

In addition, electronic communication services and services based on electronic communications are the basis of the modern development of digital technologies, digitalization of society and economy, namely: e-education, e-banking, mobile banking, e-services, telemedicine, e-government, etc. Also, the development and spread of electronic communications among many countries and broad segments of the population gave impetus to the rapid development (quantitative and qualitative indicators) of mobile applications, various software products, various software products (specialized software), as well as the rapid growth of the number of users of messengers and social networks. The next important step was the transition to the virtual space of organizations, institutions, and enterprises. Yes, today almost all authorities (central, regional, district and local levels have their own websites and communicate with the population online), educational institutions of all levels, medical institutions, financial and banking institutions, the sphere of service provision, etc. All this also requires stable and sustainable functioning for the possibility of providing various services to the population.

At the same time, experts within the framework of the study "Increasing resilience by accelerating the digital transformation of business in Ukraine" consider digitization and digital transformation as an important element "for increasing resilience and facilitating recovery" [2, p.17], which directly depend both on the level of development of electronic communications and the global data transmission network, as well as on access to them by broad sections of the population.

1. Some issues of critical infrastructure objects, Resolution of the CMU dated October 9, 2020 No. 1109. <https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text>
2. Increasing sustainability by accelerating the digital transformation of business in Ukraine. <https://surl.li/asaeds>
3. On critical infrastructure: Law of Ukraine of November 16, 2021 No. 1882-IX Vedomosti Verkhovna Rada (VVR), 2023, No. 5, Article 13. <https://zakon.rada.gov.ua/laws/show/1882-20#Text>

Інтерактивні сценарії як інструмент викладання стандартів технічного захисту інформації

УДК 004.94:004.921

Юрій Скоренький¹, Руслан Козак²,
Наталія Загородна³, Тетяна Вітенко⁴

Тернопільський національний технічний університет імені Івана Пулюя,

¹*skorenkyu@tntu.edu.ua,* ²*zagorodna.n@gmail.com,* ³*ruslank@tntu.edu.ua*

⁴*vitenko@tntu.edu.ua*

Стрімка цифровізація вищої освіти зумовила нагальну потребу в зміні парадигми в бік модульних, стійких та інтерактивних педагогічних моделей. У контексті трансформації української вищої освіти інституційне виживання значною мірою залежить від переходу від екстреного дистанційного викладання до сталої цифрової педагогіки. Викладання основ технічного захисту інформації та узгодження зі стандартами (зокрема, ISO/IEC 27001) становить значний

педагогічний виклик. Від здобувачів освіти вимагається опанування комплексних систем прийняття рішень щодо оцінки ризиків та контролю фізичного доступу. Хоча гейміфікація широко застосовується для формування базової обізнаності з питань безпеки (наприклад, антифішингу), глибоке вивчення стандартів вимагає інтеграції складних компетенцій.

Для подолання цих викликів у межах пілоотної ініціативи було здійснено перехід від статичних, перевантажених текстом матеріалів до гейміфікованого середовища в системі управління навчанням ATutor. Інтеграція інструментарію H5P дозволила створити нелінійні «сценарії розгалуження» (Branching Scenarios) на основі методології проблемно-орієнтованого навчання (PBL). Виступаючи в ролі аудиторів фізичної безпеки, студенти виявляли потенційні вразливості та приймали рішення, базуючись виключно на протоколах ISO 27001. Такі сценарії надійно занурюють здобувачів у ситуації, де вони повинні зважувати наслідки своїх дій, що стимулює критичне мислення. Емпіричні дані, отримані через навчальну аналітику з ATutor та H5P, продемонстрували важливу закономірність розвитку аналітичних навичок. Студенти, які спочатку обирали помилкові варіанти, були змушені аналізувати та виправляти змодельовані порушення і продемонстрували значно кращі результати у підсумкових комплексних оцінюваннях на критичне мислення порівняно з тими, хто пройшов сценарії з першої спроби.

Успішна реалізація цього проєкту слугує надійною моделлю для розбудови інституційного потенціалу, підтверджуючи, що інтерактивна та доступна цифрова педагогіка [1] може успішно функціонувати навіть в умовах серйозних зовнішніх викликів, ефективно озброюючи студентів критичними навичками, необхідними для майбутнього.

1. Zagorodna N., Skorenkyu Y., Kunanets N., Baran I., Stadnyk M., Augmented Reality-enhanced learning tools development for cybersecurity major. *CEUR Workshop Proceedings*. – 2022. – V. 3309. – p. 25–32.

Високопродуктивне розпізнавання облич на базі CUDA та Dlib у структурі комплексних систем забезпечення кібербезпеки

УДК 004.93

Олексій Смірнов¹, Віктор Заріцький²,
Костянтин Буравченко³, Сергій Смірнов⁴

Центральноукраїнський національний технічний університет,

¹dr.smirnova@gmail.com, ²viktorzarickiy@gmail.com,

³buravchenkok@gmail.com, ⁴smirnov.ser.81@gmail.com

Стрімкий прогрес у галузі розпізнавання образів зумовлений глибокою інтеграцією технологій штучного інтелекту в стратегічні сектори: від військової ідентифікації об'єктів БПЛА в умовах російсько-української війни до автоматизації медицини та промисловості. Це дослідження присвячене вдосконаленню систем безпеки, де детекція облич виступає фундаментальним компонентом інфраструктури "розумних міст", банківських установ та інформаційно-телекомунікаційних систем. Ключовим викликом для таких