

2. Scratch – Imagine, Program, Share. Retrieved from: <https://scratch.mit.edu/>
(дата звернення: 30.04.2025)
3. W3Schools Online Web Tutorials. Retrieved from:
<https://www.w3schools.com/> (Accessed: 20.04.2025)
4. Sololearn: Learn to Code. Retrieved from: <https://www.sololearn.com/>
(Accessed: 22.04.2025)
5. Coursera. Online Courses from Top Institutions. Retrieved from:
<https://www.coursera.org/> (Accessed: 17.04.2025)
6. Prometheus. Retrieved from: <https://prometheus.org.ua/> (Accessed: 03.05.2025)

ВІРТУАЛІЗАЦІЯ НАВЧАЛЬНОГО СЕРЕДОВИЩА ДЛЯ НАВЧАННЯ КІБЕРБЕЗПЕЦІ

Павло КІНДРАТ,

***кандидат юридичних наук, доцент, доцент кафедри цифрових технологій
та методики навчання інформатики***

Рівненський державний гуманітарний університет

Анотація: Розглянуто особливості застосування віртуальних лабораторій для навчання кібербезпеці. Розкрито спрямованість різних типів застосування віртуальних лабораторій для побудови всебічного охоплення віртуального навчального середовища.

Ключові слова: кібербезпека, віртуальна лабораторія, хмарний сервіс.

Pavlo KINDRAT. Virtual Learning Environments for Cybersecurity Education

Abstract: The features of using virtual laboratories for cybersecurity education are examined. The focus of various types of virtual lab applications is revealed, aiming to build a comprehensive virtual learning environment.

Key words: cybersecurity, virtual laboratory, cloud service.

Розвиток інформаційних технологій потребує систематичного удосконалення та актуалізації навчального процесу. Це дозволить підвищити компетентність здобувачів освіти та має бути орієнтоване на отримання ними якісного практичного досвіду який демонструватиме можливості та значимість теоретичних знань. Одним з напрямків досягнення такої мети є інтеграція в освітні середовища віртуальних лабораторій які дозволяють здійснювати моделювання прикладних систем для подальшої роботи з ними без необхідності змінювати інфраструктуру навчального закладу.

Розробка та впровадження в навчальний процес віртуальних лабораторій особливо актуальне для вивчення питань пов'язаних з кібербезпекою. Складність інформаційних систем та їх всебічна інтеграція в повсякденне життя кожної людини актуалізує потребу в наявності принаймні базового рівня розуміння засад їх захисту від шкідливого впливу.

Можливість моделювати системи різної складності та наповненості по відношенню до яких реалізовувати різні види загроз є важливою особливістю використання віртуальних лабораторій. Адже вони «дозволяють моделювати поведінку об'єктів реального світу у віртуальному комп'ютерному освітньому середовищі та допомагати тим, хто навчається, оволодівати новими знаннями та вміннями» (Палагін & Петренко, 2017)

Використання віртуальних лабораторій при вивченні питань кібербезпеки також дозволяє вирішити проблему забезпечення безпеки навчального середовища. Вони функціонують в ізолюваному середовищі віртуальної машини і обмежені у взаємодії з іншими компонентами інформаційної системи на якій вони розгорнуті. Тож робота недосвідченого користувача в «пісочниці» дозволяє йому відточити свої навички в протидії кіберзагрозам не турбуючись про можливі наслідки що можуть виникнути в наслідок некомпетентних дій.

Серед переваг застосування віртуальних лабораторій виділяють:

- формування фахових компетенцій, які можуть бути безпосередньо перенесені в реальність;

- підвищення якості самостійної навчально-пізнавальної діяльності;
- зацікавленість у вивченні дисципліни, розвиток мотиваційної діяльності;
- доступність;
- автоматизація операцій;
- постійне удосконалення програмних систем та технологій тощо.

(Бурячок, Шевченко & Складаний, 2018)

З огляду на особливості сфери кібербезпеки можна виділити три ключові напрямки застосування віртуальних лабораторій:

- вразливі лабораторії у хмарних програмах (Vulnerable Cloud Web Service Environment);
- лабораторії віртуальних комп'ютерних мереж (Virtual Networking Laboratories);
- віртуальні лабораторії локальних систем (Virtual Local System).

Віртуальні лабораторії локальних систем здебільшого розгортаються на безпосередньо користувацьких комп'ютерах через засоби віртуалізації. Їх основне призначення – дослідження налаштувань операційних систем та прикладного програмного забезпечення, а також засобів їх захисту з метою тестування ефективності протидії шкідливому програмному забезпеченню без загрози пошкодження основної системи. Для цього можна скористатись програмами-емуляторами: VirtualBox, VMware тощо.

Лабораторії віртуальних комп'ютерних мереж призначенні для відточування навичок налаштування комп'ютерних мереж, аналізу вразливостей застосованих рішень та відпрацювання засобів захисту від як зовнішніх так і внутрішніх загроз. Зважаючи на складність та ресурсоемність реалізації такого типу лабораторій їх доцільно розгортати на відповідних хмарних сервісах. Найтиповішим середовищем для цього є AWS (Amazon Web Services).

Вразливі лабораторії розгорнуті в хмарних середовищах AWS, Azure або Google Cloud – це потужний інструмент для навчання та тестування в галузі

кібербезпеки. Вони надають можливість на практиці вивчати реальні системні інфраструктури, моделювати атаки, виявляти вразливості та відпрацьовувати методи захисту в безпечному та контрольованому середовищі. Їх можна застосовувати як для навчання початківців так і профільних спеціалістів в галузі кібербезпеки.

На сьогодні існує велика кількість готових для розгортання рішень для будь-якого напрямку віртуальних лабораторій з кібербезпеки які розповсюджуються як безкоштовно так і на платній основі. Це дозволяє підібрати такий набір компонентів що відповідатиме цілям навчальної програми та сприятиме більшій віртуалізації навчального процесу забезпечуючи при цьому високу якість підготовки.

Список використаних джерел

1. Бурячок В.Л., Шевченко С.М., & Складаний П.М. (2018) Віртуальна лабораторія для моделювання процесів в інформаційній та кібербезпеці як засіб формування практичних навичок студентів. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2(2), 98–104. <https://doi.org/10.28925/2663-4023.2018.2.98104>
2. О.В.Палагін, & М.Г.Петренко (2017) Тлумачний онтографічний словник з інженерії знань. Київ:ТОВ «НВП Інтерсервіс».

References

1. Buriachok, V. L., Shevchenko, S. M., & Skladannyi, P. M. (2018). Virtual laboratory for modeling processes in information and cybersecurity as a tool for developing students' practical skills. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technology»*, 2(2), 98–104. <https://doi.org/10.28925/2663-4023.2018.2.98104>
2. Palahin, O. V., & Petrenko, M. H. (2017). *Explanatory ontographic dictionary of knowledge engineering*. Kyiv: NVP Intersystem LLC.