

Висновок

Узагальнюючи досвід роботи з означеної теми, можемо впевнено стверджувати, що нова бібліотека є не тільки корисним інформаційним ресурсом, не тільки відправною точкою для продовження самоосвіти, але й наочним результатом спільних зусиль.

Використані джерела

1. Державний стандарт базової і повної середньої освіти / ред. О.А. Кривенко. – Київ: КНТ, 2004. – 88 с.
2. Нова українська школа: посібник для вчителя: навчально-методичний посібник / Л. Гриневич, О. Елькін, С. Калашнікова [та ін.]; за заг. ред. Н.М. Бібік. – Київ: Літера ЛТД, 2018. – С. 12.

Правила безпеки в Інтернеті: поради батькам

Павлова Г., бібліотекар
Харківської академії неперервної освіти

Інтернет – найбільша у світі комп'ютерна мережа, що з'єднує дуже велику кількість комп'ютерів у велетенську світову павутину.

У наші часи діти та підлітки багато часу проводять в Інтернеті: користуються соціальними мережами, додатками та відвідують різноманітні сайти. Нерідко батьки задають собі питання: «Як же вберегти свою дитину від поганого впливу інформації?» Не допускати дитину до гаджетів? Неможливо, бо вона народжена в цифрову еру. Тож як бути?

Розглянемо декілька простих *правил для безпечного користування Інтернетом* як дорослими, так і дітьми молодшого віку, та підлітками. У наші часи з'явилося дуже багато шахраїв, як кажуть, прогрес не зупинився на місці навіть для них. У цифрову епоху набуло чинності інше поняття – кібершахрайство. Тому важливо ніколи та нікому не розголошувати свої персональні дані. Для цього, у першу чергу, треба своєчасно оновлювати програмне забезпечення. Розробники даних програм стежать за можливими загрозами, намагаються захистити свої продукти нововведеннями.

Останнім часом став популярним такий різновид шахрайства, як *Фішинг*. Фішинг – вид шахрайства, метою якого є виловлювання (виманювання) у довірливих або неуважних користувачів мережі персональних даних клієнтів онлайн-магазинів, сервісів із переказу грошей, онлайн-аукціонів тощо [7]. Шахраї виманюють усю конфіденційну інформацію через пошту. Надсилаючи електронні листи, пропонують перейти за посиланням або підтвердити інформацію. Фішинг – один із різновидів соціальної інженерії, заснований на незнанні користувачами основ мережевої безпеки.

Багато батьків взагалі не знають, чим займаються їхні діти в телефонах, планшетах чи комп'ютерах, користуючись Інтернетом, які сайти вони відвідують. Через відсутність життєвого досвіду та нерозуміння деяких життєвих моментів діти дошкільного, молодшого та середнього віку можуть зіткнутися з багатьма

онлайн-загрозами, зокрема з онлайн-насиллям, кібербулінгом, із шахрайством, педофілією та фішингом.

Компанія «Київстар» ініціювала соціологічне дослідження «Знання та ставлення українців до питання безпеки дітей в Інтернеті» (2009 р.), яке провів Інститут соціології НАН України. Результати цього соціологічного опитування шокують, бо понад 28% маленьких громадян готові відправити особисті фотокартки незнайомим людям, 17% – без усіляких вагань розповідають особисту інформацію про себе та свою родину, а от 22% дітей, на жаль, потрапляють на сайти для дорослих [3].

Отже, батькам потрібно дотримуватися правил поведінки в Інтернеті. По перше, багато джерел інформації рекомендують самому підвищувати рівень комп'ютерної грамотності для того, щоб була можливість допомогти дитині у вирішенні будь-яких питань. Щоб захистити свій Онлайн простір від небажаної взаємодії з незнайомцями, команда #stop_sexтинг створила «Топ-10 правил безпечного Інтернету» [9]. Для надійного пароля використовуйте маленькі та великі літери, а також цифри. Чим більше знаків, тим краще. Обов'язково встановіть антивірусну програму на свій пристрій, але завантажуйте ці програми з офіційних сайтів розробників. Ні в якому разі не переходьте за посиланнями, що надійшли з невідомих джерел. Пам'ятайте, після поширення фото чи відео-матеріалів над ними втрачається контроль [9]. Використовуйте блокувальник спливаючих елементів у браузері, двофакторну аутентифікацію. Закривайте впливаючі вікна клавішами Alt+F4, перевіряйте адреси вебсайтів. Видаляйте історію з браузера та кеш. Не використовуйте чужі знімні пристрої, такі як USB, жорсткі диски тощо [6].

Спробуйте проводити більше часу в Інтернеті разом із дітьми. Будьте в тренді. Цікайтесь, чим у світовій павутині живе ваша дитина, чого вона більше вподобає та якими сайтами любить користуватися. Якщо виникла ситуація, у якій довелося усе ж таки заборонити деякі сайти, але заборони не діють, тоді приділяйте більше уваги вихованню дитини. Розмовляйте з нею про правила поведінки в Інтернеті, навчіть її правила білборда: якої інформації про себе ти не бажаєш бачити на білборді, що розміщений перед твоїм будинком або перед школою. Обов'язково станьте для дитини другом і радником, для того щоб від вас нічого не приховували та ділилися з вами проблемами в опануванні Інтернету [1].

Висновок

Ми, наші діти й підлітки використовуємо Інтернет кожного дня. Він став невід'ємною частиною нашого життя. Тому завжди поведіться так у мережі, як би ви хотіли, щоб поводитися з вами. Разом із тим важливо не забувати про живе спілкування: завжди цікався, чим сьогодні живуть ваші діти, приділяйте їм більше уваги.

Використана література

1. Безпека в Інтернеті: що потрібно знати [Електронний ресурс]. – Режим доступу: <https://pon.org.ua/novyny/5427-bezpeka-v-nternet-scho-potrbno-znati.html>
3. Безпечний Інтернет у шкільній бібліотеці [Електронний ресурс]. – Режим доступу: <https://dnpb.gov.ua/ua/naukovi-zakhody/vebinary/safer-internet-day-2021>

4. Діти в Інтернеті: як навчити безпеці [Електронний ресурс]. – Режим доступу: https://rescentre.org.ua/images/Uploads/Files/internet_safety_dl/children_inter_net.pdf
5. Інтернет: енциклопедія / Ю. Солоницын, В. Холмогоров. – 3-е издание. – СПб.: Питер, 2002. – 592 с.: ил.
6. Класифікація загроз в Інтернеті [Електронний ресурс]. – Режим доступу: https://betterinternetcentre.org/wp-content/uploads/2018/01/Chernykh-Online-safety_ukr_8_9.pdf
7. Нападій Т. Безпека в цифровому середовищі / Тетяна Нападій // Методист. – 2020. – № 9-10. – С. 59-63 с.
8. Поняття слова Фішинг [Електронний ресурс]. – Режим доступу: <https://ru.wikipedia.org/wiki/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3>
9. Практикум з основ інформаційних технологій. Основи роботи з Windows, Word, PowerPoint, MicrosoftExcel та у глобальній мережі Internet / В.В. Костіна, І.В. Табарчук; за заг. ред. Т.В. Папернової. – Харків: ХОНМІБО, 2008. – 76 с.
10. Топ-10 правил безпечного Інтернету [Електронний ресурс]. – Режим доступу: <https://stop-sexting.in.ua/top-10-pravyl-bezpechnogo-internetu/>

Особливості організації роботи із суспільно значущими проєктами по згуртованості громад і розвитку інформаційного суспільства

Теницька Г. П., бібліотекарка
КЗ «Бугайівський ліцей»

Кун'євської сільської громади Ізюмського району

Велика роль у згуртованості громад відводиться молоді, яка може зробити значний внесок у життя суспільства та громади. Молоді люди здатні висувати нестандартні ідеї та пропозиції, упроваджуючи навички соціальної згуртованості в громадах, про які не подумали дорослі чи керівники. Освітні заклади, бібліотеки, медіатеки можуть стати місцем, де молодь отримає перший досвід демократичної участі в житті суспільства. Саме з метою посилення спроможності активної молоді мобілізуватися та спрямувати свій потенціал на розвиток і згуртованість своєї громади, розвиток інформаційного суспільства, прищеплення навичок мирних відносин і формування мироорієнтованих цінностей у медіатеці проводиться робота з проєктами.

Перший *проєкт* «Подолання конфліктів за допомогою освіти в галузі миробудівництва», над яким у 2017 році я розпочала працювати, був спрямований на роботу з учнями старших класів. Регіональне розмаїття України, поява в результаті збройного конфлікту на Донбасі й анексії Криму нової категорії людей – внутрішньо переміщених осіб, осіб із набутими та вродженими фізичними вадами, різна історична свідомість, орієнтація на різні культурні та цивілізаційні моделі розвитку держави, різне бачення майбутнього, поширення дитячого булінгу – усе це є одним із найбільших викликів, що стоять перед суспільством, у