

ЦИФРОВІ ІНСТРУМЕНТИ РОЗВИТКУ БАЗОВИХ КОМПЕТЕНТНОСТЕЙ ЗДОБУВАЧІВ ОСВІТИ З ОСНОВ КІБЕРБЕЗПЕКИ

Мінський Владислав Олександрович

здобувач першого (бакалаврського) рівня вищої освіти ОПП «Середня освіта (Інформатика, математика, основи STEM-навчання)

Тернопільський національний університет імені Володимира Гнатюка

minskyj_vo@fizmat.tnpu.edu.ua

Карабін Оксана Йосифівна

кандидат педагогічних наук, доцент кафедри інформатики та методики її навчання

Тернопільський національний педагогічний університет імені Володимира Гнатюка

karabin@tnpu.edu.ua

Сучасний розвиток інформаційно-комунікаційних технологій (ІКТ) спричинив суттєві зміни в усіх сферах людської діяльності, включаючи освіту. «Війна в Україні зумовила значну дестабілізацію багатьох сфер людської діяльності, зокрема й освіти. Заклади освіти різних рівнів були вимушені адаптуватися до обмежень і загроз воєнного стану, змінюючи традиційну форму навчання на дистанційну або змішану. Оскільки ключовою умовою освітнього процесу стало використання різних інформаційно-комунікаційних технологій, питання розвитку цифрових навичок та цифрової грамотності серед здобувачів освіти набуло актуальності» [4, с. 1]. Усвідомлене та відповідальне використання цифрових технологій і ресурсів є важливою передумовою запобігання кібератакам і забезпечення надійного захисту критично важливих даних, що, у свою чергу, позитивно впливає на рівень інформаційної безпеки та стійкість держави. Інформаційна безпека розглядається як стан захищеності інформації від навмисних або випадкових дій, які можуть спричинити неприпустимі наслідки для суб'єктів інформаційних відносин. Водночас це такий стан, що гарантує охорону життєво важливих інтересів суспільства і держави від внутрішніх та зовнішніх загроз в інформаційному просторі [1]. Однією з ключових вимог до сучасного суспільства є формування цифрових компетентностей, зокрема у сфері кібербезпеки. В умовах постійного зростання кількості кіберзагроз і ризиків ефективна підготовка здобувачів освіти з основ кібербезпеки стає критично важливою. У цьому контексті цифрові інструменти відіграють важливу роль у забезпеченні доступності, інтерактивності та ефективності освітнього процесу.

Кібербезпека є однією з найважливіших складових цифрової грамотності. Вона охоплює знання, навички та поведінкові моделі, які спрямовані на захист інформаційних систем, даних та особистої інформації від несанкціонованого доступу, атак чи втрат. У зв'язку з цим формування базових компетентностей у сфері кібербезпеки є необхідним як для професійної діяльності, так і для повсякденного життя. Особливу увагу слід приділити освітній підготовці молодого покоління, яке активно впроваджує цифрові пристрої у своє повсякдення. Важливо, щоб здобувачі освіти не лише опановували базові принципи та інструменти інформаційних технологій, а й формували здатність виявляти потенційні загрози у цифровому середовищі та своєчасно й адекватно на них реагувати. Адже саме усвідомлене й відповідальне використання цифрових

технологій і ресурсів є запорукою запобігання кібератакам, забезпечення захисту критично важливих даних і, відповідно, підвищення рівня інформаційної безпеки та стійкості держави. Про концептуальні аспекти цифровізації, її сутності та ролі в розвитку освіти наголошено у багатьох науково-методичних дослідженнях, зокрема у навчальному посібнику «Розвиток цифрової компетентності педагогічних працівників закладів професійної (професійно-технічної) освіти засобами інформаційно-комунікаційних технологій: навчальний посібник» [3]. Інформаційна безпека розглядається як стан захищеності інформації від навмисних чи випадкових впливів, здатних спричинити небажані або неприпустимі наслідки для суб'єктів інформаційних відносин. Вона також передбачає забезпечення охорони життєво важливих інтересів особистості, суспільства та держави від внутрішніх і зовнішніх загроз, що виникають у сучасному інформаційному просторі [1]. Саме цифрові інструменти допомагають зробити цей освітній процес більш результативним.

Нині цифрові інструменти охоплюють широкий спектр технологій, які можна використовувати для розвитку компетентностей у сфері кібербезпеки. До них належать освітні платформи, симулятори, інтерактивні курси, мобільні додатки, відеоуроки, ігрові тренажери тощо.

Освітні платформи. Платформи, такі як Coursera чи Cisco Networking Academy пропонують спеціалізовані курси з кібербезпеки. Вони дозволяють здобувачам освіти отримати доступ до якісних матеріалів, пройти тестування та отримати сертифікати. Дані платформи забезпечують інтерактивність навчання через відеолекції, практичні завдання та форуми для обговорення.

Симулятори та віртуальні лабораторії. Симулятори кіберзагроз дозволяють моделювати реальні ситуації атак на інформаційні системи. Наприклад, такі платформи, як Cyber Range створюють безпечне середовище для відпрацювання навичок реагування на інциденти. Такі лабораторії дозволяють здобувачам освіти отримати практичний досвід у вирішенні проблем без ризику для реальних систем.

Ігрові тренажери. Гейміфікація є ефективним методом залучення студентів до навчання. Ігрові тренажери з кібербезпеки, наприклад CyberSec Game або Hack The Box, дозволяють поєднати навчання з елементами гри. Такий підхід сприяє підвищенню мотивації здобувачів освіти та кращому засвоєнню матеріалу.

Мобільні застосунки також пропонують інноваційний підхід до навчання, що поєднує інтерактивність, доступність та індивідуалізацію освітнього процесу. Завдяки гейміфікації, візуалізації та практичним завданням, вони сприяють не лише засвоєнню теоретичних знань, а й формуванню практичних навичок у сфері кібербезпеки. На сьогодні існує широкий спектр мобільних застосунків, які спрямовані на розвиток компетентностей у сфері кібербезпеки. Серед них: Cyber Security Quiz пропонує серію тестів і вікторин на тему кібербезпеки, Користувачі можуть перевірити свої знання про загрози в інтернеті, безпечне використання паролів і захист персональних даних; Kaspersky Interactive Protection Simulation (KIPS) орієнтований на симуляцію реальних ситуацій із загрозами кібербезпеки, користувачі мають змогу приймати рішення в умовах кіберінцидентів і оцінювати наслідки своїх дій; CyberSafe створений для дітей і підлітків та допомагає навчитися основам безпечної поведінки в інтернеті. У ньому представлені

інтерактивні уроки про конфіденційність, фішинг та захист від шкідливого програмного забезпечення; Phishing Simulator навчає розпізнавати фішингові атаки шляхом аналізу електронних листів і вебсайтів, користувачі отримують практичний досвід у визначенні ознак шахрайства.

Відеоуроки та вебінари. Візуальні матеріали є важливим компонентом навчального процесу. Відеоуроки пояснюють складні концепції у зрозумілій формі, а вебінари забезпечують можливість спілкування з експертами в режимі реального часу.

Ефективне використання цифрових інструментів у навчанні кібербезпеки потребує врахування методологічних аспектів. Зокрема, важливо забезпечити: Системний підхід (навчальний процес має бути структурованим і охоплювати всі ключові аспекти кібербезпеки: від базових понять до складних практичних завдань), індивідуалізацію навчання (цифрові інструменти дозволяють адаптувати навчальні матеріали до рівня знань і потреб кожного здобувача освіти, що сприяє кращому засвоєнню матеріалу), інтерактивність (залучення студентів до активної участі у навчальному процесі через інтерактивні завдання, симуляції та обговорення підвищує ефективність засвоєння знань), оцінювання результатів (цифрові інструменти забезпечують можливість автоматизованого оцінювання результатів навчання через тести, контрольні завдання та симуляції).

Попри очевидні переваги цифрових інструментів, існують і певні виклики. Серед них можна виокремити недостатню технічну підготовку викладачів, обмежений доступ до сучасних технологій у деяких навчальних закладах та ризики перевантаження студентів інформацією, бо суттєвим фактором є готовність як викладача, так і здобувача освіти до роботи в цифровому середовищі [2, с. 97]. Проте перспективи впровадження цифрових інструментів у навчання кібербезпеки залишаються значними. Подальший розвиток технологій штучного інтелекту та машинного навчання відкриває нові можливості для створення персоналізованих освітніх програм і вдосконалення методів оцінювання знань.

Таким чином, інтеграція цифрових інструментів у систему освіти відкриває нові можливості для підготовки здобувачів освіти до викликів цифрової епохи. У майбутньому варто очікувати розробку більш складних і персоналізованих цифрових баз, які будуть враховувати індивідуальні потреби учнів і забезпечувати більш ефективне навчання. Їх використання у навчанні основ кібербезпеки є важливим кроком на шляху до формування компетентностей сучасного покоління. Інтерактивність, доступність і практична спрямованість цих інструментів сприяють ефективному засвоєнню знань і навичок. Водночас необхідно враховувати методологічні аспекти їх використання та долати існуючі виклики задля забезпечення високої якості освіти у сфері кібербезпеки.

Список використаних джерел

1. Виздрик В., Мельник О. Інформаційна безпека в Україні: сучасний стан. *Grail of Science*, 2023. № 24. С. 196–202.
2. Драчук М. І., Федорович З. Я. Цифрова компетентність в освітньому контексті. *Collection of scientific papers «ΛΟΓΟΣ»* (March 3, 2023). Bologna, Italy, 2023. С. 97–98.
3. Розвиток цифрової компетентності педагогічних працівників закладів професійної (професійно-технічної) освіти засобами інформаційно-комунікаційних технологій:

навчальний посібник / Івашев Є. В., Сахно О. В., Грядуща В. В., Денисова А. В., Лукіянчук А. М., Удовик С. І. Біла Церква : БІНПО, 2021. 258 с.

4. Шостак Ігор Олександрович, Ніколенко Ксенія Вікторівна, Петровська Катерина Володимирівна. Розвиток цифрової грамотності здобувачів вищої освіти в Україні як відповідь на воєнні виклики. *Вісник науки та освіти*, 2022. № 1(1). С. 1–13.

ЦИФРОВІ ТЕХНОЛОГІЇ УПРАВЛІННЯ ВОЛОНТЕРСЬКИМИ ПРОГРАМАМИ

Неживий Віктор Євгенович

здобувач третього рівня вищої освіти, спеціальність Освітні, педагогічні науки
Тернопільський національний педагогічний університет імені Володимира Гнатюка
neghuvujV@gmail.com

Цифрові технології фундаментально трансформували управління волонтерськими програмами, перетворивши його з дрібних, спрямованих на документування процесів у стратегічне, масштабоване та залучене управління людськими ресурсами. Організації, які впроваджують комплексні цифрові рішення, спостерігають збільшення кількості волонтерів.

Важливим у цифровому управлінні волонтерськими програмами є спеціалізоване програмне забезпечення для управління волонтерами. Ця платформа пропонує комплексні рішення для всього циклу залучення волонтерів. Bloomerang Volunteer, Better Impact, Volgistics, Rosterfy, POINT та VolunteerMark пропонують унікальний набір можливостей, оптимізованих для різних типів організацій [2].

Bloomerang Volunteer надає свою інтеграцію із системами управління взаємовідносинами з донорами (CRM), що дозволяє мати єдину базу даних для всіх прихильників. Better Impact пропонує рішення на рівні управління, яке обслуговує понад 25 000 організацій і мільйон волонтерів по всьому світу. Rosterfy, яка використовує понад 8 мільйонів волонтерів і персоналу в глобальному масштабі, пропонує гейміфіковану систему визнання та оптимізовані процеси адаптації. POINT забезпечує безкоштовну платформу для неприбуткових осіб з необмеженим числом профілів волонтерів та адміністраторів, підвищуючи доступність для меншої кількості організацій.

Zoom, Skype і WhatsApp забезпечують синхронну та асинхронну комунікацію, яка дозволяє регулярне оновлення, віртуальні зустрічі та командну роботу. Slack, Microsoft Teams і Trello полегшують координацію робочих процесів, спільне використання документів і моніторинг прогресу в реальному часі.

Аналіз даних волонтерів став критичною складовою сучасного управління волонтерськими програмами. Google Sheets, Airtable і Salesforce дозволяють організувати зберігання та аналіз даних про волонтерів. Платформи VMS такі як POINT автоматично формують статистичні звіти з детальної діяльності волонтерів: кількість волонтерів, коефіцієнт утримання, участь та задоволення волонтерів.

Важливими є також платформи онлайн-навчання та підготовки волонтерів. Moodle, Coursera та Khan Academy пропонують масштабовані умови навчання,