**Тетяна Шевченко**

**(Суми, Україна)**

**СТРАТЕГІЯ ЗАХИСТУ ІНФОРМАЦІЇ В ЦИФРОВОМУ ОСВІТНЬОМУ СЕРЕДОВИЩІ**

Високотехнологічна цифрова ера сьогодні вимагає від педагогів розв’язання таких завдань, як створення відкритого, технологічно, педагогічно наповненого та спрямованого на освітні пріоритети навчального середовища, де є суб’єкти спілкування, навчання, професійної діяльності та обміну досвідом мають одне спільне освітнє коло. Цифровізація (диджиталізація) освіти передбачає формування у учасників освітнього процесу навичок з цифрової грамотності, використанні інтерактивних методів навчання та іннших факторів. від. Створення такого середовища можливе при залученні всіх суб’єктів освітнього процесу за умови встановлення чітких орієнтирів, системного та цілісного усвідомлення завдань, що ставить суспільство перед своїми громадянами та відповідних професійних компетентностей вчителів.

Основні шляхи використання інформаційних технологій в освіті полягають у: створенні інформаційних середовищ закладів освіти, педагогічних програмних продуктів, створенні вебсайтів закладів освіти, розробці дистанційних курсів, використанні ІТ в управлінні закладом освіти, створенні електронних бібліотек, медіатек, та ін., виділяються позитивні та негативні дидактичні ІТ-можливості.

До позитивних відносять:

* індивідуалізацію та диференціацію навчання;
* ущільнення навчальної інформації;
* забезпечення зв’язку теорії та практики, управління пізнавальною діяльністю та формування творчих якостей та загальної культури мислення тих, хто навчається;
* створення умов для самореалізації;
* особистості, формування і розвиток інформаційної культури і розв'язування задач медіа-освіти та ін..

До негативних:

* відчуття ізоляції з боку тих, хто навчається;
* неможливість допомоги при вивченні гуманітарних дисциплін, до яких не можна застосувати формальні правила і процедури (філософія, релігія, соціологія і т.д.) та ін. .

Інформаційно-цифрове середовище закладу освіти є частиною єдиного інформаційного простору. Його слід розглядати, як системно організовану сукупність інформаційного, технічного, навчально-методичного забезпечення, спрямованих на організацію взаємодії усіх учасників навчального процесу, а також на здійснення навчально-виховних впливів, що підтримуються цифровими засобами збору та передачі даних, апаратно-програмним та навчально-методичним забезпеченням.

Інформаційний простір складається з таких головних компонентів:

- інформаційні ресурси, що містять дані, відомості та знання, зафіксовані на відповідних носіях інформації;

- організаційні структури, що забезпечують функціонування та розвиток єдиного інформаційного простору, зокрема, збір, обробку, зберігання, розповсюдження, пошук і передачу інформації;

- засоби інформаційної взаємодії громадян і організацій, що забезпечують їм доступ до інформаційних ресурсів на основі відповідних інформаційних технологій, які включають програмно-технічні засоби і організаційно-нормативні документи.

Види інформаційних ресурсів, якими можуть обмінюватися об'єкти системи: текстова, графічна інформація, бази даних, програми, аудіо-відеоінформація, а саме:

* більш широке використання цифрових технологій для викладання і навчання;
* формування і розвиток відповідних цифрових компетентностей та навичок цифрової трансформації;
* покращення освіти аналізуючи і оцінюючи стан освітніх інституцій з подальшим прогнозування їх перспективного розвитку.

Особлива увагу надається опануванню і розвитку цифрових навичок, цифровій грамотності для різних вікових категорій, сучасним підходам до навчання з використанням онлайн ресурсів, навчальних матеріалів, використанню масових відкритих онлайн курсів.

Можна зазначити наступні тематики, пов’язані з цифровим світом: дезінформація; штучний інтелект (ШІ), пов’язані з даними навички та обробки даних кожного аспекту життя; нові технології, зокрема віртуальна реальність, соціальна робототехніка, Інтернет речей; навички «зелені ІКТ» та ін. Сприяння створенню високоефективної цифрової освітньої екосистеми.

Підняття рівня цифрових навичок та компетентностей для цифрової ери залежить від:

* інфраструктура, підключення та цифрове обладнання;
* ефективне планування та розвиток цифрового потенціалу включаючи ефективні та сучасні організаційні можливості;
* компетентний у цифровому плані та впевнений у собі викладач та освітній та навчальний персонал;
* високоякісний контент, зручні інструменти та безпечні платформи дотримання приватних прав та етичних стандартів.

Використання педагогом ІКТ, здатність оперувати цифровими засобами

для здійснення професійної діяльності та власного професійного зростання безпосередньо пов’язане з виявом його громадянської позиції та ставлення до загальнолюдських цінностей у освітньому просторі та інформаційно-освітньому середовищі зокрема.

Цифрове середовище є важливою частиною сучасного світу, воно надає можливість обмінюватися інформацією, створювати та зберігати дані, виконувати різноманітні завдання та спілкуватися з іншими людьми у віртуальному просторі.

Цифрове середовище також може включати такі технології, як штучний інтелект, віртуальна реальність, розширена реальність і блокчейн. Однак, цифрове середовище також має недоліки, які можуть призвести до серйозних проблем, таких як кібербезпека, конфіденційність даних, цифрова нерівність і залежність від технологій.

Базові правила безпеки в цифровому середовищі:

Використовувати унікальні та складні паролі для всіх своїх облікових записів і пристроїв. Намагайтеся регулярно змінювати паролі; Активувати двофакторну аутентифікацію, де це можливо зробити, це забезпечить додатковий рівень захисту, оскільки окрім пароля буде потрібно підтвердження через SMS-повідомлення або спеціальний мобільний додаток; не відкривати підозрілі посилання або файли, які можуть пошкодити пристрій або викрасти дані; встановлювати надійне антивірусне програмне забезпечення, що допоможе виявити та заблокувати потенційно шкідливі файли та посилання; використовувати службу перевірки безпеки URL, яка допоможе визначити, чи є посилання безпечним; не повідомляйти свої особисті дані, паролі та коди на сумнівних веб-сайтах або через незахищені мережі Wi-Fi; захищайте свої файли та документи за допомогою резервного копіювання; оновлюйте програмне забезпечення, операційні системи, браузери та інші програми на своєму пристрої.

Оновлення часто включають патчі безпеки, які закривають вразливості і зменшують ризик атак.

Встановлюйте програми лише з офіційних сайтів. Зазвичай такі повідомлення містять заклики відправити дані, наприклад, PIN-код картки; 16 цифр, що вказані на картці; термін дії картки, CVV-код. У цьому випадку необхідно зв’язатися з банком за офіційною електронною адресою або офіційним номером телефону для з’ясування ситуації. Остерігайтеся сайтів-двійників Візуально сторінка виглядає як справжня: вона має таку саму кольорову гаму та містить приблизно таку ж інформацію, що й офіційний сайт, але гіперпосилання містять зайві літери чи цифри. Зробивши покупку або вказавши власні персональні дані на сайті-двійнику, можна попасти у пастку шахраїв. Персональні дані використовуються проти корстувача, необхідно переконатися, що це офіційний веб-сайт.

Висновки: Цифрове середовище в сучасном усвіті є надзвичайно важливим і поширеним. Інтернет, соціальні мережі, мобільні пристрої та інші цифрові технології використовуються людьми всіх вікових категорій та в різних сферах життя. Однак, разом з перевагами, які ці технології надають, існує також ризик для безпеки та конфіденційності користувачів. Якщо дотримуватися базових правил безпеки в цифровому середовищі можна захистити себе та свої дані.

**Література**

1. Про основні засади забезпечення кібербезпеки України, Закон України від 05.10.2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

2. В. Ю. Биков, О. Ю. Буров, Н. П. Дементієвська. Кібербезпека в цифровому навчальному середовищі. Інформаційні технології і засоби навчання, 2019, Том 70, №2, С. 313 – 331.

3. Основні правила кібергігієни. URL: <https://erepublic.org.ua/news/osnovnipravilakibergigiyeni/>

4. Кибербезопасность с человеческим лицом: как донести проблему до каждого. URL: <https://trends.rbc.ru/trends/industry/5fa460199a7947a946d4b37e>

5. Основні правила захистуданих — кібергігієна для активного Інтернет-користувача. URL: <https://eset.ua/ua/blog/view/38/osnovnyye-pravila-zashchity-dannykh-kibergigiyenadlyaaktivnogo-Internet-polzovatelya>