ФОРМУВАННЯ ПРОФЕСІЙНИХ НАВИЧОК СТУДЕНТІВ У ГАЛУЗІ КІБЕРБЕЗПЕКИ: МЕТОДИКА ТА ПІДХОДИ НА ЗАНЯТТЯХ З ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Василь Тищенко,
викладач спецдисциплін ДПТНЗ «Рівненський центр ПТО сервісу та дизайну»

Вступ. Сучасний розвиток інформаційних технологій та швидке поширення цифровізації значно збільшили важливість підготовки висококваліфікованих фахівців у галузі кібербезпеки. Забезпечення захисту інформаційних систем, даних та мереж стало не лише стратегічним завданням для підприємств та державних установ, а й ключовим елементом інформаційної безпеки суспільства.

Одним із важливих аспектів професійної підготовки фахівців з кібербезпеки є формування практичних навичок роботи із програмним забезпеченням, яке використовується для виявлення, аналізу та нейтралізації кіберзагроз. Ефективне викладання цієї дисципліни потребує використання сучасних методик та підходів, що сприяють не лише освоєнню теоретичних знань, але й розвитку професійних компетенцій, необхідних для роботи в реальних умовах [1].

У статті розглядаються ключові методики та педагогічні підходи до формування професійних навичок студентів на заняттях із програмного забезпечення в галузі кібербезпеки. Окрема увага приділяється практичним аспектам, таким як робота з віртуальними лабораторіями, симуляторами атак та реальними кейсами, які дозволяють студентам не лише засвоювати матеріал, але й навчатися адаптуватися до швидко змінюваних умов сучасного кіберсередовища.

Метою дослідження є обґрунтування та аналіз ефективних методик навчання, які сприятимуть підвищенню рівня підготовки студентів та їхньої готовності до викликів професійної діяльності у сфері кібербезпеки.

Основний текст статті. Сфера кібербезпеки є однією з найдинамічніших галузей сучасності. Зростання кількості кіберзагроз, складності атак та обсягів даних, що потребують захисту, висувають високі вимоги до фахівців. У зв’язку з цим, ефективна підготовка кадрів потребує особливої уваги до розвитку практичних навичок роботи із сучасними технологіями та програмним забезпеченням.

Серед ключових викликів можна виділити швидку зміну технологій, необхідність адаптації до нових загроз та інтеграцію новітніх підходів у навчальний процес. Це зумовлює потребу у використанні методик, які забезпечують не лише теоретичне, але й практичне оволодіння знаннями [1].

Віртуальні лабораторії є потужним інструментом у навчанні студентів. Вони дозволяють створювати безпечне середовище для моделювання кіберзагроз, аналізу вразливостей та тестування заходів захисту. Серед

популярних платформ для цього є Cisco Packet Tracer, VMware, VirtualBox та Cyber Range.

Перевага такого підходу полягає у можливості повторного виконання практичних завдань без ризику для реальних систем. Це також сприяє розвитку навичок аналітичного мислення та прийняття рішень у стресових умовах.

Симуляція атак (penetration testing) є одним із найефективніших способів навчання студентів ідентифікації вразливостей та реагування на кіберінциденти. Для цього можуть використовуватися такі інструменти, як Metasploit, Wireshark, Kali Linux. Навчання з використанням симуляцій дозволяє студентам відчути відповідальність за прийняття рішень у реальному часі, що важливо для їхньої майбутньої роботи.

Використання кейс-методу дозволяє студентам зануритися у реальні сценарії, з якими стикаються фахівці з кібербезпеки. Наприклад, аналіз успішних атак на корпоративні мережі або розробка стратегії захисту для малого підприємства. Такий підхід розвиває не лише технічні навички, але й уміння працювати в команді, презентувати результати своєї роботи та шукати оптимальні рішення у складних ситуаціях. Приклади кейсів, які використовуються на заняттях представлена в таблиці 1.

Таблиця 1. Приклади кейсів [3]

№ кейсу	Назва кейсу	Ситуація	Завдання
1	Аналіз DDoS-атаки	Вебсайт компанії недоступний через масовану DDoS-атаку.	Проаналізувати лог-файли, знайти джерела атаки, заблокувати шкідливий трафік, розробити заходи захисту.
2	Виявлення фішингової кампанії	Скомпрометовано обліковий запис через фішинговий лист.	Виявити ознаки фішингу, відновити обліковий запис, створити рекомендації для захисту від фішингових атак.
3	Виявлення шкідливого ПЗ	Комп’ютер користувача заражений шкідливим ПЗ, що спричинило збої в системі.	Проаналізувати систему, видалити шкідливе ПЗ, запровадити політику безпеки.
4	Захист від внутрішніх загроз	Працівник ненавмисно оприлюднив конфіденційні дані через хмарний сервіс.	Проаналізувати інцидент, створити політику безпеки, впровадити моніторинг активності в мережі.
5	Атака типу "ransomware"	Комп’ютери компанії зашифровані шкідливим ПЗ із вимогою викупу.	Знайти джерело зараження, відновити дані з резервних копій, розробити план захисту від подібних атак.
6	Перевірка безпеки вебдодатка	Новий вебдодаток може містити вразливості, що загрожують витоком даних.	Провести тестування, усунути уразливості, розробити план регулярного тестування безпеки.

Реалізація навчальних проектів, пов’язаних із розробкою або впровадженням систем захисту, є ще одним ефективним підходом. Наприклад, створення системи моніторингу мережевого трафіку або налаштування політик безпеки для локальної мережі. Проектний метод сприяє інтеграції теоретичних знань із практичною діяльністю, а також навчає планувати та організовувати свою роботу [2].

На рисунку 1, відобразимо основні педагогічні підходи, які сприятимуть досягненню позитивних результатів у формуванні професійних навичок.

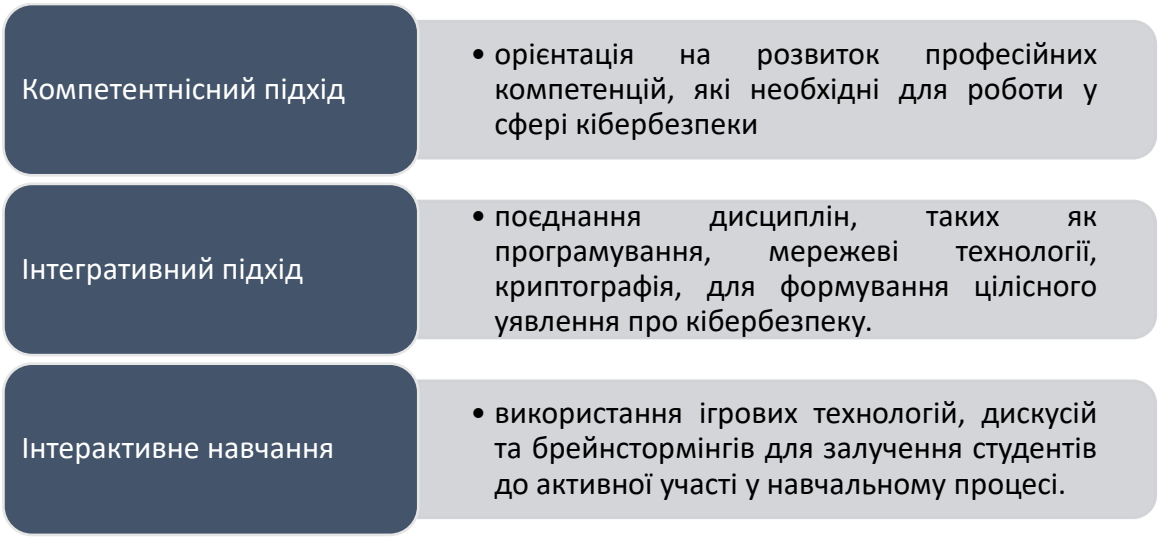

Рисунок 1. Основні педагогічні підходи

Аналіз впровадження описаних методик (рис 1.) у навчальний процес свідчить про їхню ефективність у підготовці фахівців. Студенти демонструють вищий рівень професійної підготовки, здатність швидко адаптуватися до нових викликів та ефективно працювати у команді. Розвиток таких навичок, як критичне мислення, здатність до аналізу та прийняття рішень, є ключовими для майбутніх спеціалістів у сфері кібербезпеки.

Висновок. Формування професійних навичок студентів у галузі кібербезпеки є надзвичайно важливим завданням сучасної освіти, що потребує комплексного підходу до організації навчального процесу. У статті розглянуто основні методики та підходи, які сприяють ефективному розвитку практичних компетенцій майбутніх фахівців. Практичні заняття у віртуальних лабораторіях, симуляція кіберзагроз, аналіз реальних кейсів та виконання проєктних робіт дозволяють забезпечити не лише глибоке засвоєння теоретичних знань, а й формування практичних умінь, які є необхідними для роботи у швидко змінюваних умовах сучасного цифрового світу.

Запровадження компетентнісного, інтегративного та інтерактивного підходів у навчання сприяє всебічному розвитку студентів, зокрема таких важливих навичок, як критичне мислення, командна робота, аналітичні здібності та прийняття рішень у стресових ситуаціях. Результати впровадження сучасних методик у підготовку фахівців з кібербезпеки

підтверджують їхню ефективність та практичну значущість. Це дозволяє випускникам бути конкурентоспроможними на ринку праці та готовими до викликів професійної діяльності.

Таким чином, подальший розвиток і вдосконалення методик навчання, орієнтованих на практику, є запорукою якісної підготовки фахівців у галузі кібербезпеки, здатних ефективно вирішувати актуальні завдання сучасності.

Список використаної літератури

1.Матвійчук-Юдіна, О. В. (2020). Формування професійної компетентності майбутніх учителів інформатики в процесі навчання інформаційних технологій [Електронний ресурс]**.** Дис. … д-ра пед. наук: 13.00.04. Інститут інформаційних технологій і засобів навчання НАПН України. Київ. URL: https://lib.iitta.gov.ua/id/eprint/711080/1/dis_Матвійчук-Юдіна.pdf (дата звернення: 09.12.2024).

2. Бистрова, Б. (2017), “Основні поняття досягнення та концептуальні засади професійної підготовки фахівців із кібербеспеки”, Педагогічні науки: теорія, історія, інноваційні технології, vol. 8. pp. 58–70.

3. Засоби та системи технічного захисту інформації: навч. посіб. для студентів спеціальності 125 "Кібербезпека" спеціалізації "Системи технічного захисту інформації" / І. Є. Антіпов, А. М. Олейніков, Ю. В. Ликов и др. ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків : ХНУРЕ, 2019. – 216 с.