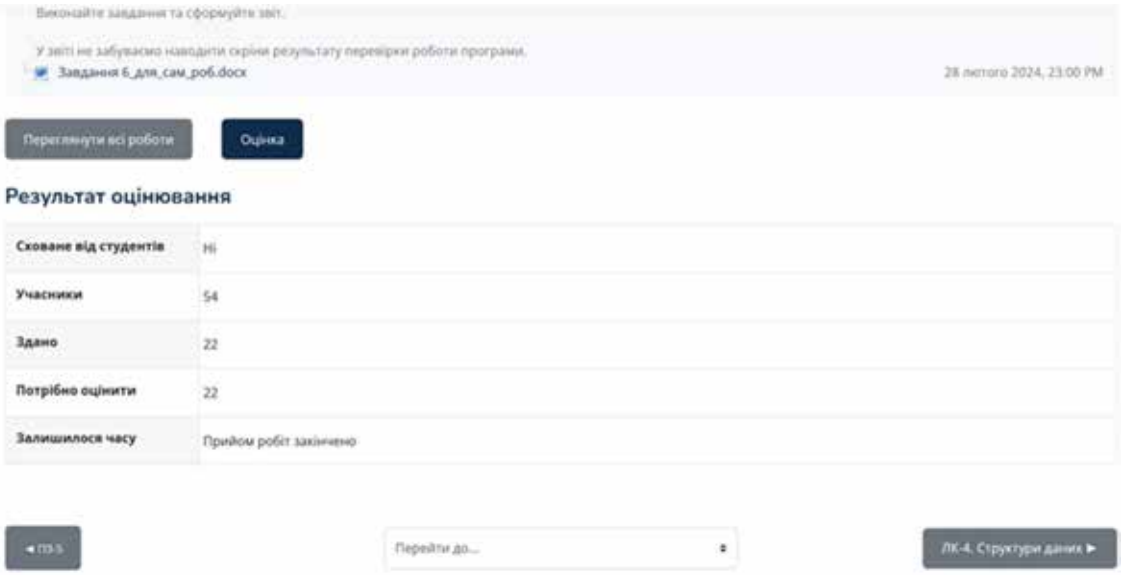

Рис. 2. Виведення результатів оцінювання здобувачів освіти у Moodle

а також отримувати безпосередній досвід роботи з реальними ситуаціями з кібербезпеки.

Висновки та перспективи подальших досліджень. У процесі дослідження автором було встановлені особливості проведення практичних робіт для майбутніх бакалаврів з кібербезпеки, та був виявлений ряд важливих аспектів, що варто врахувати при організації освітнього процесу. По-перше, ефективність навчання у цій галузі суттєво підвищується за умови належного використання сучасних інформаційних технологій та спеціалізованого програмного забезпечення. Зокрема, використання платформи Moodle дозволяє забезпечити доступ до необхідних матеріалів, створення відстеження прогресу та обмін інформацією між викладачами та майбутніми фахівцями. По-друге, практична складова освітнього процесу в кібербезпеці вимагає активної участі здобувачів у вирішенні реальних викликів та проблем, з якими вони зіштовхнуться у майбутній професійній діяльності. Це може включати виконання завдань з аналізу реальних кіберзагроз, створення заходів забезпечення кібербезпеки та вирішення ситуацій кіберінцидентів. *Перспективами подальших досліджень* вбачаємо у проведенні досліджень щодо впливу практичних занять на освітній процес, успішність здобувачів та їх підготовку до практичної роботи в галузі кібербезпеки.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Брайко Б. В. Професійна підготовка магістрів з кібербезпеки в університетах Великої Британії. 2020. № 3. 114–119.

2. Мазур М. П. Особливості розробки віртуальних практичних інтерактивних засобів навчання дисциплін для дистанційного навчання. *Інформаційні технології в освіті*. 2010. № 7. С. 40–46.

3. Самойленко О. Технологія впровадження конструктивної моделі підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища. *Український педагогічний журнал*. 2020. (4), 199–206.

4. Murphy J., Sihler E., Ebben M., Lovewell L., Wilson G. Building a Virtual Cybersecurity Collaborative Learning Laboratory (VCCLL). International Conference on Security and Management (SAM). 2014. P. 1–5.

5. Nahorniak, M. Осягнення професії: методика проведення лабораторних занять із практично орієнтованих курсів за умов дистанційного навчання (на прикладі дисципліни «Радіовиробництво»). Вісник Львівського університету. Серія журналістика. 2018. № 3 (51).

6. Segeč P., Moravčík M., Kontšek M., Papán J., Uramová J., Yeremenko O. Network virtualization tools-analysis and application in higher education. 17th International Conference on Emerging eLearning Technologies and Applications (ICETA) 2019. Starý Smokovec, Slovakia, 21–22 Nov. 2019. P. 699–708. https://doi.org/10.1109/ICETA48886.2019.9040148.