

Безпека дітей в інтернеті



Цифрове середовище, зокрема мережа Інтернет, сьогодні є не лише важливим джерелом інформації, але і способом комунікації, який нівелює перепони для спілкування. Через глобальний вплив COVID-19 діти проводять все більше часу в Інтернеті.

Зауважуємо, що *право дитини на безпеку та захист є базовим та поширюється на її життєдіяльність як онлайн, так і офлайн*. Разом з тим, не кожна дитина в Україні володіє достатнім рівнем знань щодо існуючих ризиків в цифровому середовищі та навичками безпечної поведінки в цифровому просторі. *Діти мають право отримувати знання та підтримку у використанні цифрового середовища*.

Комунікація у віртуальному просторі має свої особливості. Так, інформаційно-комунікаційні технології є важливим інструментом у житті дітей під час здобуття освіти, соціалізації, самореалізації. Водночас, *безконтрольне та безвідповідальне їх використання містить ризики для здоров'я, розвитку та благополуччям дітей*, зокрема:

- **контактні ризики** (сексуальні експлуатації та зловживання, домагання для сексуальних цілей («грумінг», розбещення), онлайн-вербування дітей для вчинення злочинів, участь у екстремістських політичних чи релігійних рухах або для цілей торгівлі людьми);
- **ризики контенту** (принизливе та стереотипне зображення та надмірна сексуалізація жінок та дітей; зображення та популяризація насильства та нанесення собі ушкоджень, зокрема, самогубств; принизливі, дискримінаційні або расистські вирази або заклик до такої поведінки; реклама, контент для дорослих);
- **ризики поведінки** (залякування, переслідування та інші форми утисків, розповсюдження без отримання згоди сексуальних зображень, шантаж, висловлювання ненависті, хакерство, азартні ігри, незаконне

завантаження або інші порушення прав інтелектуальної власності, комерційна експлуатація);

- **ризик для здоров'я** (надмірне використання призводить до позбавлення сну та фізичної шкода).

Всі перераховані вище ризики не є вичерпними, постійно оновлюються та здатні негативно вплинути на фізичне, емоційне та психологічне благополуччя дитини.

Так, одними з розваг серед підлітків в соціальних мережах, що, зокрема за умови відсутності компетентностей безпечної поведінки в цифровому просторі, можуть призвести до непоправної шкоди здоров'ю та життю дитини, стали Інтернет-челенджі та «групи смерті».

Челендж (англ. Challenge) – жанр інтернет-роликів, в яких блогер виконує завдання на відеокамеру і розміщує його в мережі, а потім пропонує повторити завдання своєму знайомому або необмеженому колу користувачів. Саме слово челендж зазвичай перекладається як «виклик» у контексті словосполучення «кинути виклик».

Найбільш небезпечними останнім часом стали челенджі:

- «вогняний челендж» (Fire challenge);
- «падіння в стрибку» (Tripping jump challenge);
- «проломити-череп-челендж» (Skull-breaker challenge);
- «отруєння капсулами для прання» (Tide pods challenge);
- «суїцидальний челендж Момо»;
- «удушення/непритомність/втрата свідомості» (Choking/fainting/pass-out challenge);
- «контрольована задуха» (Blackout challenge);
- «вибух розетки» (Outlet Challenge);
- «вистрибни з автомобіля» (Drake «In My Feelings»);
- «я без свідомості» (Pass out prank, Shocking games) тощо.

Вірусний характер поширення цих челенджів дозволяє їм швидко розповсюджуватись та продовжувати існувати, незважаючи на смертельну небезпеку. Служби технічного обслуговування та контролю за контентом популярних соціальних мереж не завжди вчасно виявляють та блокують контент, що закликає до небезпечних дій.

Однак кожен користувач, помітивши контент, який може загрожувати життю та безпеці інших, може звернутися до адміністрації сайту зі скаргою, і врятувати комусь життя.

Найбільш вразливими є підлітки (12-17 років), оскільки це етап активного формування самооцінки, інтересів, моральних уявлень, соціальних установок та потреби в спілкуванні з однолітками. Підліток прагне отримати новий

досвід та яскраві емоції, дізнатися, на що він здатний та усім продемонструвати свою винятковість, а соціальні мережі стають для нього платформою для отримання визнання та самоствердження. Однак, несформована психіка, емоційна нестабільність через великий потік інформації, можливі соціальні невдачі та бажання втекти від реальних проблем, вимушена ізоляція під час карантину знижують критичність підлітків до обраних ними способів поведінки. Підлітки в силу вікових особливостей намагаються відокремитись від батьків, відійти у бік і знайти себе. Якщо ж це не вдається, підлітки починають втрачати інтерес до життя, не даючи собі можливості знаходити інші варіанти розв'язання проблеми. Такі підлітки є найбільш вразливою групою для небезпечних челенджів та «груп смерті».

Важливо врахувати зворотній ефект інформування з метою попередження – *поширення інформації зростає пропорційно заходам, спрямованим на її видалення або попередження розповсюдження.*

Тому не варто детально зосереджуватись на суті самих ризиків цифрового середовища, зокрема суті небезпечних челенджів, щоб уповільнити таку закономірність, а сконцентрувати увагу на можливих наслідках для здоров'я та життя, на відповідальному ставленні до поведінки в цифровому просторі, критичному осмисленні та сприйнятті інформації, правилах інформаційної гігієни, а також інформуванні щодо можливостей отримати допомогу практичних психологів у критичних ситуаціях, в тому числі анонімно. Безпечна поведінка в цифровому середовищі включає в себе сукупність знань, умінь та цінностей щодо:

- 1) прав людей (зокрема права в цифровому середовищі);
- 2) електронної участі (участь у прийнятті рішень);
- 3) збереження здоров'я під час роботи з цифровими пристроями;
- 4) механізмів захисту прав, що порушуються в Інтернеті, а також способів отримати допомогу.

Додаткову інформацію, можна знайти на сайті Міністерства освіти і науки України в розділі «Безпека дітей в Інтернеті».

Позитивне спілкування між родиною та закладом освіти сприяє попередженню потрапляння дітей в небезпечні ситуації, в тому числі в цифровому середовищі, та вчасному виявленню таких ситуацій і реагуванню.

Поради для батьків:

- говорити з дитиною про безпеку в Інтернеті та допомагати розвивати критичне мислення, вчити робити аргументований вибір та нести відповідальність за його результати. Проста заборона використання гаджетів може призвести до втрати довіри дитини до дорослого та приховування нею своїх захоплень. Найперше варто говорити, пояснювати, формувати культуру використання Інтернету в повсякденному житті;

- будувати відкриті та довірливі стосунки з дитиною щодо використання технологій: підтримувати спілкування, давати поради. Дитина має знати, що дорослий поруч і готовий допомогти;
- разом з дитиною переглядати матеріали на її улюблених веб-сайтах та грати в її улюблені Інтернет-ігри. Це допоможе краще зрозуміти інтереси дитини, її захоплення та причини такого вибору. Також це може стати приводом для невимушеного початку розмови про безпеку в Інтернеті;
- формувати корисні звички використання гаджетів та цифрового середовища, розвивати цифрові, соціальні й емоційні навички, такі як: повага, емпатія, критичне мислення, відповідальна поведінка та психологічна стійкість;
- підвищувати самооцінку дитини, дозволяти дитині самостійно робити вибір і бути відповідальним за нього, вчити моделям поведінки із негативним досвідом в Інтернеті;
- заохочувати користуватись гаджетами в зонах видимості дорослих. Це допоможе тримати під контролем, з ким ваша дитина контактує в Інтернеті через телефон, планшет, смарт-телевізор, ігрову приставку та інші пристрої, підключені до Інтернету;
- встановлювати часові межі користування гаджетами, щоб балансувати час, проведений в режимі онлайн та флайн;
- контролювати додатки, ігри, веб-сайти та соціальні мережі, якими користується дитина, та їх відповідність віку дитини;
- вчитись встановлювати на гаджети дитини батьківський контроль, вимикати можливість спілкування або обміну повідомленнями в онлайн-чатах та функцію «поділитися розташуванням» у налаштуваннях додатків чи ігор, оскільки це може наразити дитину на небезпеку у вигляді небажаного контакту чи розкрити її фізичне місце розташування;
- перевіряти налаштування приватності в іграх та соціальних мережах, якими користується дитина, наявності в її профілі ввімкнених налаштувань приватності. Обмежити коло осіб, які можуть контактувати з дитиною та просити дитину радитись, перш ніж додавати нових друзів;
- використовувати доступні технології для налаштування батьківського контролю на пристроях, які можуть обмежувати шкідливий контент, контролювати дії дитини та обмежувати чи блокувати час користування підключеними до Інтернету пристроями або окремі функції (наприклад, камери, покупки через мобільні додатки);
- бути уважними до ознак страху чи тривоги, зміни поведінки, режиму сну та апетиту. Спостерігати, як дитина будує контакти зі світом: якщо більше сидить у гаджетах, замкнута й не може описати свій стан; не знаходить слова, щоби розповісти про свої почуття та проведений день; якщо

наживо не спілкується, не ходить у гості, не ходять в гості до неї; слухає депресивну, параноїдальну музику; має відсторонений погляд, апатію, дитина млява, має поганий апетит, не має інтересу в очах – у такому разі *треба звертатися до фахівців і знати, куди звернутися за додатковою порадою та підтримкою, а також повідомляти дитині, куди вона може у разі потреби звернутись по допомогу*. Важливо рахуватися з почуттями підлітка і не заперечувати їх, треба легалізувати ці почуття і дати дитині зрозуміти, що її приймають і про це можна говорити у родині.

У разі виявлення, що дитина стала жертвою будь-яких проявів насильства чи експлуатації, вербування чи маніпуляцій в цифровому просторі, варто одразу звернутись до Національної поліції України та надіслати повідомлення про правопорушення до департаменту кіберполіції Національної поліції України за посиланням (цілодобово) (див.: Поради з безпеки онлайн для батьків та опікунів).

Психологічну допомогу та підтримку можна отримати за номерами телефонів:

1) Національна гаряча лінія з питань протидії насильству та захисту прав дитини (Пн – Пт з 12:00 до 16:00):

- 0 800 500 225 (безкоштовно зі стаціонарних);
- 16 111 (безкоштовно з мобільних).

2) Онлайн консультація для підлітків в Teenenergizer.

3) Чат-бот у Telegram і Viber допоможе дізнатись, куди звертатись за допомогою.

Встановити «батьківський контроль» для пристроїв із операційною системою Windows 10 можна за такою послідовністю дій:

- 1) перейдіть з меню Пуск в розділ «Облікові записи користувачів»;
- 2) у категорії «Сім'я та інші користувачі» натисніть «Додати члена сім'ї»;
- 3) операційна система на вибір запропонує створити профіль для дитини або дорослого;
- 4) обравши відповідний пункт, введіть адресу електронної пошти. Для підтвердження адреси зайдіть в папку вхідних повідомлень електронної пошти.

Важливо: операційна система не дозволить активувати «батьківський контроль» для локального облікового запису. Створіть новий профіль для кожного користувача, якого належить контролювати.

Встановити «батьківський контроль» для пристроїв з операційною системою Android можна за такою послідовністю дій:

- 1) відкрийте програму «Play Маркет»;
- 2) у лівому верхньому кутку екрану натисніть на значок «меню» і виберіть «Установки» – «Батьківський контроль».
- 3) увімкніть означену функцію.
- 4) обмежте доступ до налаштувань «батьківського контролю», встановивши PIN-код.

5) встановіть такі фільтри: «Додатки, ігри, фільми і серіали. Виберіть максимально допустиме вікове обмеження для контенту», «Музика і книги. Забороніть завантаження і покупку контенту для дорослих».

Важливо: «батьківський контроль» діє тільки на тому пристрої, де ви його налаштували. При необхідності ввімкніть його на іншому пристрої, знову виконавши наведені вище інструкції.

Встановити «батьківський контроль» для пристроїв «iPhone», «iPad», «iPod touch» можна за такою послідовністю дій:

- 1) перейдіть в меню «Налаштування» – «Основні» – «Обмеження».
- 2) покрутіть вниз і натисніть «Обмеження», а потім «Включити обмеження».
- 3) створіть пароль функції «Обмеження». Код-пароль обмежень необхідний для зміни налаштувань або відключення обмежень.

Крім того, на сайтах підтримки від виробників можна отримати додаткову інформацію щодо принципів роботи та точного налаштування функції «батьківського контролю»

Безпека в інтернеті



Щоб запобігти всім тим негативним явищам та небезпекам, які очікують в Інтернеті, необхідно навчитися правильній поведінці та безпечним користуванням сучасними Інтернет технологіями