інформаційні (пошук даних з безпечних наукових джерел та можливість їх критичного осмислення), самоосвіти (вміння навчатись самостійно). Крім цього ДН сприяє формуванню лідерських якостей особистості: активність, самостійність, самовдосконалення, творчість.

Список використаних джерел:

1. Концепція розвитку дистанційної освіти в Україні (затверджено Постановою МОН України В. Г. Кременем 20 грудня 2000 р.).
2. Биков В.Ю. Дистанційне навчання в країнах Європи та США і перспективи для України / В.Ю. Биков // Інформаційне забезпечення навчально-виховного процесу: інноваційні засоби і технології : кол. монографія / В.Ю. Биков, О.О. Гриценчук, Ю.О. Жук та ін. / Академія педагогічних наук України, Інститут засобів навчання. – К. : Атіка, 2015. – С. 77–140.
3. Кухаренко В. М., Березенська С. М., Бугайчук К. Л., Олійник Н. Ю., Олійник Т. О., Рибалко О. В. та ін. Теорія та практика змішаного навчання : монографія. Х. : Міськдрук, НТУ ХПІ, 2016. 284 с.

РАЇСА ВАСИЛЕНКО
Інститут цифровізації освіти НАПН України,
науковий співробітник
відділу компаративістики інформаційно-освітніх інновацій

РОБОТА ВЧИТЕЛЯ З ІНТЕРНЕТ-БЕЗПЕКИ ДІТЕЙ

Ключові слова: *цифрові технології, інтернет-безпека, інтернет-ризики*

У цифрову епоху на перший рівень виходять особливі когнітивні вміння, що дозволяють успішно взаємодіяти з інформацією в режимі реального часу. Людина, якв володітиме вміннями знаходити інформацію,

а також аналізувати, структурувати та класифікувати її, матиме соціальну, культурну та економічну перевагу перед іншими.

Суттєвими когнітивними навичкамиє спроможність людини оцінити надійність інформації з урахуванням фактору часу, контексту та особистої інтерпретації. Саме ця спроможність має формуватися з початкової школи, та її значимість особливо зростає з того моменту, коли діти починають своє життя в Інтернеті. Вона безпосередньо пов'язана, особливо у шкільному віці, з медіаграмотністю та інтернет-безпекою. Кібербезпека, е-безпека, безпечний Інтернет, безпека он-лайн - ось перелік термінів, що позначають у різних країнах проблему, що виникла в останнє десятиліття у зв'язку з роботою дітей в Інтернеті. Ця проблема зараз актуальна як ніколи. У ситуації, коли Інтернет був прив'язаний до комп'ютера, що знаходиться в певному місці, вирішення проблеми безпеки було очевидним.Але при віддаленій роботі виникають проблеми, так відсутні саморегулюючі угоди між контент-провайдерами про основні принципи безпечної роботи в соціальній мережі, що значно сприяє забезпеченню безпеки користувачів молодшого віку, зареєстрованих у мережі. Подібні угоди існують, наприклад, у Євросоюзі.

Впливати на дану ситуацію може залучення вчителів та батьків до вирішення питань використання Інтернету дітьми. Існуючий так званий «технологічний розрив» між поколіннями ускладнює участь батьків у заняттях дітей. Діти більш прогресивні користувачі мережевих технологій, ніж їхні батьки, найчастіше просто з тієї причини, що можуть проводити в Інтернеті набагато більше часу і набагато активніше обмінюються інформацією один з одним. Необхідно виробляти у дітей правила свідомої та відповідальної поведінки онлайн. Ситуація, що склалася, ставить на порядок денний необхідність навчання основ інтернет-безпеки майбутніх вчителів початкової та середньої школи. Нині ж існує гостра необхідність

навчання працюючих вчителів у межах підвищення кваліфікації. Також необхідне навчання і керівного складу школи та батьків.

Розглянемо, що було б корисно знати вчителям на сьогоднішній день на тему інтернет-безпеки. У зв'язку з безперервним розвитком технологій відбуваються зміни в навколишньому світі, пропонуються нові сервіси, виникають нові тенденції. Необхідно досліджувати новинки з позицій можливих загроз для дітей, а також бути в курсі світових тенденцій у цьому питанні. І цей факт не слід забувати при формуванні навчальних програм для вчителів, вони повинні постійно доповнюватись та оновлюватися.

Почнемо із класифікації інтернет-ризиків. Існуюча класифікація, відома як три "Сі" (content, contact, conduct), була розроблена фахівцями з Лондонської школи економіки [**1**]. Вона являє собою двомірну модель, що враховує участь (або роль) дитини та зміст самого ризику. Структура досить повно охоплює існуючі різновиди ризиків та включає такі складові як:

- Контентні (дитина є пасивним одержувачем) - реклама, спам:
- Контактні або комунікаційні (дитина виступає як учасник) - харвестінг (збір особистих даних), переслідування, персональні дані, буллінг;
- Поведінкові (дитина проявляє себе як активна дійова особа) - нелегальне скачування, азартні ігри, тероризм, фінансові махінації, створення та розміщення неналежного матеріалу.

Відповідно до наведеної класифікації, роль або позиція дитини в ризиках змінюється. Очевидно, що дитина шкільного віку здебільшого стає жертвою або власної помилки, або обману. Вчителям слід знати правила грамотної користувацької поведінки в мережах і сервісах і розповідати про неї дітям. Розглянемо тепер деякі прийоми та правила

роботи в соціальних мережах та мобільних сервісах, які можуть допомогти мінімізувати перераховані вище ризики та бути корисними як дітям, так і вчителям. Саме з цих позицій розглянемо Facebook, Flickr, Instagram та інші.

Facebook - збираючись вийти з мережі, можна дезактивувати свій обліковий запис. Дезактивація облікового запису не видаляє його. Підключившись назад, користувач зможе його реактивувати та відновити всі зв'язки зі своїми друзями. Коли ж він не в мережі, ніхто не може залишити записи на стіні, або відправити приватне повідомлення, або переглядати вміст.

Flikr - cоціальний сервіс, який призначений для зберігання та подальшого використання фотографій та відеороликів. До кожної фотографії її господар може додати різні мітки, включаючи прізвища людей, зображених у ньому. Користувачі системи можуть утворювати групи за інтересами, запрошувати до групи інших користувачів. А якщо як позначки використовуються прізвища, то можна легко знайти фото людини, навіть якщо замість її фотографії в соціальній мережі використовується аватар. Тому як позначки слід вказувати не повні імена, а, можливо, просто імена або прізвиська.

Google locator, I can stalk you, Foursquare–це цілий ряд ідентичних сервісів та сайтів, які використовують можливості технології Geolocation, визначають і фіксують за GPS координати або за метаданими відзнятої фотографії або місце, де було зроблено фотографію, або місцезнаходження мобільного телефону, власником якого є дитина, і розміщують ці дані у себе. Небезпека полягає в тому, що можна дізнатися про місця, які дитина часто відвідує. Більше того, відзначаючи свою присутність, дитина нерідко вказує і координати свого будинку - таким чином, стає відома її адреса.

Щоб зробити інформацію недоступною для незнайомих людей, необхідно змінити свої налаштування.

Instagram - Соціальна мережа, яка з'явилася в 2010 році спочатку як платформа для обміну фотографіями серед користувачів мережі, але з того часу розрослася за рахунок підключення різних соціальних медіа, включаючи Twitter та Facebook. У 2012 році вона була куплена Facebook, і почала стрімко набирати популярності. Компанія оголосила нові правила обслуговування, що дозволяли перепродаж прав на розміщені фотографії. Але негайна протестна реакція громадськості змусила нових власників відмовитись від публікації фотографій. Програми дозволяють редагувати фотографії, зняті телефоном, та розміщувати їх у мережі. Як і у більшості соціальних мереж, при реєстрації потрібне облікове ім'я. У цьому випадку діти повинні знати, що необов'язково давати своє ім'я та прізвище, а слід замінювати їх псевдонімом, і в жодному разі не слід заповнювати необов'язкові поля. Існують можливості конфіденційності, що межують доступ сторонніх до перегляду фотографій, і за аналогією з Facebook, незнайомець повинен спочатку відправити запит на отримання доступу.

Вчителям необхідно постійно проводити роз'яснювальну роботу з батьками, залучаючи їх до участі у вирішенні проблем, що виникають. Як уже було сказано раніше, перешкодою в цьому питанні найчастіше є «технологічний розрив» поколінь — діти знають і вміють набагато більше, ніж їхні батьки. В цьому випадку можна порадити батькам звернутися до дитини з проханням навчити користуватися тим чи іншим сервісом. Останнім часом багато батьків у Великій Британії, США реєструються в тих же соціальних мережах, які відвідує їхня дитина. Це дозволяє відслідковувати, як дитина поводиться в мережі, з ким спілкується. Основна теза, яку потрібно донести до батьків: необхідність побудови

довірчих поважних стосунків з дитиною. Тільки під час спокійних бесід та розбору прикладів можна привернути увагу дитини до проблеми.

Слід зазначити, що технології розвиваються, виникають нові послуги, молодь їх освоює раніше за інших. Тому виникає необхідність у створенні служб в освіті, які будуть досліджувати нові сервіси з позицій можливих загроз та інформували б зацікавлену освітню громадськість. А також виникає необхідність з розвитку цифрової компетентності всіх учасників освітнього процесу: учнів, батьків, вчителів, адміністративного персоналу навчального закладу.

Список використаних джерел:

1. Livingstone S., Haddon L., Gorzig A., Olaffson K.Risks and safety on the Internet. The perspective of European children. Full findings. LSE, London, EU Kids Online. URL:http://eprints.lse.ac.uk/27052/1/Comparing_Online_Risks_(LSERO). 2011.
2. Mobilemarketing. URL:https://mobilemarketingmagazine.com/
3. Овчарук О. , Іванюк І. В., О. Гриценчук, І. Іванюк, О. Кравчина, І. Малицька, Н. Сороко. Європейський досвід розвитку цифрової компетентності вчителя в контексті сучасних освітніх реформ. *Інформаційні технології і засоби навчання:* електрон. наук. фахове вид. 2018. Вип. 3 (65). С. 316–336. URL:https://journal.iitta.gov.ua/index.php/itlt/issue/view/94/showToc