

стресостійкість, саме вона необхідна для підтримки дитини. Відсутність же цієї якості вказує на нездатність батьків здійснювати виховання та соціальний супровід власної дитини протягом усього життя, взаємодіяти з фахівцями різного рівня чи навпаки, свідчить про схильність до аутизації щодо відношення до дитини чи соціуму [3, с.45 –47].

Список використаних джерел:

1. Лавріненко Л. І. Школа для кожного (окремі аспекти інклюзивної освіти): Навчально-методичний посібник для керівників навчальних закладів, учителів та вихователів ДНЗ, ГПД, шкіл-інтернатів, методистів. Чернігівський національний технологічний університет, Чернігів, 2017. 158 с
2. Поради батькам, що виховують у сім'ї дитину з особливими потребами URL: ipro.if.ua/uprav/files/poradu_batkam.doc. (дата звернення: 07.03.2024).
3. Путівник для батьків дітей з особливими освітніми потребами: Навчально-методичний посібник у 9 книгах / За ред. А. А. Колупаєвої. К.: ТОВ ВПЦ «Літопис – ХХ». 2010. 363 с.

ФОРМУВАННЯ КОМПЕТЕНТНОСТЕЙ ЦИФРОВОЇ БЕЗПЕКИ У ЗДОБУВАЧІВ ОСВІТИ

Ольга Мехед

*докторка педагогічних наук, професорка
Національний університет «Чернігівський колегіум»
імені Т. Г. Шевченка
м. Чернігів, Україна*

Ключові слова: *цифрова компетентність, здобувачі освіти, кібербезпека*

Відповідно до Рамки цифрової компетентності для громадян України структура компетентності з цифрової безпеки майбутніх фахівців становить комплекс компетентностей: захист пристроїв і безпечне підключення до мережі Інтернет; захист персональних даних і приватності, безпека в Інтернеті; захист особистих прав споживача від шахрайства і зловживання; захист здоров'я та благополуччя; захист довкілля тощо.

Метою дослідження є вивчення умов ефективного формування базових компетентностей цифрової безпеки у здобувачів освіти.

Розкрито ключові аспекти формування компетентностей цифрової безпеки, включаючи вивчення сучасних тенденцій у кіберзлочинності, розвиток навичок виявлення та запобігання кібератак, а також етичні аспекти використання та обробки інформації в онлайн-середовищі. Формування компетентностей

цифрової безпеки у здобувачів освіти вимагає комплексного підходу та врахування різних аспектів. До основних методів, якими можна здійснювати цей процес, відносять інтеграція в навчальний план, що передбачає введення обов'язкових курсів або модулів з цифрової безпеки в освітні програми та забезпечення покриття різних аспектів, таких як кібергігієна, кіберзахист, етика в Інтернеті тощо. Також надзвичайної актуальності набувають практичні тренінги, що включають проведення симуляцій кібератак для навчання студентів виявленню та реагуванню на кіберзагрози; регулярні практичні справи з захисту особистої інформації та безпечного використання технологій.

Особливу увагу потрібно звернути на електронні ресурси та навчальні платформи, що забезпечують використання інтерактивних онлайн-ресурсів для самостійного вивчення цифрової безпеки та залучення до навчання віртуальних лабораторій та тренажерів. Також часто рекомендується використовувати так звану екстракурсову діяльність: організацію груп для студентів та учнів, які мають зацікавленість у вивченні цифрової безпеки задля участі у студентських або шкільних конкурсах з кібербезпеки. Партнерство з індустрією вимагає залучення представників індустрії цифрової безпеки для проведення лекцій, майстер-класів та стажувань; встановлення зв'язків з компаніями, які можуть надати реальний досвід у сфері кіберзахисту. Для вивчення рівня формування компетентності використовується оцінка та моніторинг, що передбачає використання систем оцінювання, що враховують рівень компетентностей у цифровій безпеці та регулярне оновлення програм на основі оцінок та змін у кіберзагрозах.

Цей комплексний підхід допомагає створити ефективну систему, що сприяє формуванню компетентностей цифрової безпеки у здобувачів освіти, готуючи їх до викликів у сучасному цифровому середовищі.

Зроблено висновок про те, що вивчення цифрової безпеки є дуже актуальним у сучасному світі, оскільки швидкий розвиток технологій призводить до зростання кількості цифрових загроз та кіберзлочинів. Здобуття навичок цифрової безпеки дозволяє особам захищати свою особисту інформацію в Інтернеті, уникати шахрайства та утримувати конфіденційні дані в безпеці. З ростом цифрової інфраструктури важливість кіберзахисту стає ключовою для забезпечення національної безпеки та уникнення кібератак на критичну інфраструктуру, що забезпечує зростання попиту на фахівців із цифрової безпеки, які здатні виявляти, запобігати та вирішувати проблеми кібербезпеки на різних рівнях. Вивчення цифрової безпеки стає необхідною складовою освіти, оскільки воно допомагає підготувати людей до ефективного взаємодії з цифровим середовищем, зберігати конфіденційні дані, та реагувати на зростаючі кіберзагрози.

Список використаних джерел:

1. Мальцева, І., Черниш, Ю., Штонда, Р. Аналіз деяких кіберзагроз в умовах війни. Кібербезпека: освіта, наука, техніка: електронне фахове наукове видання, 2022, 4 (16), 37–44. DOI: <https://doi.org/10.28925/2663-4023.2022.16.3744>.
2. Мехед О. Б., Мехед Д. Б., Мірошник В.І. Інформаційно-методичне забезпечення професійної підготовки педагога до здійснення соціально-педагогічної діяльності. The 3 rd International scientific and practical conference —Modern research in world sciencel (June 12-14, 2022) SPC Sci-conf.com.ua, Lviv, Ukraine. 2022. С.971-975
3. Мехед О. Б., Мехед Д. Б., Мехед К. М. Використання інформаційно-комунікаційних технологій при здійсненні соціально-педагогічної діяльності. Вісник Національного університету «Чернігівський колегіум» імені Т. Г. Шевченка. Вип. 14–15 (170–171). Чернігів : НУЧК, 2021. С. 27-31
4. Олексюк В.П., Олексюк О.Р. Стан сформованості компетентностей з інформаційної безпеки майбутніх учителів інформатики. Інформаційні технології і засоби навчання, 2017, 62(6), 277–291. DOI: <https://doi.org/10.33407/itlt.v62i6.1906>.
5. Опис рамки цифрової компетентності для громадян України. (2021). URL: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/3/mintsifra-oprilyudnyue-ramku-tsifrovoi-kompetentnosti-dlya-gromadyan/%D0%9E%D0%A0%20%D0%A6%D0%9A.pdf.
6. Петренко, Л.М. Цифрова безпека в професійній діяльності майбутніх викладачів педагогічних закладів вищої освіти: нормативно-правовий аспект. Вісник післядипломної освіти. Серія «Педагогічні науки», 2023, 24 (53), 138-152. DOI [https://doi.org/10.58442/2218-7650-2023-24\(53\)-138-152](https://doi.org/10.58442/2218-7650-2023-24(53)-138-152).
7. Швидкий А. Л., Мехед Д. Б., Мехед О. Б. Особливості впровадження інформаційних технологій у навчальний процес (психологічний аспект). Збірник наукових праць. Педагогічні науки. Випуск 61. Херсон : ХДУ, 2012. С. 401-406