УДК 004.056:794.8

ГЕЙМІФІКОВАНІ ПЛАТФОРМИ ДЛЯ НАВЧАННЯ КІБЕРБЕЗПЕКИ: КІЛЬКІСНА ОЦІНКА ЗНИЖЕННЯ ЛЮДСЬКОГО ФАКТОРА ЯК ІТ-РИЗИКУ

Обидало О.С.[1]; Петрова Р.В., к.т.н., доц.[2];
Пономарьова С.В.,
[1,2,3] Харківський національний університет радіоелектроніки
[1,2,3] Україна, Харків
[1] oleksandr.obydalo@nure.ua; [2] roksana.petrova@nure.ua; [3] svitlana.ponomarova@nure.ua

Анотація. *Робота присвячена підвищенню кібербезпеки завдяки гейміфікованому навчанню. Основна ідея — зменшити вплив людського фактору, який часто є слабкою ланкою в ІТ-безпеці. Розглянуто інтегровану платформу, яка об'єднує технології додаткової реальності (іммерсивні XR-технології), цифрових двійників і елементи гри. Вона дозволяє змоделювати справжні кібератаки та дослідити, як поводяться користувачі в критичних ситуаціях. Один з випадків застосування — тренажер для фахівців, які працюють на об'єктах критичної інфраструктури. В результаті відбувається менше помилок, швидше реагування на інциденти та краще засвоєння матеріалу завдяки інтерактивному підходу. Також платформа дозволяє чітко виміряти, наскільки покращились навички користувачів і як зросла їхня стійкість до кібератак.*

Ключові слова: *гейміфікація; навчання кібербезпеці; людський фактор; віртуальна реальність; цифровий двійник.*

Вступна частина. Людський фактор сьогодні вважається однією з головних причин кіберінцидентів: дослідження показують, що до 82% випадків порушення інформаційної безпеки виникають через помилки самих користувачів [1]. Так, технічний захист — брандмауери, системи виявлення вторгнень та інші засоби — справді важливий. Але він не може повністю гарантувати безпеку. Люди можуть випадково натиснути на фішингове посилання, використовувати слабкі паролі або ігнорувати оновлення — і ці дії відкривають шлях для атак, який не перекриє жодна технологія [2]. Саме тому сучасний підхід до кібербезпеки має включати не лише технічні рішення, а й увагу до поведінки користувачів. Один з ефективних способів знизити ризики, пов’язані з «людським чинником», — це гейміфіковане навчання. Простіше кажучи, це коли в навчання додають ігрові елементи, щоб зробити його цікавішим і результативнішим. Дослідження доводять, що такий підхід працює: гейміфікація значно підвищує мотивацію працівників і покращує результати навчання. Наприклад, використання ігрових методик у програмах з підвищення обізнаності щодо кібербезпеки може збільшити залученість співробітників аж на 60% [1]. Все це робить актуальним створення інтерактивних навчальних платформ, які дозволяють без ризику моделювати реальні кібератаки. Це не тільки допомагає тренувати практичні навички, а й дає змогу кількісно оцінити, як саме навчання впливає на зменшення кількості помилок. У цій роботі ми спираємось на результати дослідження [2], присвяченого гейміфікованим імерсивним тренажерам у сфері кібербезпеки і пропонуємо узагальнення щодо того, наскільки ефективними можуть бути такі підходи.

Метою дослідження є описання гейміфікованих платформ для навчання з кібербезпеки. Їх ключова особливість — можливість не просто моделювати реалістичні кібератаки й реакції

користувачів, а й точно вимірювати, як така система впливає на зменшення людського фактору як ризику для безпеки. Щоб реалізувати цю ідею, потрібно об’єднати сучасні технології — VR/XR, цифрові двійники, штучний інтелект — в єдину систему. Вона має не лише навчати, а й відстежувати поведінку користувачів у процесі. І, звісно, щоб переконатися, що все працює як треба, необхідно провести експериментальне тестування платформи в умовах, наближених до реального середовища — зокрема, в критичних інфраструктурних сферах.

Основна частина. Розглянуто інтегровану XR-платформу з елементами гейміфікації (рис.1), яка складається з трьох ключових модулів [2]:



Рис. 1 – модулі XR-платформи з елементами гейміфікації

Модуль поведінки гравця (Player Behavior Module, PBM). Цей модуль моделює дії користувачів і потенційних зловмисників. У ньому реалізовані моделі трьох типів "гравців" — атакуючого, захисника та звичайного користувача — з різними стратегіями й мотиваціями. За допомогою LLM-агентів і аналізу логів та мережевого трафіку PBM відстежує, як оператори поводяться під час стандартних задач і в умовах кібератак. Модуль збирає точні метрики: швидкість реакції, точність рішень, адаптивність у кризових ситуаціях [2]. Це дозволяє порівняти, як користувач діє в спокійних умовах і під тиском, та оцінити його прогрес після навчання.

Модуль гейміфікації (Gamification Module, GM). Відповідає за те, щоб навчання не було нудним. Модуль додає сюжет і гейміфіковану структуру: оператор виконує звичні завдання (наприклад, моніторить системи), але час від часу стикається з атакою, згенерованою AI-супротивником [2]. Так формується навичка миттєвої реакції на загрози. У процесі є бали, динамічні рівні складності, зворотний зв’язок у реальному часі — усе для підтримки інтересу й мотивації. Також цей модуль допомагає знайти баланс між ефективністю в щоденних завданнях і готовністю до криз.

Модуль симуляції (Simulation Module, SM). Забезпечує повну реалістичність тренування. Віртуальне середовище створене у формі цифрового двійника об'єкта критичної інфраструктури — наприклад, насосно-фільтраційної станції [2]. Оператор у VR-шоломі потрапляє до віртуального диспетчерського центру, де бачить знайомі прилади та датчики, що

поводяться, як справжні. Через MQTT-протокол організовано двосторонній обмін даними між VR та фізичним стендом: дії у віртуальному світі (наприклад, зміна режиму насоса) відображаються на макеті, і навпаки — зміни у фізичних пристроях видно у VR [2]. Це дозволяє без ризику моделювати наслідки атак, які в реальному житті могли б бути небезпечними. Наприклад, як вплине DDoS-атака на якість очищення води.

Цю систему протестували в реальних умовах — зокрема, для працівників насосно-фільтраційної станції [2]. Вони працювали в імерсивному тренажері, виконуючи звичні задачі, але з часом стикались із симульованими кіберінцидентами — від поломок датчиків до цілеспрямованих атак.

Дані PBM показали: після кількох VR-сесій час виявлення загроз скоротився на 40%, а кількість помилок — на 30% у порівнянні з початковими показниками. Тобто, платформа реально покращила готовність персоналу до реагування.

Ще один цікавий ефект — користувачі стали впевненішими. Гра в «небезпечні» ситуації знижувала рівень стресу, а повторюваність допомагала закріпити навички до автоматизму.

До того ж, система не просто навчає, а й адаптується. Вона збирає дані про реакції, послідовність дій і помилки, а потім через вбудований штучний інтелект на базі ChatGPT дає персоналізовані поради [2]. Це дозволяє зміцнити сильні сторони користувача й поступово усунути його слабкі місця.

Висновки. Розглянутий підхід підтверджує: гейміфіковані платформи можуть бути справді ефективними для підготовки фахівців з кібербезпеки та мінімізації ризиків, пов’язаних із людським фактором. Поєднання XR-технологій, цифрового двійника й AI-помічника створює безпечне, але максимально наближене до реального середовище, де можна детально досліджувати поведінку користувачів у критичних ситуаціях, зокрема під час кібератак [2].

Це відкриває можливість не лише точно вимірювати рівень готовності та прогрес після тренувань, а й виявляти типові помилки або затримки у реакціях — і працювати над їх усуненням.

Тренажер, розглянутий у цій роботі, був протестований на об’єкті критичної інфраструктури та продемонстрував: гейміфіковане навчання справді допомагає покращити швидкість і точність дій операторів. А це знижує ймовірність успішної реалізації кібератак.

Отримані результати добре узгоджуються з висновками в літературі: так, людина залишається “найслабшою ланкою” в системі кіберзахисту [1,3]. Але водночас саме за допомогою інтерактивного, постійного та наближеного до реальних умов навчання цю слабкість можна перетворити на передбачуваний і контрольований фактор.

У майбутньому можна адаптувати платформу для інших сфер — наприклад, у банківському секторі чи енергетиці, де поведінка персоналу під час кібератаки також має критичне значення [2].

У загальному підсумку: гейміфіковані тренажери — це не просто інновація, а реальний крок до формування сталої кібергігієни в організаціях. Вони допомагають не лише вдосконалити технічні навички, а й зміцнити відповідальність, увагу та цифрову обачність співробітників. А це — вагомий внесок у зниження IT-ризиків, які виникають через людський фактор.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Keepnet Labs. (2024, November 12). *The power of gamification in security awareness training*. [Blog post]. *(дата звернення: 30.10.2025).*
[2] Chandrashekar, N.D., Lee, A., Azab, M., & Gračanin, D. (2024). *Understanding user behavior for enhancing cybersecurity training with immersive gamified platforms*. Information, 15(12), 814. https://doi.org/10.3390/info15120814
[3] Verizon. (2023). *2023 Data Breach Investigations Report*. Verizon Enterprise. *(дата звернення: 30.10.2025).*

Obydalo O.S., Petrova R.V., Ponomarova S.V.

Gamified Platforms for Cybersecurity Training: Quantitative Assessment of Reducing the Human Factor as an IT Risk

Abstract. *The paper presents an approach to improving cybersecurity through a gamified training platform aimed at minimizing the human factor as an IT risk. The described integrated system leverages immersive XR technologies, digital twins, and gamification to simulate realistic cyberattacks and study user behavior. A case study (an immersive trainer for a critical infrastructure facility) is discussed, demonstrating a reduction in user errors and faster incident response thanks to interactive training. The platform enables quantitative evaluation of skill improvement and enhanced resilience against attacks.*

Keywords: *cybersecurity; gamified learning; human factor; virtual reality; digital twin*