

10. Salama, M.A., Ezz, M., Mohamed, S.A., et al. (2023). "A Federated Learning-Based Framework for Intrusion Detection in IoT Networks." *IEEE Internet of Things Journal*, Early Access.

ІНТЕГРАЦІЯ КІБЕРПОЛІГОНІВ В ОСВІТНІЙ ПРОЦЕС / INTEGRATION OF CYBER RANGES INTO THE EDUCATIONAL PROCESS

А.М. Глибовець, Т.А. Бабич / Hlybovets A.M., Babych T.A.

Національний університет Києво-Могилянська Академія

04655, м. Київ, вулиця Григорія Сковороди, 2, НаУКМА, Факультет інформатики, Кафедра інформатики / National University of Kyiv-Mohyla Academy

04655, Kyiv, Skovoroda Street, 2, NaUKMA, Faculty of Informatics, Department of Informatics

Контактні телефони: +38 093 793 94 54

E-mail: t.babich@ukma.edu.ua

The article highlights the theoretical foundations of cyber ranges, including an overview of the main technologies and techniques used to create virtualized cyber environments. Examples of the introduction of cyber ranges into the curriculum of higher education institutions, their impact on student motivation, as well as teaching and assessment methods using these complexes are considered. Further, the article focuses on the practical aspects of using cyber polygons in the educational process on the development and adaptation of cyber polygons for educational purposes. The article also discusses safety and ethical issues related to the use of cyber training grounds in education, as well as legal aspects of their use. Particular attention is given to the analysis of case studies of successful use of cyber training grounds, which demonstrate a significant increase in the level of student training. Сучасний світ стає дедалі більш цифровим, що спричиняє зростання потреби в захисті кіберпростору. З кожним роком кількість кібератак зростає, що підкреслює необхідність підготовки кваліфікованих фахівців у галузі кібербезпеки. Злочинці стають дедалі винахідливішими у своїх методах, а тому методи захисту мають еволюціонувати ще швидше. Враховуючи це, розуміння та застосування передових практик і технологій в галузі кібербезпеки є критично важливим для захисту особистих, корпоративних та державних інтересів. Кіберполігон — це спеціалізоване віртуалізоване середовище, призначене для моделювання кібернетичних загроз та атак, що дозволяє користувачам в безпечний спосіб відпрацьовувати реакції на них. Це середовище імітує реальну IT-інфраструктуру з усіма її компонентами, включаючи мережі, сервери та застосунки, дозволяючи таким чином відтворювати атаки і тестувати оборонні механізми без ризику для реальних систем. В освіті кіберполігони використовуються для підготовки студентів, забезпечуючи їм можливість здобути практичний досвід у виявленні, аналізі та відповіді на кіберзагрози. Особливо важливою є роль кіберполігонів у формуванні навичок роботи в команді та розвитку стратегічного мислення, що є критично важливими компетенціями для майбутніх фахівців кібербезпеки. Інтеграція кіберполігонів у освітній процес вищих навчальних закладів може забезпечити значний прогрес у підготовці фахівців у галузі кібербезпеки [13]. Кіберполігони дозволяють студентам здобувати практичний досвід в ідентифікації, аналізі та відповіді на кіберзагрози в контрольованому і безпечному середовищі. Це допомагає не лише у формуванні технічних навичок, але й розвиває критичне мислення, необхідне для ефективного реагування на інциденти в реальному світі. Збільшення кількості кіберзагроз, їхнє постійне ускладнення та висока динаміка розвитку кібератак вимагають від освітніх закладів включення інноваційних підходів до навчання. Інтеграція кіберполігонів у освітні процеси є актуальною, оскільки вона дозволяє забезпечити студентам доступ до практичного досвіду [8], що є незамінним в підготовці кваліфікованих фахівців. Практика на кіберполігоні допомагає студентам краще зрозуміти реальні кіберзагрози, відточити свої навички реагування на інциденти та розвинути здатність адаптуватися до мінливого кіберландшафту. Це також створює умови для реалізації прикладного навчання, забезпечуючи студентам розуміння теоретичних знань у практичних реальних ситуаціях [12]. Кіберполігони використовують низку технологій і методологій для створення реалістичних умов, що дозволяють користувачам відпрацьовувати відповіді на кіберзагрози [10].

Віртуалізація та імітація є ключовими компонентами кіберполігонів, що забезпечують численні переваги. Віртуалізація дозволяє швидко змінювати налаштування і масштабувати середовище в залежності від потреб навчання, без необхідності фізичної присутності обладнання. Імітація реальних кібератак в ізолюваному середовищі знижує ризики для реальних мереж і систем [6]. Використання віртуалізованих середовищ зменшує потребу в дорогому обладнанні і знижує витрати на технічне обслуговування. Імітація дозволяє створювати умови, максимально наближені до реальних кіберзагроз, забезпечуючи ефективне навчання.

Кіберполігони мають значний вплив на підготовку фахівців у галузі кібербезпеки, оскільки вони:

- Покращують практичні навички: Навчання в реалістичних умовах допомагає студентам розвивати не тільки технічні навички, але й стратегічне мислення, необхідне для аналізу та реагування на кіберзагрози.
- Забезпечують глибше розуміння кіберзагроз: Регулярна практика в кіберполігоні допомагає зрозуміти тактики, техніки та процедури, які використовують кіберзлочинці, що є важливим для розробки ефективних стратегій захисту.
- Сприяють неперервному навчанню: Кібербезпека вимагає постійного оновлення знань. Кіберполігони дозволяють впроваджувати найновіші дослідження та розробки в навчальний процес, забезпечуючи актуальність знань студентів.

Оснащення кіберполігонами стає вирішальним фактором у підготовці нового покоління фахівців з кібербезпеки, забезпечуючи їм не тільки необхідні знання, але й практичні навички, критичне мислення та здатність адаптуватися до постійно змінюваних умов кіберпростору.

Розвиток та впровадження передових технологій та методологій у сфері кіберполігонів відкриває нові можливості для освітніх закладів забезпечити високий рівень підготовки майбутніх спеціалістів, ефективно збільшуючи їхню готовність до реальних викликів сучасної кібербезпеки [10]. Віртуалізація та імітаційні техніки, які використовуються в кіберполігонах, не тільки оптимізують процес навчання, але й значно підвищують його ефективність, забезпечуючи комплексний розвиток необхідних умінь та компетенцій.

Застосування кіберполігонів у навчальних програмах вищих навчальних закладів стає все більш популярним. Наприклад, університети по всьому світу вже інтегрують кіберполігони у свої курси кібербезпеки, що дозволяє студентам здобувати практичні навички в реальних умовах [13; 14]. Деякі університети використовують кіберполігони для проведення лабораторних робіт, де студенти можуть відтворювати відомі кібератаки і відпрацьовувати стратегії захисту. Це допомагає студентам не тільки краще зрозуміти теорію, але й навчитися використовувати на практиці різні інструменти та методики оборони.

Викладання та оцінювання за допомогою кіберполігонів мають свої особливості. Заняття на кіберполігоні зазвичай включають сценарії, що імітують різні кіберзагрози, які студенти мають виявити та нейтралізувати. У рамках таких занять оцінювання здійснюється за критеріями, які включають не тільки правильність виконання задачі, але й швидкість реагування та здатність аналізувати ситуацію.

Кіберполігони мають значний вплив на мотивацію та залучення студентів. Практичний досвід, який студенти отримують під час роботи на кіберполігоні, значно збільшує їхню зацікавленість у галузі кібербезпеки. Гейміфікація та елементи змагань, які часто використовуються на кіберполігонах, значно підвищують мотивацію студентів і сприяють глибшому засвоєнню матеріалу [1; 2]. Ці елементи дозволяють студентам відчувати реальність викликів кібербезпеки і зрозуміти важливість своєї ролі у захисті інформації.

Інтеграція кіберполігонів у навчальні плани є стратегічно важливим кроком для освітніх закладів, який не тільки підвищує рівень технічної підготовки студентів, але й сприяє їхньому професійному розвитку, мотивації та залученню в процес навчання. Забезпечення студентів можливістю використовувати набуті знання в реальних умовах на кіберполігоні відкриває перед ними нові перспективи для розвитку в галузі кібербезпеки і підготовки до викликів сучасного світу.

Використані джерела

1. A systematic mapping study on gamification applications for undergraduate cybersecurity education / S. Weitzl-Harms et al. *Journal of cybersecurity education research and practice*. 2023. Vol. 2023, no. 1. URL: <https://doi.org/10.32727/8.2023.12> (date of access: 13.05.2024).

2. Balon T., Baggili I. Cybercompetitions: a survey of competitions, tools, and systems to support cybersecurity education. *Education and information technologies*. 2023. URL: <https://doi.org/10.1007/s10639-022-11451-4> (date of access: 13.05.2024).
3. Compete to learn: toward cybersecurity as a sport / T. O'Conner et al. *Journal of cybersecurity education research and practice*. 2023. Vol. 2023, no. 1. URL: <https://doi.org/10.32727/8.2023.16> (date of access: 13.05.2024).
4. Comprehensive cyber arena; the next generation cyber range. *IEEE Xplore*. URL: <https://ieeexplore.ieee.org/document/9229857> (date of access: 13.05.2024).
5. Cyber range design framework for cyber security education and training / M. N. Katsantonis et al. *International journal of information security*. 2023. URL: <https://doi.org/10.1007/s10207-023-00680-4> (date of access: 13.05.2024).
6. CyRIS: a cyber range instantiation system for facilitating security training / C. Pham et al. *SoICT '16: seventh international symposium on information and communication technology, Ho Chi Minh City Vietnam*. New York, NY, USA, 2016. URL: <https://doi.org/10.1145/3011077.3011087> (date of access: 13.05.2024).
7. Design and implementation of multi-cyber range for cyber training and testing / M. Park et al. *Applied sciences*. 2022. Vol. 12, no. 24. P. 12546. URL: <https://doi.org/10.3390/app122412546> (date of access: 13.05.2024).
8. Interactive environment for effective cybersecurity teaching and learning / W. Lazarov et al. *ARES 2023: the 18th international conference on availability, reliability and security, Benevento Italy*. New York, NY, USA, 2023. URL: <https://doi.org/10.1145/3600160.3605007> (date of access: 13.05.2024).
9. Jelo M., Helebrandt P. Gamification of cyber ranges in cybersecurity education. *2022 20th international conference on emerging elearning technologies and applications (ICETA), Stary Smokovec, Slovakia, 20–21 October 2022*. 2022. URL: <https://doi.org/10.1109/iceta57911.2022.9974714> (date of access: 13.05.2024).
10. Lateş I., Boja C. Cyber range as a competency based education instrument in cyber security. *New trends in sustainable business and consumption*. 2022. URL: <https://doi.org/10.24818/basiq/2022/08/093> (date of access: 13.05.2024).
11. Lates I. Cyber ranges implementation methodology. *Proceedings of the international conference on business excellence*. 2022. Vol. 16, no. 1. P. 1259–1269. URL: <https://doi.org/10.2478/picbe-2022-0115> (date of access: 13.05.2024).
12. Nelson C. D. Hacking the learning curve: effective cybersecurity education at scale : A Dissertation Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy. Arizona, 2024. 117 p. URL: <https://hdl.handle.net/2286/R.2.N.193577> (date of access: 13.05.2024).
13. Sandboxing the cyberspace for cybersecurity education and learning / S. Karagiannis et al. *ESORICS 2020 International Workshops, DETIPS, DeSECSys, MPS, and SPOSE, Guildford, 17 September 2020*. Cham, 2020. P. 181–196. URL: https://doi.org/10.1007/978-3-030-66504-3_11 (date of access: 13.05.2024).
14. Steiner S., Jillepalli A., Conte de Leon D. A survey of cloud-hosted, publicly-available, cyber-ranges for educational institutions. *Journal of computing sciences in colleges*, 4 November 2022. Evansville, IN, USA, 2022. P. 68–77.

15. Towards nice-by-design cybersecurity learning environments: A cyber range for SOC teams / S. Karagiannis et al. Journal of network and systems management. 2024. Vol. 32, no. 2. URL: <https://doi.org/10.1007/s10922-024-09816-w> (date of access: 13.05.2024).

РОЗРОБКА ОСВІТНІХ ІНСТРУМЕНТІВ ДЛЯ МАТЕМАТИКИ ТА ФІЗИКИ НА ОСНОВІ ІІІ: ВИКОРИСТАННЯ LATEX І ІІІ ДЛЯ СТВОРЕННЯ ТА ВИРІШЕННЯ СТРУКТУРОВАНИХ ЗАВДАНЬ

Development of AI-Driven Educational Tools for Mathematics and Physics: Leveraging LaTeX and AI to Create and Solve Structured Tasks

Сак Р.І./ Sakh R.I.

Національний університет “Києво-Могилянська академія” / National University of “Kyiv-Mohyla Academy”

04655, Київ, вул. Григорія Сковороди, 2, каф. Мережних технологій, (044) 425-77-23
e-mail: roman.sakh@ukma.edu.ua, 093-313-50-38

This thesis explores the transformation of traditional mathematics and physics education through the development of AI-powered tools capable of generating and solving tasks with complete solutions. By converting existing schoolbooks into a structured LaTeX format, parsing solutions, and using this data to train AI models, we propose a scalable, automated approach to educational content creation. The system employs advanced natural language processing (NLP) techniques and mathematical solvers to generate new tasks in a similar style, complete with detailed solutions. This paper details the processes of dataset preparation, model training, and solution architecture, emphasizing reproducibility and adaptability in educational systems.

Introduction

Mathematics and physics education relies heavily on the availability of diverse, well-structured problems accompanied by detailed solutions. While textbooks offer a finite number of tasks, educators often need to supplement these resources with new problems tailored to their students' needs. This demand underscores the potential of artificial intelligence (AI) to not only generate educational content dynamically but also validate its correctness by providing solutions.

In this paper, we propose a system that digitizes and parses existing schoolbooks into a machine-readable format using LaTeX, then trains AI models on these datasets to generate new, contextually relevant problems with solutions. The system's goal is twofold: enhance the variety of educational resources and provide students and educators with an interactive tool to explore complex concepts.

Dataset Preparation

1. Digitization and Conversion to LaTeX

Existing schoolbooks form the foundation of our dataset. Textbooks are digitized and converted into LaTeX format to ensure structural consistency and flexibility. LaTeX, a typesetting system widely used for scientific and mathematical documentation, allows precise representation of equations, diagrams, and logical structures.

The digitization process involves:

- **Optical Character Recognition (OCR):** Extracting textual content from physical books.
- **Semantic Parsing:** Identifying and tagging problems, examples, and solutions.
- **Conversion to LaTeX:** Encoding problems and solutions using LaTeX to preserve mathematical notation.

2. Parsing Solutions

Solutions are parsed into step-by-step instructions. Each step is tagged with metadata, including:

- Problem type (e.g., algebra, calculus, mechanics).