

Цифрові права та онлайн безпека: як захистити дітей в інтернеті

Вікторія Омеляненко аналітикиня громадської організації МІНЗМІН

А чи знаєте ви самі, які цифрові права маєте?

Насправді всі ті ж, що гарантуються Загальною декларацією прав людини 1948 року, тільки із застосуванням у цифровому світі.

Це також стосується і дітей. У рекомендаціях Ради Європи CM/Rec (2018)7 йдеться про зобов'язання держав-членів забезпечити кожній дитині всі права, закріплені в Конвенції ООН про права дитини, у Конвенції про захист прав людини та основних свобод та їхніх протоколах.

Загалом, можна визначити 4 основних цифрових права дітей. І їх варто розглядати в контексті буденних ситуацій.

Що ж, поговоримо про цифрові права, які має кожна дитина.



1

Право вільно висловлювати думки в мережі

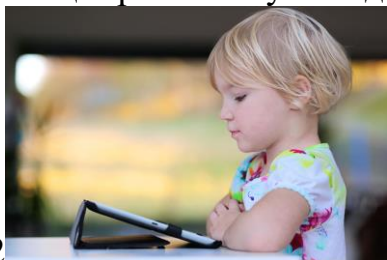
Дитина може вести блог в мережі, ділитися своїми думками.

Але є певні обмеження для цього права. Не можна висловлювати думки, які шкодять іншим людям або державному порядку денному.

Наприклад, якщо це стосується соцмереж, то дітям не можна постити контент, який суперечить політикам використання цих соцмереж.

Порушувати політики може жорстокий, расистський чи дискримінаційний контент; матеріал, який є образливим, порнографічним чи містить конфіденційну інформацію.

У соцмережі можуть видалити такий контент, тоді як акаунт – заблокувати.



2

Право доступу до мережі

Власне, дитина має право доступу до мережі інтернет з метою здійснення та користування іншими своїми правами.

В Україні, як і в світі загалом, є проблема з доступом до інтернету. У 2017 році в африканському регіоні близько 60% дітей не мали доступу до мережі, а в Європі цей показник складав менше 4%.

У нас ця проблема пов'язана з відсутністю всеукраїнського широкосмугово доступу до інтернету, що ускладнює доступ до інформації для дітей, які мешкають у селах та невеликих містечках.



3

Право на інформацію

Кожна дитина має право на доступ до інформації та матеріалів з різних національних і міжнародних джерел, особливо тих, які сприяють її здоровому фізичному та психічному розвитку; соціальному, духовному та моральному благополуччю.

А також дитина має право знати, яку інформацію про неї зберігає адміністрація школи, поліція чи соціальна мережа.



4

Право на приватність

Варто розуміти, що веб-сайти та кожна соціальна мережа збирають певні персональні дані про кожного користувача за його дозволом.

Цей дозвіл ми даємо, коли погоджуємося з політиками використання соцмереж. У таких політиках прописано, які дані про нас збирає соцмережа та як вони можуть бути використані.

Якщо це, наприклад, Instagram, то кожен користувач може подати запит і дізнатися, які дані про нього має ця мережа.

Насправді це не лише ім'я користувача, а й, крім того, дата, коли користувач змінив пароль, інформація про відвідані сайти, пошукові запити, користувачів, за якими ви слідкуєте; групи, на які підписані, лайки, збережені публікації тощо.

Приватність є однією з умов безпеки дітей у цифровому середовищі. Але не лише соцмережі можуть її порушувати.

Наприклад, коли батьки чи вчителі фотографують дітей без їхнього дозволу з різною метою, це також є порушенням права дітей на приватність.

До того ж варто зазначити, що діти мають право на безпеку в цифровому середовищі.

Так, станом на 11 листопада в Україні, за статистикою, було помічено 90128 мережових атак на користувачів. Крадіжка персональних даних,

зняття коштів із картки, злам акаунтів у соцмережах – це лише невеликий перелік загроз для дітей у інтернеті.

Тому необхідно піклуватися про цифрову безпеку дітей у школі та вдома. Наприклад, уникати публічних Wi-fi, придумувати складні паролі, використовувати разом із дітьми двофакторну автентифікацію в соцмережах. А ще важливо не забувати нагадувати дітям ставити під сумнів інформацію, яку вони споживають щодня, щоб розвивати їхнє критичне мислення. Висновок у тому, що інтернет, хоч і надає значну кількість можливостей, сповнений ризиків для дітей. Говорячи просто мовою, його можна порівняти з містом, де є багато красивих затишних місць та приємних людей, але є й місця, у які краще не заходити та люди, із якими краще не заводити розмову.

Кілька простих порад, які допоможуть мінімізувати ризики для дітей у інтернеті

Вони базуються на рекомендаціях, розроблених Міжнародним союзом електрозв'язку для батьків та вчителів.

■ Перевіряйте, якими додатками користуються діти та яку інформацію додатки про них збирають.

Для цього потрібно читати умови та політики використання застосунків чи соціальних мереж.

■ Подавайте скарги на контент або профілі, який ви бачите в мережах і який не слід бачити дітям. Розповідайте також і дітям, як це робити.

Чим більше ви скаржитесь, тим менше незрозумілих профілів та шкідливого контенту буде в соцмережах.

Те ж стосується і реклами, яка не відповідає інтересам дітей або є дуже нав'язливою.

11 правил безпеки в інтернеті, яких батьки мають навчити дітей

■ Намагайтеся забезпечити наявність доступу до інтернету для дітей.

Не варто забороняти дітям користуватися смартфонами та новітніми технологіями. Навпаки, їх потрібно зробити друзями та помічниками для них, а не ворогами.

■ Якщо діти користуються соціальними мережами, то потрібно знати, що їм має бути щонайменше 13 років для цього.

Або ж навіть якщо їм уже виповнилося 13 років, для використання TikTok, наприклад, потрібна згода батьків.

Не забувайте про функцію батьківського контролю. За допомогою неї ви можете фільтрувати контент і профілі, за якими слідкують діти.

■ Говоріть із дітьми про приватність. Розповідайте, яку інформацію про себе краще не публікувати. Це наприклад, документи, дані кредитних карток, місцезнаходження.

Нагадайте також, що діти мають певну онлайн-репутацію. І контент, який вони публікують, може побачити будь-хто. Змінити його після публікації може бути складно. Тому в соцмережах дуже рекомендовано налаштувати приватний

доступ до профілів, щоб контролювати, хто може бачити публікації дітей, хто може коментувати дописи тощо.

■ Перед тим, як фотографувати та публікувати світлини дітей у інтернеті, запитайте в них дозволу. Або якщо ви вчитель, то вам потрібно мати дозвіл батьків для цього.

■ Слідкуйте за своєю онлайн-репутацією. Особливо це стосується вчителів. Перевіряйте інформацію, на яку натрапляєте в інтернеті та нагадуйте про це дітям. Не поширюйте сумнівні дописи, які можуть бути фейкові.

■ Намагайтеся облаштувати безпечне середовище для дітей із використанням технологій.

Перевірте, чи встановлені на комп'ютерах в школі та вдома антивірусні програми та чи оновлене ліцензійне програмне забезпечення.

Встановлюйте складні паролі на телефони й комп'ютери та переконайтеся, що вони є на пристроях у дітей. І не забувайте про двофакторну автентифікацію.

■ Якщо дитина має онлайн-друга та хоче зустрітися із ним/нею вживу, то не дозволяйте йому/їй іти самій на таку зустріч, враховуючи, що люди не завжди можуть виявитися в реальному житті тими, ким видають себе в соцмережах.

■ Говоріть із дітьми про їхню онлайн-активність. Цікавтеся тим, що вони роблять у інтернеті, із яких джерел отримують новини тощо.

Важливо, щоб у дітей не виникало відчуття, що батьки їм не довіряють.

Отже, завданням батьків та вчителів залишається розповідати дітям про їхні цифрові права, критичне мислення і цифрову безпеку, а також і собі дотримуватися порад та правил.

Якщо деякі з рекомендацій є для вас незрозумілими чи складними, обов'язково перегляньте безкоштовний курс "Цифрові права та безпека для дітей", створений громадською організацією "МІНЗМІН".

Завдяки ньому ви зможете самостійно дізнатися детальніше про основні цифрові права дітей; про те, до кого звертатися, якщо їх порушують, та як цифрові права застосовані в Instagram, TikTok і YouTube.

У курсі знайдете також прості рекомендації, які допоможуть зробити вас захищеними від Інтернет-загроз та покажуть, як відрізнити правду від фейків.

Вчіться самі та навчайте дітей, бо цифрові компетенції є основою для безпечного життя в цифровому світі, який давно став новою реальністю не лише для дітей, але й для кожного з нас.

Джерело: <https://life.pravda.com.ua/columns/2020/12/1/243194/>