ЦИФРОВА БЕЗПЕКА МАЙБУТНІХ ПЕДАГОГІВ ПРОФЕСІЙНОГО НАВЧАННЯ

Близнюк М. М.
доктор педагогічних наук, професор, професор кафедри професійної освіти, дизайну та безпеки життєдіяльності
Полтавський національний педагогічний університет імені В.Г. Короленка

В умовах пандемії та повномасштабного вторгнення росії в Україну, освітяни змушені були перевести свою діяльність у онлайн формат. Проте представники освітянської спільноти мають дуже різні рівні сформованості цифрових знань, умінь та навичок. Однією з найслабших сторін у них є саме розуміння та дотримання базових правил цифрової безпеки, що є надважливою складовою цифрової компетентності освітян. Особливої уваги звертаємо до даного питання у процесі підготовки майбутніх педагогів професійного навчання.

Цифрова безпека сьогодні є наріжним каменем нашого життя. Адже цифрові застосунки, платформи, гаджети оточують нас в усіх сферах і кількість цифрових небезпек, на жаль, невпинно збільшується. Звичайно, це стосується і сфери освіти.

Варто зазначити, що виклики цифрової безпеки були актуальні в освіті вже досить давно [1-2]. Більше того, ще взимку 2019-2020 р.р. уряд України запровадив спеціальну державну платформу цифрової освіти «Дія: Цифрова освіта» як частину плану цифрової трансформації країни. Справжні виклики постали у березні 2020 року, коли ми остаточно поринули у пандемію COVID-19. Як тільки ситуація почала відносно нормалізуватись і світ намагався оговтатися від наслідків пандемії, в українських реаліях, вторгнення росії в Україну знову змусило освітян перейти в онлайн, де окрім викликів фізичної небезпеки додалось чимало викликів цифрової безпеки (шахрайства з гуманітарною допомогою, кібератаки з метою поширення паніки та неправдивої інформації, шкідливе програмне забезпечення для відслідковування переміщення цивільних та військових осіб, фішинг тощо).

Саме тому, у різноманітних дослідженнях автори звертають увагу на декілька основних правил, що допоможуть створити безпечне та надійне освітнє середовище під час організації та проведення навчального процесу. Так М. Попадюк [3] зазначає базові правила цифрової безпеки для освітян:

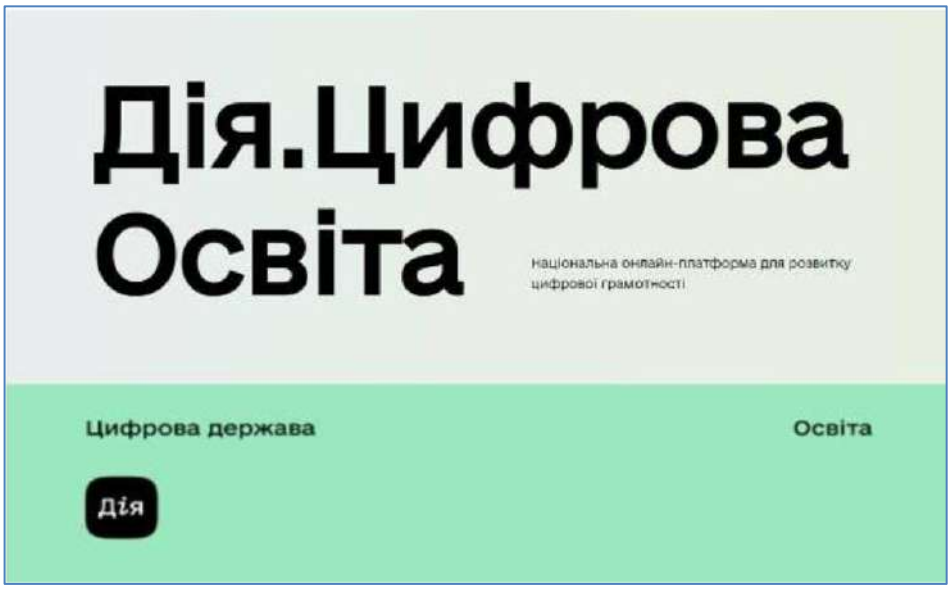

Рис. Державна платформа цифрової освіти «Дія: Цифрова освіта»

1. Не забувайте чому це для вас важливо

На жаль, не всі викладачі та студенти змогли бути однаково готовими до викликів дистанційного та змішаного форматів навчання. Причини такої ситуації справді різні, проте володіння базовими цифровими навичками, що потрібно для безпечної діяльності в Інтернеті, сьогодні є не просто чудовим доповненням для користувача, а справжньою необхідністю.

Окрім суспільної актуальності ми знаходимо основу у нормативно-правовій базі, зокрема Державні професійні й освітні стандарти передбачають володіння фахівцями поміж інших і «інформаційно-цифровими компетентностями», що включають здатності до здійснення пошуку в інформаційному просторі, критичного оцінювання інформації, ефективне використання і створення цифрових ресурсів та здатність використовувати їх в освітньому процесі. До того ж наскрізні змістові лінії у навчальних програмах передбачають формування громадянської відповідальності і у сфері використання цифрових технологій. При цьому в освітній процес також стійко впроваджується Рамка цифрових компетентностей для громадян DigComp (версії 2.1 та 2.2) та підходи до цифрового громадянства.

2. Дбайте про вибір перевірених освітніх платформ

Під час планування дистанційного та змішаного форматів навчання рекомендується уділити окрему увагу вибору безпечних онлайн-платформ призначення завдань студентам, організації відеоконференцій та обміну повідомленнями. Варто переконатися, що платформа, якою ви користуватиметесь захищена від доступу неавторизованими користувачами (як от, Google Classroom або Microsoft Teams), а доступ до онлайн-класів не є

публічним, а може відбуватися виключно під вашим контролем, наприклад, лише за електронною поштою. Що стосується відеоконференцій, то використовуються ті платформи, що пропонують наскрізне шифрування комунікації (Google Meet, Zoom, Microsoft Teams). Не доречно розміщувати посилання та коди доступу до зустрічей у публічному просторі. Окрема увага на навчальні платформи чи застосунки, що можуть бути доповненням до занять, застосовуватися під час та після них. Тут у нагоді може стати перелік дистанційних платформ для навчання, саморозвитку та отримання допомоги і перевіреної інформації розроблений Міністерством освіти на науки України.

3. Захищайте свої пристрої

Значну роль у створенні безпечного освітнього середовища відіграє вибір та захист пристроїв якими ми користуємось. Це стосується як робочих персональних комп'ютерів, ноутбуків, так і персональних пристроїв, таких як планшети та мобільні телефони. Часто освітяни не достатньо піклуються убезпеченням своїх девайсів та гаджетів аргументуючи це тим, що втрата чи витік освітньої інформації «не нестиме ніякої загрози». Проте це далеко не так, доступ шахраїв до облікових записів навчального закладу, може нести за собою небезпеку витоку персональних даних учнів та подеколи створювати навіть фізичну небезпеку для них.

Для уникнення цих ризиків потрібно встановлювати перевірене антивірусне програмне забезпечення та відповідні брандмауери. Слід пам'ятати, що зловмисники не втомлюються шукати нові шляхи отримання незаконного доступу до тих чи інших даних, тому, будь-які системи безпеки будуть ефективними лише тоді, коли регулярно оновлювати як програмне забезпечення самого пристрою, так і застосунків, якими користуємося. Зазвичай, оновлення відбувається автоматично та безкоштовно, проте деколи потребує погодження, як от у Play Market або App Store. Також ніколи не завантажується на власні пристрої неперевірені програми, навіть якщо здається, що потенційна користь перевищує потенційні ризики.

4. Дбайте про свою поведінку та цифровий слід у віртуальному середовищі

Чи часто ви замислювались над тим, скільки інформації про вас розміщено в Інтернеті? Спробуйте пошукати інформацію про себе і ймовірно ви дізнаєтесь щось, чого не планували розміщувати. Але це лише зовнішній вимір, адже інтернет збирає чимало інформації про нашу поведінку в інтернеті - що ми шукаємо, читаємо, дивимось, зберігаємо тощо. Таким чином вибудовується цифровий портрет користувача, який згодом використовується для створення персоналізованої реклами та оголошень.

Крім цього для дотримання безпечної поведінки необхідно:

– використовувати надійні та складні паролі (за можливості скористайтесь менеджером паролів);
– вмикайте двофакторну аутентифікацію, де це можливо;
– звертайте увагу, які дозволи ви надаєте застосункам чи сайтам, якою інформацією ділитесь;
– шифруйте дані;
– робіть резервні копії даних;
– обережно користуйтесь публічними Wi-Fi та точками доступу, захистіть домашню мережу надійним паролем та увімкніть шифрування WPA2;
– свідомо поширюйте персональну інформацію.

5. Навчайте правил цифрової безпеки співробітників

У теперішніх умовах одним з наскрізних елементів освітнього та виховного процесу стає формування інформаційно-цифрових компетентностей. Саме тому викладачеві потрібно не лише своїм прикладом показувати як безпечно поводитись в цифровому середовищі, але і втілювати підходи «Про-через-Для» під час навчання:

– розповідайте в чому актуальність дотримання правил цифрової безпеки. Чому важливо уникати підозрілих посилань, використовувати антивіруси, встановлювати надійні паролі, перевіряти безпечність посилань та електронних листів тощо (Про);

– створюйте безпечне навчальне середовище, налагоджуйте ефективні процеси обміну інформацією, моделюйте практичні ситуації та ризики на основі яких можна було б підвищити рівень своїх компетентностей (Через);

– мотивуйте студентів до реалізації проєктів у сфері цифрової безпеки, які б мультиплікували знання та досвід серед ширшої аудиторії. Мотивуйте їх дотримуватись правил цифрової безпеки у побутовому житті, з ровесниками, батьками для формування широкого безпечного суспільного простору (Для).

Дуже важливо також звертати увагу на поведінку слухачів в інтернеті та спілкуватися з ними у випадку підозрілих активностей.

Цифрова безпека – це комплекс заходів, спрямованих на захист конфіденційності, цілісності та доступності інформації від вірусних атак і несанкціонованого втручання. Основні рекомендації щодо цього:

- *сильні паролі*. Використовувати унікальні та складні паролі для всіх онлайн-акаунтів. Паролі повинні містити комбінацію літер (у верхньому та нижньому регістрах), цифр та спеціальних символів. Уникати використання особистих інформаційних даних у паролях;

- *багатофакторна аутентифікація.* Увімкнути багатофакторну аутентифікацію (МФА) для онлайн-акаунтів, де це можливо. МФА додає додатковий рівень захисту, вимагаючи не лише пароль, але й додатковий код перевірки або пристрій для входу в обліковий запис;
- *оновлення програмного забезпечення.* Регулярно оновлювати операційні системи та програмне забезпечення на всіх пристроях. Оновлення часто містять виправлення вразливостей та забезпечують захист від нових загроз;
- *безпечне підключення до мережі.* Уникати використання відкритих та ненадійних Wi-Fi мереж. При підключенні до відкритої мережі, використовувати віртуальну приватну мережу (VPN), щоб зашифрувати дані та забезпечити конфіденційність;
- *обережність в інтернеті.* Бути обережними при відкриванні посилань в електронних листах, повідомленнях та на незнайомих веб-сайтах. Уникати завантаження та встановлення програм з ненадійних джерел;
- *антивірусне програмне забезпечення.* Встановити надійне антивірусне програмне забезпечення на пристрої та регулярно його оновлювати. Антивірус допомагає виявляти та блокувати шкідливі програми;
- *захист конфіденційної інформації.* Бути обережним з розкриттям особистої та фінансової інформації в онлайн-середовищі. Уникати надсилання конфіденційних даних через незахищені канали зв'язку;
- *освіта та поінформованість.* Постійно дізнаватися про нові загрози та методи захисту. Бути уважним до цифрової безпеки та навчати колег про базові принципи цифрової безпеки.

Крім цих основних принципів, існує багато інших заходів та практик, які можуть бути застосовані для захисту цифрової інформації користувачів [4]. Важливо постійно стежити за новими загрозами та бути пильним в онлайн-середовищі.

Підсумовуючи, можемо наголосити, що дотримання базових правил цифрової безпеки підвищуватиме рівень громадянських та професійних компетентностей освітян. А в умовах того, що цифрова безпека сьогодні стала ключовим компонентом дистанційного та змішаного навчання, для викладачів та вчителів неймовірно важливо залишатися в курсі актуальних заходів безпеки та ділитись досвідом зі своїми учнями та їх батьками. При цьому, розуміння важливості заходів безпеки, піклування про надійні та перевірені онлайн-платформи, захист своїх пристроїв, свідома поведінка в Інтернеті є запорукою становлення ефективного та безпечного освітнього процесу.

Список використаних джерел

1. Біленчук П.Д., Близнюк М.М., Кобилянський О.Л., Ковальчук Ю.І. та

ін. Е-суспільство: цифрове майбутнє України: монографія : за ред. проф. П.Д. Біленчука. Київ: УкрДГРІ, 2018. 216 с.

2. Близнюк М.М., Дебре О.С. Цифрова безпека освітнього процесу: європейський поступ Естонії та перспективи України. *Наукові записки Бердянського державного педагогічного університету. Серія : Педагогічні науки* : зб. наук. пр. Вип.1. Бердянськ : БДПУ, 2022. С.65-77.

3. Попадюк М. Базові правила цифрової безпеки для освітян. *GURT Resource Center*. Apr 28, 2023. URL: https://ua.hive-mind.community/blog/375,bazovi-pravila-cifrovoyi-bezpeki-dlya-osvityan

4. Nataliia Nahorna, Nataliia Orlova, Pavlo Kuzmenko, Maryna Kondratenko, Oleksandr Sotnychok, Mykola Blyzniuk, Valentyna Tsyna. Digitalization of project, technological, and design activities in the process of training future teachers of labor education and technology. *Brazilian Journal of Education, Technology and Society* (BRAJETS). Vol. 16 No. se2: The Global Development of Innovative Technologies and their Impact on the Education P.20-29, 2023. DOI: https://doi.org/10.14571/brajets.v16.nse2.20-29.

ЗАСТОСУВАННЯ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ ПРИ ВИВЧЕННІ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ЦИВІЛЬНИЙ ЗАХИСТ» У ВИЩОМУ НАВЧАЛЬНОМУ ЗАКЛАДІ

Титаренко В. М.

кандидат педагогічних наук, доцент, доцент кафедри професійної освіти, дизайну та безпеки життєдіяльності Полтавського національного педагогічного університету

У XXI столітті людство всього світу опановує нову стадію свого розвитку–інформаційну, яка характеризується виникненням та впровадженням нових сучасних технологій.

Усі країни сучасного світу, особливо розвинені країни, розробляють та впроваджують ці технології у систему освіти.

В України впровадження сучасних інформаційних технологій набирає масштабних обсягів. Здобувачі вищої освіти сьогодні надають великого значення інтерактивним технологіям, які за твердженнями професорсько-викладацького складу закладів вищої освіти підвищують рівень успішного виконання завдань та покращення якості навчання.

Досвід практичної роботи у закладі вищої освіти переконує у тому, що вони повинні не тільки володіти сучасними інформаційними та комп'ютерними