УДК 004.056.(55+53)

https://doi.org/10.52058/2786-6300-2025-12(42)-1734-1743

Кіндрат Павло Вадимович кандидат юридичних наук, доцент кафедри цифрових технологій та методики навчання інформатики Рівненського державного гуманітарного університету, м. Рівне, https://orcid.org/0000-0003-0351-3349

Антонюк Микола Степанович кандидат педагогічних наук, доцент кафедри цифрових технологій та методики навчання інформатики Рівненського державного гуманітарного університету, м. Рівне, https://orcid.org/0000-0002-6888-6392

Антонюк Антон Миколайович магістрант спеціальності 015 Професійна освіта (Цифрові технології) Рівненського державного гуманітарного університету, м. Рівне

ВИКОРСИТАННЯ ВІРТУАЛЬНИХ СЕРЕДОВИЩ ДЛЯ ПРАКТИЧНОЇ ПЕРЕВІРКИ ЗНАНЬ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. У статті розглянуто актуальну проблему застосування систем автоматизації перевірки завдань з інформаційної безпеки яка набуває статусу критично важливої складової успішного розвитку суспільства. Розкрито роль закладів вищої освіти які є визначальною при формуванні фундаментальних знань та професійних компетентностей у сфері кібербезпеки. Акцентовано увагу на оновлення освітніх програм, впровадження практикоорієнтованих методів навчання, використання сучасних технологій симуляції кібератак, систем моніторингу та аналітики.

Зауважено, що підвищення вимог до випускників висуває фундаментальний виклик перед освітніх закладів: здійснення об’єктивної оцінки комплексних, практико-орієнтованих навичок. Додатково проаналізовано предметну область, доведено невідповідність традиційних методів контролю знань потребам ринку та обґрунтовано необхідність застосування кіберполігонів – ізольованих, реалістичних, віртуальних тренувальних середовищ, як єдиного легального способу формування практичних навичок. Визначено, що існуючі системи управління навчанням створюють технологічний бар’єр через примітивність перевірки, а спеціалізовані платформи не надають деталізованої, педагогічно ефективної оцінки методології роботи студента.

Обґрунтовано вибір методів викладання що потребують реалізації в системі навчання та контролю. Ключовим елементом визначено інтеграцію зі

штучним інтелектом для виконання якісного аналізу методології виконання завдань.

Спроєктовано архітектуру програмного забезпечення на основі трирівневої клієнт-серверної моделі. Розроблено систему яка забезпечує систематичне та об'єктивне оцінювання, надаючи викладачам інструмент для ефективного управління навчальним процесом та підготовки висококваліфікованих фахівців з кібербезпеки..

Ключові слова: кібербезпека, оцінювання знань, автоматизація перевірки, кіберполігон, цифровізація освіти.

Kindrat Pavlo Vadymovych candidate of law science, associate professor of the department of digital technologies and methods of teaching informatics, Rivne state university of the humanities, Rivne, https://orcid.org/0000-0003-0351-3349

Antoniuk Mykola Stepanovych candidate of pedagogical science, associate professor of the department of digital technologies and methods of teaching informatics, Rivne state university of the humanities, Rivne, https://orcid.org/0000-0002-6888-6392

Antoniuk Anton Mykolaiovych master's student of the specialty 015 Professional education (Digital technologies), Rivne state university of the humanities, Rivne

USE OF VIRTUAL ENVIRONMENTS FOR PRACTICAL ASSESSMENT OF KNOWLEDGE IN INFORMATION SECURITY

Abstract. The article addresses the current issue of applying automated systems for assessing information security tasks, which is becoming a critically important component of successful societal development. The role of higher education institutions is highlighted such as: key actors in forming fundamental knowledge and professional competencies in the field of cybersecurity. Emphasis is placed on updating educational programs, implementing practice-oriented teaching methods, and using modern technologies for cyber-attack simulation, monitoring, and analytics.

It is noted that increasing requirements for graduates pose a fundamental challenge for educational institutions: ensuring objective evaluation of complex, practice-oriented skills. Additionally, the subject area is analyzed, demonstrating the inconsistency between traditional knowledge-assessment methods and current market needs, and substantiating the necessity of applying cyber ranges – isolated, realistic, virtual training environments. Which are the only legal meaning of developing practical skills. It is determined that existing learning management systems create a

technological barrier due to primitive assessment mechanisms, while specialized platforms fail to provide detailed, pedagogically effective evaluation of students' working methodologies.

The choice of teaching methods that must be implemented in the learning and assessment system is substantiated. The integration of artificial intelligence for high-quality analysis of task-solving methodologies is identified as a key element.

The architecture of the software system is designed based on a three-tier client-server model. A system has been developed that ensures systematic and objective assessment, providing instructors with a tool for effective management of the educational process and the training of highly qualified cybersecurity specialists.

Keywords: cybersecurity, knowledge assessment, automated checking, cyber range, digitalization of education.

Постановка проблеми. Розвиток інформаційних технологій та їх все глибше проникнення у повсякденне життя супроводжується постійним зростанням кількості кіберінцедентів як технічного так і антропогенного характеру. Це призводить до зростання ролі спеціалістів з кібербезпеки у забезпеченні коректного та безперервного функціонування інформаційних систем які слугують підґрунтям для функціонування не лише для підприємств чи організацій, а й суспільства в цілому. А це, в свою чергу, стимулює зростання попиту на спеціалістів у сфері інформаційної безпеки. На сьогодні в Україні підготовка спеціалістів за даним профілем відповідає спеціальності F5 «Кібербезпека та захист інформації». Ключовою специфікою вивчення зазначеної спеціальності у закладах освіти є акцентування на розвитку практичних навичок адміністрування, моніторингу та технічної підтримки інформаційних систем.

Ключовим завданням на шляху виховання якісного спеціаліста залишається необхідність належної верифікації досягнення студентом цільових компетентностей по своїй спеціальності. Це породжує потребу у забезпеченні належної перевірки рівня засвоєння отриманих знань та оцінюванні якості виконання завдань які притаманні для інформаційної безпеки.

Традиційні методи навчання та контролю знань (усні відповіді, тестові перевірки) у закладах освіти не можуть повноцінно оцінити здатність студента до комплексних дій у реальних, стресових умовах кіберзагрози. Сучасний фахівець повинен мати практичні навички у таких сферах, як безпека застосунків, аудит вихідного коду, DevSecOps, тестування на проникнення та управління доступом. Фахівець має вміти здійснювати оцінювання можливості несанкціонованого доступу та вирішувати задачі управління процесами відновлення штатного функціонування систем [1]. А це потребує створення та впровадження відповідних програмних комплексів.

Аналіз останніх досліджень і публікацій.

Дослідження існуючих систем управління навчанням (LMS) засвідчують, що за своєю природою вони є технологічно-агностичними до завдань з інформа-

ційної безпеки (ІБ). Їхній функціонал не прив'язаний до специфічних вимог практичної ІБ-освіти, тому вони створюють технологічний бар'єр для об'єктивного оцінювання комплексних практичних навичок.

Їхні обмеження полягають у тому що:

1) LMS не можуть створювати ізольовані віртуальні мережі, які імітують корпоративну інфраструктуру, що є необхідним для практичного відпрацювання Pentest, Blue Teaming або реагування на інциденти.

2) у загальнодоступних LMS автоматизована перевірка обмежується лише бінарним результатом (правильно/неправильно) або відповіддю типу «прапор» (Flag).

Існуючі LMS, такі як Moodle, є необхідними для адміністративного управління курсами, але вони створюють технологічний бар'єр для об'єктивного оцінювання комплексних практичних навичок з кібербезпеки [2]. Це унеможливлює повноцінне впровадження принципу контролю та корекції знань, оскільки викладач не отримує якісної інформації про методологію роботи студента.

Мета статті полягає в обґрунтуванні системи автоматизованої перевірки якості виконання практичних завдань з інформаційної безпеки для застосування в освітньому процесі закладів вищої освіти.

Виклад основного матеріалу. Проблема традиційного оцінювання полягає у його статичності та відірваності від контексту. Тести перевіряють знання фактів, а не здатність до застосування цих знань у агресивній мережі. У реальному світі кібератаки ніколи не обмежуються одним питанням із чотирма варіантами відповіді; вони є ланцюгом послідовних дій (Kill Chain), що вимагають креативного мислення та не шаблонних рішень [3].

Отже, компетентність фахівця з кібербезпеки не може бути адекватно виміряна без:

1) стресового фактора: здатність працювати під тиском часу, коли критична інфраструктура перебуває під загрозою.

2) комплексності системи: взаємодія з багатокомпонентними мережами, які імітують корпоративну чи промислову інфраструктуру, а не лише ізольовані віртуальні машини.

3) етичної безпеки: потреба відпрацьовувати методи експлуатації вразливостей, які є незаконними на живих мережах.

Оцінити здатність до виконання «пентестів» або до застосування теорій захисту в умовах реалізації загроз різних класів можливо лише у спеціалізованих симуляційних середовищах. Оскільки освітні заклади, як публічні заклади, не можуть використовувати власні робочі мережі для відпрацювання атак та експлуатації вразливостей, виникає абсолютна необхідність застосування Кіберполігонів (Cyber Ranges) – ізольованих, реалістичних, віртуальних тренувальних

середовищ [4]. Кіберполігони є єдиним легальним та безпечним способом сформувати та оцінити ці практичні навички.

Для забезпечення ефективності та об'єктивності такого практико-орієнтованого навчання викладачам необхідні зручні та ефективні механізми перевірки. Контроль має бути максимально індивідуалізованим та систематичним, з чіткими та зрозумілими критеріями оцінювання. Чим досконалішим та об'єктивнішим є контроль, тим успішніше буде здійснюватися управління навчальним процесом, та в цілому позитивно впливатиме на ефективність навчання. Це вимагає від викладачів використання нових форм і методів практичної перевірки знань, зокрема ситуаційних вправ та ділових ігор, які дозволяють оцінювати готовність до застосування знань у критичних ситуаціях.

У контексті стратегічної необхідності системної та якісної підготовки кібербезпекових кадрів, виникає назріла потреба в автоматизації процесів оцінювання. Автоматизація перевірки якості завдань з інформаційної безпеки перетворюється з бажаного інструменту на критично важливий елемент сучасної освітньої інфраструктури.

В результаті можна винести кілька ключових проблем:

1) масштабованість та систематичність: забезпечення можливості одночасної перевірки практичних навичок великої кількості студентів та інтеграції практичних занять у модульну структуру курсую.

2) педагогічна ефективність: надання студентам миттєвого та конструктивного зворотного зв'язку про процес виконання завдання, а не лише про кінцевий результат.

Зважаючи на вимоги спеціальності та специфіку роботи закладів освіти, під час навчання часто застосовуються специфічні методи викладання, які покликані підвищити зацікавленість студентів до навчання із застосуванням обмежених ресурсів. До них відносяться:

1. віртуалізація навчального середовища – полягає у широкому використанні віртуальних машин для безпечного проведення лабораторних робіт та практичних занять по взаємодії зі шкідливим програмним забезпеченням та протидії атакам без ризику для основної мережі навчального закладу.

2. гейміфікація навчання – полягає у залученні студентів до змагань у форматі Capture The Flag на початковому рівні, що суттєво підвищує мотивацію та розуміння принципів функціонування інформаційних систем та необхідності дотримання вимог щодо їх захисту.

3. проектна робота – полягає у залучені студентів до проектування захищених мереж та систем під час виконання курсових та дипломних робіт. Це дозволяє залучати студентів до розвитку навчальної та мережевої інфраструктури навчального закладу шляхом подальшої інтеграції в неї найкращих проектів.

4. етично-правовове виховання студентів – воно полягає у необхідності формування чіткого морально-етичного кодексу поведінки, розумінні різниці

між правомірним і неправомірним використанням отриманих знань, усвідомлені професійної відповідальності.

Не варто забувати, що система перевірки знань має базуватися на принципі «навчання через дію». Тож контроль не повинен бути відокремленим від навчального середовища. Він має поєднувати автоматизовані тести та практичних кейсів виконання яких відбувається у віртуальному середовищі.

Будь-яка перевірка практичних навичок має відбуватись виключно в ізольованому віртуальному середовищі, щоб не зашкодити реальному мережевому середовищі навчального закладу. Самі завдання мають моделювати типові робочі ситуації.

Для забезпечення об'єктивності та повноти перевірки знань доцільно використовувати трирівневу архітектуру системи оцінювання:

- модуль теоретичного контролю – для нього можуть бути використані існуючі платформи оцінювання знань чи супроводу навчального середовища (Moodle, Google Classroom, Canvas тощо) з різнотиповими питаннями. В цьому модулі не варто обмежуватись виключно питаннями типу «одна вірна відповідь». Водночас не забуваючи про градієнт складності питань і вагу кожного питання;
- модуль практичного тренінгу – для нього можуть бути використані як віртуальні машини так і власні розробки для автоматизованої перевірки якості виконання практичних завдань. Останні можуть застосовувати скрипти для перевірки налаштовуваної конфігурації системи цільовим показникам;
- змагальний модуль – для нього може застосовуватись концепція CTF (Capture The Flag). Цей модуль можна застосовувати для проведення підсумкового контролю або атестації, адже він дозволяє найкраще оцінити нешаблонне мислення, стресостійкість та відповідність ключовим компетентностям спеціальності.

В якості форми подачі матеріалу для перевірки та оцінювання доцільно використовувати звіти, які за структурою відповідають звітам про інциденти та їх вирішення. Для забезпечення достовірності в звіт має бути включена вимога доказовості, яка може буде реалізована як шляхом прикріплення відповідного скріншоту з часовою міткою, так і шляхом додаванням скрипта який використовувався для вирішення завдання.

Сама ж система перевірки має включати різного роду запобіжники. До таких можуть бути віднесені: унікальні завдання (кожен студент отримує свій варіант IP-адресації або унікальний «ключ» (прапор), який генерується динамічно), захист звіту (скріншоти мають містити унікальні ідентифікатори).

Система автоматизованої перевірки також має включати в себе підсистему зворотнього зв'язку. Вона повинна видавати коментар при помилці який описуватиме суть помилки. Це потрібно щоб контроль також виконував навчальну функцію.

Програмне забезпечення системи автоматизованої перевірки якості виконання завдань з інформаційної безпеки доцільно реалізувати на основі трирівневої (триланкової) клієнт-серверної архітектури, що дозволяє досягти високої масштабованості, надійності та незалежності компонентів. Ця архітектура чітко розділяє логіку представлення, логіку застосунку та логіку даних і зовнішніх сервісів, що є найкращою практикою для розподілених систем, які використовують хмарні обчислення та штучний інтелект.

Перший рівень, рівень клієнта, відповідає за безпосередню взаємодію з користувачем, забезпечуючи інтуїтивно зрозумілий інтерфейс для Студентів та Викладачів. Цей рівень побудований на технологіях HTML та CSS, з використанням фреймворку Bootstrap для забезпечення повної адаптивності та професійного вигляду на всіх пристроях. Клієнт відповідає за відображення навчальних матеріалів, форм для подачі результатів роботи з Кіберполігону, а також за структурну візуалізацію деталізованих звітів, згенерованих ШІ, підкреслюючи критичні оцінки та рекомендації.

Другий рівень, рівень сервера застосунку, є центральним хабом, що реалізує основну бізнес-логіку системи та координує роботу всіх зовнішніх сервісів. Він реалізований як мікросервіс на основі Python та фреймворку Flask. Сервер містить Менеджер завдань, який обробляє запити від клієнта та ініціює процеси оцінювання. Ключовими тут є два модулі: Модуль Інфраструктурного Керування, який взаємодіє з Terraform для ініціації розгортання та знищення ізольованих інстансів Кіберполігону на хмарній платформі AWS, і Модуль ШІ-аналізу, який використовує бібліотеку gemini. Цей модуль формує структурований запит на основі наданих Студентом логів чи результатів, надсилає його до API ШІ, отримує якісну оцінку методології та обробляє її для подальшого зберігання.

Третій рівень, рівень даних та зовнішніх сервісів, включає всі постійні сховища та високоспеціалізовані сервіси. Тут розташована база даних, яка для гнучкості та простоти розгортання може бути реалізована на SQLite3, зберігаючи інформацію про користувачів, курси та деталізовані результати оцінювання. Фізично інфраструктура розгортається на AWS, яка надає обчислювальні потужності (EC2) для роботи самого сервера та Кіберполігону. Управління життєвим циклом цих ресурсів здійснюється за допомогою Terraform, а ізольовані, відтворювані цільові машини створюються за допомогою Docker. Нарешті, Зовнішній ШІ-провайдер (Gemini) є ключовим сервісом на цьому рівні, надаючи моделі машинного навчання для виконання якісного аналізу методології виконання завдань, що є основною цінністю продукту. Ця чітка архітектура забезпечує гнучке, незалежне та масштабоване функціонування всієї системи.

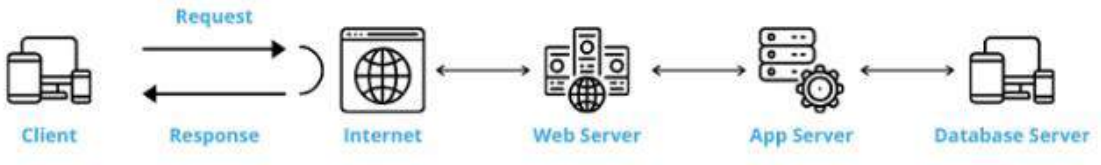

Рис. 1. Ілюстрація клієнт-серверної архітектури

Функціональні вимоги до системи визначають, що саме вона повинна виконувати для задоволення потреб користувачів у контексті управління навчанням та оцінювання:

1) управління доступом та ролями: Система має забезпечувати надійну автентифікацію та авторизацію користувачів, чітко розмежовуючи права доступу для ролей «Студент» та «Викладач».

2) управління навчальним контентом: викладач повинен мати функціонал для створення, редагування та публікації практичних завдань з кібербезпеки, включаючи встановлення термінів здачі та критеріїв оцінювання.

3) розгортання інфраструктури кіберполігону: система повинна інтегруватися з Terraform та AWS для автоматичного та швидкого розгортання персоналізованого, повністю ізольованого інстансу тренувального середовища для кожного студента за єдиним шаблоном.

4) надсилання результатів: система повинна надавати студенту зручні механізми для надсилання результатів виконання завдання, які можуть включати логі роботи, скрипти чи знайдені ідентифікатори («прапори»/Flags).

5) автоматизована ШІ-перевірка якості: система повинна використовувати бібліотеку gemini для програмного надсилання даних роботи студента до моделі штучного інтелекту з метою деталізованої оцінки методології виконання завдання.

Для гнучкого оцінювання доцільно застосовувати систему штрафів та винагород, які можуть визначати кінцеву оцінку та диференціювати рівень оволодіння матеріалом навіть серед студентів які показали однаковий кінцевий результат. Для цього, за необхідності, встановлюються ліміти на кількість спроб та час виконання, що дозволяє запобігти використанню прямого перебору можливих комбінацій для досягнення потрібного результату. Також варто застосовувати динамічне оцінювання на результат якого можуть впливати: швидкість виконання, кількість спроб, частка коректно виконаних етапів завдання тощо.

При підготовці завдань та налаштуванні системи автоматичної перевірки виконаних завдань викладачеві слід уважно поставитись до налаштування системи зворотного зв’язку яка не має бути бінарною («завдання виконано», або «завдання не виконано»), а містити більш розлогий коментар. Попри те що в

розробленій системі ця функція покладається на ШІ, все ж щоразу перед публікацією завдань доцільно переконатись, щодо коректності відповіді на основні помилки які можуть допустити студенти.

Висновки. Впровадження розробленої системи автоматизованої перевірки завдань з інформаційної безпеки змінює сприйняття процесу виконання лабораторних та практичних робіт. Воно накладає на викладача системно іншого підходу до формування завдань: більш ретельно пропрацьованого та структурно орієнтованого. Як наслідок вона надає змогу перевіряти не те, що студент запам’ятав, а те, чи зрозумів він завдання, чи зміг належно налаштувати конфігурацію обладнання, чи коректно написати скрипт.

Самі завдання, які можна реалізовувати в системі, поділяються на:

1. налаштування конфігурації – вони полягають у перевірці коректності налаштування параметрів операційної системи та окремих програмних за стосунків. Для перевірки коректності виконання передбачається використання скриптів;

2. пентест – результатом є знаходження відповідних «прапорців» під час вдало організованої «атаки»;

3. скриптування – написання програмних модулів для автоматизації процесів інформаційної безпеки. Для перевірки можна скористатись відповідними unit-тестами.

Важливо пам’ятати, що попри автоматизацію процесу перевірки та оцінювання якості виконання завдань з інформаційної безпеки, остаточне рішення про зарахування результату перевірки приймає викладач. Система ж має на меті лише спростити процес оцінювання та надати викладачу зручний інструмент для збору даних про результати перевірки комплексних та об’ємних рішень.

Література:

1. Puchkov O. Sustainable development of the system of formal cyber education: reflection of modern concepts. / O. Puchkov, O. Uvarkina // Collection "Information Technology and Security". – 2023. №11(1), p.60–68. https://doi.org/10.20535/2411-1031.2023.11.1.283635

2. Поліщук Н. В. Підвищення якості вищої освіти за допомогою цифрових технологій та дистанційного навчання для здобувачів вищої освіти в Україні. / Н.В. Поліщук, Т.І. Бугаєнко, Н.В. Лемешева // Академічні візії. – 2024, № 38, С. 1–7. https://doi.org/10.5281/zenodo.14537287

3. Сус В. Аналіз моделі прогнозування кіберзагроз «Cyber Kill Chain». / В. Сус // Modeling, control & information technologies. – 2024. № 1(63). https://doi.org/10.31713/MCIT.2024.063

4. Василенко В. Роль змагань Capture-The-Flag (CTF) у дослідженнях та навчанні з кібербезпеки: Аналіз машини «Editorial». / В. Василенко, Г. Грицкевич, І. Кузнецов // Кібербезпека: освіта, наука, техніка. – 2025. № 4(28), С. 75–84. https://doi.org/10.28925/2663-4023.2025.28.762

References:

1. Puchkov O., & Uvarkina O. (2023). Sustainable development of the system of formal cyber education: reflection of modern concepts. *Collection "Information Technology and Security", 11(1),* 60–68.

2. Polishchuk N., Bugajenko T., & Lemesheva N. (2024). Pidvyshchenja jakosti vyshchoji osvity za dopomogoju cyfrovyh tehnologij ta dystancijnogo navchanja dla zdobuvachiv vyschchoji osvity v Ukraini. [Improving the quality of higher education through digital technologies and distance learning for higher education students in Ukraine]. *Akademichni viziji, 38*, 1–7. [in Ukrainian]

3. Sus V. (2024). Analiz modeli prognozuvanja kiberzagroz «Cyber Kill Chain». [Cyber threat prediction model «Cyber Kill Chain» analysis] *Modeling, control & information technologies*, 63 *(1)*. Retrieved from: https://doi.org/10.31713/MCIT.2024.063 [in Ukrainian]

4. Vasylenko V., Gryckevych G., & Kuznecov I. (2025). Rol zmagan Capture-The-Flag (CTF) u dislidgenah ta navchani kiberbezpeky: analiz mashyny «Editorial». [The role of Capture-The-Flag (CTF) challenges in cybersecurity research and training: analysis of the «editorial» machine] Kiberbezpeka: osvita, nauka, tehnika, *4(28)*, 75–84.