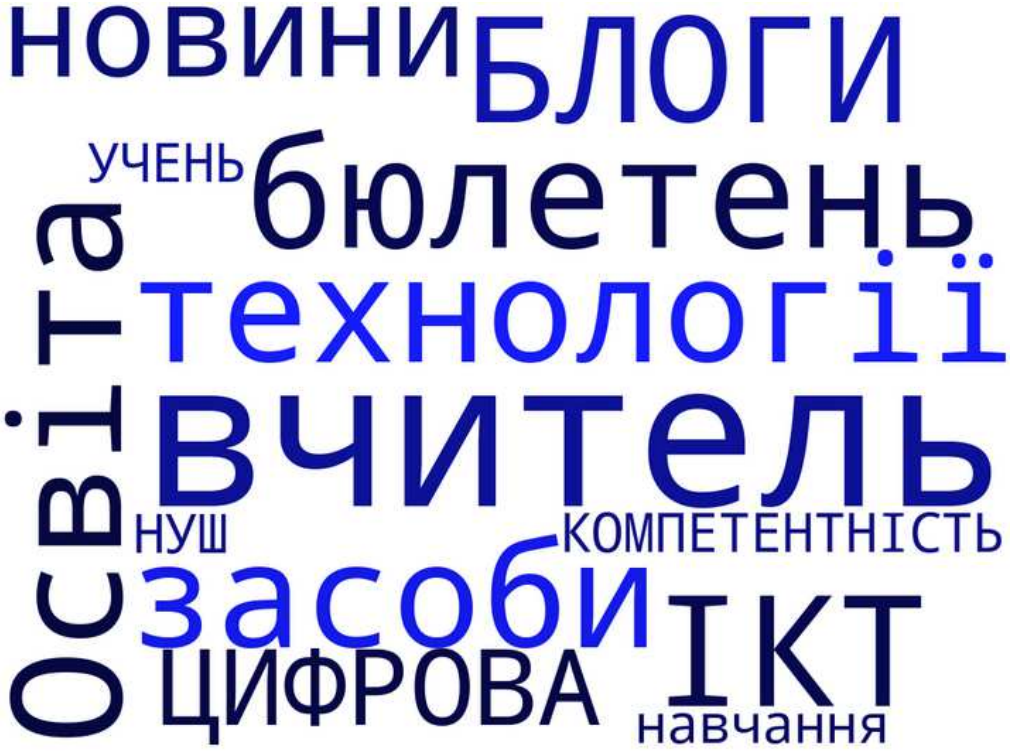
ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І ЗАСОБІВ НАВЧАННЯ НАПН УКРАЇНИ

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ОСВІТНЬОМУ ПРОЦЕСІ: МІЖНАРОДНІ ТЕНДЕНЦІЇ

ЗБІРНИК ІНФОРМАЦІЙНИХ МАТЕРІАЛІВ



КИЇВ – 2019

УДК 373.5(4):008-022.218:004
Автори: *Овчарук О.В., Малицька І.Д., Іванюк І.В., Гриценчук О.О., Кравчина О.Є., Сороко Н.В.*

Загальна редакція: *Овчарук О.В., канд.пед.наук, ст. наук співр.*
Укладач: *Гриценчук О.О., наук співр.*
Схвалено рішенням Вченої ради Інституту інформаційних технологій і засобів навчання НАПН України (Протокол № 10 від 28 листопада 2019 р.)

Використання сучасних інформаційних технологій у освітньому процесі: міжнародні тенденції. Збірник інформаційних матеріалів : [Овчарук О.В., Малицька І.Д., Іванюк І.В., Гриценчук О.О., Кравчина О.Є., Сороко Н.В.]. – К.: ІІТЗН НАПН України - 2019. – (40) с.

Збірник інформаційних матеріалів «Використання сучасних інформаційних технологій у освітньому процесі: міжнародні тенденції» укладено в рамках здійснення НДР «Розвиток інформаційно-комунікаційної компетентності вчителів в умовах хмаро орієнтованого навчального середовища» (реєстраційний № 0117U000198). Збірник містить добірку новітніх зарубіжних напрямів використання ІКТ у освітньому процесі зарубіжжя, прикладів педагогічних практик, що застосовуються при підготовці та підвищенні кваліфікації вчителів різних предметів. Може бути використаний в системі післядипломної педагогічної освіти та закладами, що здійснюють підвищення кваліфікації вчителів та методистів в системі ЗНЗ.

ЗМІСТ

І Н Ф О Р М А Ц І Й Н И Й Б Ю Л Е Т Е Н Ь
№ 1 , 2019

ЕЛЕКТРОННІ ОСВІТНІ РЕСУРСИ ДЛЯ РОЗВИТКУ ЦИФРОВОЇ КОМПЕТЕНТНОСТІ ВЧИТЕЛІВ У СКАНДИНАВСЬКИХ КРАЇНАХ (НОРВЕГІЯ, ФІНЛЯНДІЯ)

У рамках впровадження сучасної вітчизняної освітньої реформи «Нова українська школа» важливим напрямом роботи є розвиток інформаційно-цифрової компетентності вчителів. Важливо розглянути та врахувати досвід впровадження сучасних освітніх реформ в європейських та скандинавських країнах на рівні створення практичних електронних освітніх ресурсів та інструментів для розвитку та оцінювання рівня цифрової компетентності вчителів.

Керівники закладів загальної середньої освіти (ЗЗСО) Норвегії можуть використовувати електронні освітні ресурси, запропоновані Норвезьким Центром ІКТ в освіті, щоб розробити власну стратегію використання ІКТ для своєї установи. Наприклад:

«ІКТ у практиці» (https://iktipraksis.iktsenteret.no/) – це портал, який заохочує вчителів до обміну ресурсами та практичними розробками;

«Національна цифрова навчальна арена» (https://ndla.no/) пропонує навчальні ресурси з основних навчальних предметів у ЗЗСО, які доступні всім. Ресурси публікуються під рубрикою «Спільна творчість», а викладачам пропонується доповнювати та розвивати їх;

«Шкільні карти» (https://kartiskolen.no) – безкоштовний сервіс, який пропонує оновлені норвезькі карти з багатьох державних і дослідницьких установ, а також дані, адаптовані для ЗЗСО. Сервіс включає в себе базові карти, тематичні карти та готові плани уроків, які використовують актуальні дані. Міністерство освіти в 2006 році підписало угоду з національним проектом географічних даних «Цифрова

Норвегія», в який входить близько 600 партнерів, щодо надання географічних даних, що використовуються в шкільних картах;

«Ovttas» (http://ovttas.no) – це освітній портал на трьох саамських і норвезькій мовах, який надає повний і доступний огляд ресурсів для навчання саамів. Портал містить зображення, книги, фільми, аудіофайли та статті на теми, пов'язані з навчанням, а також педагогічні поради. Це ресурс для співробітників дитячих садків і вчителів. Портал був розроблений у співпраці з Парламентом Саамі.

Національні наукові центри відіграють ключову роль у розвитку якості освіти в певних галузях, таких як математика, природничі науки, читання та іноземні мови. Центри пропонують електронні освітні ресурси у вільному доступі, наприклад:

•*ресурси з природознавства для вчителя*, розроблені Норвезьким центром науки в освіті (доступні норвезькою мовою) http://naturfag.no;

•*ресурси в галузі науки для 8-12 класі*в, розроблені Норвезьким центром для наукової освіти (доступні різними мовами) http://viten.no;

•*ресурси з іноземних мов*, розроблені Норвезьким національним центром іноземних мов в освіті (доступні різними мовами) http://www.fremmedspraksenteret.no;

•*веб-сайт для учнів та вчителів* ЗЗСО, який пропонує різні односерійні та багатосерійні фільми. Кожна серія з відповідними завданнями, ресурсами та оглядом поточних цілей щодо формування відповідної компетентності (доступно норвезькою мовою, деякі фільми та серіали доступні англійською мовою) http://kraftskolen.no;

•*ресурси з читання*, розроблені Норвезьким центром освітнього читання та дослідження (доступно англійською мовою) http://www.lesesenteret.no;

•*ресурси з математики*, розроблені Норвезьким центром математичної освіти (доступні англійською мовою) http://www.matematikksenteret.no.

Навчальні ресурси на паперовому носієві все ще широко використовуються вчителями норвезьких ЗЗСО, але видавці та інші компанії, що розвиваються, все частіше розробляють он-лайн навчальні матеріали та програми. Основні постачальники електронного навчального контенту спільно відкрили Інтернетмагазин Brettboka.no, щоб сприяти використанню електронних книг та

полегшити процедуру закупівлі. Електронна навчальна продукція норвезьких освітніх компаній вже має понад 40 мільйонів користувачів по всьому світу.

У Фінляндії за розроблення електронного навчального контенту також в основному відповідають комерційні видавництва. Великі компанії виробляють як традиційні книги, так і цифрові матеріали. Нові невеликі видавничі компанії спеціалізуються лише на цифровій продукції.

Навчальні платформи вибираються місцевими провайдерами освіти. Найбільш поширеними є: Pedanet, Moodle, Optima, Its learning, Claned. На сьогоднішній день цифрові навчальні матеріали безпосередньо пов'язані з навчальними платформами через інтерфейси. Це дозволяє гнучко переносити дані навчального матеріалу на навчальну платформу, і навпаки. На додаток до цього багато нових платформ цифрових навчальних матеріалів включають інструменти для оцінки, спілкування та зворотного зв'язку тощо. Наведемо приклади трьох навчальних платформ.

Linkkiapaja (https://linkkiapaja.edu.fi) – це національний відкритий портал для обміну навчальними ресурсами. Він містить відібрані навчальні матеріали для викладання та навчання. Linkkiapaja підтримується Фінською національною агенцією з освіти.

Finna (https://finna.fi) – це сучасна платформа для збирання навчальних матеріалів щодо музеїв та музейних архівів.

Edustore (https://edustore.fi) – це торговий центр і канал розповсюдження комерційних електронних навчальних матеріалів серед фінських муніципалітетів. Edustore має комерційні цифрові навчальні матеріали від 29-ти видавців.

Розглянемо основні напрями розвитку та електронні освітні ресурси для розвитку цифрової компетентності вчителів, які використовуються у Фінляндії.

Створення нових навчальних просторів. Наприклад, *«Oppimaisema»* (https://oppimaisema.fi/) – портал, який демонструє приклади оформлення сучасних навчальних просторів, враховуючи архітектуру будівлі закладу освіти.

Впровадження ініціатив із застосування обчислень, кодування, обчислювального мислення. Наприклад, *«Innokas»* (http://www.innokas.fi/en) – національна мережа для просування робототехніки, кодування та використання ІКТ в освіті фінансується Національним агентством освіти Фінляндії. Мережа «Innokas»

спрямовує та заохочує вчителів, адміністраторів закладів освіти й інших зацікавлених сторін бути творчими та інноваційними за допомогою наявних ІКТ.

Тести на основі використання ІКТ для вчителів щодо перевірки рівня цифрової компетентності. Асоціація дослідників з соціології освіти розробила *Сервіс тестування цифрової компетентності для вчителів* (https://rosa.utu.fi/taitotesti/). Наприкінці тесту вчителі отримують особисте портфоліо компетентності відповідно до своєї діяльності. Організація (ЗЗСО, муніципальне управління закладів освіти тощо) отримує звіт про своїх співробітників. Тести представлені лише фінською мовою.

Національні інструменти самооцінки/робочі рамки для вчителів щодо визначення рівня цифрової компетентності *«Opeka»* розроблені Тамперевським дослідницьким центром інформації та медіа для керівників ЗЗСО (http://ropeka.fi/en), вчителів (http://opeka.fi/en), учнів (http://oppika.fi/). «Opeka» - це онлайн інструмент для вчителів і керівництва ЗЗСО для вимірювання та аналізу рівня використання ІКТ в освітньому процесі. Він надає вчителям, адміністраторам ЗЗСО та місцевій владі інформаційні дані для порівняння рівня використання ІКТ з іншими вчителями, ЗЗСО на національному рівні. Opeka пропонує: зворотній зв’язок для вчителя; аналіз ситуації у вигляді звіту та рекомендації про те, як розвивати використання ІКТ у школі далі; підтримку щодо складання плану використання ІКТ; можливість відслідковувати та оцінювати результати подальшого розвитку. Онлайн інструмент використовується для оцінювання того, як вчителі використовують ІКТ, наскільки забезпечено ІКТ середовище та культуру використання ІКТ у ЗЗСО.

З одного боку, «Opeka» базується на 4-х рівневій класифікації цифрової компетентності. Наприклад, вчитель має відповісти на чотири блоки питань:

• цифрове середовище на роботі (наприклад: наявність ІКТ обладнання та мережного з'єднання; який з наведених у переліку пристроїв роботодавець надає для особистого користування вчителя тощо);

• організаційна культура (наприклад, використання ІКТ у робочому співтоваристві; професійний розвиток тощо);

• педагогічна діяльність (наприклад, особисте використання ІКТ у сфері освіти; думаючи про типовий навчальний тиждень, як часто вчитель використовує ІКТ (комп'ютери та програмне забезпечення); використання ІКТ учнями; практики оцінювання; набуття навичок медіа-освіти; використання ІКТ у ЗЗСО тощо);

• компетентності (цифровий зміст та навчальні середовища; безпечна та відповідальна діяльність; медіа навички тощо).

Іншою основою для «Орека» є «Національний план розвитку ІКТ для навчання», відповідно до якого суб'єкти освітнього процесу отримують певні рекомендації. Для вчителів онлайн інструмент пропонує можливість скласти список особистісних цифрових навичок та готовності використовувати комп`ютерно орієнтоване навчальне середовище у ЗЗСО; планувати особистий розвиток через використання ІКТ у навчанні; впливати на культуру викладання та навчання в ЗЗСО; порівняти власні вміння використання ІКТ з рівнем вміння інших вчителів. Для адміністраторів школи «Орека» пропонує: звіт про актуальні потреби ЗЗСО; погляд на готовність ЗЗСО до використання новітніх ІКТ в цілому; статистику та аналіз потреб у навчанні та підвищенні кваліфікації вчителів; підтримку планового розвитку використання ІКТ, середовища ІКТ та культури викладання й навчання у ЗЗСО; порівняння з іншими ЗЗСО на муніципальному та національному рівнях; щорічну оцінку успіху реалізації плану з використання ІКТ; освітні інновації для розвитку ІКТ у ЗЗСО. Для освітніх відділів муніципальної влади «Орека» пропонує: звіти та сучасний аналіз щодо готовності ЗЗСО до використання ІКТ; інформацію для планування використання ІКТ у муніципалітетах; щорічну оцінка розвитку та реалізації планів щодо використання ІКТ на рівні районів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Іванюк І. В. Формування цифрової компетентності вчителів Фінляндії у світлі сучасних освітніх реформ [Електронний ресурс] / І. В. Іванюк // Звітна наукова конференція Інституту інформаційних технологій і засобів навчання НАПН України: Збірник матеріалів наукової конференції. – Київ : ІІТЗН НАПН України, 2018. – с. 94 – 95. – Режим доступу: http://lib.iitta.gov.ua/711730/

2. Іванюк І. В. Формування цифрової компетентності вчителів та учнів у скандинавських країнах / І. В. Іванюк // Педагогіка і психологія. Вісник НАПН України. – 2019. – №1 (102). – с.69 – 77

Матеріал підготувала: Іванюк І.В.

І Н Ф О Р М А Ц І Й Н И Й Б Ю Л Е Т Е Н Ь
№ 2 , 2019

БЕЗПЕКА ВИКОРИСТАННЯ ХМАРНИХ СЕРВІСІВ В ОСВІТІ

Впровадження та вдосконалення інформаційних технологій займає важливе місце серед численних інноваційних напрямків розвитку навчання і освіти в цілому. Розробляється безліч інформаційних сервісів, які вчитель може впроваджувати і ефективно використовувати в навчальному процесі та для свого професійного розвитку. Одним з перспективних напрямків розвитку сучасних інформаційних технологій є хмарні технології, які роблять доступним освітній контент для студентів, школярів і вчителів, служать для зберігання і синхронізації файлів, управлінням навчальним процесом, зберігання закладок і заміток; керування часом тощо. Проте "хмара" часто прихована за програмами, такими як "платформа для навчання" або "інформаційна платформа" (наприклад bettermarks [1] або SchulCommSy [2]) .

Такі IT-послуги пропонують та експлуатуються компаніями, що мають офіси у Німеччині, в ЄС або за межами Європи. У рідкісних випадках такі сервіси використовуються державними органами (наприклад, шкільними радами, школами чи іншими установами). Багато шкіл користуються такими хмарними сервісами, але не займаються питаннями захисту даних, можливо, це пов'язано з тим, що технічні

аспекти такого хмарного сервісу невідомі. Але захист інформації є дуже важливим, оскільки використовуються особисті дані учнів та вчителів, навчальні матеріали та результати навчання, всі ці дані автоматично обробляються за допомогою хмарного сервісу. Необхідно відмітити, що використання хмарних сервісів в освітньому процесі мають ряд переваг, серед яких:

- можливість доступу до даних з будь-якого комп'ютера, що має вихід в Інтернет;
- можливість організації спільної роботи з даними різних учасників навчального процесу;
- висока ймовірність збереження даних навіть у разі апаратних збоїв;
- освітні організації мають можливість безкоштовно використовувати хмарні сервіси;
- немає необхідності займатися придбанням, підтримкою та обслуговуванням власної інфраструктури зі зберігання даних, що, в кінцевому рахунку, зменшує загальні витрати;
- процедури з резервування та збереження даних виробляються провайдером «хмарного» центру, яка не втягує в цей процес користувача цих послуг.

Важливим фактором є те, що в призначених для користувача угодах хмарних сервісів ніколи не містяться зобов'язання щодо збереження конфіденційності і цілісності даних. Користувачам цих послуг слід пам’ятати про необхідність забезпечувати весь комплекс вимог по обробці та захисту персональних даних, що не завжди реалізується в хмарі. Основні ключові загрози хмарної безпеки за версією Cloud Security Alliance [5] (CSA - некомерційна організація, лідер в області стандартів, рекомендацій та ініціатив, спрямованих на підвищення безпеки і захищеності використання хмарних обчислень), з якими стикаються ті чи інші організації, що використовують хмарні сервіси, а саме:

1. витік даних - через велику кількість даних, які переносяться в хмари, майданчики хмарних хостинг провайдерів стають привабливою метою для зловмисників (серйозність потенційних загроз безпосередньо залежить від важливості і значимості даних, що зберігаються), а втрата

цих даних завдає значної шкоди репутації окремо взятої компанії;

2. компрометація (доступ сторонньої особи до інформації) облікових записів і обхід аутентифікації (процедура перевірки справжності) – витік даних найчастіше є результатом недбалого ставлення до механізмів організації перевірки автентичності, коли використовуються слабкі паролі, а управління ключами шифрування і сертифікатами відбувається неналежним чином (наприклад, коли кінцевим користувачам призначаються значно більші повноваження, ніж в дійсності необхідно або коли користувач переводиться на іншу позицію або звільняється, але при цьому не змінюється повноваження згідно з новими ролями);
3. зламування інтерфейсів та API - від того, наскільки добре відпрацьовані механізми контролю доступу, шифрування в API, залежить безпека і доступність хмарних сервісів (при взаємодії з третьою стороною, що використовує власні інтерфейси API, ризики значно зростають, оскільки виникає необхідність надавати додаткову інформацію, таку як, логін та пароль користувача);
4. вразливість використовуваних систем - проблема, яка трапляється в хмарних середовищах (елемент архітектури програмного забезпечення, де єдиний екземпляр додатку, запущеного на сервері, обслуговує безліч організацій-клієнтів «орендарів») та вирішується за допомогою регулярного сканування на виявлення вразливостей, застосування останніх патчів і швидкої реакції на повідомлення щодо загрози безпеці;
5. викрадення облікових записів - сервісні акаунти і облікові записи користувачів необхідно контролювати, детально відстежуючи виконувані транзакції (група логічно об'єднаних послідовних операцій по роботі з даними, що обробляється або скасовується повністю);
6. інсайдери-зловмисники - інсайдерська загроза може виходити від нинішніх або колишніх співробітників, системних адміністраторів, підрядників або партнерів по бізнесу (у випадку з хмарою зловмисники можуть повністю або частково зруйнувати інфраструктуру, отримати

доступ до даних);

7. цільові кібератаки – це напад хакерів на обраний об’єкт, що призводить до втрати та розкриття цінної інформації;
8. перманентна втрата даних - хмарні хостинг провайдери для дотримання заходів безпеки рекомендують відокремлювати призначені для користувача дані від даних додатків, зберігаючи їх в різних локаціях, а також не варто забувати про ефективні методи резервного копіювання на зовнішні альтернативні захищені майданчики;
9. недостатня обізнаність - коли команда розробників з боку клієнта недостатньо знайома з особливостями хмарних технологій і принципами розгортання хмарних додатків, виникають операційні та архітектурні проблеми;
10. зловживання хмарними сервісами - хмари можуть використовуватися легітимними і нелегітимними організаціями, а метою останніх є використання хмарних ресурсів для здійснення зловмисних дій: запуску DDoS-атак, відправки спаму, поширення шкідливого контенту тощо;
11. DDoS-атаки - в результаті DoS-атак може сильно сповільнитися або зовсім припинитися робота значущих для споживача послуг сервісів;
12. спільні технології, загальні ризики – постачальники хмарних послуг надають віртуальну інфраструктуру, хмарні додатки, але якщо на одному з рівнів виникає вразливість, вона впливає на все оточення.

Дебра Литлджон Шиндер (Debra Littlejohn Shinder), яка є авторкою низки книг з комп'ютерних операційних систем, мереж та безпеки, у своїй статті "П'ять способів захистити себе в багатофункціональному, багато платформеному світі" [3] та Філіп Шауманн (Philipp Schaumann), спеціаліст з інформаційних технологій та інформаційної безпеки, викладач в Дунайському університеті в Кремсі та Університеті прикладних наук Хагенберг, в статті «Як захистити себе при використанні хмарних сервісів?» [4] надають поради щодо захисту своїх даних та інформації у віртуальному просторі. Ось деякі з них:

1. Захист паролем – задайте унікальний та надійний пароль для кожного сервісу та

включайте дворівневу автентифікацію (процедура перевірки автентичності) всюди, де це можливо (ім'я користувача плюс пароль або PIN-код як і раніше є найбільш поширеним способом, за допомогою якого ми автентифікуємо себе системами, мережами, сайтами та службами). Зловмисник може отримати доступ до вашого пароля різними способами: шкідливі програми, ключі для реєстрації даних, груба сила, соціальна інженерія.

2. ***Налаштування пристрою*** – є безліч різних обчислювальних пристроїв, різних операційних систем та різних версій ОС, неможливо включити кожен з них. Ось деякі загальні поради щодо захисту мобільних пристроїв: виберіть модель свого мобільного пристрою з урахуванням безпеки та дізнайтеся, які пристрої підтримують віддалене стирання, шифрування файлів, двохфакторну автентифікацію та інші функції безпеки; тримайте свої пристрої під контролем та не залишайте їх без уваги на "хвилину" на конференціях або ділових зустрічах, не позичайте їх іншим без вашого прямого нагляду; захистіть свої дані у разі крадіжки пристрою, на ноутбуках увімкніть програми BitLocker або інші програми шифрування, на планшетах і смартфонах, увімкніть захист пароля / PIN-коду; якщо ваш пристрій пропонує двофакторну автентифікацію, наприклад, відбиток пальців або розпізнавання обличчя, використовуйте її, встановіть програму відстеження та блокування мобільних пристроїв, увімкніть можливості віддаленого стирання, регулярно створюйте резервну копію даних на вашому комп'ютері. Вимкніть мережі та послуги, які вам не потрібні (wi-fi, bluetooth, інфрачервоний зв'язок, мобільні мережі, обмін файлами). Якщо у вас ввімкнено Bluetooth, встановіть його в нерозпізнаний режим. Встановіть доступ до електронної пошти до зашифрованого з'єднання. Переконайтеся, що на пристроях Android вимкнено налагодження USB. Переконайтеся, що резервне копіювання iPhone налаштовано на зашифроване. Встановіть PIN-код на SIM-карті, щоб його не можна було використовувати на іншому пристрої.

3. ***Бездротова служба безпеки.*** Ретельно оцініть дані, які ви помістили в хмарі. Не зберігайте там дуже цінні дані. Не зберігайте там *єдину* копію ваших даних, робіть резервне копіювання. Ретельно оцінюйте постачальників хмар, які ви вирішили

використовувати. Попередньо ознайомтеся з опублікованими гарантіями та безпекою надання послуг: шифрування даних, яка інформація зберігається на серверах, ознайомтеся з їх умовами обслуговування та політикою конфіденційності. Зрозумійте, що жодна хмарна служба (і, звичайно, не безкоштовне хмарне сервісне обслуговування) не надає вам повної гарантії щодо безпеки ваших даних.

4. ***Загальне анти-шкідливе ПЗ***

1. Це категорія з порадами щодо захисту ваших пристроїв від багатьох типів атак, які поширені на сьогодні:
2. завжди застосовуйте оновлення програмного забезпечення якомога швидше та запустіть антивірусне і анти шпигунське програмне забезпечення;
3. необхідно бути обережними при встановленні нових програм, попередньо ознайомтеся з відгуками, прочитайте інформацію про те де і як вони використовуються та не дозволяйте програмам автоматично оновлюватися, якщо ви не впевнені, що довіряєте розробнику програми;
4. необхідно бути обережними щодо відвідування невідомих веб-сайтів, які можуть приховано завантажувати шкідливе програмне забезпечення на ваш пристрій;
5. використовуйте захищені версії (https) веб-сайтів, коли ви маєте такий варіант;
6. використовуйте ті самі запобіжні заходи, коли читаєте на своєму телефоні чи планшеті, а також на своєму комп'ютері (не відкривайте вкладення), і пам'ятайте, що текстові повідомлення SMS також можуть передавати шкідливе програмне забезпечення;
7. якщо ви користуєтеся мобільним зв'язком для використання свого ноутбука чи планшета для підключення передачі даних 3G / 4G на своєму телефоні, не підключайтесь до точки доступу та обов'язково використовуйте WPA2, щоб захистити свою мережу Wi-Fi.

5. Планування особистого відновлення пошкоджень. Це означає, що ви можете дистанційно відстежувати, блокувати та / або видаляти дані на своїх мобільних пристроях, вибираючи безпечне та надійне програмне забезпечення.

Відповідно освітні установи та особисто вчителі мають розумітися на захисті, як своїх персональних даних, так і даних учнів та їх батьків, мають дотримуватися різних правил захисту даних. Так освітяни мають знати про законодавчі акти щодо захисту персональних даних; бажано офіційно укладати договір з постачальником обраного, для роботи хмарного сервісу; перевіряти в якій державі знаходиться провайдер та в яких місцях розташовані сервери; перевірити чи схвалене держорганами освіти, використання відповідного хмарного сервісу.

Варто зазначити що хмарні сховища мають безліч недоліків, але в той же час і не меншу кількість переваг. Потрібно чи ні довіряти свої персональні дані «хмарам» - це особисте питання для кожного користувача, але компанії, що надають дані послуги, з кожним роком намагаються збільшити безпеку своїх сховищ та зацікавлені в нових користувачах, а ті, в свою чергу, потребують конфіденційності, тому ступінь захисту персональних даних буде тільки збільшуватися.

Список використаних джерел

1. Bettermarks URL: https://de.bettermarks.com/ (дата звернення: 24.12.2018).
2. Schul Comm Sy Schleswig-Holstein URL: https://schulintern.sh.schulcommsy.de/ (дата звернення: 24.12.2018).
3. Five ways to protect yourself in a multi-device, multi-platform world URL: http://www.techrepublic.com/blog/security/five-ways-to-protect-yourself-in-a-multi-device-multi-platform-world/8233 (дата звернення: 24.12.2018).
4. Wie schützt man sich bei der Nutzung von Cloud-Diensten? URL: https://sicherheitskultur.at/Cloud_Security.htm (дата звернення: 24.12.2018).
5. Cloud Security Alliance URL: https://www.networkworld.com/article/3042610/security/the-dirty-dozen-12-cloud-security-threats.html (дата звернення: 24.12.2018).

Матеріал підготувала: Кравчина О.Є.

АКТУАЛЬНІ ТЕМИ МІЖНАРОДНИХ МАСОВИХ ВІДКРИТИХ ОН-ЛАЙН КУРСІВ ДЛЯ РОЗВИТКУ ІНФОРМАЦІЙНО-ЦИФРОВОЇ КОМПЕТЕНТНОСТІ ВЧИТЕЛЯ (2019)

Стрімкий розвиток інформаційно-комунікаційних технологій та проблема їх впровадження у загальні заклади освіти для підвищення якості результату навчально-виховного процесу суттєво впливає на вимоги до професійних компетентностей вчителів, зокрема інформаційно-цифрової. З огляду на це виникла проблема щодо постійного підвищення кваліфікації вчителів та створення відповідних курсів, що відповідатимуть викликам освіти. Згідно з цим актуальності набувають Масові відкриті он-лайн курси (англ. Massive open online course, MOOC).

Слід відмітити, MOOC у межах проекту European Schoolnet (europeanschoolnetacademy.eu). Вони включають в себе теоретичні та дидактичні матеріали, відео-лекції, вебінари, інструкції з практичного використання ІКТ у професійній діяльності вчителів та ін. Кожен такий курс передбачає надання його учасникам сертифікату. Модуль кожного курсу розрахований на тиждень, його можна пройти у будь-який зручний для учасника час, але до вказаної дати його завершення.

Наприклад, у 2019 році тьюторами MOOC у межах проекту European Schoolnet було запропоновано такі курси: «Навчання ІКТ із запитом» (англ. Teaching ICT with Inquiry), «Тиждень коду Європейського Союзу» (англ. EU Code Week – Deep Dive MOOC), «Мережний вчитель – викладання в 21 столітті» (англ. The Networked Teacher – Teaching in the 21st Century), «Ігри в школі» (англ. Games in Schools).

Курс «Навчання ІКТ із запитом» (рис.1), тобто відповідно до запитів освіти, проходив з 9 вересня 2019 року по 17 жовтня 2019 р. Метою цього курсу було розвиток вмінь і навичок вчителів щодо впровадження STEM–підходу (англ.

Science, Technology, Engineering and Maths, STEM) у навчально-виховний процес школи за допомогою ІКТ. Наприкінці цього курсу учасники створювали власну педагогічну діяльність (урок, навчальний проект та ін.) на основі запитів щодо використання ІКТ та STEM-підходу, згідно з інтересами певної аудиторії навчання та їхніх потреб (від початкової школи до випускних класів).

Рис. 1. Логотип курсу «Навчання ІКТ із запитом»

На курсі пропонувалося використовувати Екосистему Go-Lab (рис. 2), що надає можливості:

- учням проводити експерименти в он-лайн лабораторіях з предметів STEM, брати участь у навчальних проектах;

- вчителям створювати та підбирати дидактичні матеріли для викладання своїх предметів із використанням STEM–підходу, ділитися своїм педагогічним досвідом.

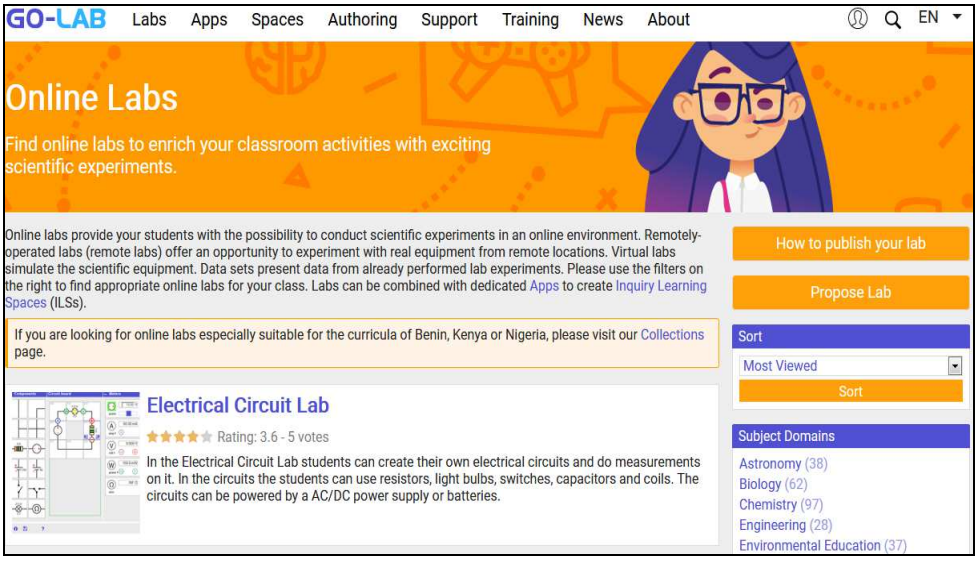


Рис.2. Екосистема Go-Lab (https://www.golabz.eu/)

Курс «Тиждень коду Європейського Союзу» (рис.3) проходив з16 вересня 2019 р. по 31 жовтня 2019 р. Його результатом мав стати план тижня коду в закладі освіти.

Рис. 3. Логотип курсу «Тиждень коду Європейського Союзу»

Тьютори курсу спеціально створили сайт Code Week 4 All challenge, на якому вчителі, після проходження курсу, завантажують плани заходів, відео, поради та інші матеріали для проведення тижня коду.

У курсі вчителі отримали ідеї, безкоштовні навчальні матеріали, плани уроків та дидактичні ресурси, метою яких є допомога вчителям запровадити підхід обчислювального/алгоритмічного мислення при викладанні своїх навчальних дисциплін. Наприкінці роботи у курсі учасники організовували заходи щодо запровадження тижня коду зі своїми учнями і колегами. Ці заходи зареєструвалися на карті тижня коду ЄС.

Курс «Мережний вчитель – викладання в 21 столітті» (рис. 4) проходив з 14 жовтня 2019 р. по 20 листопада 2019 р. Мета курсу: розвивати педагогічну інформаційно-цифрову компетентність вчителя, вивчаючи спільні та активні підходи до викладання та навчання за допомогою ІКТ, спілкуючись з викладачами-колегами з різних країн Європи, щоб ділитися ідеями та будувати свою майбутню мережу професійного навчання.

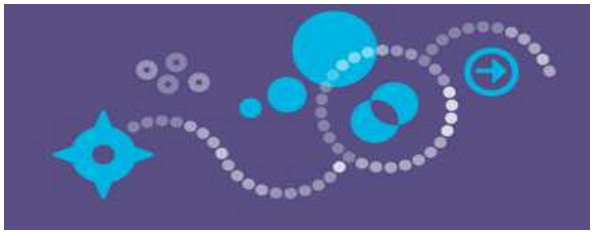


Рис. 4. Логотип курсу «Мережний вчитель – викладання в 21 столітті»

Курс «Ігри в школі» (рис. 5) проходив з 14 жовтня 2019 р. по 5 грудня 2019 р. Мета курсу: навчити вчителів використовувати цифрові ігри як інструменти для навчання у школі для викладання різних навчальних дисциплін.

Рис. 5. Логотип курсу «Ігри в школі»

Вчителі обговорювали поняття ігровий метод навчання, його актуальність та потенційні можливості, проблеми, що пов'язані з навчанням на основі ігор.

Серед ігор, що пропонувалися тьюторами курсу, були такі:

- мовні додатки та ігри: Duolingo, fluentU, Babbel, Bravolol, Mindsnacks, Elegy, Myst, Riven (sequel to Myst);
- додатки та ігри для руху: Just Dance 2019, Run Keeper, FitBit, Google Fit, Zombies, Run!, Harry Potter Wizzards Unite, Pokémon Go, Geocaching;
- додатки та ігри для когнітивного розвитку: Dr Kawashima's Brain Training, Mangahigh, Peak Brain Training, Elevate, Lumosity, Fit Brains, Cognito, Sudoku;
- ігри та додатки для імітації (англ. Simulation): Roller Coaster Tycoon Adventures, Farming Simulator 19, Train Simulator, Flight Simulator X, Forestry 2019 – The simulation, Football Manager 2019, Total War: Rome II, Universe Sandbox, Stop Disasters!

Наприкінці роботи у курсі учасники створювали навчальні заходи, що включали елементи ігор для мотивації учнів щодо навчання та оцінювання їхньої навчальної діяльності

Отже, масові відкриті он-лайн курси – це можливість:

- обміну позитивним педагогічним досвідом між учителями всього світу;
- навчання впродовж життя;
- підвищення кваліфікації без відриву від роботи;
- розвитку інформаційно-цифрової компетентності;

- отримання даних щодо нових технологій, педагогічних підходів, актуальних проблем освіти та ін.

Матеріал підготувала: Сороко Н.В.

І Н Ф О Р М А Ц І Й Н И Й Б Ю Л Е Т Е Н Ь
№ 4 , 2019

РОЗВИТОК ІК-КОМПЕТЕНТНОСТІ ВЧИТЕЛЯ НОВОЇ УКРАЇНСЬКОЇ ШКОЛИ

Вчитель – це агент змін

Умотивований учитель - це вчитель, який має свободу творчості й розвивається професійно
(НУШ)

***«…завжди, коли починаєш зміни, є агенти змін, які підтримують; є ті, хто чинить опір; є ті, хто чекає і дивиться, до чого це все приведе. Але в нас немає часу і ресурсу боротися з тими, хто чинить опір. Наше завдання – підтримати тих агентів змін, які роблять, і разом з ними боротися за ту частину, яка визначається…»**, – П. Хобзей, 2019, з інтерв'ю https://osvita.ua/school/reform/58418/*

Розвиток цифрової компетентності вчителя є важливим питанням, що пов'язане з викликами сучасного інформаційного суспільства та швидкоплинними технічними й технологічними процесами.

Вчителі, як основні агенти змін у системі шкільної освіти, повинні йти в ногу з часом, швидко та ефективно реагувати на виклики XXI століття, бути здатними використовувати новітні цифрові засоби, вміти створювати відповідне середовище

для своїх учнів, знати шляхи та засоби безпечного поводження у мережі Інтернет та вміти захищати особисту інформацію у цифровому просторі.

У 2018 р. європейською спільнотою було розроблено рамку цифрової компетентності для освітян (DigCompEdu), що розроблена на основі концептуальної моделі і є науково обґрунтованою структурою, що детально описує компетентність вчителя у цифрових технологіях. Дана рамка спрямована на вчителів та викладачів на всіх рівнях освіти, від раннього дитинства до вищої освіти та освіти для дорослих, включаючи загальну та професійну освіту та навчання, освіту з особливими потребами та контексти неформального навчання. DigCompEdu детально описує 22 компетентності, організовані в шести галузях. Основна увага зосереджена не на технічних навичках, а на деталізацію того, як цифрові технології можуть бути використані для розвитку та використання інновацій у сфері освіти та навчання. Рамка DigCompEdu сприяє нещодавно ухваленій Європейською Комісією програмі підготовки кадрів для Європи межах програми «Європа 2020».

Цифрова компетентність включає в себе впевнене, критичне та відповідальне використання та взаємодію з цифровими технологіями для навчання, роботи та участі у суспільстві. Це включає в себе інформаційну грамотність та грамотність даних, комунікацію та співпрацю, створення цифрового контенту (включаючи програмування), безпеку (включаючи цифрове благополуччя та компетентності, пов'язані з кібербезпекою) та розв'язання проблем.

Рамка для освітян визначає цифрову компетентність, вміння використовувати цифрові технології для підтримки творчості, активного громадянства та соціальної інтеграції, співпраці з іншими людьми для досягнення особистих, соціальних або комерційних цілей. Вона включає цифрову та інформаційну грамотність, комунікацію та співпрацю, створення цифрового контенту (зокрема програмування), кібербезпеку та вирішення проблем.

Рис.1. Шість галузей цифрової компетентності вчителя (DigCompEdu)[2,4]

До поданих на Рис.1 шести галузей відносяться наступні:

- Професійна залученість, спрямована на використання професійного середовища, тобто використання педагогами цифрових технологій у професійній взаємодії з колегами, учнями, батьками та іншими зацікавленими особами та на власний індивідуальний професійний розвиток, а також на розвиток установи.
- Цифрові ресурси - необхідні для ефективного і відповідального використання та створення контенту, а також для обміну цифровими ресурсами для потреб навчання.
- Викладання та навчання – сфера, спрямована на управління та організацію цифрового використання технологій для потреб викладання та навчання.
- Оцінювання – галузь, що призначена для використання цифрових стратегій для підтримки процесів оцінювання.
- Розширення можливостей учнів - зосереджена на використанні потенціалу цифрових технологій для здійснення навчання учнів.
- Сприяння цифровій компетентності учнів - спрямована на розвиток таких професійних компетентностей, що сприяють формуванню цифрової компетентності учнів та студентів.

Ядро структури DigCompEdu визначається в межах сфер 2-5. Разом ці сфери пояснюють сутність цифрової педагогічної компетентності педагогів, тобто педагогам з цифровою компетентністю необхідно розвивати ефективні, інклюзивні

та інноваційні стратегії викладання та навчання. Галузі 1, 2 і 3 мають бути закріплені на етапах, характерних для будь-якого навчального процесу, незалежно від того, чи підтримуються вони ІКТ. Складові, які перераховані в цих сферах, детально описують, як необхідно здійснювати ефективне та інноваційне використання цифрових технологій при плануванні (галузь 2), реалізація навчання (галузь 3), оцінювання (галузь 4) викладання та навчання. Галузь 5 визначає потенціал цифрових технологій для здійснення стратегій навчання та навчання, орієнтованих на учнів. Ця галузь є трансверсальною (наскрізною) для інших галузей 2, 3 і 4, тобто вона містить керівні принципи, які стосуються складових інших галузей, а також доповнюють їх.

Рис.2. Поступ педагога у розвитку цифрової компетентності[3,4].

Запропонована модель є моделлю поступу цифрової компетентності педагога і має на меті допомогти педагогам зрозуміти їхні особисті сильні та слабкі сторони, описуючи різні етапи або рівні розвитку цифрової компетентності. Для зручності використання, ці етапи розвитку цифрової компетентності пов'язані з шістьма рівнями знань, які використовуються іншими спільними європейськими рамками. Слід зазначити, що етапи розвитку цифрової компетентності та їхня логіка розвитку

розроблені у відповідності таксономії Блума, що застосовано до пояснення когнітивних етапів прогресу у навчанні. Так, рівні розвиненості цифрової компетентності розподілені за принципом зростання від А1 до С2. (новачок, дослідник, інтегратор, експерт, лідер, піонер) (Рис.2).

Взаємодія з цифровими технологіями та змістом передбачає відкрите та перспективне ставлення до їхнього розвитку. Водночас це потребує критичного аналізу, обґрунтованості, надійності та впливу інформації і даних, які доступні через цифрові засоби, а також етичного, безпечного та відповідального підходу до використання цих інструментів педагогами.

Вчителі створюють, використовують та поширюють серед колег ресурси, які розвивають як фахові компетентності, так і цифрові навички та компетентність. Для прикладу, можна звернути увагу на подані нижче ресурси:

Рис. 3 Віртуальна школа ІКТ – дистанційний майданчик для навчання вчителів

Віртуальна школа ІКТ пропонує на постійні основі 10 дистанційних курсів за такими темами:

Курс1. Хмарні сервіси для навчання

Курс 2. Блог вчителя на **Blogger**

Курс 3. Персональний сайт вчителя на платформі **WIX**

Курс 4. Сервіси Web 2.0 – інструмент для творчості.

Курс 5. Використання Інтернету та хмарних технологій для дистанційного та перевернутого навчання. Віртуальна школа **Moodle**

Курс 6. Створення власних мультимедійних матеріалів

Курс 7. Застосування Office 365 в педагогічній діяльності

Курс 8. Сервіси Web 2.0 (частина 2)

Курс 9. Створення власного дистанційного курсу (за зразком Віртуальної школи ІКТ)

Курс 10. "Цифрові компетентності сучасного вчителя (стартовий курс)"

Реєстрацію на курси Віртуальної школи ІКТ відкрито постійно! http://i-math.com.ua/vsikt/sample-page/programa/

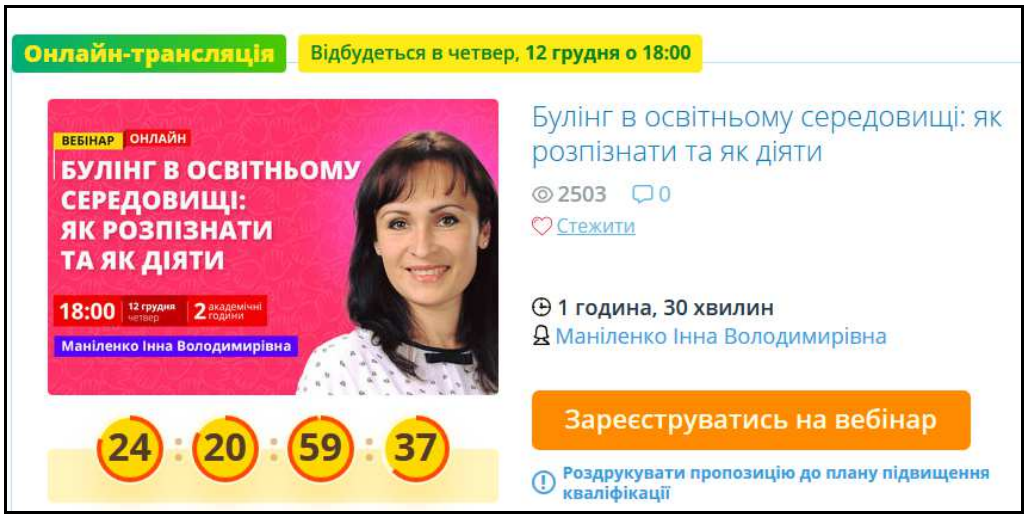


Рис.4. Портал «Всеосвіта»

Портал «Всеосвіта» є Всеукраїнським експериментом, затвердженим постановою КМУ № 800 від 21.08.2019 р., де вчителі можуть підвищувати кваліфікацію та отримати офіційний сертифікат. Пропонуються різноманітні курси для вчителів різних предметів,серед тематик «Цифрові практики Нової української школи: створення відео проекту», «Розроблення і використання цифрового освітнього контенту в освітньому процесі Нової української школи», «Розвиток цифрового інтелекту учителя: путівник по цифрових інструментах в ефективній організації і проведенні освітнього процесу» та ін.

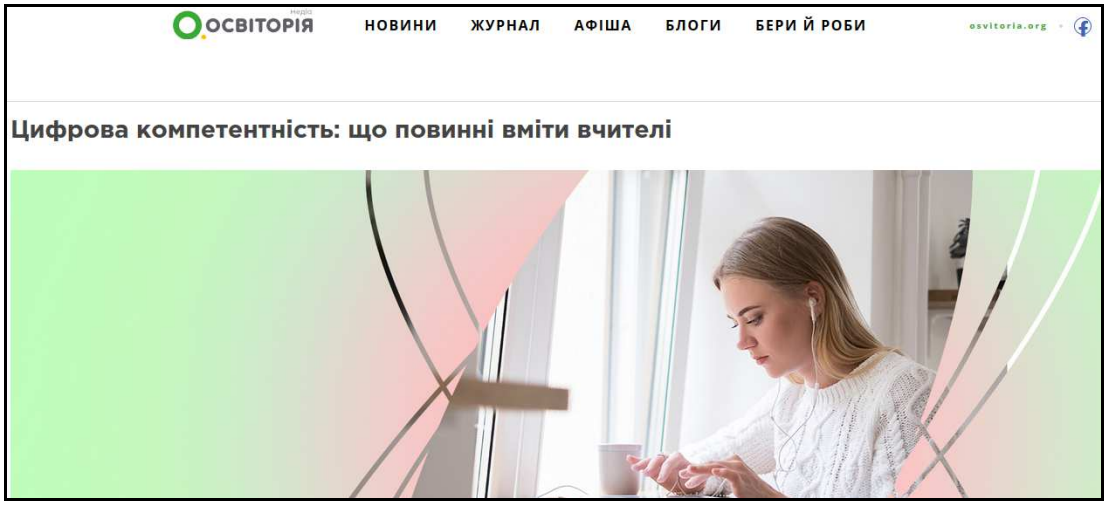


Рис.5. Освіторія. Потрал для вчителів.

«Освіторія» є блогом для вчителів, де розміщуються освітні новини, різноманітні матеріали, що можуть бути корисними для вчителя, серед яких: «Цифрова компетентність: що повинні вміти вчителі» - https://osvitoria.media/experience/tsyfrova-kompetentnist-shho-povynni-vmity-vchyteli/ та ін.

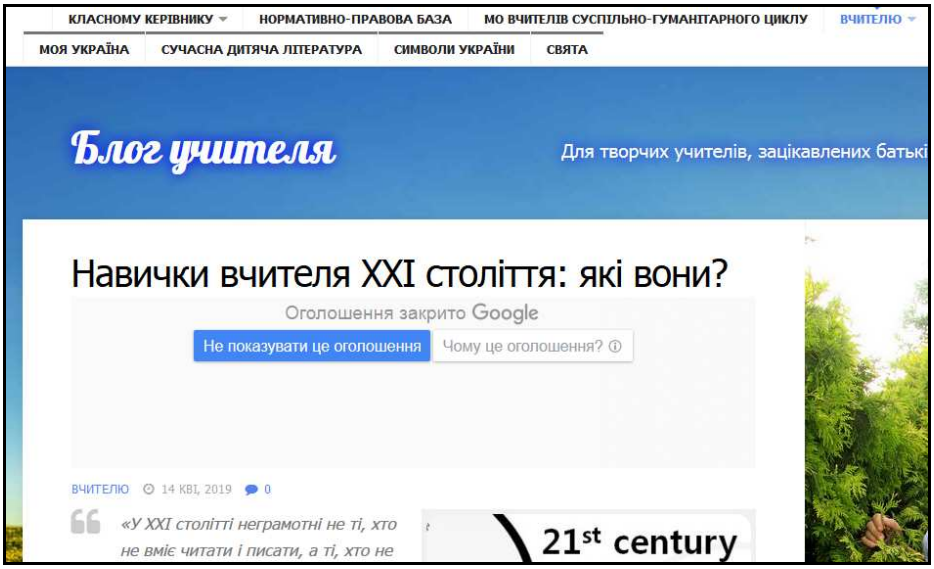


Рис.6 Блог вчителя «Навички XXI століття»

Блог вчителя «Навички XXI століття» є прикладом авторського блогу, який веде вчитель. Для вчителів пропонуються конспекти уроків, тести, презентації. Цікавими є вітруальні екскурсії, проекти та різноманітні заходи для учнів - https://uchilka.in.ua/.

Цікавим є ресурс, що призначений для вчителів, студентів та науковців Educators Technology».

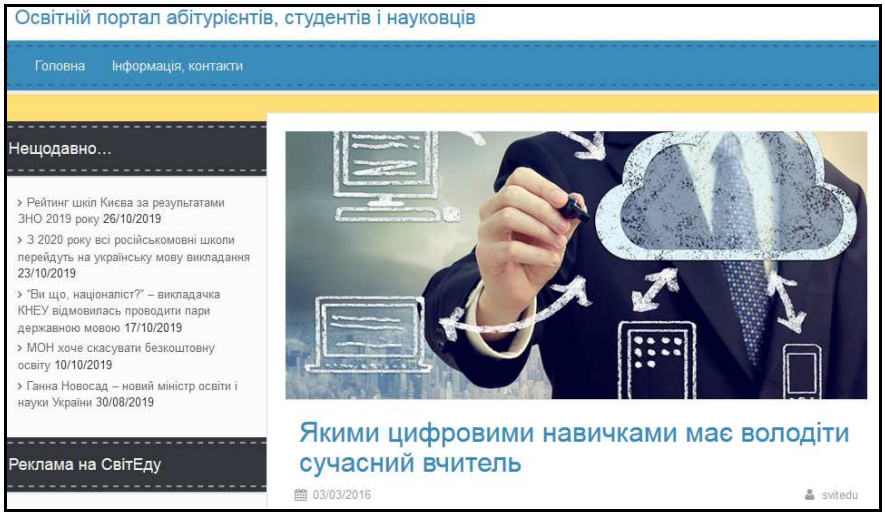


Рис.7. Блог «Educators Technology» - https://svitedu.com.ua/yakimi-tsifrovimi-navichkami-maye-voloditi-suchasniy-vchitel/

Блог Educators Technology поділився описом важливих педагогічних умінь, серед яких є десять цифрових навичок:

- Знаходити і оцінювати навчальні онлайн-матеріали;
- Створювати візуально цікаві матеріали;
- Створювати віртуальні майданчики для свого класу: блоги, сайти, вікі-платформи;
- Вміти ефективно шукати інформацію в мережі;
- Використовувати можливості соціальних мереж для професійного розвитку;
- Рекомендувати і поширювати навчальні ресурси;
- Створювати, редагувати і поширювати цифрові портфоліо;
- Створювати, редагувати і поширювати мультимедійний контент;
- Використовувати онлайн-інструменти для впровадження сучасних педагогічних практик: перевернутий клас, змішане навчання, мобільне навчання, проектне навчання і.т.д.
- Налагоджувати зв'язки з іншими викладачами.

Ключові слова: *цифрова компетентність, ключова компетентність, рамка цифрової компетентності, вчитель, блог, ІКТ.*

Список використаних джерел

1. Блог «Educators Technology» - https://svitedu.com.ua/yakimi-tsifrovimi-navichkami-maye-voloditi-suchasniy-vchitel/
2. Блог вчителя «Навички XXI століття» - Блог «Educators Technology» - https://svitedu.com.ua/yakimi-tsifrovimi-navichkami-maye-voloditi-suchasniy-vchitel/
3. Всеосвіта. Віртуальна школа ІКТ - http://i-math.com.ua/vsikt/sample-page/programa/
4. Нова українська школа. Концептуальні засади реформування середньої освіти / Міністерство освіти і науки України . – 2016 . – С . 11–12 [Електронний ресурс] . – Режим доступу: https://www .kmu .gov .ua/storage/app/media/reforms/ukrainska-shkola-compressed.pdf
5. Освіторія. Потрал для вчителів - https://osvitoria.media/experience/tsyfrova-kompetentnist-shho-povynni-vmity-vchyteli/
6. Цифрова компетентність вчителя DigCompEdu. Дистанційна освіта. Блог про дистанційне та змішане навчання інформатики. Технології та системи дистанційного навчання. Moodle. – Режим доступу: https://www: http://dystosvita.blogspot.com/2018/04/digcompedu.html
7. DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptual Reference Model. – Режим доступу: https://www.https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digcomp-20-digital-competence-framework-citizens-update-phase-1-conceptual-reference-model.
8. European Framework for the Digital Competence of Educators: DigCompEdu. – 2017. - [Електронний ресурс] . – Режим доступу: https://www.ec.europa.eu/jrc/en/digcompedu.pdf.

Матеріал підготувала: Овчарук О.В.

І Н Ф О Р М А Ц І Й Н И Й Б Ю Л Е Т Е Н Ь
№ 5 , 2019

ОСВІТНЯ ТЕХНОЛОГІЧНА СТРАТЕГІЯ ВЕЛИКОЇ БРИТАНІЇ: НАВЧАЛЬНІ ІНСТРУМЕНТИ

З метою розвитку конкурентоспроможної цифрової економіки країни на основі Цифрової стратегії та Промислової стратегії Великої Британії була розроблена Цифрова стратегія Великої Британії 2017 (UK Digital Strategy 2017), реалізація якої потребує значної кількості спеціалістів з високим рівнем ІК-компетентності у різних сферах.

З огляду на те, що освіта виступає як постачальник необхідних для промисловості професійних кадрів, їх підготовки відповідно до державної політики з розвитку конкурентоспроможної цифрової економіки країни, у 2018 році розроблено і реалізується Освітня технологічна стратегія (EdTech strategy).

У підготовці і впроваджені нової освітньої стратегії окрім освітянських організацій (Департамент освіти Великої Британії (Department for Education), Департамент зі стандартизації в освіті, послуг та навичок для дітей (Ofsted)), бізнес структур (Департамент бізнесу, інновацій і навичок Англії (BIS), Академія з комп'ютингу BCS, Конфедерація Британської промисловості CBI (The Confederation of British Industry)), брали участь компанії Google, Microsoft, Intellect**,** інші інституції системи освіти країни, консультативні організації, які формують сучасний ринок праці.

Визначено сім основних пріоритетних напрямів EdTech:

1. Створення Професійної рамки цифрового навчання
2. Визначення Статусу вчителя EdTech (EdTechTS)
3. Забезпечення доступності навчання

4. Створення навчальних співтовариств EdTech

5. Забезпечення і підтримка постійного професійного розвитку

6. Підтримка обміну досвідом

7.Залучення інвестицій, постачальників освітніх послуг, які сприятимуть розвитку цифрових технологій в галузі освіти

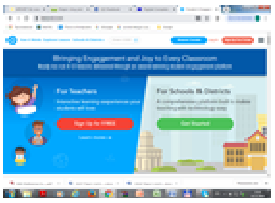
На цей час зроблені перші кроки з впровадження стратегії – розроблена Професійна рамка цифрового навчання (Digital Teaching Professional Framework), яка адаптована до Європейської рамки цифрової компетентності педагогів (DigCompEdu) і визначає три рівні компетентності:

- Рівень 1: Навчання - засвоєння нової інформації та розвиток базових цифрових навичок
- Рівень 2: Адаптація - застосування і розвиток цифрових навичок на практиці
- Рівень 3: Лідерство – передача отриманих знань, критичний підхід до вибору технологій, розвиток нових технологій

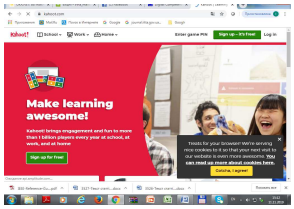
Впровадження Освітньої технологічної стратегії (EdTech strategy) сприяє і підтримує створення та оновлення різноманітних програм, онлайн сервісів, продуктів та інструментів, які використовуються у різних ланках системи освіти. З огляду на це освітянами країни було проведено дослідження і аналіз вже існуючих пропозицій з боку компаній-постачальників освітніх послуг та їх продукції. З величезної кількості перевірених і протестованих навчальних інструментів виділено декілька, які рекомендовані для використання у професійній діяльності освітян. Одними з найбільш популярних можна зазначити такі як:

Twinkl (https://www.twinkl.co.uk) - освітня видавнича компанія з інноваційними напрямами роботи, яка об’єднує освітян різних континентів (Велика Британія, США, Австралія). На створеному сайті компанії розміщені плани уроків, навчальні інструменти, інтерактивні освітні ігри з використанням комп’ютерів,

планшетів і смартфонів. Є можливість використання безкоштовних навчальних ресурсів, створивши безкоштовний обліковий запис.



Nearpod (https://nearpod.com) – навчання через мобільні пристрої, забезпечує велику кількість повністю інтерактивних уроків, розроблених фахівцями з різних предметів для всіх рівнів середньої освіти. Крім того, програма Nearpod дозволяє вчителям імпортувати уроки з будь-якого типу файлів і починати додавати до них інтерактивні елементи, веб-посилання або фрагменти відео. Після цього викладачі можуть синхронізувати свої підготовлені уроки з усіма учнівськими пристроями, одночасно відправляючи урок кожному студенту і мають можливість контролювати весь навчальний процесс протягом усього уроку.



Kahoot! (https://kahoot.com) - платформа для навчання на основі ігор, одна з найшвидше зростаючих світових навчальних брендів з більш ніж 40 мільйонами щомісячних активних користувачів у 180 країнах. Дозволяє легко створювати, відкривати, відтворювати та обмінюватися навчальними іграми за лічені хвилини - для будь-якої теми, будь-якою мовою, на будь-якому пристрої, для учнів будь-якого віку.

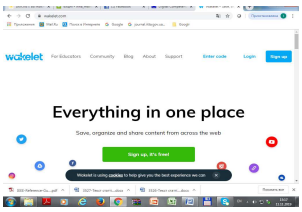
Безкоштовна платформа Kahoot! створена у 2013 році, з метою зробити навчання захоплюючим, залучаючи соціальний, змістовний і потужний педагогічний досвід. Завдякі платформі вчителі мають можливість самостійно швидко створювати навчальні ігри для учнів. Після створення гри учні можуть використовувати будь-який пристрій для входу у «кімнату» гри, застосовуючи унікальний код і змагатися з однолітками.

Відображення питань і гри на дисплеї заохочує учнів використовувати свої особисті пристрої лише для вибору відповіді. Протягом всього сеансу підтримується і заохочується командна співпраця. Крім цього підвищується мотивація учнів щодо досягнення своїх навчальних цілей, підвищення рівня цифрової грамотності, зацікавленості в освоєнні наданого матеріалу та його спільному обговоренні.

Buncee (https://www.edu.buncee.com/about) – інструмент, який сприяє впровадженню концепції 4С впродовж навчального процесу, розвиваючи критичне мислення, спілкування, співпрацю і творчість. Buncee дає можливість створювати спільний графічний дизайн, записувати аудіо та відео, використовувати YouTube і Pixabay тощо.

Завдяки самостійній роботі з використанням новітніх технологій зацікавленість студентів у вивченні нового матеріалу значно підвищується. Учні віком від шести до семи років використовують Buncee для створення мультимедійних презентацій, які демонструють освоєння навчального матеріалу, критичне мислення та творчий підхід. Вчителі інтегрують Buncee як інструмент для індивідуалізованого, диференційованого навчання, вивчення мов, спеціальної освіти, а також уроків і проєктів з будь-якого предмету.

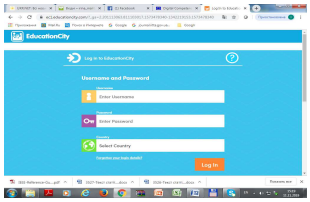
Matific (https://www.matific.com/ua/uk/home) - збірник математичних онлайн-вправ, за допомогою яких учні навчаються розв'язувати задачі та критично мислити, використовуються ігрові принципи. Крім цього, розміщені й більш звичні інструменти такі як: робочі аркуші, плани уроків, звітність у реальному часі. Весь контент Matific узгоджено з навчальною програмою або підручником, його можна переглядати, визначати завдання для класної або домашньої роботи. Ресурс має україномовну версію, рекомендований Міністерством освіти і науки України.



Wakelet (https://wakelet.com) - платформа, популярність якої швидко розповсюджується серед педагогів у всьому світі. Вона дозволяє швидко організовувати та обмінюватися контентом зі своїми учнями, надавати цифрові завдання та створювати портфоліо. Завдяки платформі кожен має можливість започаткувати інтерактивні колекції, оздоблюючи свої сторінки відео, повідомленнями соціальних медіа, доповнюючи статтями, подкастами, зображенням, нотатками та інше. Можна

змінювати макети, реорганізувати вміст і робити оновлення в будь-який час, що значно допомагає у плануванні і поширенні інформації.

Особливістю Wakelet є можливість відображати будь-який онлайновий контент, підвищуючи зацікавленість у створенні своєї цифрової розповіді, що стає все більш важливим для педагогів.



Education City (https://www.educationcity.com) - один з провідних ресурсів онлайн-навчання, викладання та оцінювання, створений у 1999 році. На цей час має користувачів у більш ніж 70 країнах світу. Спрямований на дітей віком від 3 до 12 років. Інтерактивні освітні ресурси Education City охоплюють англійську мову, математику, природничі науки, обчислювальну техніку, французьку, іспанську та англійську як додаткову мову. Пропонуючи різноманітні типи контенту, ресурс підходить для груп та цілих класів, а також персоналізованого навчання. Він може використовуватися в будь-який час і в будь-якому місці на різних пристроях, включаючи інтерактивні дошки, ноутбуки і мобільні пристрої, а також включає в себе багато функцій, які заощаджують час для вчителя. Як ресурс, що базується на навчальному плані, EducationCity відображається у навчальних програмах Великої Британії.

Матеріал підготувала Малицька І.Д.

ПРОБЛЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ ЯК АСПЕКТ ЦИФРОВОЇ КОМПЕТЕНТНОСТІ УЧНІВ ТА ВЧИТЕЛІВ В ІНФОРМАЦІЙНО-ОСВІТНЬОМУ СЕРЕДОВИЩІ В ПРОЦЕСІ ВИХОВАННЯ ГРОМАДЯНИНА: ДОСВІД НІДЕРЛАНДІВ

Пріоритетами громадянської освіти у сучасному суспільстві, які визнані більшістю європейських країн та Україною, є фундаментальні цінності, проголошені Радою Європи та визнані і закріплені іншими міжнародними документами, резолюціями, положенням та т.і., а саме: верховенство права, демократія та права людини. Разом з цим, навчання і виховання у цифрову еру вимагає сучасного підходу до організації середовища, у якому має відбуватися процес освіти – інформаційно-освітнього середовища. Громадянська освіта здійснюється у інформаційному цифровому просторі й від педагогів та учнів вимагається бути компетентним як у галузі громадянської освіти, так і у використанні ІКТ. Громадянська компетентність учасників навчально-виховного процесу, і вчителів зокрема, безпосередньо пов’язана з відповідальним ставленням до інформації та володінням ІКТ, повагою до приватного життя, толерантністю та етичною поведінкою у цифровому світі та ін., що дає можливість забезпечити політику конфіденційності та безпеки у інформаційно-освітньому середовищі. Нідерланди – європейська розвинена країна, де закладались основи міжнародного права та демократичні цінності, має певний досвід щодо розв’язання проблеми інформаційної безпеки та конфіденційності використання цифрових технологій, що застосовуються у школі. Обмін персональними даними, політика щодо паролів, кодекс поведінки для безпечного використання цифрових ресурсів та персональних даних, угоди про соціальні медіа, тощо – аспекти інформаційної безпеки та

конфіденційності, якими опікуються голландські освітяни та про що йдеться у звіті Національного конгресу з питань інформаційної безпеки та конфіденційності в галузі освіти, що відбувася у м. Ньювейген, Нідерланди, у 2019 р. Як зазначають експерти, легковірно та недостатньо відповідально поводяться у Інтернеті не тільки діти, а й вчителі, що пов'язане з недостатньою обізнаністю, технологічними аспектами та впровадженням політики школи щодо інформаційної безпеки та конфіденційності. Фішинг, який є однією із форм шахрайства в Інтернеті, визнаний учасниками конгресу найбільшою проблемою школи сьогодні. Прості паролі доступу, неуважність при натисканні кнопок, відкриваючи електронні листи чи посилання, надання особистої та фінансової інформації підробним веб-сайтам становить реальну загроза я особисту, так і для всієї школи. Результати Моніторингу інформаційної безпеки та конфіденційності, 2019р. продемонстрували, що 80% хакерських нападів спроможні зламати електронну шкільну мережу. Отже, демократичність, прозорість і доступність освіти, відкритість і вільний доступ до інформації у цифровому світі, вимагають від вчителів та учнів набувати і розвивати громадянську та ІК компетентності.

Політика освітнього закладу Нідерландів щодо інформаційної безпеки та конфіденційності спрямована на створення правил та рамкових умов, встановлення відповідальності учасників освітнього процесу. Голландський фонд Kennisnet (https://www.kennisnet.nl), що займається впровадженням ІКТ у освіту, у 2019 р. запропонував оновлений підхід до формування і впровадження політики інформаційної безпеки та конфіденційності, розроблений завдяки плідній співпраці фонду з Радою в галузі середньої освіти (https://www.vo-raad.nl/), Радою в галузі початкової освіти (https://www.poraad.nl/) та Радою з питань охорони здоров'я. Для реалізації оновленого підходу також створено наповнений інструментарієм єдиний веб-портал з інформаційної безпеки для шкіл та забезпечено умови комфортного переходу на нього з попередніх шкільних сайтів. Ефективне впровадження ІК технологій у навчальне середовище, в якому застосовуються хмарні сервіси, цифрові ресурси і засоби, забезпечується рекомендаціями, що розроблені фахівцями у вигляді покрокового плану, які можуть допомогти школі запровадити політику

інформаційної безпеки та конфіденційності навчального закладу. Покроковий план складається із п'яти розділів, що називаються: *політика та відповідальність, визначення обмежень та ризиків, прозорий обмін персональними даними, обробка та зберігання персональних даних та оцінка*. Розділ І Політика та відповідальність складається з таких тем: політика інформаційної безпеки та конфіденційність – та ролі та обов'язки. Кодекс поведінки щодо безпечного використання ресурсів та персональних даних ІКТ, політика щодо паролів та процедура повідомлення про інциденти з порушення безпеки – аспекти розділу ІІ Визначення обмежень та ризиків. Питання конфіденційності за замовчуванням та конфіденційності процесу розробки, угоди про соціальні медіа, обмін персональними даними та ін. розкриваються у розділі ІІІ Прозорий обмін персональними даними. Угоди про обробку та зберігання даних, правила та юридичне підґрунтя містяться у Розділ IV Обробка та зберігання персональних даних. Інструкції щодо процесів підзвітності та інформування містяться у розділі V Оцінка. До інструментарію, що забезпечує політику інформаційної безпеки та конфіденційності, також належить укладений глосарій, що визначає основні терміни та поняття, серед яких: анонімізація, псевдонімізація, аутентифікація, матриця авторизації, хмара, мінімізація даних, шифрування, хакер, аналіз ризиків, конфіденційність, конфіденційність за замовчуванням, шифрування та ін.

Молоді люди виростають в цифровому світі, який пропонує багато можливостей, та має й багато ризиків. Робота з молоддю, просвітницька діяльність у напрямі впровадження політики безпеки та конфіденційності у цифровому світі в Нідерландах здійснюється не тільки освітніми установами. Управління захисту даних Нідерландів, що забезпечує нагляд за дотриманням законів щодо захисту персональних даних та здійснює консультування та інформування громадян, окремо опікується освітньою галуззю. Фахівцями управління зазначається, що серйозна проблема полягає в питанні, чи розуміють молоді люди, які дані вони надають і як це відбувається. Задля розв'язання цієї проблеми було розроблено два навчальні пакети: для учнів під назвою "Ви керуєте своїм телефоном?" *(«Ben jij je telefoon de baas?», нідер.*) та для вчителів, що називається «Конфіденційність» *(«Privacy»,*

нідер.). Навчальний пакет "Ви керуєте своїм телефоном?" (Рис.1), що створений для учнів початкової та середньої школи, допомагає перевірити, на скільки відповідально і безпечно дитина користується своїм смартфоном, та набути необхідних знань і навичок. До складу цього навчального пакету входить гра https://autoriteitpersoonsgegevens.nl/, презентація якої була присвячена Тижню медіаграмотності, що пройшов у листопаді 2019 р.

Рис.1. Інтерфейс навчальної гри "Ви керуєте своїм телефоном?"

Навчальна гра побудована на завданнях, що імітують ситуації, з якими стикається або може стикнутися дитина, користуючись своїм смартфоном для он-лайн ігор, спілкування в мережах та ін. Наприклад, дитині допомагають зрозуміти, що давши відповідь на запитання: «Кожного року на твій день народження ми будемо надсилати тобі у подарунок кролика. Скільки кроликів буде у тебе, коли тобі виповниться 18 років?» можна дізнатися про її особисті дані, а саме – рік її народження. Завдяки грі учні дізнаються, що через додатки, комп'ютерні ігри, сайти, соціальні мережі та ін. їх дані можуть потрапити до нечесної людини із сумнівними намірами, що зловмисники можуть отримати доступ до відеокамери і мікрофону, підслуховувати розмови чи непомітно робити фото, привласнити ім'я дитини і видавати себе за неї, та навіть отримати відбиток пальця, доступ до рахунків та здійснювати з них покупки та ін. https://autoriteitpersoonsgegevens.nl/.

Виконуючи завдання навчальної гри учні дізнаються, з якими ризиками вони могли б зіткнутися, якщо не дотримуватись правил безпечної поведінки у цифровому світі та як цьому запобігти.

Безкоштовний навчальний пакет "Конфіденційність" від Нідерландського управління захисту даних надає вчителю навчальні матеріали та он-лайн інструменти, за допомогою яких розкривається тема конфіденційності «Конфіденційність стосується всіх!» (Рис.2).

Рис.2. Навчальний пакет «Конфіденційність стосується всіх!»

Зміст навчального пакету висвітлює тему в новому ракурсі, виходячи від права на приватність. На 3 уроках тривалістю по 45 хвилин «Хто ти в Інтернеті?», «Оплатити своїми персональними даними», «Ви маєте право на приватність!» вчитель викладає матеріал з теми конфіденційності та захисту особистих даних. Учнів знайомлять з темінологією за темою, за допомогою практично орієнтованих завдань та заохочуючи до критичного аналізу запропонованих ситуацій, вони усвідомлюють, чому різні організації часто цікавляться їх даними та які права на конфіденційність вони мають. Вчитель разом з учнями обговорює теми: «Як Ви робите пошук?», «Яку рекламу ви отримуєте?», «Чи всі отримали однакові результати під час пошуку?», «Мої особисті дані коштують багато», «Безкоштовно ?! Читаєте ви умови, перш ніж погодитися?», «Ваш цифровий слід» та ін.

Корисним та цікавим прикладом впровадження основ інформаційної безпеки та конфіденційності в Інтеренеті є спеціально створений Молодіжний веб-сайт поліції Нідерландів https://www.vraaghetdepolitie.nl, що надає інформацію та допомагає молодим людям вийти з небезпечних ситуацій або запобігти їм (Рис.3.).

Рис.3. Сайт для молоді поліції Нідерландів.

Сьогодні молода людина стикається з багатьма ризиками і інтернеті і потребує відповідей на запитання: чи може хтось шпигувати за мною через веб-камеру без мого відома? Як захистити свої дані в Інтернеті? Чи можу я дізнатися, чи надсилаю повідомлення анонімно? Як видалити фотографію в Twitter? У мене є фотографії, на яких я стріляю на стрільбу з пневматичної зброї. Чи можу я поширити його через соціальні медіа? Чи небезпечно зустрітись з людиною, яку ви знаєте лише з Інтернету? Чи правда, що інші можуть бачити мене через веб-камеру без мого відома? Чи може незнайомець отримати мою адресу через мою IP-адресу? Чи можу я довіряти модельному агентству, яке звертається до мене через Інтернет? Чи можу я просто дати кожному свій номер? Чи можна запобігти інтернет-аферам? Чому ви не можете просто довіряти всім в Інтернеті? Чому я маю бути обережним при поширенні власних фотографій в Інтернеті? Чому я повинен бути обережним із веб-камерою? На що слід звернути увагу на фотографії профілю? Що таке безпечний пароль? Що можна і чого не можна розміщувати на профільних веб-сайтах? Хто мої друзі в Інтернеті? Чи є доказами зйомки камер? та багато інших. Знайшовши у переліку питання, яке потребує відповіді, користувач може натиснути на нього та перейшовши за посиланням, знайти поради і інструкції для його розв'язання.

Сучасний навчально-виховний процес відбувається у інформаційно-освітньому середовищі, яке постійно розвивається і змінюється. Сьогодні це комп'ютерно орієнтоване та хмаро орієнтоване навчальне середовище, у якому питання безпеки і конфіденційності край важливе. Воно вимагає від вчителів, учнів та інших учасників освітнього процесу бути компетентними, відповідальними та свідомими користувачами, бути освіченим громадянином та виявляти власну громадянську позицію. Дані, що використовуються вчителем або учнем, зберігаються не тільки на власному комп'ютері, а все частіше розміщуються у хмарі, учасники навчально-виховного процесу користуються хмарними сервісами, спілкуються, співпрацюють, навчаються й розвиваються засобами соціальних мереж, блогів, форумів і чатів тощо. Тому зарубіжний досвід і практичні розробки Нідерландів, зокрема, можуть стати у нагоді вітчизняним фахівцям. Перспективами для подальших пошуків можуть бути практичні розробки уроків з безпеки та конфіденційності, що є невід'ємною складовою громадянської освіти.

Використані джерела:

1. Фонд Kennisnet, https://www.kennisnet.nl.
2. Радою в галузі середньої освіти, https://www.vo-raad.nl.
3. Радою в галузі початкової освіти, https://www.poraad.nl.

Матеріал підготувала: Гриценчук О.О.

Адреса: Україна, 04060, м. Київ, вул. Максима Берлинського, 9
тел./факс: (044) 440–47-03
http://iitlt.gov.ua ***e-mail: iitlt@iitlt.gov.ua***