залежить передусім від системності підготовки, а не від віку педагога [4, с. 275].

Отже, спрощене протиставлення «цифрових аборигенів» та «цифрових іммігрантів» серед педагогів не відповідає складності реальної ситуації. Цифрова компетентність є багатовимірним конструктом, що формується внаслідок взаємодії вікового досвіду, професійної мотивації, якості підготовки та системної підтримки. Для ефективної реалізації стратегій Digital Skills 2030 необхідно відмовитися від вікових стереотипів та будувати системи підвищення кваліфікації, орієнтовані на індивідуальний профіль цифрової компетентності кожного педагога, незалежно від його віку та стажу роботи.

Список використаних джерел:

1. Спірін О. М. Інформаційно-комунікаційні та інформатичні компетентності як компоненти системи професійно-спеціалізованих компетентностей вчителя інформатики. *Інформаційні технології і засоби навчання*. 2009. Т. 13. № 5. С. 1–16.
2. Іванюк І. В., Овчарук О. В. Результати онлайн-опитування «Потреби вчителів щодо використання цифрових засобів та ІКТ в умовах карантину» : аналіт. матеріали. Київ : ІІТЗН НАПН України, 2020. 50 с.
3. Жалдак М. І. Проблеми інформатизації навчального процесу в середніх і вищих навчальних закладах. *Комп'ютер у школі та сім'ї*. 2013. № 3. С. 8–15.
4. Сисоєва С. О., Осадча К. П. Стан, технології та перспективи дистанційного навчання у вищій освіті України. *Інформаційні технології і засоби навчання*. 2019. Т. 70. № 2. С. 271–284.

Надія Власова
здобувачка вищої освіти,
Миколаївський національний аграрний університет
Науковий керівник: ***Вячеслав Курепін***
кандидат економічних наук, доцент,
доцент кафедри методики професійного навчання
Миколаївського національного аграрного університету

ЦИФРОВІ ОСВІТНІ ПЛАТФОРМИ КРІЗЬ ПРИЗМУ КІБЕРБЕЗПЕКИ

Розвиток сучасного суспільства безумовно залежить від цифровізації освіти, оскільки вона забезпечує доступність навчальних ресурсів, гнучкість освітнього процесу та можливість використання інноваційних педагогічних технологій. Завдяки впровадженню цифрових освітніх

платформ, хмарних сервісів і дистанційних форм навчання розширюються можливості здобувачів вищої освіти та викладачів, підвищується ефективність комунікації й управління освітнім процесом. Цифровізація сприяє формуванню цифрових компетентностей, необхідних для успішної професійної діяльності в умовах інформаційного суспільства.

Але цифрова трансформація освіти споріднена з кіберризиками. Активне використання онлайн-платформ і цифрових сервісів пов'язане з обробкою значних обсягів персональних даних, що підвищує загрозу їх витоку або несанкціонованого доступу. Освітнє середовище дедалі частіше стає об'єктом кібератак, зокрема фішингу, поширення шкідливого програмного забезпечення та використання методів соціальної інженерії [1, с. 473]. У зв'язку з цим питання кібербезпеки та формування навичок кібергігієни набувають особливої актуальності, адже безпечна цифровізація освіти можлива лише за умови усвідомлення ризиків і впровадження комплексних заходів захисту інформації.

Сучасний освітній процес активно інтегрує цифрові технології, що дозволяє зробити навчання більш гнучким, персоналізованим та доступним. Важливу роль у цьому відіграють різноманітні цифрові освітні платформи, серед яких системи управління навчанням (LMS), хмарні сервіси та платформи дистанційного навчання.

LMS забезпечують організацію навчального процесу, дозволяють викладачам планувати курси, контролювати успішність студентів та надавати матеріали у структурованому вигляді. Хмарні сервіси сприяють збереженню та обміну навчальними ресурсами, спільній роботі здобувачів вищої освіти над проєктами та доступу до інформації з будь-якого пристрою та місця.

Платформи дистанційного навчання, у свою чергу, відкривають можливість повністю віддаленого навчання, проводити інтерактивні заняття, онлайн вебінари та тестування, що особливо актуально для молоді, які не можуть відвідувати аудиторії оф-лайн. Ці інструменти значно підвищують ефективність освітнього процесу, дозволяючи адаптувати його під індивідуальні потреби здобувачів вищої освіти та забезпечити безперервність навчання в будь-яких умовах.

Розширюючи можливості навчання, сучасне цифрове освітнє середовище одночасно створює нові ризики для безпеки інформації [2, с. 89]. Одна з загроз - витік даних, коли конфіденційна інформація здобувачів вищої освіти, викладачів потрапляє у чужі руки через неналежний захист систем або людські помилки. Фішинг стає ще однією небезпекою, адже користувачі можуть отримувати підроблені повідомлення або посилання, що маскуються під офіційні ресурси, і в результаті розкривати свої логіни,

паролі або фінансову інформацію.

Не менш серйозним є несанкціонований доступ до освітніх платформ, що дозволяє зловмисникам змінювати або видаляти навчальні матеріали, отримувати доступ до особистих даних і порушувати освітній процес. Соціальна інженерія доповнює ці загрози, маніпулюючи користувачами для отримання доступу до інформації шляхом обману або психологічного впливу.

Для забезпечення кібербезпеки цифрових освітніх платформ важливо впроваджувати комплексний підхід, що поєднує технічні та організаційні заходи захисту інформації. До технічних аспектів належить використання сучасних систем аутентифікації та шифрування даних, забезпечення регулярного оновлення програмного забезпечення та оперативне усунення вразливостей. Важливу роль відіграє моніторинг мережевої активності та впровадження систем виявлення та запобігання вторгненням, що дозволяє оперативно реагувати на потенційні загрози.

Організаційні заходи включають навчання персоналу та молоді правилам безпечної роботи у цифровому середовищі [3, с. 256]. Особлива увага приділяється контролю доступу до ресурсів платформи, резервному копіюванню даних і планам відновлення інформації у разі інцидентів.

Таким чином, розвиток цифрових освітніх платформ має відбуватися паралельно з удосконаленням систем кібербезпеки, що сприятиме сталості освітнього процесу, довірі до цифрових технологій та підвищенню якості освіти в умовах цифрової трансформації.

Список використаних джерел:

1. Самойленко О. О., Бацуровська І. В., Курепін В. М. Кібергігієна та безпека життєдіяльності як ключові елементи цифрової компетентності здобувачів освіти. Національні інтереси України. 2025. № 11(16). С 461-477. DOI:https://doi.org/10.52058/3041-1793-2025-11(16)-461-476.
2. Іваненко В.С. Основні принципи безпеки користування Інтернетом // Обліково-аналітичне і фінансове забезпечення діяльності суб'єктів господарювання: національні, глобалізаційні, євроінтеграційні аспекти : матеріали Міжнародної науково-практичної інтернет-конференції, 16-17 листопада 2022 р., Миколаїв. Миколаїв : МНАУ, 2022. С. 88-90. URL:https://dspace.mnau.edu.ua/jspui/handle/123456789/11943.
3. Курепін В. М., Самойленко О. О., Бацуровська І. В. Кібербезпека цифрового освітнього середовища як складова системи безпеки праці та життєдіяльності. Суспільство та національні інтереси: журнал. 2025. № 11(19). С 255-268. https://doi.org/10.52058/3041-1572-2025-11(19)-255-267. https://dspace.mnau.edu.ua/jspui/handle/123456789/22584.