

5. Онаць О. М. Зміст суб'єктної партнерської взаємодії у реалізації державно-громадського управління закладами освіти Проблеми сучасного підручника: навчально-методичне забезпечення освітнього процесу в умовах воєнного часу: збірник тез доповідей / [ред. кол.; голов. ред. – О.М. Топузов]. [Електронне видання] – Київ : Педагогічна думка, 2023. – С.53-56 https://undip.org.ua/wp-content/uploads/2023/12/PSP_tezy_2023-1.pdf

УДК 373.3/.5.09:004.056.5

0009-0009-6211-1412

Володимир Савельєв,

*доктор історичних наук, професор,
професор кафедри соціальної філософії,
філософії освіти і освітньої політики
Українського державного університету*

ім. М. Драгоманова

0000-0002-3359-340X

Вадим Абизов,

*кандидат політичних наук,
доцент, завідувач кафедри управління
та адміністрування*

*Донецького обласного інституту
післядипломної педагогічної освіти*

0000-0002-1039-2963

Яна Бобилева,

*кандидат педагогічних наук, доцент,
доцент кафедри управління та адміністрування
Донецького обласного інституту
післядипломної педагогічної освіти*

ОСНОВНІ ПРОБЛЕМИ ОРГАНІЗАЦІЇ КІБЕРБЕЗПЕКИ ОСВІТНЬОГО ПРОЦЕСУ В ЗАКЛАДІ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ

У сучасному цифровому світі, де технології швидко розвиваються, кібербезпека стає все більш актуальною темою.

Особливо важливо організувати кібербезпеку освітнього процесу, оскільки школи та інші заклади освіти працюють з великою кількістю цифрових даних та інформації. Однак організація кібербезпеки в освітньому процесі може стикатися з низкою проблем, які потребують уваги та вирішення, що знайшло відображення в Законі України «Про основні засади забезпечення кібербезпеки України» [1].

20 грудня 2002 р. Генеральною Асамблеєю ООН була прийнята резолюція 57/239 «Елементи для створення глобальної культури кібербезпеки», якою визначено дев'ять основоположних взаємодоповнювальних елементів, що формують глобальну культуру кібербезпеки: поінформованість; відповідальність; реагування; етика; демократія; оцінка ризику; проектування та впровадження засобів забезпечення безпеки; управління забезпеченням безпеки; переоцінка. Тобто змістове тло кібербезпеки складається з технологічних, організаційних, соціальних та культурних складників. Як було відзначено в матеріалах міжнародних форумів у Давосі (2011–2019 рр.), особливо актуальною стає проблема кібербезпеки, яка стосується майже всіх сфер життя та діяльності людини, особливо в умовах повної інформатизації освіти [2].

Існує кілька причин, чому кібербезпека не отримує достатньої уваги у навчальних програмах ЗЗСО. Насамперед це відсутність усвідомлення проблеми: багато шкіл та педагогічних працівників не мають достатнього усвідомлення потенційної загрози від онлайн-середовища та не розуміють необхідності включення кібербезпеки до навчальних програм. Відсутність ресурсів: школи можуть мати обмежені фінансові ресурси, що ускладнює впровадження курсів з кібербезпеки та придбання необхідного обладнання та програмного забезпечення. Відсутність підготовленості вчителів: навчання кібербезпеці вимагає наявності кваліфікованих учителів, які мають достатні знання та навички у цій сфері. Однак не всі школи можуть мати таких учителів.

Недостатня увага до кібербезпеки у навчальних програмах середніх шкіл може мати серйозні наслідки. Передусім це виток конфіденційної інформації: якщо учні не навчаються захищати свої особисті дані та інформацію, це може призвести до її

витоку та використання зловмисниками.

Кібератаки: без належного навчання з кібербезпеки учні можуть стати жертвами кібератак, таких як фішинг, віруси та зловмисне програмне забезпечення. Відсутність цифрової грамотності: абсолютна невідповідність до життя в сучасному суспільстві, позиція жертви в стосунках у мережі.

Щоб покращити вивчення кібербезпеки у середній школі, необхідно вжити такі заходи: включити кібербезпеку до основних предметів, тобто кібербезпека повинна бути включена до освітньої програми. Це дозволить учням отримати базові знання з кібербезпеки, незалежно від їх спеціалізації. Створити спеціалізовані курси: школи можуть упровадити спеціалізовані курси з кібербезпеки, де учні матимуть можливість більш детально вивчити цю тему. Ці курси можуть бути включені до вибіркового предмету, щоб учні мали можливість обрати їх залежно від своїх інтересів. Підготувати вчителів: навчання кібербезпеки вимагає наявності кваліфікованих учителів. Школи повинні забезпечити підготовку вчителів у цій сфері, або запрошувати фахівців із кібербезпеки для проведення спеціальних занять із запровадженням практичних завдань.

Для забезпечення безпеки своєї цифрової інфраструктури українські школи повинні впроваджувати комплексні заходи з кібербезпеки. Ці заходи включають:

Безпеку мережі: упровадження брандмауерів, систем виявлення вторгнень та безпечних Wi-Fi мереж для захисту від несанкціонованого доступу та порушень безпеки даних.

Шифрування даних: шифрування конфіденційних даних для запобігання несанкціонованому доступу та забезпечення конфіденційності особистої інформації.

Аутентифікацію користувачів: упровадження суворих політик створення паролів, багатофакторної аутентифікації та контролю доступу користувачів для запобігання несанкціонованому доступу до системи.

Освіту користувачів: проведення навчання та інформаційних кампаній для учнів, учителів та батьків з питань кібербезпеки, щоб підвищити рівень свідомості та знань про безпеку в Інтернеті.

Резервне копіювання даних: регулярне створення резервних копій даних для запобігання втраті інформації в разі кібератаки

або технічної несправності.

Нове покоління, яке вже народжується у цифрову епоху, виростає, навчається і працює, використовуючи різноманітні гаджети, що є частиною мережі. Це стає їхнім звичним середовищем. Їхнє життя формується під впливом цифрового простору, який має свої старі та нові загрози. Значної важливості набувають когнітивні фактори, такі як інтерфейс, контент, моделі поведінки. З'являються нові проблеми, пов'язані з життям і діяльністю у цифровому просторі, відповідні фактори впливу, способи їх уникнення та відповідні нові засоби та інструменти. Тому виникає необхідність обговорення філософії проблеми кібербезпеки.

Одним із філософських аспектів кібербезпеки є питання етичності та відповідальності. Українська школа повинна вчити учнів важливості етичного поведіння у цифровому просторі. Вони повинні розуміти, що їхні дії в Інтернеті мають вплив на інших людей, і що вони несуть відповідальність за свої вчинки в цьому середовищі. Важливо навчати учнів поважати приватність інших, уникати кібербулінгу та інших форм цифрового насильства.

Також філософський підхід до кібербезпеки може включати роздуми про роль технологій у нашому житті. Це може стосуватися питання про вплив технологій на наші моральні цінності, самоідентифікацію та взаємодію з іншими людьми. Українська школа може пропонувати учням філософські дискусії про те, як технології впливають на наше сприйняття світу, наші стосунки та нашу культуру загалом.

Крім того, філософський підхід до кібербезпеки може спонукати до роздумів про етичні аспекти використання штучного інтелекту та автоматизованих систем. Як ми можемо забезпечити справедливість та недискримінацію при використанні таких систем? Як ми можемо зберегти людську автономію та контроль у цифровому світі?

Для успішного реагування на кіберзагрози треба проводити тренінгові підготовки для учнів, педагогів та батьків з врахуванням того, що в умовах війни можливі часті кіберінциденти в закладах освіти зокрема. Треба вчитися виживанню в сучасній мережі за допомогою правил кібергігієни.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України: Закон України <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (date of access: 11.11.2023).
2. Національний інститут стратегічних досліджень. «Підсумки Всесвітнього економічного форуму в Давосі в контексті удосконалення процесів глобального управління: висновки для України». <https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosini/pidsumki-vsesvitnogo-ekonomichnogo-forumu-v-davosi-v-konteksti> (date of access: 11.11.2023).

УДК 373.3/.5.018.43:004.8

0000-0002-3359-340X

Вадим Абизов,

*кандидат політичних наук,
доцент, завідувач кафедри управління
та адміністрування
Донецького обласного інституту
післядипломної педагогічної освіти
0000-0002-1039-2963*

Яна Бобилева,

*кандидат педагогічних наук, доцент,
доцент кафедри управління та адміністрування
Донецького обласного інституту
післядипломної педагогічної освіти*

ПЕРСПЕКТИВИ ТА ОБМЕЖЕННЯ ВВЕДЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОСВІТНЮ ПРОГРАМУ ЗЗСО

З появою магічних функцій ChatGPT, Google Bard, Midjourney, Canva тощо штучний інтелект (ШІ) швидко стає невід'ємною частиною нашого повсякденного життя, трансформуючи галузі та змінюючи те, як ми працюємо, навчаємося та спілкуємося. Цей швидкий технологічний прогрес підкреслює важливість включення освіти зі штучним інтелектом у навчальну програму не лише для того, щоб усі учні шкіл були