Переклад документа створений за ініціативи Міністерства цифрової трансформації України громадською організацією “МІНЗМІН” за фінансової підтримки Міжнародного союзу електрозв’язку (МСЕ). Документ не було перекладено МСЕ, і його не слід вважати офіційним перекладом чи публікацією. МСЕ не несе відповідальності за будь-який зміст або помилку в цьому перекладі.

Захист дітей у цифровому середовищі: рекомендації для батьків та освітян

Слова подяки

Чинні Рекомендації розроблені Міжнародним союзом електрозв'язку (МСЕ) та робочою групою авторів із провідних установ, що працюють у індустрії інформаційно-комунікаційних технологій (ІКТ) і переймаються проблемами захисту дитини (в цифровому середовищі), зокрема, з таких організацій, як-от:

ECPAT International, The Global Kids Online network, Міжнародний союз інвалідів, Міжнародний союз електрозв'язку (МСЕ), Лондонська школа економіки та політичних наук, Internet matters, Parent Zone International і Центр безпечного Інтернету Сполученого Королівства/SWGfL Робочу групу очолював Карл Хопвуда (Мережа Інсейф Центру безпечного Інтернету (Insafe та координувала Фанні Ротіно (МСЕ).
Вагомий внесок зробили також COFACE-Families Europe, Комісаріат з електронної безпеки Австралії, Європейська комісія, Європейська рада, Група e-Worldwide Group (e-WWG), Міжнародний центр із пошуку зниклих та експлуатованих дітей (ICMEC), Молодь та соціальні мережі/Центр Беркмана Клейна з питань дослідження Інтернету та суспільства Гарвардського університету, а також урядів окремих країн і зацікавлених сторін приватного сектора, об'єднаних спільною метою – зробити інтернет кращим та більш безпечним місцем для дітей і молодь.

Ці Рекомендації не змогли б реалізуватися без витраченого авторами часу, властивого їм ентузіазму та самовідданості.
Далі перелічені партнери, яким МСЕ висловлює подяку за те, що вони виділили свій дорогоцінний час та поділилися власними поглядами (перелік наводиться в алфавітному порядку за назвою організації):

• Джулія Фоссі та Елла Серрі (Комісаріат з електронної безпеки Австралії) • Мартін Шмальцрід (COFACE-Families Europe)
• Лівія Стойка (Рада Європи)
• Джон Карр (ECPAT International)
• Мануела Марта (Європейська комісія)
• Сальма Аббасі (e-WWG)
• Лаурі Ташарскі (ICMEC)
• Люсі Річардсон (Міжнародний союз інвалідів)
• Кароліна Бантінг (Internet matters)
• Фанні Ротіно (МСЕ)
• Соня Лівінгстон (Лондонська школа економіки та Global Kids Online) • Кліфф Мейнінг та Віккі Шотболт (Parent Zone International)
• Девід Райт (Центри безпечного Інтернету Сполученого Королівства/SWGfL) • Сандра Кортезі (Youth and Media)

У рамках Connecting Europe Facility (CEF) мережа European Schoolnet керує від імені

Європейської комісії платформою «Розширення доступу до Інтернету для дітей», зокрема, координує діяльність безпечної мережі європейських Центрів безпечного Інтернету. Докладніша інформація доступна за адресою: www.betterinternetforkids.eu

ISBN
978-92-61-30144-6 (друкована версія)
978-92-61-30474-4 (електронна версія)
978-92-61-30134-7 (версія EPUB)
978-92-61-30484-3 (версія Mobi)

Будь ласка, згадайте про довкілля, перш ніж друкувати цей звіт

Передмова

Свій перший комплект Рекомендацій щодо захисту дитини в цифровому середовищі МСЕ розробив 2009 року. Тоді наша мета полягала в тому, щоб надати різним зацікавленим сторонам – батькам та педагогам, галузевим організаціям, директивним органам та дітям – узгоджені на міжнародному рівні принципи задля надання наймолодшим користувачам Інтернету можливостей безпечного, достатнього та впевненого перебування в цифровому середовищі.

Відтоді Інтернет зазнав разючих змін. Він став безмежним джерелом для дітей, що пропонує їм навчальні ігри, різного роду розважальні заходи, а також численні способи обміну інформацією, отримання знань та цілеспрямованої взаємодії з друзями, родиною та зовнішнім світом. Проте водночас він став для них надто небезпечним місцем для занять без нагляду.

Сьогодні діти та їхні опікуни наражаються на численні ризики й виклики: від проблем захисту конфіденційності, поширення свідомо неправдивих новин та «глибоких підробок» до контенту з елементами насильства та іншого неналежного контенту, інтернет-шахрайства, а також загроз у вигляді грумінгу, сексуальних зловживань й сексуальної експлуатації в цифровому середовищі.

Крім цього, глобальна пандемія COVID-19 призвела до збільшення кількості дітей, які вперше почали користуватися Інтернетом для продовження своєї освіти та підтримки соціальної взаємодії. Обмеження, зумовлені вірусом, означають не лише те, що чимало дітей більш юного віку починають спілкуватися в Мережі набагато раніше, ніж, можливо, планували їхні батьки, але й те, що через необхідність перегляду своїх робочих зобов'язань багато батьків, як виявилося, не в змозі контролювати своїх дітей, наражаючи їх на ризик доступу до неприйнятного контенту або перетворення на мішень для злочинців, що створюють матеріали, пов'язані із сексуальними зловживаннями стосовно дітей.

Визнаючи це, держави – члени МСЕ вимагали дещо більшого, ніж своєчасне оновлення Рекомендацій щодо СОР, яке до цього ми проводили періодично. І ми підготували ці нові переглянуті Рекомендації, які були переосмислені, переформульовані та перебудовані від початку до кінця, щоб відтворити фундаментальні зміни у цифровому середовищі, що оточує нинішнє покоління дітей.

Стосовно вас, користувачів цих Рекомендацій, наша мета полягала в тому, щоб підвищити вашу обізнаність про масштаби проблеми та надати джерело інформації, яке допоможе вам ефективно підтримувати молодь щодо їх взаємодії з онлайновим світом. Ці Рекомендації дозволять привернути вашу увагу до потенційних ризиків й загроз і допоможуть сформувати здорове середовище, що розширює права та можливості вдома та в школі. У них зосереджена увага на важливості відкритого спілкування й постійного діалогу з дітьми, створення безпечного середовища, де молоді користувачі Інтернету усвідомлюють власне право порушувати питання, які їх бентежать.

Окрім додавання нових розробок у сфері цифрових технологій та платформ, у цьому новому виданні усунено значну прогалину: в ньому приділяється увага становищу дітей з інвалідністю, для якихцифрове середовищевідкриває надважливі можливості щодо забезпечення повноцінної участі в соціальному житті. У цьому документі також враховані особливі потреби дітей-мігрантів та інших вразливих груп.

Я пишаюся тим, що ці Рекомендації є результатом спільної роботи на загальносвітовому рівні, та їх співавторами є фахівці з широкої міжнародної спільноти, що відповідає

справжньому призначенню МСЕ як глобального організатора.

Також залюбки представляю нового талісмана – Санго – доброзичливого, непосидючого та відважного персонажа, створеного групою дітей у межах нової міжнародної програми МСЕ зв'язків з молоддю.

В епоху, коли дедалі більше молоді залучаються до онлайн-технологій, ці Рекомендації із СОР є надважливими. Батьки й освітяни, галузеві організації, директивні органи та самі діти – усі відіграють життєво важливу роль у гарантуванні безпеки дітей в цифровому середовищі. Сподіваюся, ви вважатимете їх корисними, коли будете доглядати за дітьми в їхній захоплюючій подорожі, що відкриває численні приголомшливі можливості, які пропонує Інтернет.

Дорін Богдан-Мартін

Директор Бюро з розвитку електрозв'язку

Зміст

Перелік таблиць та малюнків

Таблиці

Малюнки

Резюме

Згідно з даними МСЕ у 2019 році, Інтернетом користувалися приблизно 4,1 мільярда людей, що на 5,3% більше в порівнянні з 2018 роком.

Діти та молодь використовують Інтернет з різною метою: від отримання інформації в межах практичних шкільних занять до спілкування з друзями. Вони дуже вміло опановують складні програми та додатки, приєднуючись до Інтернету за допомогою мобільних телефонів, планшетів та інших портативних пристроїв, наприклад, годинників, iPod Touch, електронних книг та ігрових приставок1.

Інтернет слугує також як важливий інструмент у житті різних вразливих груп дітей та молодь. Наприклад, він допомагає дітям-мігрантам підтримувати зв'язок із родиною та друзями і відкриває вікно в культурне життя в їхньому новому помешканні. Він дозволяє дітям та молодим особам-інвалідам спілкуватися й брати участь у різних видах діяльності, недоступної для них за умов відсутності доступу до Інтернету і надає їм можливість бути на рівних з однолітками в цифровому середовищі, вирізняючись радше своїми здібностями, ніж фізичними вадами.

З іншого боку, поряд з наданням доступу та різних можливостей Інтернет несе в собі ризики та шкоду, до яких дехто схильний більше, ніж інші. Наприклад, для дітей та молодь-мігрантів наслідки онлайнового порушення конфіденційності інформації можуть мати драматичний характер: в чужих руках отримані дані можуть бути використані для

виявлення та цілеспрямованого впливу на людей через їхню етнічну приналежність, імміграційний статус або інший символ приналежності2; дітей та молодь з розладами аутистичного спектра (ASD) такі соціальні виклики, як труднощі з розумінням намірів інших, можуть залишити в уразливому стані перед обличчям так званих «друзів», які переслідують погані наміри; а діти та молодь-інваліди більше схильні до соціальної ізоляції, знущання й маніпулювання.

Чимало батьків та опікунів схильні до звичних помилок, вважаючи, що їхні діти перебувають у більшій безпеці, якщо користуються комп'ютером вдома або в школі, ніж в будь-якому іншому місці. Це небезпечна помилка, тому що Інтернет здатен переносити дітей та молодь практично в будь-який куточок світу, і саме в цей час вони можуть наражатися на потенційно небезпечні ризики, майже ідентичні тим, коли б вони перебували в реальному світі. При цьому діти та молодь, отримуючи доступ до Інтернету за допомогою смартфонів, планшетів або інших портативних пристроїв, відчувають лише незначну загрозу заподіяння шкоди. Це пояснюється тим, що такі портативні пристрої надають їм миттєвий доступ до Інтернету з будь-якого місця та з меншою ймовірністю контролю з боку батьків чи опікунів.

Ці Рекомендації були підготовлені в межах ініціативи із захисту дитини в цифровому середовищі (COP) як частина Глобальної програми з кібербезпеки МСЕЗ, щоб слугувати підґрунтям для безпечного та захищеного кіберсвіту не тільки для нинішньої молоді, а й для майбутніх поколінь. Вони орієнтовані також на дітей із вразливих груп населення, зокрема, на дітей-мігрантів, дітей з ASD та дітей з інвалідністю.

Передбачається що ці Рекомендації слугуватимуть як програма, що може бути адаптована та використовуватися з урахуванням чинних національних або місцевих звичаїв та законів, і допоможе вирішити проблеми, які можуть стосуватися усіх дітей та молодь віком до 18 років.

Рекомендації для батьків та освітян щодо захисту дитини в цифровому середовищі

Конвенція ООН про права дитини визначає дитину як особу віком до 18 років. Ці Рекомендації стосуються проблем, що постають перед усіма особами, які не досягли 18 років, в усіх частинах світу. Однак малоймовірно, що семирічний користувач Інтернету матиме ті самі потреби та інтереси, що й 12-річний учень середньої школи або 17-річний підліток на межі дорослості. Ці Рекомендації розроблені для того, щоб запропонувати пораду або рекомендації, що застосовуються до різних умов, оскільки особливі потреби вимагають індивідуального розгляду, а різні місцеві, правові та культурні чинники справляють значний вплив на те, як ці Рекомендації можуть використовуватися або витлумачитися в певній країні або регіоні.

1. Вступ

На глобальному рівні кожен третій користувач Інтернету молодше 18 років – гігантська величина, зважаючи на той факт, що у 2018 році більше половини населення світу застосовувало Інтернет. У країнах, що розвиваються, основними користувачами Інтернету є діти, які дорослішають разом з Інтернетом і першими долучаються до рухомого зв'язку .

В умовах, коли дедалі більше дітей у всьому світі отримують доступ до Інтернету,

реалізація їх прав часто-густо формуватиметься під впливом того, що відбувається у Мережі. Доступ до Інтернету має істотне значення для реалізації прав дітей.

Тепер, коли кожна третя дитина є користувачем Інтернету, у світі ще залишаються 346 мільйонів дітей, які не мають можливості під'єднання до Мережі . Ті, хто, здавалося б, мають в першу чергу скористатися можливостями, що надаються Інтернетом, зазвичай є найменш долученими. Ми бачимо, що в африканському регіоні приблизно 60 відсотків дітей не мають доступу до Мережі, тоді як в Європі їх кількість становить 4 відсотки .

Що стосується доступу до Інтернету, то тут також існують істотні відмінності залежно від статевої приналежності. Дослідження показують, що в кожному регіоні, за винятком Північної та Південної Америки, кількість чоловіків-користувачів Інтернету чисельно перевершує кількість жінок-користувачів. У багатьох країнах дівчатка не мають таких самих можливостей доступу, як хлопчики. І навіть тоді, коли вони мають ці можливості, над ними нерідко здійснюється контроль та на них поширюється набагато більше обмежень щодо використання Інтернету.

Цифровий розрив не обмежується проблемою доступу. Діти, які використовують переважно мобільні телефони, а не комп'ютери, можуть придбати тільки другий за якістю онлайновий досвід, а ті, в кого відсутні цифрові навички, або ті, хто володіє тільки мовою етнічних меншин, нерідко не можуть знайти в Мережі відповідний контент. У дітей із сільських районів з більшою ймовірністю можуть бути зламані паролі або поцуплені гроші. Крім того, вони гірше володіють цифровими навичками, витрачають більше часу в Мережі (зокрема, граючись в ігри) та відчувають менше посередництва й контролю з боку батьків .

Як діти, так і дорослі повідомляють, що цифровий розрив викликає у них постійне занепокоєння, а отже вимагає цільового інвестування та творчих рішень. За таких умов кількість дітей в Мережі постійно збільшується, проте чимало з них не отримують належного керівництва з боку батьків, освітян та інших авторитетних дорослих. У результаті діти продовжують наражатися на ризик. Інтернет став технологією, що надає істотні переваги й можливості. Переваги Інтернету та пов'язаних з ним цифрових технологій особливо помітні дітям та молодим особам. Ці технології змінюють спосіб нашого спілкування один з одним та відкривають безліч нових шляхів для ігор, прослуховування музики й участі у різноманітних культурних заходах, долаючи численні бар'єри. Перебуваючи в цифровому середовищі, діти можуть розширити свої горизонти, скориставшись можливостями збору інформації та встановлення зв'язків. Доступ до ІКТ дозволяє їм набути навичок, що доповнять інші форми їх участі поза мережею. Інтернет є засобом отримання доступу до послуг у сфері охорони здоров'я та освіти, а також інформації, яка має неабияке значення для молодь, але може розглядатися як табу в суспільстві, до якого вони належать. Діти та молодь нерідко стають першими, хто приймає та застосовує нові можливості, що представлені Інтернетом.

Рекомендації для батьків та освітян щодо захисту дитини в цифровому середовищі

Звісно, не можна заперечувати той факт, що з появою Інтернету виникло безліч завдань щодо гарантування безпеки дітей та молоді, які потребують рішення, як через те, що вони є значущими самі по собі, так і через те, що важливо донести до кожного, хто сумнівається, той факт, що Інтернет є тим середовищем, якому можна довіряти. Так само важливо не допустити того, щоб занепокоєння з приводу захисту дітей та молоді в

цифровому середовищі стало приводом для виправдання звинувачень у порушенні свободи слова, свободи вираження своїх думок та свободи зібрань.

Надважливо, щоб наступне покоління могло впевнено використовувати Інтернет, щоб воно мало змогу, своєю чергою, продовжувати користуватися перевагами його розвитку. Таким чином, під час обговорення питань з безпеки дітей та молоді в цифровому середовищі вкрай важливо обрати золоту середину.

Потрібно відкрито обговорювати ризики, з якими можуть мати справу діти та молодь в цифровому середовищі, щоб навчити їх розпізнавати ризики, а також запобігати або ліквідувати збитки, якщо вони були заподіяні, без надмірного залякування дітей та перебільшення небезпеки.

Малоймовірно, що підхід, де враховуються винятково або в основному негативні аспекти технології, серйозно сприйматиметься дітьми та молодими особами. Батьки та освітяни можуть нерідко опинитися у невигідному для себе становищі, оскільки молодь часто-густо знає про технології та їх можливості більше, ніж люди старших поколінь. Дослідження показали, що велика частина дітей здатна відрізнити кіберБулінг від простого жарту або підсміювання в Мережі, усвідомлюючи, що кіберБулінг має на меті заподіяти шкоду. У багатьох частинах світу діти дійсно добре розуміють ризики, з якими вони мають справу в Мережі .

Однак, хоча можна зробити висновок, що зусилля з навчання дітей навичкам керування онлайновими ризиками є ефективними, ще існують можливості для підвищення інформованості багатьох в усьому світі, надто з лав уразливих груп, і саме на цих дітей мають бути спрямовані узгоджені зусилля, зокрема, для того, щоб підвищити їх обізнаність про наявність служб допомоги жертвам кіберБулінг та інших форм онлайнових ризиків.

Попереду ще багато проблем. Проблеми створює не тільки доступ до підключеного світу. Стрімкість змін в технологіях створює проблеми гарантування безпеки дитини в цифровому середовищі. Багато дітей досліджують складний ландшафт цифрових засобів. Досягнення у сферах штучного інтелекту та машинного навчання, віртуальної та доповненої реальності, великих даних, розпізнавання осіб, робототехніки й Інтернету речей покликані ще більше змінити способи роботи в середовищі.

Важливо, щоб усі зацікавлені сторони планували свої дії, осмислювали наслідки таких змін для дітей та знаходили способи надання підтримки у формуванні в них необхідної цифрової грамотності, щоб не тільки вижити, а й досягти успіхів у цифровому майбутньому. Потрібні додаткові капіталовкладення у розвиток цифрових навичок та формування грамотності у батьків і освітян, щоб допомогти дітям розвинути критичне мислення та навички оцінки, що дозволить їм швидко досліджувати нинішні потоки інформації різної якості, а також інформації від батьків та освітян до дітей, щоб стати сучасними цифровими громадянами .

Проведені МСЕ консультації показали, що деякі країни прагнуть виділити достатні ресурси для формування цифрової грамотності та гарантування безпеки дитини в цифровому середовищі. Разом з тим діти повідомляють, що батьки, освітяни, технологічні компанії

Рекомендації для батьків та освітян щодо захисту дитини в цифровому середовищі

та державні органи є важливими гравцями у розробці рішень на підтримку їх безпеки в

цифровому середовищі. Дослідження МСЕ, проведені серед держав-членів, показують наявність широкої підтримки ідеї активного обміну знаннями та докладання узгоджених зусиль до гарантування безпеки для дітей в цифровому середовищі.

Проблемою залишається пошук балансу між можливостями та ризиками, пов'язаними з діяльністю дітей в цифровому середовищі. Держави – члени МСЕ також звернули увагу на те, що хоча зусилля, спрямовані на сприяння використанню можливостей, що відкриваються перед дітьми в цифровому середовищі, як і раніше мають залишатися одним з основних пріоритетів, вони повинні бути добре збалансовані з правами на безпечні умови, в яких діти могли б брати участь в цифровому світі та користуватися результатами цієї участі .

2. Що таке захист дитини в цифровому середовищі?

Онлайн-технології надають дітям та молодим особам численні можливості для спілкування, набуття нових навичок, творчості та участі у створенні кращого суспільства. Водночас вони можуть також принести із собою нові ризики, наприклад, ставлячи перед ними питання конфіденційності, наражаючи їх на такі небезпеки, як незаконний контент, домагання, кіберБулінг, неправомірне використання персональних даних, грумінг та навіть сексуальні зловживання щодо дітей.

Ці Рекомендації визначають цілісний підхід до реагування на будь-які потенційні загрози та шкоду, з якими можуть мати справу діти та молодь під час набуття цифрової грамотності. У них визнається той факт, що всі зацікавлені сторони відіграють свою роль в реалізації стратегії кібербезпеки, забезпеченні добробуту та захисту дітей, користуючись водночас можливостями, які може запропонувати Інтернет.

Захист дітей – це спільна відповідальність, і всі відповідні зацікавлені сторони мають забезпечити стійке майбутнє для кожного. Щоб домогтися цього, директивні органи, представники приватного сектора, батьки, опікуни, освітяни та інші зацікавлені сторони мають забезпечити можливість дітям реалізувати свій потенціал – в цифровому середовищі та в реальному житті.

Батьки, опікуни та освітяни також несуть відповідальність за забезпечення того, щоб діти та молодь використовували інтернет-сайти безпечно та відповідально.

В останні роки масштаби доступу до мобільного Інтернету значно зросли, і для захисту дітей та молоді в цифровому середовищі не існує єдиного вірного рішення. Це глобальна проблема, що вимагає глобального рішення за участю усіх верств суспільства, зокрема, дітей та молоді.

У пошуках вирішення цих нагальних проблем в умовах стрімкого розвитку ІКТ, МСЕ виступив у листопаді 2008 року з багатосторонньою міжнародною ініціативою щодо захисту дитини в цифровому середовищі (СОР) . Ця ініціатива продовжує об'єднувати партнерів з усіх секторів глобального співтовариства з метою дотримання безпечних сприятливих умов для онлайнового спілкування дітей та молодь у всьому світі. У ній сформульовані Рекомендації для всіх зацікавлених сторін, включаючи самих дітей та молодь, в усіх частинах світу щодо того, як зберегти свою та чужу онлайнову безпеку. Ці Рекомендації слугують як програма, яка може бути адаптована та використана з урахуванням національних або місцевих традицій та законів.

Цей звіт підготовлено в рамках ініціативи СОР робочою групою експертів-представників багатьох зацікавлених сторін та має на меті надати батькам, опікунам і педагогам інформацію, поради та підказки з безпеки щодо захисту дитини в цифровому середовищі.

Робоча група експертів МСЕ стала одним зі співавторів Рекомендацій, що містяться в цьому звіті, взявши за основу перші Рекомендації МСЕ із СОР, випущені 2009 року та оновлені 2016 року. На прохання держав-членів МСЕ розпочав у 2019 році процес перегляду розробки другої версії Рекомендацій.

Ці нові Рекомендації враховують особливу ситуацію дітей з інвалідністю, аналізуючи ризики та шкоду, яка може бути заподіяна в цифровому середовищі, а також проблеми, пов'язані

з розвитком нових технологій, як-от мобільний Інтернет, додатки, Інтернет речей, іграшки, поширені в Інтернеті, онлайн-ігри, робототехніка, машинне навчання та штучний інтелект.

3. Діти та молодь в об’єднаному світі

За наявними оцінками, на глобальному рівні кожна третя дитина є користувачем Інтернету, а кожен третій користувач Інтернету є особою молодше 18 років15. У 2017 році половина населення світу використовувала Інтернет; в групі осіб віком від 15 до 24 років ця частка збільшилася до приблизно двох третин.

«Ми дорослішали разом з Інтернетом. Я хочу сказати, що Інтернет завжди був поруч з нами. Дорослі кажуть щось на кшталт: «Дивіться, Інтернет з'явився», тоді як для нас це абсолютно нормально,

- хлопчик 15 років із Сербії.

Серед дітей та молоді найпопулярнішим засобом доступу до Інтернету є мобільний телефон. Це символізує одну з найбільш важливих змін, що відбулися за останнє десятиліття. У Європі та Північній Америці перше покоління користувачів Інтернету входило в систему з використанням настільного комп'ютера, проте в більшості країн, що розвиваються, користувачі Інтернету орієнтуються насамперед на мобільні пристрої.

Діти та молодь віддають перевагу використанню мобільних телефонів, оскільки вони можуть носити їх скрізь; їм не доводиться ділитися своїм пристроєм з іншими членами родини; телефон дозволяє одночасно виконувати кілька функцій, наприклад, надсилати текстові повідомлення, спілкуватися, вибирати меню, обмінюватися зображеннями та отримувати доступ до ресурсів; і він постійно увімкнений.

«З телефоном якось простіше. Ми можемо носити його із собою всюди, він менший за своїми розмірами та на ньому легше працювати. У цьому сенсі мені подобається більше [працювати на ньому] пальцями, а не на клавіатурі»,

- дівчинка 12 років із Сербії.

Дослідження показали, що серед дітей та молоді, що мають доступ до Інтернету, дівчатка та хлопчики однаковою мірою використовують мобільні телефони для виходу в онлайнове середовище. Для порівняння, настільні комп'ютери частіше використовують хлопчики.

На практиці діти та молодь здебільшого здійснюють доступ до Інтернету з використанням декількох пристроїв, при цьому в кожній країні, що досліджувалася, хлопчики використовують, як правило, більше пристроїв, ніж дівчатка.

Діти та молодь витрачають в середньому приблизно дві години на день для роботи в Мережі протягом тижня і приблизно вдвічі більше в кожен з вихідних днів. Дехто з них відчуває себе постійно підключеними. Разом з тим багато людей ще не мають доступу до Інтернету у себе вдома або мають лише обмежений доступ. Проте статистичні дані надто відрізняються, й існує чимало різних думок щодо того, скільки часу діти проводять у Мережі. Останні дослідження, проведені організацією DQ Institute, показують, що діти та молодь в Австралії можуть витрачати до 38 годин на тиждень на роботу в Мережі16.

«Я прямую до кафе, тому що в мене немає комп'ютера вдома У нас немає доступу у Інтернету в школі»,

- хлопчик віком 15-17 років, Південна Африка.

«[Я маю Інтернет] увесь день, однак не можна сказати, що я використовую його протягом усього дня», – хлопчик віком 13-14 років, Аргентина.

Незважаючи на висновки Global Kids Online (GKO) про те, що загальна кількість дівчаток та хлопчиків, що мають доступ до Інтернету, приблизно є рівною, в деяких країнах хлопчики мають більше свободи у використанні Інтернету, ніж дівчатка, причому дівчатка частіше піддаються контролю та обмеженням під час використання Інтернету.

Світ розваг

Діти та молодь досить часто виходять вцифрове середовищев пошуках позитивних вражень та різновидів розваг. Найпопулярнішим видом діяльності як хлопчиків, так і дівчаток, в 11 країнах, які були досліджені, є перегляд відеокліпів. Понад три чверті дітей та молодь, які використовують Інтернет, кажуть, що вони переглядають відео в Інтернеті принаймні один раз на тиждень окремо або з членами своєї родини.

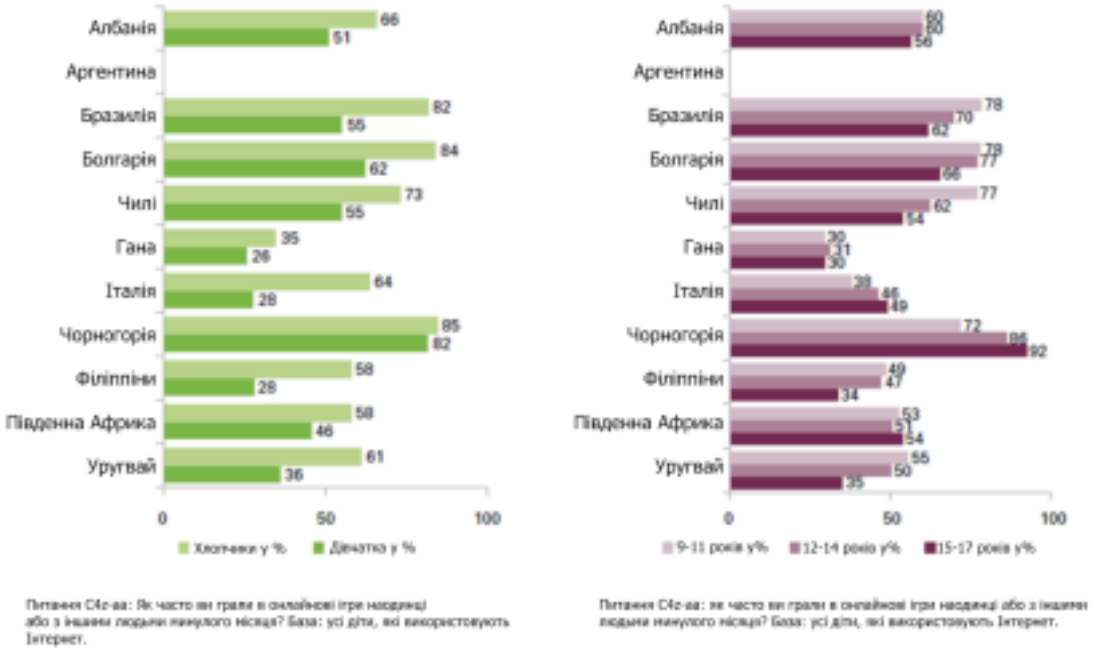
«Коли мама купила ноутбук, ми почали проводити більше часу разом; кожен вихідний ми вибирали певний фільм і переглядали його з бабусею», – дівчинка 15 років з Уругваю.

Діти та молодь віддають перевагу також онлайновим іграм, реалізуючи тим самим своє право грати, а іноді – своє право дізнаватися щось нове. Хлопчики охочіше грають в онлайн ігри в усіх країнах, що досліджувались. Втім, значна кількість дівчаток, які використовують Інтернет, також грають в онлайн-ігри, наприклад, більшість дівчаток грають в онлайн-ігри: в Болгарії (60%) та Чорногорії (80%). Як і з переглядом відео, діти та молодь охочіше грають в онлайн-ігри, коли мають більш зручний доступ до Інтернету.

«Я граю в онлайн-ігри та заробляю на них гроші», – хлопчик 17 років, Філіппіни.

Дорослі занепокоєні тим, що діти та молодь забагато часу проводять біля екрана, або вважають, що вони марнують час за онлайновими розвагами. Згідно з Global Kids Online такі поширені види діяльності можуть забезпечити дітям та молодим особам гарні стартові можливості, які допоможуть їм сформувати відповідні інтереси та навички, що знадобляться для подальшого набуття в цифровому середовищі досвіду у навчанні, інформативного досвіду та досвіду суспільного життя.

Малюнок 1: Діти (у %), які грають в онлайн-ігри не рідше одного разу на тиждень, з розподілом за статтю та віком



Джерело: UNICEF

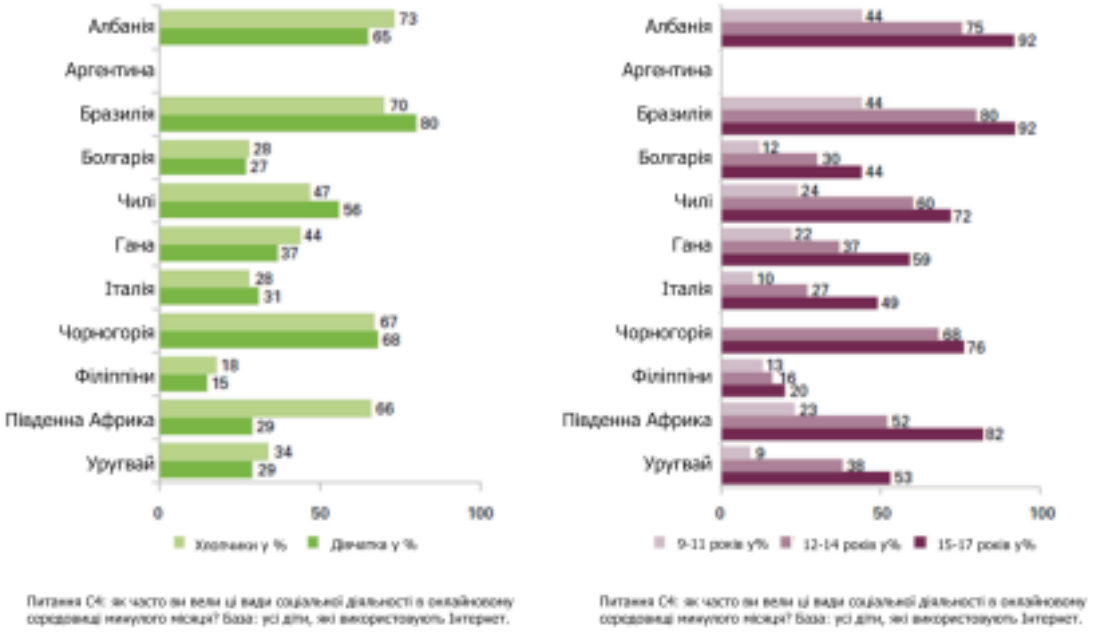
Встановлення нових зв'язків

Інтернет з його засобами миттєвого обміну повідомленнями та соціальними мережами став важливим місцем зустрічей, де діти та молодь можуть реалізувати право на вільне висловлення своїх думок, з'єднуючись зі своїми друзями, членами родини, іншими дітьми та молодими особами, які поділяють їхні інтереси. Багато дітей та молодь в 11 країнах, які досліджувалися, можуть вважатися активними учасниками соціального середовища в тому сенсі, що вони щотижня активно беруть участь низках онлайнових видів діяльності в соціальних мережах, наприклад, спілкуючись з друзями та членами своєї родини, використовуючи різні засоби обміну повідомленнями та взаємодіючи з людьми, що поділяють їхні інтереси. Дехто з дітей повідомляє також, що їм легше висловити власне «Я» в цифровому середовищі.

«В цифровому середовищі я можу проявити своє справжнє «Я», тут немає жодних правил... У мене понад 5000 друзів в Інтернеті», – хлопчик, який вважає себе геєм, віком 15 років, Філіппіни.

Онлайнова соціальна взаємодія також зростає в міру збільшення віку його учасників через різні причини. Так, наприклад, вебсайти деяких соціальних мереж встановлюють мінімальні вікові обмеження для дітей та молодь, оскільки зі збільшенням віку зазвичай надається більше свободи.

Малюнок 2: Діти (у %), які ведуть не менше трьох видів соціальної діяльності в цифровому середовищі не рідше одного разу на тиждень, з розподілом за статтю та віком



Примітка: Дітям та молодим особам було поставлено питання, як часто вони вели такі види соціальної діяльності в цифровому середовищі минулого місяця: використовували Інтернет для спілкування з людьми з місць або верств суспільства, що відрізняються від ваших; відвідували вебсайти соціальних мереж; розмовляли з членами родини або друзями, що живуть в інших місцях; використовували миттєвий обмін повідомленнями; відвідували вебсайти, на яких люди діляться інформацією про свої інтереси й улюблені заняття.

Джерело: UNICEF

З наданих вище даних видно, що Інтернет відкриває нові можливості для встановлення соціальних зв'язків, хоча батьки часто скаржаться, що Онлайн-взаємодія дітей та молодь завдає шкоди особистим контактам в реальному світі.

«На вечірці вони сидять за столом, причому в усіх десяти в руках маленькі пристрої», – батько підлітків віком 15-17 років, Чилі.

Така поведінка характерна не тільки для дітей та молоді. Дехто з батьків телефонує або переглядає Інтернет під час громадських заходів, що непокоїть багатьох дітей та молодь.

«За столом, коли ми їмо, тато користується своїм телефоном. Це рідкісний випадок, коли ми всі збираємося разом, і це дійсно роздратовує», – дівчинка 14 років, Уругвай.

З розширенням доступу до Інтернету діти та молодь можуть розширювати свої горизонти, збирати інформацію та поглиблювати свої зв'язки. В умовах зростаючої соціальної взаємодії, як онлайнової, так і особистої, вони накопичують власний досвід та знання. Дослідження

GKO показують, що діти та молодь, які активно спілкуються в соціальних мережах Інтернету, краще справляються з керуванням конфіденційністю в цифровому середовищі, що допомагає їм зберігати власну безпеку.

Радість творчості

Частина онлайнового контенту, яку діти та молодь знаходять і поціновують, створюється іншими дітьми та молодими особами. Зазвичай від 10 до 20 відсотків дітей та молодь в 11 країнах, які досліджувалися Global Kids Online, щотижня створюють та завантажують відео або музику, щотижня роблять запис у блозі, викладають будь-які події або створюють вебсторінки.

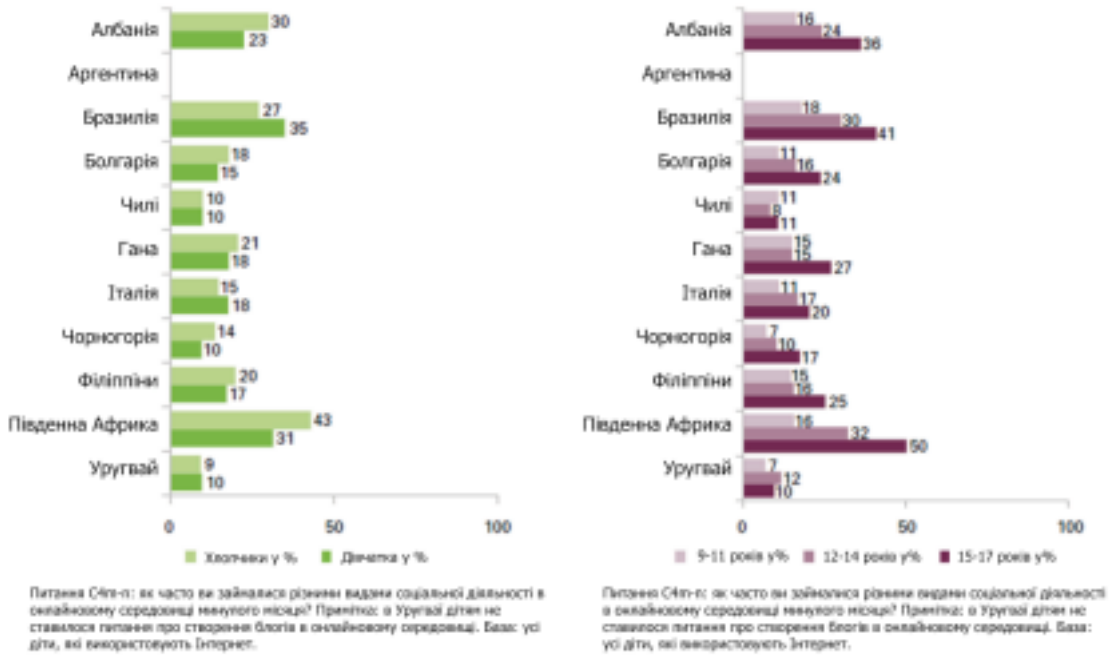
«Я веду блог і регулярно оновлюю його», – дівчинка віком 15-17 років, Філіппіни.

«Ви можете обмінюватися відео та іграми. Ви можете обмінюватися музичними творами. Ви можете обмінюватися зображеннями, ідеями, іграми», – дівчинка віком 9-11 років, Гана.

«Я виготовляю листівки власноруч і розміщую їх в Мережі. Вони подобаються моїм друзям», – дівчинка віком 15-17 років, Філіппіни.

«Так, я вмію [зламувати комп'ютери], але я цим більше не займаюся», – хлопчик віком 15¬17 років, Філіппіни.

Малюнок 3: Діти (у %), які щотижня займаються бодай одним видом творчої діяльності в цифровому середовищі, з розподілом за статтю та віком



Рекомендації для батьків та освітян щодо захисту дитини в цифровому середовищі

Примітка: Дітям та молодим особам було поставлено питання, як часто вони займалися наступними

видами творчої діяльності в цифровому середовищі минулого місяця: створили свої власні відео або музичні твори та поділилися ними в цифровому середовищі; створили свій блог чи вебсайт або виклали будь-яку подію в цифровому середовищі; розмістили відео або музичний твір, створені кимось іншим.
Джерело: UNICEF

Жага інформації

Так само, як і дорослі, діти та молодь використовують Інтернет для реалізації свого права на отримання інформації. Від однієї п'ятої до двох п'ятих дітей та молодь можуть вважатися «мисливцями за інформацією» в тому сенсі, що вони щотижня відпрацьовують кілька форм пошуку інформації в цифровому середовищі, щоб дізнатися щось нове, отримати інформацію про роботу або можливості навчання, ознайомитися з новинами, прочитати медичну інформацію або знайти заходи, що організовуються неподалік.

Багато дітей та молодь різного віку використовують Інтернет для роботи вдома, і навіть для того, щоб надолужити згаяне через пропущені заняття.

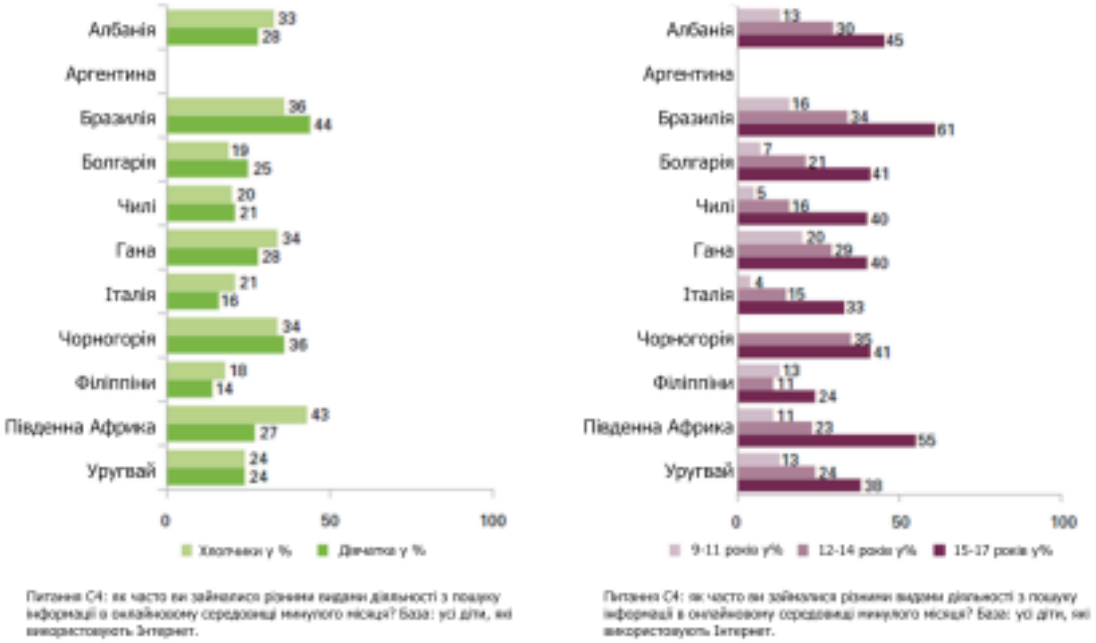
«Вони просили нас знайти прізвища міністрів у Гані, інформацію про країни та їхні валюти. Ви можете дізнатися новини про інші країни», – дівчинка віком 12-14 років, Гана.

«В Інтернеті ми можемо знайти все, що нам потрібно до школи, та те, що ми не можемо знайти у книжках», – дівчинка 9 років, Сербія.

«Мені поставили «двійку» з математики, і тому мені довелося переглянути декілька відео, де пояснювалося, що я маю вивчити», – хлопчик віком 15-17 років, Аргентина.

«Якщо ви не пішли до школи, ви можете поговорити зі своїм другом та з'ясувати, що ви пропустили, і знайти цю інформацію. Тому важливо мати WhatsApp своїх друзів», – дівчинка віком 16-17 років, Південна Африка.

Малюнок 4: Діти (у %), які здійснюють не менше трьох видів діяльності з пошуку інформації не рідше одного разу на тиждень, з розподілом за статтю та віком



Примітка: Дітям та молодим особам було поставлено питання, як часто вони займалися наступними видами діяльності з пошуку інформації минулого місяця: дізнавалися щось нове шляхом пошуку в цифровому середовищі; шукали інформацію про роботу або можливості навчання; використовували Інтернет для виконання шкільних завдань; здійснювали пошук ресурсів або заходів, організованих неподалік; займалися пошуком новин в цифровому середовищі; шукали медичну інформацію для себе або свого знайомого. Аргентина не була показана через відсутність даних.
Джерело: UNICEF

Дехто з дітей та представників молоді частіше використовують Інтернет, ніж інші, в пошуку інформації. Дані показують, що діти та молодь, які використовують Інтернет для різноманітної діяльності, пов'язаної з пошуком інформації, належать найчастіше до старшої категорії, яка, як правило, може брати участь в більш широкому колі онлайнових видів діяльності і зустрічають підтримку та сприяння з боку батьків щодо використання ними Інтернету. Це наводить на думку про те, що в міру того, як діти та молодь стають старшими, і за належної підтримки з боку батьків, вони, як правило, набувають більше онлайнового досвіду та використовують Інтернет із суттєвою перевагою для себе.

За такої кількості інформації, доступної в онлайновому режимі, діти та молодь повинні мати необхідні навички, що дозволяють їм знаходити правильний контент і перевіряти правдивість знайденого.

Щодо цього між дівчатками та хлопчиками існують деякі відмінності, причому діти та молодь, після досягнення підліткового віку, стають до того ж фахівцями з пошуку того, що їм потрібно. Діти та молодь, які переглядають більше відео кліпів у режимі онлайн, мабуть, мають значні навички з пошуку інформації завдяки тому, що вони дізнаються, як знайти те, що їм потрібно, частіше переглядаючи онлайновий контент.

Якість та кількість інформації, яку діти та молодь збирають в цифровому середовищі, залежатиме від їх інтересів та мотивації. Однак те, що вони знаходять, залежатиме від обсягу доступної інформації, що буде завеликим для більшості поширених мов. Проте меншини також можуть скористатися можливостями пошуку інформації, навіть коли їх чисельність обмежена.

«Оскільки в нашій школі ніхто не спілкується нашою мовою, я виставляю в пошук в YouTube будь-що румунською і слухаю, як вона звучить. Це добре, адже мені все зрозуміло», – хлопчик з народності рома, 12 років, Сербія.

Одна річ – добре вміти шукати інформацію в Інтернеті, а інша – вміти перевіряти, чи є знайдена інформація правдивою.

«Я переглядаю міжнародні новинні програми, тому що мені цікаво дізнатися, як та чи інша країна оцінює одну й ту саму ситуацію. Тому що завжди є дві сторони. Наприклад, Америка може мати свій погляд щодо певного питання, а Росія може мати цілком інший погляд», – дівчинка 16 років, Сербія.

У порівнянні з відсотком дітей та молодь, які заявили про впевнене володіння навичками з пошуку інформації в Інтернеті, лише кілька дітей та молодь повідомили, що вміють критично оцінювати знайдену інформацію.

«Сьогодні в Інтернеті безліч фальшивих новин», – хлопчик 15 років, Філіппіни.

Загалом створюється враження, що діти та молодь поки ще не зовсім уміють користуватися всіма перевагами пошуку та перевірки інформації в цифровому середовищі. Для цього (особливо дітям молодшого віку) знадобиться більш активне сприяння батьків, школи або постачальників цифрових послуг, аби надихати їх та допомагати їм відстоювати свої права у цифровому світі.

На шляху до ролі активного громадянина

Крім пошуку інформації та створення контенту, діти та молодь за допомогою Інтернету можуть також брати участь у громадській або політичній діяльності. Відповідно до Конвенції про права дитини дитина має цивільні права, зокрема, право бути заслуханою, право вільно висловлювати свою думку, а також право зустрічатися з іншими людьми. Однак з дослідження Global Kids Online випливає, що порівняно невелика кількість дітей та молодь використовують можливості участі у цивільній діяльності в цифровому середовищі.

Молодь більше схильні брати участь у політичній діяльності в цифровому середовищі.

«Політика. Можливо, вона не прагне в ній брати участь навмисне. Але, наприклад, дочка читає про неї у Facebook», – батько дитини 13-14 років, Аргентина.

«Але вони також висловлюють свою думку у Twitter і таким чином беруть участь у процесі», – батько дитини 15-17 років, Аргентина.

Схильність до ризиків та заподіяння шкоди

В цифровому середовищі діти та молодь наражаються на нові ризики, які можуть призвести до заподіяння їм шкоди. Вони можуть випадково виявити інформацію про те, як завдати

собі шкоди або скоїти самогубство. Вони також можуть мати справу з агресивними висловлюваннями або матеріалами насильницького чи сексуального характеру. Згідно з висновками дослідження, проведеного Global Kids Online в різних країнах, діти та молодь, які беруть участь у більшій кількості видів онлайнової діяльності, наражалися навіть на більшу кількість онлайнових ризиків, причому, можливо, внаслідок вищого ступеня вразливості або більш впевненого вміння користуватися Інтернетом.

Важливо пам'ятати про те, що ризик не завжди призводить до заподіяння шкоди. Діти та молодь, що наражаються на Онлайн-ризики, не постраждають, якщо мають необхідні знання та вміння впоратися з отриманим досвідом. Тому важливо визначити, хто з них є найбільш вразливим перед заподіянням шкоди в цифровому середовищі і як саме ризики призводять до заподіяння шкоди для того, щоб надійно захистити дітей та молодь в цифровому середовищі, уникаючи необґрунтованих обмежень їх можливостей.

Загалом приблизно 20% дітей та молодь, які взяли участь в обстеженні Global Kids Online, заявили, що протягом минулого року вони знаходили вебсайти або онлайн-обговорення, присвячені темі заподіяння людьми собі фізичної шкоди або каліцтва, а приблизно 15% дітей та молодь знаходили контент, що стосується суїциду. За даними дослідження, діти та молодь також наражалися на агресивні висловлювання.

У Чилі майже половина підлітків у віковій групі від 15 до 17 років заявляли, що за минулий рік в цифровому середовищі сталося щось таке, що їх збентежило або засмутило. Коли їх просили розповісти про те, що трапилося, докладніше, вони згадали широкий спектр проблем, зокрема, шахрайство в Інтернеті, «спливаючу» рекламу порносайтів, образливі дії, неприємні або відлякувальні новинні історії чи зображення, дискримінацію та домагання. У Болгарії діти та молодь наражаються на ризик, який представляють сайти, що рекламують швидке схуднення; їх переглядала чверть респондентів дослідження.

«Трапляються огидні коментарі про інших людей», – дівчинка 13-14 років, Південна Африка.

Від чверті до третини дітей та молоді, які брали участь у дослідженні з цього питання, мали справу з насильницьким контентом в цифровому середовищі або сексуальним контентом в різних засобах інформації. Іноді діти та молодь випадково знаходять контент сексуального характеру; часом його рекомендують їхні друзі або ж надсилають інші люди, в тому числі незнайомі. Дехто з дітей та молодь зверталися до когось із проханням надіслати зображення сексуального характеру.

«Я дуже засмутилася, коли хлопець надіслав мені порнографічні світлини», – дівчинка 12-14 років, Гана.

«Одного разу незнайомий чоловік запитав, «скільки я коштую»: тобто його цікавило, скільки коштує зайнятися зі мною сексом», – хлопчик 16 років, Філіппіни.

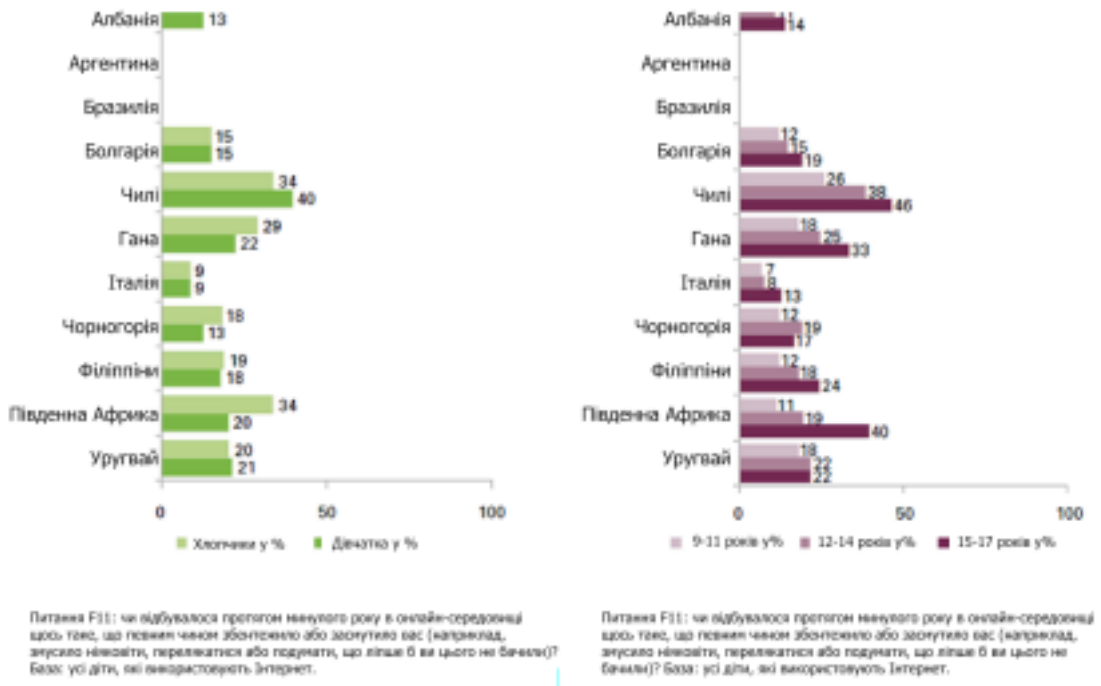
Багато дітей та молодь у низці країн наражалися на різного роду Онлайн-ризики, проте набагато менша кількість заявляє про те, що в результаті відчули, що їм було завдано шкоди. Висновки за країнами варіюються, причому молодь більше схильна до заподіяння шкоди, ніж діти молодшого віку, можливо через те, що проводять більше часу в Інтернеті і схильні брати участь в більш широкому спектрі видів діяльності в цифровому середовищі.

«В Instagram я клікнув на один коментар, який був дуже кумедним. Я хотів прочитати, що пишуть інші, натиснув на посилання, і раптом з'явилися оголені жінки», – хлопчик 10 років, Сербія.

«Мені подобаються коні, це всім відомо. Одного разу я шукала світлини для заставки та натрапила на моторошне фото, на якому людина зарізає коня», – дівчинка 10 років, Сербія.

«Я дуже перелякався, побачивши фото мертвого хлопчика – його застрелили», – хлопчик 12-14 років, Гана.

Малюнок 5: Діти (у %), які постраждали від завданої шкоди в цифровому середовищі, з розподілом за статтю та віком



Джерело: UNICEF

Діти та молодь можуть наражатися на ставлення, що завдає морального болю як в цифровому середовищі, так і в реальному житті. В рамках інтернет-платформ шкода може бути заподіяна образливими або болісними за сприйняттям повідомленнями, вилученням з групової діяльності або погрозами. Такі дії часто-густо називаються «кіберБулінгм». Але такої шкоди може бути завдано дітям та молодим особам аналогічним чином і в буденному житті поза Інтернетом. Приблизно однакова кількість дітей та молоді, що піддаються Булінгу з боку інших, страждають від неї особисто та в цифровому середовищі.

«Усі почали дражнити та висміювати одного хлопчика. Зрештою він залишив групу», –

хлопчик 13-14 років, Аргентина.

«Мене бентежить кіберБулінг, тому що воно може завдати мені серйозної емоційної шкоди», – дівчинка 14 років, Уругвай.

Рекомендації для батьків та освітян щодо захисту дитини в цифровому середовищі

Як діти та молодь реагують на інциденти, що завдають моральної шкоди в цифровому середовищі? Спочатку вони звертаються до друзів, братів та сестер. Потім дехто розповідає про те, що трапилося, батькам. Дуже невелика кількість дітей та молодь в країнах, де проводилося дослідження, звернулися б за сприянням до освітянив. Хоча молодь наражаються на більшу кількість ризиків, ніж діти молодшого віку, завдана їм шкода не вважається серйозною: це може свідчити про те, що з досвідом у них формується стійкість до впливу середовища.

Варто зазначити, що діти та молодь не завжди поділяють у своїй свідомості онлайновий простір та реальний світ. У розумінні дітей та молоді досвід, отриманий в цифровому середовищі, – як позитивний, так і негативний – тісно переплітається з іншими аспектами їхнього життя.

Пріоритетне значення недоторканності приватного життя

Недоторканність приватного життя – це право дитини відповідно до Конвенції про права дитини. Вона є важливою для набуття самостійності та самовизначення і тісно пов'язана з правом дитини на

Багато дітей та молодь заявили про наявність впевнених навичок забезпечення конфіденційності під час керування своїми міжособистісними відносинами в цифровому середовищі; так, наприклад, вони обізнані про те, яку інформацію не слід розголошувати в цифровому середовищі, а також, як змінювати налаштування конфіденційності у своїх облікових записах в соціальних мережах або видаляти контакти зі списку. Отже, можна припустити, що початкові зусилля з поширення принципів збереження конфіденційності серед дітей та молоді мали певний успіх. Багато дітей та молоді розробили стратегії власного захисту в цифровому середовищі й усвідомлюють, що вони повинні враховувати певні ризики під час користування Інтернетом.

«У мене один обліковий запис у Facebook для реальних друзів, а інший – для тих друзів, з якими я спілкуюся тільки в Інтернеті», – дівчинка 14 років, Філіппіни.

«Коли я заходжу в Інтернет, я особисто несу відповідальність за свої дії», – дівчинка 17 років, Уругвай.

Більш серйозною проблемою є те, що діти та молодь в цифровому середовищі можуть наражати інформацію, світлини та повідомлення особистого характеру на ризик потенційного зловживання й неналежних і небажаних контактів.

Крім того, діти та молодь можуть познайомитися в цифровому середовищі з людьми, з якими вони згодом зустрінуться особисто, хоча це як і раніше відбувається в рідкісних випадках. В усіх країнах менше чверті дітей та молодь зустрічалися особисто з тими, з ким познайомилися в Інтернеті.

Можливо, це дивно, але діти та молодь в основному радіють своїм особистим зустрічам зі знайомими з Інтернету і заявляють про те, що задоволені своїм спілкуванням; це

дозволяє зробити висновок, що вони виграють від такого розширення кола друзів. З іншого боку, навіть невеличка кількість випадків, коли діти та молодь залишилися засмученими від цих зустрічей, є приводом до занепокоєння.

Батьки, які діляться контентом про своїх дітей, мають замислюватися над тим, як це може відобразитися на дитині. Виникають побоювання, що «шарентінг» (з англ. «sharenting»

– розміщення батьками даних та світлин своїх дітей в Інтернеті) може порушити право дитини на недоторканність приватного життя, призвести до Булінг, виникнення незручних ситуацій або негативно позначитися на подальшому житті . Батьки дітей з інвалідністю іноді діляться такою інформацією в пошуках сприяння або поради, тим самим наражаючи дітей з інвалідністю на більш високий ризик негативних наслідків.

Будинок там, де Wi-Fi

Одним зі способів запобігання ситуаціям, в яких ризики призводять до заподіяння шкоди дітям та молоді, є вдосконалення Рекомендацій для батьків та інших осіб з питань використання Інтернету дітьми та молодими особами.

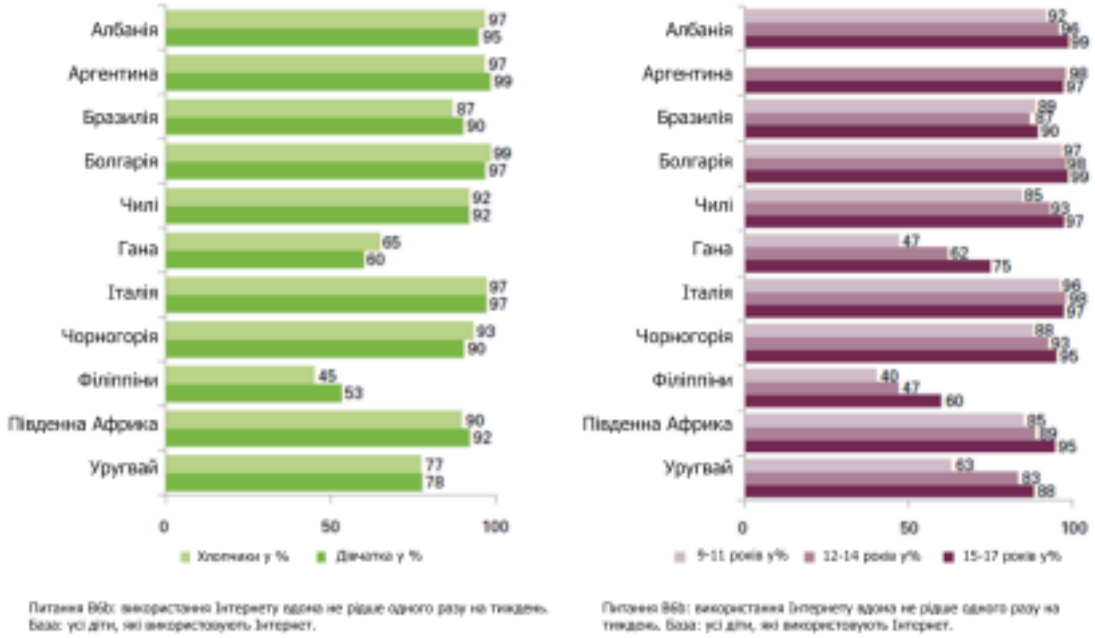
«Дорослі справляють неабиякий вплив на більш молоде покоління та мають подавати йому гідний приклад для наслідування», – дівчинка 13 років, Уругвай.

Як правило, батьки мають у своєму розпорядженні всі можливості дітям та молодим особам сприяти у вирішенні питань використання Інтернету, оскільки останні в основному користуються домашнім доступом до Інтернету.

Однак через складність та стрімкість розвитку технологій чимало батьків не відчувають себе досить впевненими або компетентними для того, щоб контролювати дітей та молодь, які є доволі обізнаними у технічних моментах. Крім того, батьки відчувають поширене занепокоєння у зв'язку з такими факторами, як «час перед екраном», «інтернет-залежність» та «небезпека спілкування з незнайомцями». Тому батьки схильні радше обмежувати дітей та молодь у використанні Інтернету, наприклад, з точки зору часу, відведеного на спілкування в цифровому середовищі, або шляхом заборони користуватися цифровими пристроями в спальні, під час їжі або перед сном, ніж надавати їм можливості і спрямовувати їх в більш продуктивну діяльність в цифровому середовищі.

У більшості країн батьки беруть активну участь у процесі опанування Інтернету дітьми молодшого віку, допомагаючи їм орієнтуватися в цифровому просторі й водночас встановлюючи для них більш суворі обмеження, ніж для молодь. У міру того, як діти дорослішають, ступінь втручання зменшується, хоча, безсумнівно, батьки продовжують конструктивно спрямовувати підлітків на те, що стосується можливостей і ризиків в цифровому середовищі.

Малюнок 6: Діти (у %), які використовують Інтернет удома не рідше одного разу на тиждень, з розподілом за статтю та віком



Джерело: UNICEF

Одна з причин, через яку батьки не наважуються брати участь у процесі використання Інтернету своїми дітьми, полягає в нестачі у них самих спеціальних знань.

4. Діти, які перебувають у вразливому становищі

Діти та молодь можуть перебувати у вразливому становищі з цілої низки причин. Згідно з проведеним у 2019 році дослідженням24, «життя в цифровому середовищі дітей та молодь, які перебувають у вразливому становищі, не супроводжується тим особливим і уважним ставленням, яке в реальному житті обумовлюється їх несприятливою ситуацією». Крім того, в документі мовиться, що «в кращому випадку вони [діти та молодь] отримують ті самі загальні рекомендації щодо гарантування безпеки в цифровому середовищі, що й усі інші діти та молодь, тоді як їм потрібна спеціалізована допомога».

Тут розглядаються три конкретні категорії дітей у вразливому становищі (діти-мігранти, діти з розладами аутистичного спектру та діти-інваліди), проте їх існує значно більше.

Діти-мігранти

Діти та молодь із середовища мігрантів часто-густо прибувають у країну (або вже живуть в ній) з певним комплексом соціокультурних знань та установок. Незважаючи на те що технології зазвичай розглядаються як чинник, що сприяє налагодженню зв'язків та громадській участі, рівень онлайн-ризиків та можливостей може значно варіюватися залежно від умов. Крім того, отримані емпіричним шляхом дані та практичні дослідження25 свідчать про найважливішу роль цифрових засобів загалом:

• вони є важливими для орієнтування (у разі переїзду до нової країни). • Це найважливіший засіб освоєння та ознайомлення із суспільством/культурою країни, що приймає.

• Соціальні мережі можуть відігравати ключову роль у підтриманні зв'язку з родиною та однолітками, а також в отриманні доступу до інформації загального характеру.

Поряд з багатьма позитивними аспектами цифрові засоби можуть також створювати для мігрантів труднощі, як-от:

- Інфраструктура: важливо замислюватися про створення безпечного онлайн-простору, для того щоб діти та молодь – мігранти могли користуватися Інтернетом безпечно та конфіденційно.
- Ресурси: мігранти витрачають більшу частину грошей на телефонні картки з попередньою оплатою.
- Інтеграція: поряд із доступом до технологій дітям та молодим особам – мігрантам також потрібна добра цифрова освіта.

Діти з розладами аутистичного спектру (ASD)

Аутистичний спектр охоплює дві основні сфери поведінкової діагностичної класифікації DSM-5.

• Обмежена і повторювана поведінка (потреба в одноманітності). •
Труднощі спілкування та комунікації.

- Дуже часті випадки у поєднанні з розумовою відсталістю, мовними та аналогічними проблемами. Технології та Інтернет відкривають дітям та молоді безмежну кількість можливостей для навчання, спілкування та ігор. Однак поряд з перевагами є значна кількість ризиків, на які можуть більшою мірою наражатися діти та молодь з ASD, наприклад:

- Інтернет може дати дітям та молодим особам з аутизмом можливості у сфері соціалізації та реалізації особливих інтересів, яких у них може не бути в реальному житті.
- Проблеми соціального характеру, як-от труднощі в розумінні намірів інших людей, можуть призвести до того, що представники цієї групи виявляться вразливими перед «друзями» з недобрими намірами.
- Проблеми, що виникають в цифровому середовищі, часом зумовлені основними характерними особливостями аутизму: конкретні та точні Рекомендації можуть сприяти адаптації цих осіб до онлайн-середовища, проте їхні базові проблеми залишаться.

Діти-інваліди

Згідно з одним з перших консультативних досліджень, присвячених темі досвіду дітей з інвалідністю у цифровому середовищі, ці діти вважають, що їх життя у цифровому та цифровому середовищі багато в чому дуже схоже з життям дітей без інвалідності. Проте існує низка чітких та важливих відмінностей . Під час їх розгляду варто зважати на те, що труднощі та бар'єри, з якими мають справу діти-інваліди, значно варіюються залежно від виду та характеру порушень. Їх особливі потреби повинні враховуватися на індивідуальній основі .

Діти та молодь з інвалідністю піддаються ризикам в цифровому середовищі так само, як діти та молодь без інвалідності, проте вони також можуть піддаватися і конкретним ризикам, обумовленим їхньою інвалідністю. Так, для них ризик постраждати від кіберБулінг на 12% вищий, ніж для дітей та молодь без інвалідності. Дехто з дітей та молодь – інвалідів не володіють достатньо розвиненими навичками управління

міжособистісними відносинами в цифровому середовищі або розпізнавання правдивої чи помилкової інформації. Декотрими також легко маніпулювати в питаннях, пов'язаних з витратою грошей, розкриттям неналежних відомостей тощо. Діти та молодь – інваліди нерідко мають справу з маргіналізацією, стигматизацією та бар'єрами (фізичними, економічними, соціальними, а також бар'єрами, що відносяться до ставлення з боку інших людей) для участі в житті своїх спільнот. Подібний досвід може негативно позначитися на дитині-інвалідові, яка прагне до соціальної взаємодії та пошуку друзів в інтернет-просторі, що в чомусь іншому могло б зіграти позитивну роль, сприяючи зміцненню самоповаги та формуванню мереж підтримки. Проте це може призвести до підвищеного ризику таких дій щодо цих дітей та молодь, як грумінг, схиляння в цифровому середовищі до дій сексуального характеру та/ або сексуального домагання. Згідно з дослідженнями, діти та молодь, які мають труднощі в реальному світі, а також відчувають проблеми психологічного характеру, наражаються на підвищений ризик подібних інцидентів .

Серед осіб, які скоюють такі правопорушення, як грумінг, схиляння в цифровому середовищі до дій сексуального характеру та/або сексуальні домагання щодо дітей та молодь з інвалідністю, можуть бути не лише порушники, які обирають своїми жертвами саме дітей та молодь, а й також ті, котрі обирають саме дітей і молодь з інвалідністю. До таких порушників належать так звані «девоті» – особи без інвалідності, які відчувають сексуальний потяг до осіб з інвалідністю (зазвичай до осіб з ампутованими кінцівками або до осіб, що пересуваються за допомогою засобів, які покращують мобільність), причому дехто з них прикидається людиною з інвалідністю . Ці особи можуть вчиняти такі дії, як завантаження фото і відео дітей та молодь з інвалідністю (які самі по собі нешкідливі) та/або їх поширення через спеціально створювані форуми й облікові записи в соціальних мережах.

Рекомендації для батьків та освітян щодо захисту дитини в цифровому середовищі

Механізми інформування в межах форумів і соціальних мереж часто не передбачають можливостей припинення таких дій.

Дехто з дітей та молодь – інвалідів можуть мати справу з труднощами в опануванні онлайнового середовища або навіть бути вилученими з нього через недоступний формат (наприклад, додатків, в яких не можна збільшити розмір шрифту), відсутність необхідних пристосувань (наприклад, програм голосового відтворення тексту або адаптивних засобів керування комп'ютером), або потреби у відповідному сприянні (наприклад, у навчанні щодо використання обладнання, індивідуальної допомоги в адаптації до соціальної взаємодії) .

Деякі батьки дітей та молодь – інвалідів іноді виявляють зайву опіку, оскільки не мають достатніх знань про те, як ліпше спрямовувати своїх дітей щодо використання Інтернету або захистити їх від Булінг і домагань . Хтось із батьків дітей та молодь – інвалідів іноді ділиться інформацією або матеріалами (фото, відео) про своїх дітей в пошуках сприяння або поради, тим самим наражаючи дитину на ризик порушення конфіденційності як в конкретний момент, так і в майбутньому. Це також створює для самих батьків небезпеку стати мішенню неосвічених або неохайних людей, що пропонують різного роду лікування, терапію або «зілля» від інвалідності дитини.

5. Нові ризики та труднощі, що формуються

Інтернет речей

Інтернет змінив спосіб життя людей. Він відкриває доступ до всієї сукупності людських знань в будь-який час, в будь-якому місці. Для декого життя стало набагато простішим та комфортнішим, ніж було раніше. Однак подібні зміни згубно позначилися на низці традиційних способів життя як в господарській діяльності, так і в приватному житті. Так, наприклад, колишні бізнес-моделі були повністю змінені або відкинуті; на особистісному рівні розвиток Інтернету призвів до зменшення безпосереднього спілкування між людьми.

Важливо враховувати існування відкритого Інтернету та інтернету речей: відкритий Інтернет представляє просто віртуальне середовище і не існує в повсякденній реальності; взаємодія з ним відбувається факультативно. Цього не можна сказати про інтернет речей, в якому фізичні об'єкти знаходять життя за допомогою інтернет-з'єднань, щоб зробити наше життя кращим: один з наочних прикладів – тостер, що використовує Twitter.

Можливості інтернету речей (IoT) невичерпні. Він уже присутній в портативних

електронних пристроях, домашньому освітленні, камерах, автомобілях, туалетах, процесі упаковки, лічильниках електроенергії, медичних датчиках... Цей список безмежний. IoT здатен змінити все на краще. Дехто вважає його по суті невіддільною складовою «четвертої промислової революції».

Коли ці предмети використовуються поблизу дітей (наприклад, в їхніх оселях), останні можуть наражатися на ризики, пов'язані з використанням «розумних» портативних електронних пристроїв або предметів одягу, які потенційно здатні відправляти інформацію про їх місцезнаходження.

IoT відкриває колосальні ринкові можливості. Однак він також приховує в собі низку потенційних проблем:

Технічні проблеми / проблеми конфіденційності

• Безпека пристроїв: забезпечення належного рівня безпеки може бути відносно дорогим; загрозу безпеки пристроїв несуть віруси/шкідливі програми.

• Безпека комунікацій: застосовується менш криптостійке шифрування, оскільки енергія є стримуючим фактором. Існує ризик маніпуляції третіми сторонами/крадіжки ідентичності тощо.

• Зв'язок «завжди увімкнений»: зростає залежність від пристроїв, які використовують зв'язок в режимі «завжди увімкнений».

• Безпека даних в хмарі: по суті ви не маєте жодного уявлення, хто використовує ваші дані.

Соціальні проблеми

• Маргіналізація людей.

• Потенційна можливість зловживання даними.

• Потенційна можливість того, що технології сприятимуть виникненню ситуацій жорстокого поводження в родині .

Економічні проблеми

• Втрата зайнятості.

Екологічні проблеми

• Забруднення на кожному етапі (50 млрд пристроїв за п'ять найближчих років).

Іграшки та робототехніка, що мають доступ до Інтернету

З нарощуванням технічного прогресу відбуваються фундаментальні перетворення в житті людей, які дедалі більше використовуються не тільки дорослими, а також (зважаючи на появу «інтернету іграшок») дітьми та молодими особами. Оскільки дедалі більше аспектів нашого життя перетворюються на комп'ютеризовані дані, посилюється необхідність приділяти увагу способам захисту дітей та молодь, щоб забезпечити для них можливість зростання в безпечному і надійному цифровому світі. Відбулося зрушення в розумінні робототехніки; широко обговорювалося питання «роботизації» життя дітей . Роботи, які колись вважалися примітивними, брудними, небезпечними виробничими машинами, що загрожують людській праці на фабриках, тепер перетворилися на механізми, які розглядаються як високорозвинені, готові прийти на допомогу, соціальні; як щось, з чим можна взаємодіяти у побуті та на дозвіллі. Хоча іграшки вже тривалий час виготовляються у вигляді роботів, потрібні були колосальні перетворення, щоб зробити роботів більш досконалими. Тепер вони не просто приймають форму та вигляд типового робота з наукової фантастики: вони оживають, перетворюючись на іграшки, здатні ходити, говорити і мислити.

За роботизацією стоять значні технічні зміни, які можна стисло описати

нижче: • Експоненціальне зростання обчислювальної потужності.

• Встановлення рухомих з'єднань.

• Датафікація та мережева інформація.

• Мініатюризація датчиків, мікрофонів та камер.

• Обчислення в хмарних робототехнічних системах.

• Прогрес у розвитку штучного інтелекту та машинного навчання.

Мабуть, сьогодні найпоширеніший робот, з яким взаємодіють діти та молодь, – це Siri; бесіда з цифровим помічником, яка видається потішною, свідчить про глибину зрілості штучного інтелекту (ШІ) і алгоритмів, які ним керують. Соціального робота можна визначити як «штучний олюднений пристрій, здатний сприймати (соціальне) середовище і цілеспрямовано та автономно взаємодіяти з цим середовищем (суб'єктами в ньому), відповідно до соціальних правил, що були задані його роллю». Соціальні роботи можуть надто залучати дітей та

молодь, оскільки останні стрімко опановують нові технології і нерідко розглядаються саме як користувачі нових технологій. Крім того, діти та молодь зазвичай вирізняються наявністю неоднорідної сфери різноспрямованих інтересів, що формується. Однак в результаті саме діти та молодь можуть випробувати на собі найсильніші наслідки взаємодії з роботами.

До типових характеристик взаємодії дитини та робота належать:

• Рухливість.

• Інтерактивність/обопільність.

• «Натуралізація» (мова, жести, використання зору замість тексту). •

Пристосовність взаємодії.

• Персоналізація.

• (Пере)втілення.

При цьому процеси відображають:

• Антропоморфізм (демонстрація людських рис або поведінки).

• Соціальна присутність.

• Участь.

• Схожість, що сприймається.

Існує ціла низка потенційних наслідків взаємодії з роботами дітей та молоді для їх когнітивного розвитку, як позитивних, так і негативних. До позитивних результатів належать успіхи у навчанні, яке адаптується спеціально під дитину, постійно оновлюється та сприяє самонавчанню. Менш позитивні результати пояснюються проблемою «освітніх бульбашок», аналогічних до «бульбашок фільтрів» в Інтернеті, коли відбувається обмеження контенту. У таких випадках є ризик фрагментації знань дитини та отримання надмірної кількості фактів, при тому, що в основі стилю викладання покладено суто алгоритмічний метод навчання. Так, наприклад, коли дитина ставить питання Alexa (так само, як він може поставити його системі Google або Bing), вона отримує лише одну відповідь, що заважає розвитку в неї вміння критично оцінювати контент, з яким вони ознайомлюються.

Аналогічні побоювання виникають щодо формування особистості дитини. Як свідчать дані наукових досліджень , роботи здатні відігравати важливу роль у житті дітей та молоді, допомагаючи їм розширювати й вдосконалювати процес пошуку своєї ідентичності в міру дорослішання. Однак застосування роботів порушує питання конфіденційності, оскільки існує ризик використання їх, наприклад, як машин спостереження: ведення за їх допомогою запису мови/відео всіх, хто перебуває поблизу, і створення таким чином значних загроз безпеці як для батьків, так і для дітей та молоді.

Щодо аспектів спілкування, то взаємовідносини з роботами не завжди відображають реальні відносини в житті. З одного боку, це може призвести до поступової ізоляції дітей та молоді від суспільства через те, що вони знайшли алгоритм, який слугує для них засобом заспокоєння та розради. Разом з тим це передбачає, що роботи є такою собі «віддушиною», дозволяючи «обговорювати» питання, які нелегко порушувати під час бесіди з батьками та

однолітками. Система наших взаємин з роботами завжди вибудовуватиметься за принципом слуга/господар, проте вони можуть вчитися дедалі краще «прикидатися такими, що здатні відчувати», тому діти та молодь можуть бути введені в оману, якщо повірять у справжню та взаємну природу подібних взаємовідносин.

Як зазначив Йохен Петер, «роботи вміють значно більше, ніж традиційні іграшки; однак вони несуть в собі колосальні ризики для наймолодших користувачів» .

Онлайн-ігри

За кількістю клієнтів та обсягом доходів індустрія ігор залишила позаду як кіноіндустрію, так і музичну індустрію. Ба більше, з появою мобільних ігор, в які можна грати на маленьких пристроях, кількість шанувальників ігор зросла до історичного максимуму. Згідно з дослідженням стану справ в області онлайнових ігор за 2019 рік, яке враховує відповіді 4500 клієнтів з Франції, Німеччини, Індії, Італії, Японії, Сінгапуру, Республіки

Кореї, Сполученого Королівства та Сполучених Штатів Америки віком 18 років і старше, що грають у відеоігри не рідше одного разу на тиждень, 51,8% гравців становлять чоловіки, а 48,2% – жінки . Крім того, в Сполучених Штатах Америки з 2010 року особи молодше 18 років становлять 21% від загальної кількості гравців відеоігор .

Нещодавні дослідження, проведені у Франції, Німеччині, Іспанії та Сполученому Королівстві, виявили, що відеоіграми охоплено 54% населення віком від 6 до 64 років, при цьому 77% з них грають не менше однієї години на тиждень. Крім того, в Німеччині, Іспанії, Італії, Сполученому Королівстві та Франції у відеоігри грає три чверті дітей віком від 6 до 15 років; їхня загальна кількість, за даними GameTrack по п'яти європейських ринках, становить понад 24 мільйони. Вони користуються різними пристроями, проте приблизно 7 з 10 застосовують приставки або «розумні» пристрої .

У світі налічується понад 2,5 млрд гравців відеоігор. Найвищий показник за кількістю гравців зафіксований у грі «PUBG», який сягнув 3 мільйонів протягом однієї години .

Однією з провідних платформ для перегляду ігрового відеоконтенту в усьому світі є Twitch, на частку якої у 2017 році припадало 54% всього доходу платформ ігрового відеоконтенту.

Дедалі більш значущою складовою онлайнових ігор стають внутрішньоігрові покупки. Завдяки вдосконаленню з'єднань та підвищенню швидкості Інтернету гравці дедалі частіше вважають за краще завантажувати ігри, а не купувати їх фізичні копії. У Південній Африці з 2018 по 2019 рік онлайнові продажі зросли на 13% .

Незважаючи на різноманітність аудиторій, індустрія ігор, де як і раніше переважають розробники-чоловіки, часто прагне відповідати інтересам можливої гетеросексуальної чоловічої аудиторії. На жаль, це нерідко призводить до створення надмірно сексуальних жіночих персонажів та достеменної нестачі нечоловічих ігрових персонажів і персонажів з іншим, окрім білого, кольором шкіри.

Крім розмаїття мобільних ігор, колосальне зростання відзначається в сфері онлайнових ігор. Не в усі ігри можна грати в онлайновому режимі, проте сьогодні всі ігрові приставки оснащені функцією доступу до Інтернету. Онлайн-ігри також означають, що користувачі можуть грати в Інтернеті з іншими користувачами. У деяких іграх можлива тільки гра з людьми, зареєстрованими як «друзі»; в інших ви потрапляєте у групу гравців з усіх регіонів світу, іноді у випадковому порядку, а часом відповідно до рівня ігрових навичок або переваг.

Існує безліч різних видів ігор, і вони постійно змінюються. Деякі з популярних ігор та жанрів наведені нижче:

Шутер від першої особи (FPS)– екшен-ігри, сенс яких полягає в боях, які ведуться з використанням вогнепальної або іншої зброї з видом від першої особи, як, наприклад, Call of Duty, Overwatch, BioShock, Battlefield.

Екшен-пригода – ігри, в яких гравець долає та опановує середовище, нерідко бере участь в боях або розгадує загадки, як, наприклад, Grand Theft Auto (GTA), Super Mario, Uncharted, The Legend of Zelda, God of War.

Спорт – ігри, які імітують стратегію та фізичні процеси реально існуючих професійних ігрових видів спорту, як, наприклад, FIFA, Madden NFL, NBA.

Пісочниця/ Відкритий світ – ігри з мінімальною сюжетною лінією та обмеженнями або зовсім без них, де гравець вільно переміщується віртуальним світом, змінюючи його на свій розсуд, як, наприклад, Minecraft, Terraria, Skyrim, Fallout.

Онлайнова бойова арена з багатьма користувачами Moba) – онлайн-ігри, де беруть участь дві конкуруючі команди, що прагнуть захопити або знищити бази одне одного, як, наприклад, Dota 2, League of Legends, Heroes of the Storm, Paragon.

Викликає занепокоєння залежність від онлайнових ігор, яку Всесвітня організація охорони здоров'я у 2018 році визначила як ігровий розлад . Відповідно до визначення, наведеного в 11-му переглянутому виданні Міжнародної класифікації хвороб, це «модель ігрової поведінки (щодо «цифрових ігор» або «відеоігор»), що відрізняється порушенням контролю за грою, відведенням грі дедалі більшого пріоритету в порівнянні з іншими видами діяльності до такої міри, що їй віддається перевага перед іншими інтересами і повсякденними заняттями, а також продовженням або інтенсифікацією ігрової діяльності, попри появу небажаних наслідків». Важливо зважати на те, що для того, щоб діагностувати ігровий розлад, відповідна йому модель поведінки має стійко спостерігатися протягом щонайменше одного року.

Ще одна причина для занепокоєння щодо ігор – це їх зв'язок з онлайновими азартними іграми. Наприклад, деякі ігри спонукають користувачів спробувати удачу з лутбоксом: гравець купує ящик, розплачуючись ігровими грошима (ігрова валюта купується за справжні гроші), сподіваючись отримати винагороду, яка виникає випадково .

Згідно з висновками нещодавно проведеного дослідження обсяг глобального ринку лутбоксів оцінюється в 20 млрд фунтів стерлінгів .

Штучний інтелект і машинне навчання

Тема штучного інтелекту викликає жвавий інтерес у засобів масової інформації. Розширюється спектр додатків ШІ, що проходять випробування. ШІ також викликає тривогу і стурбованість у зв'язку з можливим виникненням у нього помилкових суджень.

Важливо надати визначення ШІ та машинного навчання, проте єдине й універсальне визначення для них є неможливим. Воно залежить від мети, спрямованості та конкретних завдань. Розмаїття визначень також відображає й різні визначення «людського інтелекту». Крім того, існує відмінність у виконанні конкретних та загальних завдань: тоді як з виконанням перших успішно справляються люди, ШІ незамінний у виконанні конкретних завдань.

Машинне навчання здебільшого передбачає методи, що дозволяють машинам навчатися на основі даних. Воно націлене на узагальнення даних для формування моделей. Машинне навчання покладено в основі 80% існуючих додатків ШІ.

У контексті ШІ необхідно розглянути низку питань:

- Відсутність чітко сформульованих проблем: визначити проблему – це запорука успіху.
- Наявність даних: наявні дані дуже часто невірні, неактуальні, «брудні» або неповні.

Для підготовки та розробки ШІ й алгоритмічних систем досить часто використовуються дані, що збираються серед дорослих користувачів. Це означає, що алгоритмічні системи прийняття рішення і програми розпізнавання образів, в яких використовується ШІ, можуть бути значною мірою орієнтовані на дорослих, і, як наслідок, їх функції можуть ґрунтуватися на неточній оцінці і невірній категоризації ризиків, на які наражаються діти, або їх поведінки. Аналогічно набори даних та моделі, що використовуються для формування та інформаційного супроводу процесів прийняття рішень на основі ШІ, можуть неточно відображати та враховувати потреби деяких людей через їх національність, гендерну приналежність, інвалідність тощо. Таким чином, діти з числа таких недостатньо представлених груп можуть опинитися в ще більш несприятливому становищі через міжсекторальні фактори, яке буде посилюватися або навіть використовуватися ШІ.

• Нехтування розумінням: іноді модель працює нестабільно або ж працює добре, але не для вирішення спочатку поставленого завдання – наприклад, в ЗМІ останнім часом з'являються статті про те, що ШІ при пошукових запитах невірно інтерпретує зображення.

• Ціна помилки.

Штучний інтелект – приголомшлива розробка, однак дилема, що виникла у зв'язку з її появою, дуже нагадує «проблему вагонетки» в контексті безпілотних автомобілів.

6. Розуміння ризиків та джерел шкоди

На Малюнку 7 показана класифікація ризиків, на які наражаються діти в цифровому середовищі. Визнано, що існують також ризики для здоров'я та добробуту (надмірне використання Інтернету, дефіцит сну, тощо).

Малюнок 7: Класифікація ризиків, на які наражаються діти в онлайновому средовищі

	Контент Дитина як споживач (масового виробництва)	**Контакт** Дитина як споживач (дії, ініційовані дорослим)	**Поведінка** Дитина як активна дійова особа (порушник/жертва)
Агресивного характеру	**Жорстокість/сцени насильства**	**Домагання, переслідування**	**Цькування, ворожа поведінка однолітків**
Сексуального характеру	**Порнографічні матеріали**	**Грумінг, сексуальні зловживання під час зустрічі з незнайомцями**	**Сексуальні домагання, секстинг**
Ціннісного характеру	**Расистський контент/Контент, що розпалює ненависть**	**Ідеологічне переконання**	**Потенційно шкідливий контент, створений користувачем**
Комерційного характеру	**Реклама, прихований маркетинг**	**Використання персональних даних, зокрема неналежне**	**Азартні ігри, порушення авторських прав**

Джерело: дослідницька мережа ЄС «Діти в цифровому середовищі»
(Лівінгстон, Хаддон, Герциг і Олафссон (2011 р.)

Дослідження конкретної ситуації 1

В цьому прикладі розглядається випадок з хлопчиком, який переглянув відеозапис вбивства йорданського льотчика терористами ІДІЛ1. Хлопчик дізнався про те, що трапилося, з новин, які транслювалися по радіо, коли він зі своєю матір'ю повертався зі школи додому. Він почав розпитувати її про це, але вона не була готовою таке обговорювати. Жінка вимкнула радіо, і всю дорогу до будинку вони їхали мовчки. Хлопчика дуже збентежило те, що він почув – адже льотчика спалили живцем. І після повернення додому він почав шукати в Інтернеті подробиці, намагаючись зрозуміти, що сталося. Серед запропонованих пошуковою системою результатів був відеозапис про те, що сталося, розміщений на сайті новинного каналу. Хлопчик розповів, що коли він увімкнув це відео, він зрозумів, що йому не варто його переглядати, але не міг зупинитись і подивився його цілком. Те, що він побачив, його надто вразило; йому почали снитися жахи – вся ця історія його дуже травмувала, проте він нікому не висловлювався, оскільки побоювався реакції дорослих і щиро вважав, що його почнуть дорікати. З одного боку, поведінку матері можна зрозуміти, і вона показує те, що дорослі часто й гадки не мають, як реагувати на деякі види контенту в Інтернеті. Однак, попри те, що некомфортно та складно обговорювати такі речі, все ж обговорювати їх надважливо. Батьки мають бути готовими вислухати своїх дітей, і їм слід створити таку атмосферу, в якій діти могли б обговорювати з ними будь-які питання, які їх бентежать.

Контент

- Вплив незаконного та/або потенційно шкідливого контенту, зокрема, порнографії, азартних ігор, вебсайтів, що містять матеріали, пов'язані із заподіянням собі шкоди, та інших матеріалів, неприйнятних для дітей та молодь. У більшості випадків оператори цих вебсайтів не вживають ефективних заходів для обмеження доступу до них дітей та молодь.
- Вплив контакту з іншими користувачами.
- Заподіяння собі шкоди, деструктивна та жорстока поведінка.
- Вплив радикалізму та расизму й інших дискримінаційних висловлювань і зображень. • Довіра або використання неточної чи неповної інформації, знайденої в Інтернеті, або інформації з невідомих чи ненадійних джерел.
- Створення, перегляд та поширення незаконного або шкідливого контенту.

Маніпулювання в цифровому середовищі

Сьогодні відзначається як ніколи широка присутність дітей та молодь в цифровому середовищі, зокрема, в соціальних мережах, де вони піддаються впливу різного контенту, який фільтрується за допомогою алгоритмів для вчинення на них того чи того маніпулятивного впливу. Як приклад можна навести політичне маніпулювання (пропаганда певних політичних точок зору), фальшиві новини (поширення неправдивої інформації з політичною, комерційною чи іншою метою) та рекламу (формування у дітей та молоді переваг на користь конкретних брендів або продуктів у ранньому віці).

Таке алгоритмічно індивідуалізоване середовище може мати серйозний вплив на нормальний розвиток, думки, уподобання, цінності та звички дітей і молодь внаслідок їх ізоляції у створених фільтрами «бульбашках» і перешкоджати їх вільному доступу до широкого розмаїття думок і контенту та їх аналізу.

Контакт

- Зловмисник може видавати себе за іншу людину, часто-густо за іншу дитину, з метою умисного заподіяння шкоди іншій особі, домагання або Булінг.

Схиляння до дій сексуального характеру, або грумінг, в цифровому середовищі

У Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуальних зловживань (Лансаротська конвенція) грумінг (домагання стосовно дітей із сексуальною метою) визначається як умисна пропозиція про зустріч, з якою дорослий за допомогою інформаційних¬ та комунікаційних технологій звертається до дитини, яка не досягла встановленого на законодавчому рівні віку сексуальної згоди, з метою вчинення сексуальних зловживань або виробництва матеріалів, що містять сцени сексуальних зловживань стосовно дітей . Схиляння до дій сексуального характеру не завжди передбачає особисту зустріч. Це може здійснюватися в цифровому середовищі, проте навіть у цьому випадку дитині завдається серйозна шкода, наприклад, внаслідок виробництва матеріалів, що містять сцени сексуальних зловживань стосовно дітей, володіння ними або їх передавання третім особам .

У контексті схиляння до дій сексуального характеру, або грумінгу, основна увага приділяється процесу віктимізації, оскільки відповідні дослідження проводяться головним чином серед самих дітей та молоді.

Дослідження конкретної ситуації 2

У цьому прикладі розглядається випадок 13-річної дівчинки, якій незнайомий чоловік надсилав непристойні світлини в Instagram. Чоловік надсилав світлини самого себе в оголеному вигляді і просив дівчинку відправити йому свої фото без одягу. Дівчинка не погодилася це зробити, заблокувала його і поскаржилася на його сторінку в Instagram, а також розповіла про подію кільком своїм друзям – раптом з ними теж траплялося щось подібне, і з'ясувалося, що траплялося. Незважаючи на те що дівчинка все зробила правильно, вона нічого не розповіла батькам, побоюючись їх реакції. Вона була впевнена, що вони заборонять їй використовувати Instagram, а вона цього категорично не хотіла. Як вона пояснила, в Instagram вона та її друзі ділилися новинами й плітками, планували своє спільне дозвілля, обговорювали, що сталося в школі за день, тощо. Дівчинка щиро вважала, що її батьки (в прагненні захистити її) накажуть їй перестати використовувати цю платформу (Instagram). Але ж річ у тім, що дівчинка не зробила нічого поганого – це чоловік, який надсилав їй фотографії, поводився неналежно. Прагнення батьків захистити дитину в такій ситуації є цілком зрозумілим, проте карати її за те, що зробив хтось інший, абсолютно неправильно. Ми повинні виходити з того, що майже всі або всі дії дівчинки в Instagram були абсолютно прийнятними. Батькам дуже важливо реагувати осмислено, якщо діти розповідають їм про проблеми, на які вони наражаються в Інтернеті. Їм також потрібно вислухати свою дитину та підтримати її.

Булінг і домагання

Булінг є Булінг, незалежно від того, де і яким чином вона відбувається. Булінг в цифровому середовищі може особливо травмувати та нашкодити, оскільки воно, як правило, отримує дедалі більше поширення, і його свідками стає величезна кількість людей. Крім того, контент, що поширюється за допомогою електронних засобів, може спливти знову в будь-який момент, через що жертві Булінг складніше пережити і забути цей інцидент; Булінг може мати форму зображень, що дискредитують, або образливих слів; такий контент доступний вдень і вночі. Булінг за допомогою електронних засобів може чинитися цілодобово, 7 днів на тиждень, тобто воно може втручатися в приватне життя жертви навіть там, де за інших обставин жертва була б у «безпеці», наприклад вдома; персональна інформація може бути спотворена, світлини змінені і потім передані іншим людям. Більш того, Булінг може бути анонімним.

Діти та молодь, що піддаються докорам в реальному житті, часто-густо стають жертвами також і в онлайновому средовищі. Згідно з нещодавно проведеними дослідженнями, діти інваліди частіше мають справу з різного роду зловживаннями зокрема, стають жертвами сексуальних домагань, і, відповідно, наражаються на вищий ризик в цифровому середовищі. Віктимізація може набувати форми Булінг, домагання, ізоляції та дискримінації за ознакою реальної чи уявної інвалідності дитини, або ж у зв'язку з певними особливостями, зумовленими

її інвалідністю, – це можуть бути особливості мови і поведінки, або обладнання, або послуги, якими вона користується. До можливих ризиків належать:

- Дифамація та шкода репутації;
- Використання кредитних карток без дозволу, зокрема, використання кредитних карток батьків або інших людей для оплати членських внесків, купівлі інших послуг або товарів;
- Спроби зловмисників видати себе за інших користувачів Інтернету, головним чином для отримання фінансових вигод. У деяких випадках може мати місце розкрадання особистих даних, хоча з таким видом шахрайства, як правило, частіше мають справу дорослі;
- Небажана реклама: деякі компанії через веб-сайти надсилають дітям спамові повідомлення з пропозицією купити товари. У зв'язку з цим виникає питання про згоду користувача і про те, як її слід отримувати. Законодавство в цій галузі недосконале, і доволі проблематично визначити, коли діти та молодь починають розуміти процес передавання даних. Питання про те, як слід застосовувати відповідні норми в Інтернеті, саме по собі вже досить складне, а доступність мобільних телефонів робить цю проблему нагальною;
- Небажані контакти, надто у випадках, коли дорослі люди видають себе за інших або представляються дітьми або молодими особами.

Поведінка

• Розкриття персональної інформації, що призводить до ризику фізичного насильства; • Заподіяння фізичної шкоди під час реальних зустрічей з особами, знайомство з якими було заведено в Інтернеті, в тому числі можливе фізичне й сексуальне насильство. • «Секстинг – пересилання інтимних світлин, яке може стати причиною сексуального домагання, секс-вимагання, грумінгу або експлуатації зображень.

Секстинг

«Секстинг» (пересилання за допомогою мобільних телефонів повідомлень або зображень сексуального характеру) – поширена практика серед підлітків. Такими зображеннями та повідомленнями часто обмінюються люди, що перебувають у стосунках, або потенційні партнери, проте іноді такий контент надається для широкого загалу. Вважається, що молодь здебільшого не здатна адекватно оцінити можливі наслідки таких дій і потенційно пов'язані з ними ризики .

Одне із серйозних побоювань щодо секстингу полягає в тому, що діти та молодь можуть створювати незаконні матеріали, пов'язані із сексуальними зловживаннями стосовно дітей, що може спричинити суттєві правові санкції. До небезпек належать:

• Адресна розсилка спаму та реклами компаніями через вебсайти з метою просування продуктів для людей певного віку або певних інтересів;

• Поведінка, що несе в собі небезпеку для здоров'я, наприклад проведення великої кількості часу перед екраном: маніакальне або надмірне використання Інтернету та/або онлайнових ігор на шкоду соціальним заходам або активним видам відпочинку, важливим для підтримки здоров'я, вибудовування довірчих відносин, соціального розвитку і загального благополуччя.

Рекомендації для батьків та освітян щодо захисту дитини в цифровому середовищі

• Порушення власних прав або прав інших людей в результаті плагіату і розміщення в Інтернеті контенту (особливо фотографій) без дозволу. Як було продемонстровано, завантаження та розміщення в Інтернеті світлин неналежного характеру без дозволу може нашкодити іншим людям.

• Недотримання авторських прав інших людей, наприклад, шляхом завантаження з Інтернету музики, фільмів або ТВ-програм, за які слід було б заплатити.

• Зазначення особами невірного віку – або дитиною, що видає себе за людину більш старшого віку для отримання доступу до вебсайтів, що містять не відповідний для її віку контент, або дорослою людиною, що видає себе за дитину.

• Використання електронної пошти батьків без їх згоди: згода батьків потрібна для активації деяких онлайнових облікових записів, які згодом батькам буває дуже складно видалити. Щоб не просити дозволу у батьків, діти та молодь вдаються до такого методу.

У межах дослідження, проведеного в 2020 році дослідницькою мережею ЄС «Діти в цифровому середовищі», було зроблено порівняння того, як діти та молодь використовують нові засоби інформації, і того, як вони використовують такі засоби, на думку дорослих . Було також проведено дослідження на тему того, як в уявленні дітей повинні захищатися їхні права в цифровому середовищі , а також роботу, присвячену досвіду взаємодії з цифровим середовищем дітей з інвалідністю .

Основна мета кампанії по забезпеченню безпеки в Інтернеті полягає в тому, щоб змінити модель поведінки, в тому числі за рахунок стимулювання більш безпечної поведінки дітей та молодь в цифровому середовищі, а також ефективної участі батьків та інших людей, які взаємодіють з дітьми (родичі, освітяни тощо), в навчанні дітей заходів безпеки в Інтернеті.

Безпеку дітей та молоді в Інтернеті слід розглядати не як окрему проблему, а як питання, що має тісний зв'язок з різними ініціативами, що стосуються дітей і молодь, їх безпеки та Інтернету.

7. Роль батьків та опікунів

Батьки повинні надавати дітям та молодим особам підтримку з тим, щоб ті могли користуватися перевагами технологій безпечно. Їм варто дотримуватися збалансованого підходу і зважати на те різноманіття можливостей, які пропонує Інтернет. Нерідко батьки зосереджують свою увагу на безлічі онлайнових освітніх ресурсах і можливостях для розвитку навичок, проте їм також варто знати та враховувати, що Інтернет надає дітям низку можливостей щодо соціального розвитку – наприклад, основною мотивацією для використання Інтернету можуть бути ігри або особисті захоплення дітей. Коли батьки це розуміють, вони можуть вибудувати більш ефективну взаємодію з дітьми і краще їх підтримати. Для того щоб зробити поведінку дітей та молодь при використанні вебсайтів більш безпечною та відповідальною, батькам й опікунам варто виходити з необхідності:

1) Дізнатися про наявні в цифровому середовищі ризики та можливості для дітей і молодь. Важливо вміти розпізнавати потенційні загрози, на які можуть наражатися діти, але при цьому пам'ятати, що наявність ризиків не означає, що неодмінно буде завдано шкоди.

2) Активно цікавитися тим, що роблять діти в Інтернеті, який тип контенту вони переглядають, надсилають або створюють, якими послугами та платформами вони користуються і в які бавляться ігри, а також з якими людьми вони спілкуються. Батькам завжди корисно самим спробувати скористатися тими послугами, якими користуються їхні діти.

3) Батькам слід вивчити питання про те, якими є хороші навчальні та розважальні вебсайти та ігри, котрі вони могли б використовувати зі своїми дітьми. Гарний вебсайт або гра відрізняються тим, що в них є окрема сторінка, присвячена питанням безпеки, зі зрозумілими посиланнями, механізмами подання скарг та вказівками для дітей і молодь, а також їх батьків/опікунів.

4) Підтримувати регулярний, щирий та відкритий діалог з дітьми і молодими особами на

актуальні для їхнього віку теми, які повинні з часом змінюватися.

a) Переконайтеся, що діти і молодь розуміють, з якими ризиками вони можуть мати справу, і домовтеся з ними про те, яких заходів вони вживатимуть в разі виникнення реальної небезпеки – наприклад, що їм бажано просто розповісти про це вам.

b) Заохочуйте дітей та молодь замислитися про те, як слід поводитися сумлінному цифровому громадянину, зокрема, про те, якою інформацією про себе та інших вони діляться, допомагаючи їм сформувати позитивну модель онлайнової поведінки.

c) Навчайте дітей критично ставитися до того, що вони бачать в Інтернеті; розкажіть, що не всі люди є тими, за кого себе видають, і що те, що вони бачать, може бути неправдою. Розкажіть їм, що люди в Мережі можуть створювати ідеальний образ самих себе, а також про фальшиві новини, спрямовані на маніпулювання людьми.

d) Обговоріть з дітьми проблему тиску з боку однолітків і страх бути неприйнятим в колективі, а також питання вибудовування дружніх відносин в Інтернеті. е) Обговоріть з дітьми привабливість імерсивних технологій, що викликають залежність, особливо тих, що представлені на безкоштовних платформах, де час,

який люди проводять в Інтернеті, або дані, якими вони обмінюються, є валютою або основою бізнес-моделі.

5) Переконатися, що дитина знає, коли варто звернутися за допомогою і до кого. Це може бути їхній батько або опікун, вчитель або будь-яка інша доросла людина, якій вони довіряють. Слід домовитися про правило, що в разі будь-якого неприємного інциденту діти мають обговорити його з дорослим, якому вони довіряють.

6) Розробити правила для всієї родини щодо використання підключених до Інтернету пристроїв і пам'ятати про те, що у своїй поведінці в цифровому середовищі діти беруть приклад з батьків або опікунів.

7) Вжити заходів для того, щоб діти дотримувалися збалансованої «цифрової дієти», тобто щоб вони проводили час в Інтернеті з користю, займаючись різними видами діяльності, зокрема, навчання, творчість та спілкування в позитивному сенсі. Використовувати вбудовані інструменти для відстеження статистики за кількістю часу, що витрачається на різні програми та послуги.

8) Стати впевненими користувачами пристроїв та навчити своїх дітей. Існує ціла низка інструментів, які можуть допомогти батькам в управлінні підключеними до мережі пристроями – як удома, так і за його межами.

a) Потрібно врахувати усі під'єднані до Інтернету пристрої, а не тільки очевидні – смартфони, планшети та ПК. Зверніть увагу на ігрові приставки, особисті помічники, під'єднані до Інтернету телевізори і будь-які інші пристрої, що мають доступ до Інтернету.

b) При прийнятті рішень про те, до якого контенту, ігор, додатків і послуг діти та молодь матимуть доступ, керуйтеся віковими обмеженнями. Зважте, що вікові обмеження в магазинах додатків і на самих платформах відрізняються. За допомогою налаштувань можна контролювати, які програми та ігри буде

дозволено завантажувати і використовувати.

c) Розгляньте можливість використання контент-фільтрів, що досить часто називаються системами батьківського контролю, і безпечних пошукових систем або обмежень доступу, щоб фільтрувати контент, який діти та молодь можуть переглядати в Інтернеті.

d) Як батьки, ви мусите розуміти, як і коли слід поскаржитися на той чи інший контент, який засмутив, збентежив або призвів до стурбованості ваших дітей або який, на їхню думку, порушує умови використання. Ви повинні знати, як заблокувати небажані або непрошені контакти.

e) Ретельно зважте усі за та проти використання моніторингових додатків і технологій, що відстежують дії дитини в Інтернеті. Побічним ефектом їх використання може стати ще більш прихована онлайнова поведінка, а також це може призвести до конфліктів в сім'ї, у тому числі насильницьких. Якщо ви все ж таки використовуєте їх, то поясніть своїй дитині, що саме ви відстежуєте і навіщо.

f) У міру дорослішання та розвитку дітей і молоді необхідно коригувати контроль й обмеження доступу з тим, щоб вони відповідали віку; важливо формувати стійкість у ваших дітей, щоб вони могли повною мірою користуватися перевагами онлайнового середовища.

Рекомендації для батьків та освітян щодо захисту дитини в цифровому середовищі

9) Пояснити дітям, що не можна повідомляти свої паролі доступу друзям або братам і сестрам. Звертати увагу на те, коли і де вони повідомляють свою персональну інформацію – наприклад, в загальнодоступному профілі має сенс використовувати деперсоніфіковані зображення як фотографії профілю і вказувати мінімум персональної інформації, такої, як вік, школа та місце проживання.

10) Не потрібно вважати, що в Інтернеті геть усі бажають заподіяти вашій дитині шкоду. Як правило, дитячі веб-сайти безпечні й надають неабиякі можливості для творчої соціалізації та навчання вашої дитини, однак варто лишатися залученим і пильним.

11) Зберігайте спокій і не робіть поспішних висновків, якщо ви почули або побачили щось, що стурбувало вас в поведінці вашої дитини або в поведінці одного з його онлайнових друзів. Не слід погрожувати, що ви позбудетеся пристроїв або відберете їх, оскільки для декого з молодь вони є найважливішими інструментами соціалізації. Якщо ваші діти побоюватимуться, що в них відберуть пристрої, вони, швидше за все, менш охоче будуть розповідати вам про свої проблеми і переживання.

12) Здатність впоратися з неприємностями і робити висновки є найважливішим елементом формування стійкості до впливу цифрового середовища. Коли діти в цифровому середовищі наражаються на ризики або їм заподіюється шкода, батьки можуть допомогти їм знайти способи впоратися з цією ситуацією, щоб вони в подальшому могли в міру можливості безпечно користуватися благами онлайнового середовища, уникаючи при цьому ізоляції.

Куди звернутися по допомогу?

У багатьох країнах є служби допомоги, куди діти та молодь можуть повідомити про проблему. Їх діяльність широко висвітлюється, і в різних країнах задля поширення відповідної інформації використовуються різні підходи. Важливо, щоб діти та молодь розуміли, що ніколи не пізно повідомити про проблему і що, зробивши це, вони можуть допомогти іншим.

Хоча діти та молодь усвідомлюють, що вони іноді поводяться ризиковано, вони не виявляють великого занепокоєння щодо можливих ризиків, пов'язаних з такою поведінкою, і вважають за краще вирішувати проблеми самостійно або в колі своїх однолітків. Таким чином, вони звертаються по допомогу до батьків або інших дорослих тільки при виникненні потенційно «критичних» проблем. Такий підхід найбільш поширений серед хлопчиків старшого віку, які здебільшого вважають за краще використовувати тільки кнопку «Поскаржитися»60 (наприклад, таку, як розроблена Віртуальною глобальною цільовою групою) замість того, щоб розповісти про те, що сталося, батькам або іншим дорослим. Проте це стосується не всіх дітей та молодь. Ми бачимо, що діти та молодь, яким відомо про ризики, стежать за власними діями, але

почасти не поділяють тієї точки зору на нові технології, яка передбачає, що основна роль з оцінки та контролю за поведінкою дітей і молоді має належати батькам61. Варто проявляти обережність при проведенні простих відмінностей між реальним та онлайновим світами, оскільки наше повсякденне життя стає дедалі більш залежним від онлайнових технологій. Це означає, що багатьом дітям та молодим особам доводиться шукати тонкий баланс між можливостями, які надають технології (як-от розкриття власної індивідуальності, вибудовування близьких взаємин і більш активне спілкування), та ризиками, пов'язаними з комунікацією в Інтернеті (пов'язаними з недоторканністю приватного життя, непорозумінням і недобросовісними практиками)62.

Батьки та освітяни повинні знати, що коли вони запідозрили, що дитина зазнала сексуальних зловживань в Інтернеті, то зловмисника потрібно заблокувати, а листування зберегти як доказ. Батьки не повинні за жодних обставин переглядати зображення сексуального характеру, зроблені їх власними або чужими дітьми. Необхідно передати ці матеріали до правоохоронних органів і повідомити про сексуальні зловживання щодо дітей або їх сексуальної експлуатації в Інтернеті у відповідне відомство. Батьки ніколи не повинні вступати в контакт від імені своєї дитини в спробі «довести» факт зловживань.

Додаткову інформацію про те, як поскаржитися на фотографії дітей сексуального характеру, можна знайти тут:

Фонд спостереження за Інтернетом – https://www.iwf.org.uk/.

Національний центр допомоги зниклим та експлуатованим дітям (NCMEC) – https://report. cybertip.org/.

Європол - https://www.europol.europa.eu/report-a-crime/law-enforcement-reporting-channels child-sexual -coercion-and-extortion.

8. Рекомендації для батьків та опікунів

Поради щодо гарантування безпеки підготовлені на основі аналізу зібраних даних і результатів наявних досліджень. У цьому розділі звіту пропонуються рекомендації для батьків та опікунів (для освітян – в окремому переліку), які допоможуть їм навчити дітей та молодь тому, як гарантувати свою безпеку й отримати позитивний та цінний досвід в цифровому середовищі.

Батьки та опікуни, перш ніж прийняти рішення про те, які умови найкраще підійдуть для їхньої дитини, повинні точно оцінити характер різних сайтів, ступінь розуміння їх дітьми небезпек та вірогідності того, що батьки можуть сприяти зменшенню відповідних ризиків.

Інтернет має величезний потенціал щодо надання дітям та молодим особам можливостей

з пошуку матеріалів, що їх цікавлять. Основне завдання полягає в тому, щоб навчити їх позитивним та відповідальним формам онлайнової поведінки. У Таблиці 1 в рамках кожного питання подані Ключові поради, які слід брати До уваги батькам та опікунам.

Таблиця 1: Ключові поради, які слід брати До уваги батькам та опікунам

Безпека 1 і надійність ваших технологій 1. Поспілкуйтеся зі своїми дітьми. Спробуйте організувати спільно з ними будь-яку онлайнову діяльність. Поцікавтеся тим, що вони роблять в Інтернеті, розпитайте їх про це. Важливо, щоб у дітей та молодь не виникало відчуття, що батьки їм не довіряють. Налаштування фільтрів, відстеження і обмеження доступу важливі, однак це має супроводжуватися діалогом та обговоренням. Коли діти та молодь проводять час поза домом з іншими людьми, у них з'являється доступ до інших (можливо, без обмежень доступу) пристроїв, тому довірливе спілкування має велике значення: чи розкажуть вони вам, коли щось трапиться? Коли діти та молодь розповідають вам про будь-який інцидент, що стався в Інтернеті, важливо реагувати стримано. Найголовніше, що вони вам про це повідомили, і адекватна реакція з вашого боку зміцнить їх на думці, що ви можете їм допомогти, а отже, вони звернуться до вас знову, якщо подібне повториться. Дітям та молоді бажано мати уявлення про те, що таке Інтернет, для того, щоб вони краще розуміли, що таке «інтернет-простір», в якому розміщені їх улюблені платформи, як-от Instagram, Snapchat та YouTube. Інтернет часто видається дітям та молоді якимось абстрактним місцем, і за відсутності певного розуміння його роботи їм може бути складно усвідомити та розпізнати ризики, наочно собі їх уявити. Можна провести аналогію з великим містом, в якому є багато чудових місць та приємних людей, але також є й місця, куди ви б не пішли в жодному разі, тому що там небезпечно. Це допоможе дітям та молоді замислитися про різний «контингент», який можна зустріти в Інтернеті, про те, як може поширюватися інформація тощо. Батьки повинні проявляти інтерес до того, чим займаються їхні діти в Інтернеті, і бути готовими розповісти про власний онлайновий досвід з метою вибудовування довірчих відносин та відкритого діалогу.

Рекомендації для батьків та освітян щодо захисту дитини в цифровому середовищі

2. Визначте, які технології, пристрої та послуги використовуються у вашій родині/у вас вдома.

3. Встановіть на всіх пристроях брандмауер та антивірусну програму. Поміркуйте над тим, чи будуть корисними та чи підходять для вашої родини програми фільтрації, блокування або відстеження.

Правила 4. У колі родини домовтеся про умови використання Інтернету і особистих пристроїв, приділяючи особливу увагу питанням конфіденційності, вікової відповідності змісту сайтів, додатків та ігор, Булінг, кількості проведеного перед екраном часу та небезпеки з боку незнайомців. Крім того, створіть вдома атмосферу підтримки задля того, щоб діти та молодь знали, що можуть звернутися за допомогою до батьків/ опікунів.
Почніть з пристроїв: визначте, які пристрої у вас вдома мають доступ до Інтернету, включаючи мобільні телефони, ноутбуки, планшети, а також «розумні» телевізори, ігрові приставки та фітнес-трекери, – все, чим користуються члени вашої родини. Визначте, якими онлайновими послугами та додатками користуються члени вашої родини за допомогою усіх цих пристроїв.

Встановіть на всіх ваших пристроях антивірусну програму та захист від шкідливих програм і регулярно оновлюйте їх. Навчіть ваших дітей основам безпеки в Інтернеті. Наприклад, чи оновлена операційна система? Чи використовуєте ви найновішу версію програми? Чи встановлені останні оновлення для системи безпеки? Програми фільтрації та відстеження досить ефективні, однак у разі їх використання слід враховувати питання довіри та недоторканності приватного життя. Батьки повинні пояснити своїм дітям, що вони використовують ці програми для того, щоб гарантувати безпеку сім'ї.

Щойно діти та молодь починають користуватися технологіями, обговоріть та виробіть разом з ними набір загальних правил. Ці правила повинні визначати, коли дітям та молодим особам дозволено користуватися Інтернетом і яким чином, а також скільки часу їм можна проводити перед екраном.

Зразок поведінки у цифровому середовищі: важливо, щоб батьки подавали дітям гарний приклад.

У дітей набагато швидше сформується модель правильної поведінки, якщо у них перед очима буде відповідний приклад їх батьків/опікунів.

Така сама логіка може бути застосована і до фотографування та розміщення знімків в Інтернеті: перш ніж публікувати світлини в Мережі, слід отримати згоду. Батькам варто звертати увагу на те, якою інформацією про своїх дітей вони діляться в соціальних мережах і в Інтернеті загалом, зокрема, це стосується особистих історій про дітей або їхніх світлин. Пам'ятайте про недоторканність приватного життя вашої дитини – як в даний момент часу, так і в перспективі.

Діти та молодь повинні мати можливість обговорювати будь-які труднощі та проблеми, з якими вони мають справу в цифровому середовищі (і в реальному житті). Один зі способів ініціювати таке обговорення – взяти приклад новин зі ЗМІ, в якому йдеться про ту чи іншу поведінку в Інтернеті. Це дозволить знеособити проблему і дасть змогу дітям та молоді висловити свою точку зору.

Рекомендації для батьків та освітян щодо захисту дитини в цифровому середовищі

Навчання батьків та опікунів

мобільні послуги використовують ваші діти (соціальні мережі, веб¬сайти, додатки, ігри тощо), а також усвідомте, як ваші діти проводять час в Інтернеті.

7. Контролюйте використання кредитних карток та інших платіжних механізмів

6. Зверніть увагу на вік «цифрової згоди»

8. Механізми подання скарг

Огляд можливостей інтернет-сайтів

5. Будьте в курсі того, які онлайнові та

9. Реклама, недостовірна інформація та дезінформація

Вивчіть питання про те, як забезпечити максимальну ступінь безпеки дітей та молодь при використанні додатків і платформ, у тому числі за рахунок налаштувань приватності облікових записів, обліку вікових обмежень тощо.

Використовуйте інструменти для мобільних пристроїв, як-от Family Link та інші інструменти батьківського контролю. Перевіряйте, чи продаються певні продукти та чи можливо здійснення покупок у додатках.

Спробуйте зрозуміти мотивацію поведінки дітей та молодь в цифровому середовищі. Чому вони використовують конкретні вебсайти та послуги? Що надають їм різні вебсайти та послуги стосовно спілкування в колі друзів, самоідентифікації та відчуття приналежності? Розуміння цих речей також допоможе вам ліпше зрозуміти, з якими соціальними та емоційними проблемами (які іноді можуть стати причиною ризикованої поведінки) можуть мати справу діти та молодь, і ви зможете дати їм поради про те, як розвивати стійкість.

У деяких країнах діють закони, що встановлюють мінімальний вік, починаючи з якого компанії або вебсайти можуть просити молодь повідомити персональну інформацію без попереднього отримання підтвердженої згоди батьків. Вік «цифрової згоди» зазвичай варіюється в межах 13-16 років. У деяких країнах практика вимагати згоду батьків перед тим, як запитувати у молодь особисту інформацію, має рекомендаційний характер, тоді як в інших країнах це передбачено законодавчому рівні (див. статтю 8 Загального регламенту ЄС про захист даних (GDPR)). На багатьох веб¬сайтах, призначених для дітей молодшого віку, потрібна згода батьків для реєстрації нового користувача. Перевіряйте кожну послугу на наявність вимог до мінімального віку.

Існує безліч пристроїв, додатків та послуг, що дозволяють здійснювати покупки і суворо контролювати доступ до облікових записів батьків, що містять платіжні механізми й дані кредитних карток. Важливо стежити за збереженням даних ваших кредитних та дебетових карток і нікому не повідомляти пін-коди, щоб уникнути несанкціонованого доступу.

Дізнайтеся, як повідомити про проблему на платформах, якими користуються ваші діти, і як видалити профіль або змінити зазначену в ньому інформацію, і, коли діти подорослішають, переконайтеся, що вони теж уміють це робити. Крім того, з'ясуйте, які є місцеві «лінії допомоги», куди можна звернутися зі скаргою.

Майте на увазі, що реклама може мати неприйнятний зміст або вводити в оману. Розкажіть своїм дітям, як вони можуть поскаржитися на рекламу та більшою мірою контролювати те, який контент їм пропонується. Важливо розуміти, що все, що діти та молодь бачать в Інтернеті, може впливати на їх погляди. Допомагайте їм підвищувати їх рівень медійно-інформаційної грамотності.

Рекомендації для батьків та освітян щодо захисту дитини в цифровому середовищі

Навчання дітей

10. Створіть атмосферу Діти та молодь мають розуміти, що підтримки онлайновий світ є відображенням реального світу – в ньому є як хороше, так і погане.Важливо, щоб діти та молодь знали, що завжди можуть звернутися до вас за допомогою і підтримкою, коли щось станеться, і що вони самі можуть надати комусь підтримку в Інтернеті.

Залежно від віку ваших дітей може мати сенс цікавитися тим, який контент вони розміщують в Інтернеті і яку інформацію вказують в онлайнових профілях.

Діти та молодь повинні вміти розпізнавати Онлайн-ризики – деякі з них цілком зрозумілі, але є не настільки очевидні – як-от примус, шантаж, публічне висміювання. Ці прийоми часто використовують зловмисники та злочинці.

Діти та молодь повинні також розуміти, що доступ до Інтернету передбачає певну відповідальність. Їм належить знати, що закони діють не тільки в реальному світі, а й в цифровому середовищі і їм слід поводитися відповідним чином.

11. Оскільки діти та молодь дедалі більше дізнаються про онлайновий світ, вони можуть мати бажання зустрітися з людьми, з якими вони незнайомі в реальному житті, але підтримують зв'язок в Інтернеті. Вам необхідно доступно пояснити їм, чим небезпечні зустрічі з незнайомцями, з якими вони спілкуються в Інтернеті.

12. Важливість персональної інформації

Діти та молодь можуть наражатися на реальну небезпеку, якщо вони вирішують зустрітися наживо з незнайомцями, з якими спілкувалися тільки в Інтернеті. Люди в Інтернеті можуть виявитися не тими, за кого себе видають. Та якщо все ж таки сформувалася міцна онлайнова дружба, і ваша дитина бажає влаштувати зустріч, не дозволяйте їй іти одній або без супроводу, а дайте зрозуміти, що збираєтеся піти разом з нею, або переконайтеся, що з нею піде інший дорослий, якому ви довіряєте. Звісно, все залежить від віку дитини.

Крім того, важливо брати до уваги, що останнім часом почастішали випадки злочинів без фізичного контакту, в яких мета злочинців та зловмисників полягає не в тому, щоб зустрітися з дитиною, а в тому, щоб отримати від неї матеріали сексуального змісту.

Поясніть дітям та молодим особам, що їм слід ділитися тільки тією інформацією, яку, на вашу і на їхню думку, дозволено побачити стороннім. Їм не слід ділитися інформацією, що дозволяє встановити їх особистість. Нагадайте дітям та молодим особам, що в них є онлайн репутація, за якою необхідно стежити. Після того як контент опубліковано, його може бути складно змінити або скорегувати.

Рекомендації для батьків та освітян щодо захисту дитини в цифровому середовищі

Навчання дітей

13. Переконайтеся, що діти та молодь розуміють, що означає публікація світлин в Інтернеті, в тому числі їх власних фотографій та фотографій їх друзів.

Поясніть вашим дітям, що фотографії можуть розкривати безліч персональної інформації. Діти та молодь повинні розуміти ризики, пов'язані з використанням камер та опублікуванням контенту. Бажано, щоб світлини інших людей не викладалися без їхньої згоди. Це також стосується і батьків, які роблять та публікують знімки своїх дітей.

Крім того, важливо, щоб діти та молодь розуміли, що іноді інформацію може розкрити хтось із їхніх друзів або членів сім'ї, тому їм варто поговорити про це зі своїми друзями та родичами і розповісти про небезпеку надмірного розкриття інформації. Порадьте своїм дітям не викладати свої фотографії або фотографії друзів, на яких є елементи, які легко піддаються ідентифікації, як-от таблички з назвами вулиць, автомобільні номери або назва школи на толстовках.

9. Роль освітян

Дуже важливо, щоб освітяни не вважали зрозумілим те, що дітям та молодим особам щось відомо або щось невідомо щодо питань гарантування безпеки в Інтернеті; наприклад, важлива роль освітян полягає в тому, щоб пояснити дітям та молодим особам, навіщо потрібні паролі і як забезпечити їх збереження, а також як придумати надійний пароль: багато підлітків передають паролі один одному – це зазвичай вважається вищим проявом дружби.

Питання недоторканності приватного життя дітей та молоді в Інтернеті є предметом активних дискусій, і за підсумками фактологічного огляду, проведеного Лондонською школою економіки, зроблено висновок, що діти та молодь серйозно ставляться до недоторканності свого приватного життя і вживають заходів захисту, однак при цьому вони високо цінують можливості онлайнової взаємодії. Крім того, під час огляду було

виявлено, що «посередництво з боку батьків, що сприяє», має велике значення щодо розширення можливостей дітей та молодь, оскільки воно дозволяє їм мати справу з деякими ризиками і водночас навчатися незалежним стратегіям безпечної поведінки. В огляді також зазначалося, що «необхідно розробляти ресурси та навчальні програми з розвитку медійно-інформаційної грамотності для батьків, освітян та працівників, які надають підтримку дітям, оскільки факти свідчать про те, що у дорослих є значні прогалини у знаннях щодо онлайнових ризиків, на які наражаються діти та молодь, і методів захисту даних та недоторканності приватного життя».

У школах є можливість скорегувати програму навчання, аби допомогти учням розкрити свій потенціал і підвищити стандарти освіти в галузі ІКТ. Однак також важливо те, щоб діти та молодь навчилися безпечно користуватися цими новими технологіями, зокрема, такими, як платформи та послуги соціальних мереж, які є найважливішим елементом продуктивного та креативного соціального навчання. Сьогодні діти та молодь легко можуть створювати власний контент і ділитися ним з широкою аудиторією через платформи соціальних мереж, більшість з яких надають змогу ведення прямої потокової трансляції.

Освітяни можуть сприяти тому, щоб діти та молодь використовували технології розумно та безпечно, зокрема, шляхом:

- забезпечення прийняття в школі набору суворих правил та процедур і регулярної оцінки та перегляду їх ефективності;
- сприяння формуванню цифрових навичок та цифрової грамотності за допомогою включення в навчальні плани навчальних дисциплін з цифрового громадянства. В рамках дисциплін з онлайнової безпеки слід приділяти увагу соціальним та емоційним аспектам навчання, бо це допоможе учням краще розуміти та контролювати свої емоції і, як наслідок, вибудовувати здорові та поважні взаємини – як в цифровому середовищі, так і в реальному житті;
- забезпечення загальної обізнаності про правила допустимого використання (AUP) та необхідності їх дотримання. Наявність AUP є дуже важливим, і вони мають бути відповідним до віку;
- закріплення в шкільній політиці проти Булінг положень, що стосуються Булінг в Інтернеті за допомогою мобільних телефонів та інших пристроїв, а також встановлення ефективних санкцій за порушення;
- призначення координатора з питань онлайнової безпеки;

Рекомендації для батьків та освітян щодо захисту дитини в цифровому середовищі

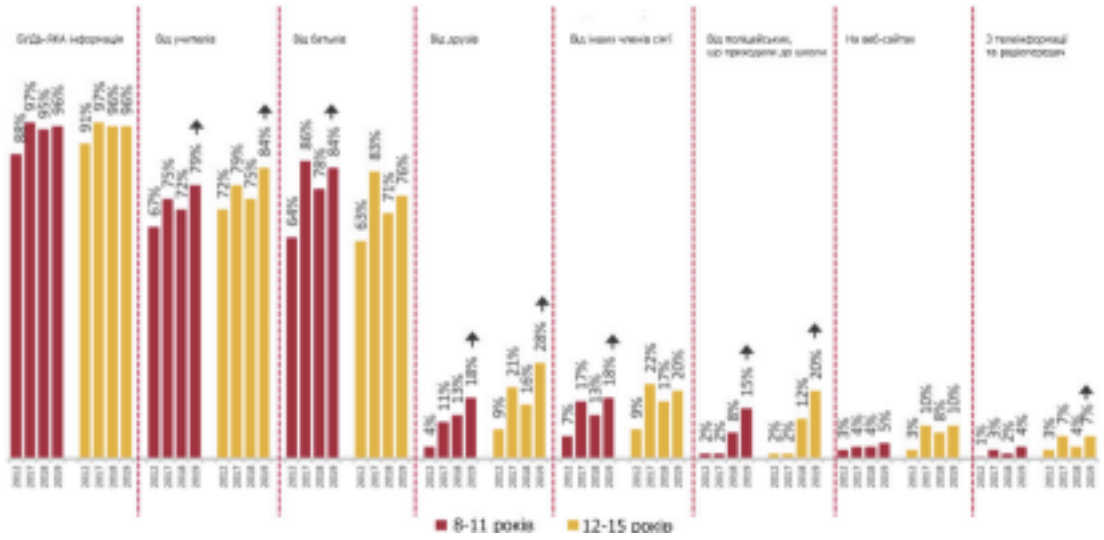
- забезпечення захищеності та надійності шкільної мережі;
- використання послуг офіційного інтернет-провайдера;
- використання програмних продуктів для фільтрації/моніторингу; • організації для всіх дітей та молодь навчання з питань онлайнової безпеки із зазначенням того, де, як і коли таке навчання буде проводитися;
- забезпечення достатнього рівня підготовки усіх співробітників (зокрема, технічний персонал), а також регулярного підвищення їх кваліфікації;
- призначення в школі спеціального координатора і створення можливостей для обліку та реєстрації інцидентів, пов’язаних з онлайновою безпекою, з метою формування цілісного уявлення про наявні в школі проблеми та тенденції, що вимагають уваги;
- вживання заходів для того, щоб адміністративно-управлінський персонал та керівники були достатньо обізнані в питаннях онлайнової безпеки в школі;
- проведення регулярної перевірки усіх заходів у сфері онлайнової безпеки; • прийняття до уваги потенційного впливу Інтернету та онлайнових технологій на навчання та

психіку дітей і молодь;

В останні роки показники використання дітьми та молодими особами інтернет-технологій різко зростають, внаслідок чого збільшується і занепокоєння з приводу питань безпеки в цифровому середовищі. Історично так склалося, що суспільство періодично охоплює хвиля «моральної паніки» у зв'язку з потенційною небезпекою комунікаційних технологій – особливо це стосується молодих жінок. Однак дехто стверджує, що безпосереднє вивчення такої небезпеки дозволяє зробити висновок про те, що джерелом небезпеки часто є не сама технологія, а дедалі більш активне використання цієї технології дітьми та молодими особами, що супроводжується зростаючим занепокоєнням з приводу втрати батьківського контролю. Вважається, що освітяни відіграють найважливішу роль у формуванні та прищепленні культури інтернет-безпеки. Судячи з усього, батьки в усьому світі вважають, що школа має відігравати головну роль у навчанні дітей та молодь навичкам безпечного використання технологій, однак, як показують дослідження, основним джерелом інформації про проблеми, з якими мають справу діти та молодь в цифровому середовищі, є не тільки школа, а й батьки64. Додаткові рекомендації щодо компетенцій, які необхідно включити до відповідного навчання, були запропоновані в рамках освітнього проекту Ради Європи, присвяченого цифровому громадянству.

Рекомендації для батьків та освітян щодо захисту дитини в цифровому середовищі

Малюнок 8: Діти, які повідомили, що вони отримували будь-яку інформацію або поради щодо безпечного використання Інтернету, з числа тих, хто користується Інтернетом вдома (2012 р.) або поза домом (2017, 2018 та 2019 рр.), з розподілом за віком



Джерело: Ofcom

- Спочатку підходи до забезпечення онлайнової безпеки ґрунтувалися головним чином на застосуванні технологій, як-от програми фільтрації, проте в останні роки спостерігається зростаюча мобільність інформаційних технологій, внаслідок чого звичні настільні комп'ютери вже не є єдиним засобом доступу до Інтернету. Дедалі більша кількість мобільних телефонів, планшетів, персональних цифрових помічників та ігрових приставок надають можливості широкосмугового зв'язку, і діти та молодь можуть користуватися Інтернетом у школі, вдома, в бібліотеці, в інтернет-кафе, ресторанах швидкого харчування, молодіжних клубах або навіть в громадському транспорті дорогою до школи. Школи надають можливість спільної роботи в Інтернеті всередині закритої мережі або просто в оточенні інших дітей та молодь. Очевидним першочерговим заходом є забезпечення ефективного захисту такої мережі. При цьому у дітей та молоді можуть бути особисті пристрої, які не охоплюються мережевим захистом, і тому навчання, обговорення та діалог мають ключове значення.
- Політика у сфері онлайнової безпеки має розроблятися та здійснюватися таким чином, щоб вона охоплювала широке коло зацікавлених груп і сторін. До них, зокрема, відносяться:
- директори шкіл;
- керівник;
- старший адміністративно-управлінський персонал;
- учителі;
- технічний персонал;
- батьки або опікуни;
- співробітники місцевих органів влади;
- де це можливо – постачальники послуг Інтернету і ті, хто забезпечує під'єднання до Інтернету та доступ до послуг широкосмугового зв'язку в школах.

Рекомендації для батьків та освітян щодо захисту дитини в цифровому середовищі

Оскільки усі ці групи можуть зробити свій унікальний внесок у формування шкільної політики, важливо проконсультуватися з представниками кожної з них. Проте власне наявності політики недостатньо, і кожному, хто взаємодіє з дітьми та молодими особами, слід дотримуватися активного підходу, що допомагає персоналу визначити, якою має

бути безпечна поведінка і як сформувати відповідні навички. Залучення усіх цих груп на початковому етапі дозволить кожному усвідомити важливість такої політики, а також особисту відповідальність за її реалізацію.

Створення безпечних умов для вивчення ІКТ передбачає наявність низки важливих елементів, включаючи:

- механізм забезпечення загальної обізнаності;
- відповідальність, правила та процедури;
- ефективний набір технологічних інструментів;
- всебічна освіта з питань електронної безпеки;
- програми навчання для всіх у межах установи;
- процес огляду, що забезпечує безперервний моніторинг ефективності умов навчання у сфері ІКТ.

Усі ці елементи повинні бути інтегровані в діючу в школі політику щодо гарантування безпеки дітей і не мають розглядатися як такі, що належать тільки до сфери відповідальності фахівців з ІКТ. Безглуздо вважати, що Булінг в Інтернеті або за допомогою мобільних пристроїв дуже відрізняється від Булінг в реальному житті. Проте варто не забувати, що технології можуть зробити вагомий внесок у вирішення цієї проблеми, зокрема, за рахунок встановлення:

- програм антивірусної профілактики та захисту;
- систем моніторингу для відстеження того, хто і що завантажує, коли це було завантажено і на якому комп'ютері;
- програм фільтрації та контролю контенту для зведення до мінімуму передачі неприйнятного контенту у шкільній мережі.

З проблемами, що виникають у зв'язку з новими технологіями, мають справу не всі діти та молодь; крім того, поява цих проблем залежить від віку дітей та молодь, які користуються такими технологіями. Наприкінці 2008 року американська Технічна цільова група з безпеки в Інтернеті випустила звіт з питань підвищення рівня безпеки дітей в контексті онлайнових технологій, в якому представлено змістовний огляд літературних джерел, покладених в основу опублікованого оригінального дослідження з проблематики схиляння до дій сексуального характеру в цифровому середовищі, онлайнових домагань та Булінг, а також впливу шкідливого контенту . У цьому звіті наголошується, що «викликає стурбованість той факт, що ці страхи сильно перебільшуються засобами масової інформації, тоді як реальні ризики, на які наражається молодь, далеко не такі жахливі». Більше десяти років по тому це зауваження як і раніше є слушним: батьків та освітян з усіх боків атакують зухвалі заголовки, які радше змусять дорослих обмежити доступ до онлайнових послуг, ніж спонукають їх навчати та підтримувати дітей щодо питань їх безпечного використання.

Внаслідок цього виникає небезпека, що відомі ризики залишаться без уваги, і знижується ймовірність того, що суспільство вживе заходів для усунення факторів, що призводять до них, а це, своєю чергою, може призвести до ненавмисної шкоди. Те, як злочини, вчинені стосовно дітей та молоді в Інтернеті, висвітлюються засобами масової інформації, багато в чому відображає поділ на два протилежних табори в середовищі професіоналів та науковців,

які займаються цими питаннями, де, з одного боку ті, хто побоюється перебільшення загрози, на яку наражаються діти та молодь, а з іншого – ті, хто вважає цю загрозу

недооціненою.

Так чи інакше, існує занепокоєння з приводу того, що дехто з дітей та молодь можуть бути вразливими при використанні інтернет-технологій, в зв'язку з чим на педагогах, так само як і на батьках та опікунах, покладена певна відповідальність. Віктимізація дітей та молоді в цифровому середовищі може мати такі форми:

- схиляння дітей до дій сексуального характеру, або грумінг;
- вплив шкідливих або незаконних матеріалів;
- вплив середовища, яке може провокувати небезпечну поведінку з боку декого з представників молоді;
- кіберБулінг.

Класифікація ризиків, на які наражаються діти в цифровому середовищі, наочно представлена на Малюнку 7.

Неформальне освітнє середовище

Окрім школи та домівки діти часто користуються Інтернетом та відповідними послугами в неформальному середовищі, наприклад в молодіжних клубах або церковних групах. Через взаємопов'язаність онлайнового середовища і реального світу у дітей та молодь велика ймовірність того, що дорослі, що працюють з ними в таких організаціях, впливатимуть на уявлення дітей про цифрове середовище і про навички онлайнової безпеки, навіть коли їхня діяльність безпосередньо не пов'язана з цими питаннями. Таким чином, усі, хто працюють з дітьми в неформальному середовищі, повинні мати певне уявлення про Онлайн-ризики та можливості і знати, як правильно надати дітям підтримку або де можна отримати допомогу і навчитися необхідних навичок.

Ключові поради та принципи, що містяться в Рекомендаційях для освітян, актуальні, зокрема, і для таких неформальних ситуацій, проте залежно від контексту можуть вимагатися їх корегування або додаткові міркування.

Керування пристроями, фільтрацією та комунікацією

У неформальному середовищі допоміжний персонал, волонтери та діти можуть частіше користуватися послугами за допомогою особистих пристроїв, або ж системи керування пристроями та фільтрації контенту можуть бути менш доступними чи надійними, ніж у школах. Отже, в умовах неформального середовища передусім необхідно потурбуватися про те, щоб практичні працівники та діти знали, як

убезпечити свої пристрої, і вміли ними керувати. Також, враховуючи те, що наявні можливості фільтрації можуть бути досить примітивними, педагогам та дітям не слід надто розраховувати на такий захист.

У відповідних організаціях має існувати сувора та добре продумана політика і Рекомендації щодо захисту дітей – хоча у освітян та волонтерів далеко не завжди є доступ до місцевих пристроїв або службової електронної пошти. Отже, додаткову увагу у відповідній політиці та при її реалізації варто приділяти питанням використання особистих пристроїв, а також наявності/методів контролю та моніторингу безпеки такого використання.

Аналогічним чином, за відсутності доступу до освітніх технологій, обладнання та підтримки в неформальному середовищі, як правило, частіше, ніж у школах, використовуються соціальні мережі та месенджери. Таким чином, може знадобитися додатковий розгляд аспектів організаційної політики, практики та навчання, аби визначити порядок їх використання і методи безпечного керування ними.

Навчання та підтримка

Освітяни та волонтери, які працюють у неформальному середовищі, можуть мати менше можливостей для навчання та вдосконалення навичок, а також доступу до підтримки, яка зазвичай доступна педагогам, які працюють у сфері формального навчання. Відповідно, слід розглянути питання про те, яким чином такі неформальні організації можуть шукати, організовувати та оплачувати навчання і підтримку в цій галузі.

Деякі Ключові поради, які слід брати До уваги педагогам, наведені в Таблиці 2.

10. Керівні вказівки для освітян

Слід визнати, що освітяни/освітяни не зможуть самостійно реалізувати деякі рекомендації, запропоновані в Таблиці 2 нижче, – зокрема, це стосується фільтрації та моніторингу. Передбачається, що відповідні заходи будуть вживатися на рівні школи або іншої освітньої організації.

Таблиця 2: Ключові поради, які слід брати До уваги

педагогам

Безпека та надійність пристроїв	1 Переконайтеся в тому, що всі пристрої надійно захищені та на них встановлено пароль.	учителі, були достатньо захищені (надійним паролем) і заблоковані в ті моменти, коли вони не використовуються (наприклад, якщо вчителю потрібно вийти з класу, він має заблокувати усі пристрої, які використовував, або завершити сеанс роботи/вийти з облікового запису).
	2 Встановіть антивірусне програмне забезпечення та брандмауер. Учителі є настільки ж вразливими перед кібератаками, шкідливими програмами, вірусами та зламами, як і всі інші. Важливо, щоб усі пристрої, які використовують	Встановіть на всіх пристроях брандмауер та антивірусну програму і стежте за тим, щоб вони регулярно оновлювалися.
Політика	3 В усіх школах має бути політика, що регулює, де і яким чином можуть використовувати технології різні учасники навчального процесу в межах школи, а також встановлює порядок реагування на інциденти,	пов'язані з безпекою дітей, зокрема, в цифровому середовищі. Учителям необхідно дотримуватися політики щодо використання мобільних технологій та інших електронних пристроїв. Важливо, щоб при використанні пристроїв учителі подавали приклад правильної поведінки. У школах варто встановити правила щодо того, де і коли можна користуватися мобільними пристроями.
	4 Фотографії учнів. У школах варто встановити правила щодо того, чи можна фотографувати учнів. Чи можуть співробітники школи робити знімки учнів з освітньою метою? Чи було отримано на те дозвіл від батьків/опікунів/самих учнів? Бажано, щоб у правилах було прописано, що в інтересах безпеки учнів та співробітників для цих цілей забороняється використовувати особисті пристрої.	

Рекомендації для батьків та освітян щодо захисту дитини в цифровому

середовищі

Фільтрація та моніторинг

5 Забезпечте фільтрацію та моніторинг даних, що передаються через шкільне під'єднання до Інтернету.

Учні не повинні отримувати доступу до шкідливого або неприйнятного контенту через шкільні ІТ-системи. Жодна система фільтрації не дає стовідсоткового захисту, і тому важливо підкріплювати технологічні рішення якісним навчанням та ефективним наглядом. Системи фільтрації мають щонайменше блокувати доступ до незаконного контенту, а також контенту, який вважається неприйнятним або шкідливим. Зокрема, мовиться про такі категорії шкідливого контенту:

• дискримінація
• агресивні висловлювання
• зловживання наркотиками та психоактивними речовинами
• екстремізм
• порнографія
• піратство та привласнення авторського права • матеріали, пов'язані із заподіянням собі шкоди або суїцидом
• надзвичайна жорстокість

Рекомендації для батьків та освітян щодо захисту дитини в цифровому

середовищі

Онлайн-репутація/ цифровий слід

Як забезпечити безпеку
професійної комунікації

	батьками та іншими зацікавленими сторонами.	стосується їх діяльності в цифровому середовищі. Для будь-яких контактів між співробітниками школи та учнями або батьками завжди необхідно використовувати шкільну електронну пошту. Шкільна комунікаційна політика або кодекс ділової етики можуть передбачати заборону на контакти сам на сам та будь-які контакти, не пов'язані з освітньою діяльністю, або ж контакти на платформах, що не мають стосунку до школи. Бажано, щоб для спілкування з учнями або батьками/опікунами не використовувалися особисті пристрої. Варто уникати цифрового спілкування сам на сам. На випадок проведення відеоконференцій або занять у віддаленому режимі, школи мають установлювати чіткі приписи як для співробітників, так і для учнів (наприклад, що бажано підготувати місце для віддаленого заняття/сеансу зв'язку, що не варто проводити його в спальні та потрібно в принципі подбати про тих, хто перебуває поруч – чи то вдома або в класі).
Поведінка учнів, їх вразливість в цифровому середовищі та наслідки для їх безпеки і добробуту 6 Варто усвідомлювати значення цифрового сліду та онлайнової репутації.	8 Варто розуміти, чим Інтернет може бути для учнів небезпечний і чим корисний. Учителям необхідно розуміти, що їхні слова та дії в Інтернеті можуть вплинути на їх власну репутацію, а також репутацію школи/ навчального закладу. Учителям належить пам'ятати про власний професійний статус та поводитися в цифровому середовищі відповідно. Потрібно також розповісти дітям про важливість онлайнової репутації і про те, як правильно її формувати.	Учителям необхідно знати, як діти і молодь проводять час в Інтернеті. Яким ризикам вони при цьому піддаються та яку користь можуть отримати.
7 Слід визнати важливість професійної онлайнової комунікації з учнями,	Між приватним та професійним життям учителів завжди має бути чітка межа, і це, зокрема,	

11. Висновок

Інформаційно-комунікаційні технології (ІКТ) змінили стиль життя сучасної людини. Вони дають нам змогу спілкуватися в режимі реального часу й отримувати транскордонний та практично необмежений доступ до інформації і широкого спектру інноваційних послуг. Водночас ці технології створюють нові можливості для експлуатації та зловживань. За відсутності належних заходів захисту діти та молодь – які є одними з найбільш активних користувачів Інтернету – наражаються на ризик нав'язливого схиляння до дій сексуального характеру і домагань, а також небажаного впливу жорстокого контенту, контенту сексуального характеру та інших травмуючих матеріалів.

Без відповідних механізмів, що створюють безпечну кіберзлочинність, діти та молодь залишатимуться вразливими. Незважаючи на зростаючий рівень обізнаності про ризики, пов'язані з небезпечним використанням ІКТ, в цій області ще належить виконати значну роботу. Тому надважливо, щоб батьки та освітяни обговорювали і вирішували разом з дітьми та молодими особами, що є для них прийнятним та безпечним при використанні таких технологій, а також у чому полягає відповідальна поведінка при використанні ІКТ.

Діючи спільно, батьки, освітяни, діти та молодь зможуть користуватися перевагами ІКТ, зводячи до мінімуму можливі небезпеки для дітей та молоді.

Термінологія

Наведені далі визначення ґрунтуються в основному на наявній термінології, розробленій у рамках Конвенції про права дитини 1989 року, а також складеній міжвідомчою робочою групою із сексуальної експлуатації дітей в межах Рекомендацій із термінології в сфері захисту дітей від сексуальної експлуатації та сексуальних зловживань (Люксембурзькі Рекомендації, 2016 р.), Конвенції Ради Європи про захист дітей від експлуатації та наруг сексуального характеру 2012 року, а також доповіді Global Kids Online 2019 року.

Підліток

Підлітки – це особи віком від 10 до 19 років. Важливо зазначити, що в міжнародному праві відсутній обов'язковий термін підлітки, та особи молодше 18 років розглядаються як діти, тоді як 19-річні особи вважаються дорослими, крім випадків, коли повноліття настає раніше, відповідно до національного законодавства.

Штучний інтелект

У найширшому сенсі цей термін розпливчасто визначає системи, що належать до сфери суто наукової фантастики (так званий «сильний» ШІ, що володіє формою самосвідомості), і системи, вже чинні та здатні виконувати дуже складні завдання (розпізнавання голосу або осіб, водіння автомобіля: ці системи описуються як «слабкий» або «середній» ШІ).

Системи ШІ

Система ШІ – це система на основі машин, яка в рамках встановленого певною людиною набору цілей може складати прогнози, виносити рекомендації або приймати рішення, що впливають на реальне або віртуальне середовище, і призначена для функціонування з різним рівнем автономності.

Alexa

Amazon Alexa, відома як просто Alexa, представляє систему ШІ – віртуального помічника, розроблену Amazon. Вона підтримує такі функції, як голосова взаємодія, відтворення музики, складання списку справ, установлення будильнику, відтворення підкастів та аудіокниг, повідомлення прогнозу погоди, даних про ситуацію на дорогах, спортивні події та іншої інформації в режимі реального часу, зокрема, новин. Alexa також може контролювати декілька «розумних» пристроїв, функціонуючи як система побутової автоматизації. Користувачі можуть розширювати функціонал Alexa шляхом встановлення «вмінь» (додаткових функціональних можливостей, що розробляються сторонніми постачальниками, які в інших випадках зазвичай іменуються додатками, наприклад програми відстеження погоди та аудіофункцій).

Найкращі інтереси дитини

Описує усі елементи, необхідні для прийняття рішення в конкретній ситуації для конкретної дитини або групи детей.

Дитина

Відповідно до статті 1 Конвенції про права дитини дитиною є будь-яка особа молодше 18 років, якщо національним законодавством не передбачено більш ранній вік повноліття.

Сексуальна експлуатація та сексуальні зловживання стосовно дітей (CSEA)

Це поняття описує усі форми сексуальної експлуатації та сексуальних зловживань (Конвенція про права дитини 1989 р., стаття 34), наприклад: «a) схиляння або примус дитини до будь-якої незаконної сексуальної діяльності; b) використання з метою експлуатації дітей в проституції або в іншій незаконній сексуальній практиці; c) використання з метою експлуатації дітей в порнографії та порнографічних матеріалах», а також «статевий контакт, як правило, із застосуванням сили стосовно особи без її згоди». Сексуальна експлуатація та сексуальні зловживання стосовно дітей дедалі частіше вчиняються з використанням Інтернету або пов'язані з онлайновим средовищем.

Матеріали, пов'язані з сексуальною експлуатацією та сексуальними зловживаннями стосовно дітей (CSAM)

Стрімкий розвиток ІКТ призвів до появи нових форм сексуальної експлуатації та сексуальних зловживань стосовно дітей в цифровому середовищі, які можуть відбуватися у віртуальній формі і не обов'язково передбачають особисту зустріч з дитиною. Хоча в багатьох юридичних системах зображення та відеоматеріали, пов'язані із сексуальними зловживаннями стосовно дітей, як і раніше розглядаються як «дитяча порнографія» або «непристойні зображення дітей», в цих Рекомендаційях вони іменуватимуться сукупно матеріалами, пов'язаними із сексуальними зловживаннями стосовно дітей (тут і далі CSAM). Це відповідає Керівним настановам Комісії з широкосмугового зв'язку та моделі реагування на національному рівні, розробленої Глобальним альянсом WePROTECT. Цей термін точніше описує цей контент. Порнографія передбачає законне комерційне виробництво; в Люксембурзьких Рекомендаційях надається наступне визначення використанню терміна «Дитяча порнографія»: він «може (довільно або мимоволі) сприяти полегшенню ступеня тяжкості, зменшенню значущості або навіть легітимізації того, що по суті є сексуальними зловживаннями стосовно дітей та/або їх сексуальною експлуатацією [...] Термін «Дитяча порнографія» створює небезпеку його тлумачення таким чином, ніби дії відбуваються за згодою дитини і представляють законний матеріал сексуального характеру».

Термін CSAM стосується матеріалу, що втілює у собі діяння, які є сексуальними зловживаннями стосовно дітей та/або їх сексуальною експлуатацією. Це містить, зокрема, запис матеріалів, пов'язаних із сексуальними зловживаннями щодо дітей з боку дорослих; зображення дітей, залучених до відвертих сексуальних дій, статевих органів дітей, коли зображення створюються або використовуються насамперед з метою сексуального характеру.

Діти та молодь (молодь)

Означає, що це особи до 18 років, при цьому до дітей, які в цих Рекомендаційях також іменуються дітьми молодшого віку, належать усі особи до 15 років, а молодь (молодь) утворюють вікову групу від 15 до 18 років.

Іграшки, що мають доступ до Інтернету

Іграшки з доступом до Інтернету під'єднуються до нього за допомогою таких технологій, як Wi-Fi та Bluetooth, і зазвичай працюють у поєднанні зі спеціальними додатками, забезпечуючи дітям можливість інтерактивної гри. Згідно з проведеним компанією Juniper Research дослідженням, в 2015 році обсяг ринку іграшок, що мають доступ до Інтернету, сягнув 2,8 млрд дол. США і, згідно з прогнозами, до 2020 року зросте до 11 млрд дол. США. Ці іграшки збирають та зберігають персональну інформацію про дітей, зокрема: імена, дані геолокації, адреси, світлини, аудіо- та відеозаписи .

Кібербулінг, що також іменується булінгом в цифровому середовищі

КіберБулінг означає навмисну агресивну дію, що неодноразово вчиняється групою осіб або окремою особою за допомогою цифрових технологій та спрямована проти жертви, якій важко захистити себе . Зазвичай воно передбачає «використання цифрових технологій та Інтернету для розміщення чутливої інформації про будь-кого, навмисне поширення відомостей особистого характеру, небажаних фотографій або відео, надсилання повідомлень з погрозами або образами (електронною поштою, у форматі миттєвого обміну повідомленнями, в чатах та текстових повідомленнях), поширення пліток і неправдивої інформації про жертву або навмисне вилучення її з онлайнового спілкування» . Воно може відбуватися безпосередньо (в чатах або текстових повідомленнях), в рамках спільноти з обмеженим доступом (розсилання постів та дратівливих повідомлень за списком електронних адрес) або ж в громадському доступі (наприклад, створення сайтів спеціально для знущання над жертвами).

Кіберненависть, дискримінація та насильницький екстремізм

«Кіберненависть, дискримінація та насильницький екстремізм представляють виразну форму кібернасильства, спрямованого проти колективної ідентичності, а не проти окремих людей [...] і нерідко стосується раси, сексуальної орієнтації, релігії, національності або імміграційного статусу, статевої/гендерної приналежності та політичного аспекту» .

Цифрове громадянство

Цифрове громадянство означає корисну, відповідальну та компетентну діяльність у цифровому середовищі із застосуванням навичок ефективної комунікації та творчого підходу для втілення форм соціальної участі, що ґрунтуються на повазі до прав людини та людської гідності, шляхом відповідального використання технологій .

Цифрова грамотність

Цифрова грамотність означає наявність навичок, необхідних для життя, навчання та роботи у суспільстві, де комунікації та доступ до інформації дедалі більше забезпечуються через використання цифрових технологій, як-от інтернет-платформи, соціальні мережі та мобільні пристрої . Вона містить безпосередньо комунікації, технічні навички та критичне мислення.

Стійкість до впливу цифрового середовища

Цей термін описує здатність дитини емоційно впоратися зі шкідливими факторами в цифровому середовищі. Стійкість до впливу цифрового середовища передбачає

наявність емоційних ресурсів, необхідних для того, щоб розуміти, коли дитина піддається ризику в Інтернеті, знати, як звертатися за допомогою, здобувати практичні уроки та відновлюватися після невдалого досвіду .

Освітяни

Педагог – це особа, яка провадить систематичну роботу з удосконалення знань іншої особи з цього предмета. Роль педагога передбачає як роботу в школі, так і більш неформальну педагогічну діяльність, наприклад таку, коли для надання інформації про безпеку в цифровому середовищі або проведення навчальних курсів на базі громади чи школи для того, щоб діти та молодь були в безпеці в цифровому середовищі, використовуються платформи сайтів соціальних мереж.

Робота педагога може варіюватися залежно від умов його діяльності та вікової групи дітей та молодь (або дорослих), на навчання яких спрямовані його зусилля.

Керівники

Відноситься до всіх осіб, які обіймають посади в шкільному керівництві/керівних структурах.

Грумінг в цифровому середовищі

Грумінг/грумінг в цифровому середовищі, згідно з Люксембурзькими керівними настановами, означає процес налагодження/побудови взаємин з дитиною особисто або за допомогою Інтернету чи інших цифрових технологій, з метою домогтися сексуальних зв'язків з цією особою в цифровому середовищі або в реальному житті, схиливши дитину вступити в сексуальний зв'язок . Процес, спрямований на заманювання дітей у дії чи бесіди сексуального характеру, як з їх відома, так і без нього, або процес, що передбачає спілкування та встановлення взаємин між порушником і дитиною, з метою зробити останню вразливішою перед сексуальними зловживаннями. Термін «грумінг» не передбачено у міжнародному праві; в деяких юридичних системах, зокрема, в Канаді, використовується термін «заманювання».

Інформаційно-комунікаційні технології (ІКТ)

Інформаційно-комунікаційні технології означають усі інформаційні технології, де основний акцент зроблено на комунікацію. До них належать усі послуги та пристрої, які використовують під'єднання до Інтернету, як-от комп'ютери, ноутбуки, планшети, смартфони, ігрові приставки, телевізори та годинники тощо. Сюди ж належать послуги, наприклад радіо, широкосмуговий зв'язок, мережеве обладнання та супутникові системи.

Онлайн-ігри

Термін «онлайн-ігри» означає участь у будь-яких платних цифрових іграх із одним або багатьма гравцями з використанням будь-якого пристрою, що має доступ до Інтернету, як-от спеціальні приставки, стаціонарні комп'ютери, ноутбуки, планшети та мобільні телефони.

«Екосистема онлайнових ігор», згідно із визначенням, містить спостереження за процесом відеоігор інших людей з використанням платформ електронного спорту,

потокового відео або обміну відеоматеріалами, які зазвичай передбачають для глядачів можливість залишати коментарі або спілкуватися з гравцями та іншими представниками аудиторії .

Інструменти батьківського контролю

Програмне забезпечення, яке дозволяє користувачам (зазвичай батькам) контролювати деякі функції комп'ютера чи іншого пристрою, здатного підтримувати зв'язок з Інтернетом. Зазвичай такі програми дозволяють обмежувати інтернет-доступ до певних видів або категорій вебсайтів або онлайнових послуг. Деякі також мають налаштування часу, тобто пристрій можна налаштувати так, щоб він під'єднувався до Інтернету лише у певні проміжки часу. Досконаліші версії дозволяють вести запис усіх текстових повідомлень, що надсилаються або отримуються через пристрій. Зазвичай такі програми захищені паролями .

Батьки та опікуни

На деяких сайтах в Інтернеті є узагальнене згадування про батьків (як, наприклад, на «батьківській сторінці» або згадування «батьківського контролю»). Тому було б доцільно визначити тих людей, які будуть найліпше надавати дітям можливості максимального використання Інтернету, з безпечним та відповідальним використанням інтернет-сайтів дітьми та молодими особами, а також надавати їм свою згоду на отримання доступу до конкретних інтернет-сайтів. У цьому документі термін «батьки» означає будь-яку особу (окрім педагога), яка несе юридичну відповідальність за дитину. Ступінь відповідальності батьків, а також юридичні батьківські права є різними в різних країнах.

Персональна інформація

Термін означає індивідуально визначену інформацію про особу, яка збирається в онлайн-режимі. До неї належать повне ім'я, контактна інформація, зокрема, домашня адреса та адреса електронної пошти, номери телефонів, відбитки пальців або дані для розпізнавання осіб, номери страховок чи будь-які інші відомості, що дозволяють вступити у фізичний або віртуальний контакт чи визначити місце перебування особи. У цьому контексті персональна інформація також означає будь-яку інформацію про дитину та її оточення, яка збирається в онлайн-режимі постачальниками послуг Інтернету, включаючи іграшки з доступом до Інтернету й інтернету речей, а також будь-які інші технології, що використовують з'єднання з Інтернетом.

Конфіденційність

Конфіденційність нерідко оцінюється з точки зору поширення персональної інформації в цифровому середовищі, наявності відкритого профілю в соціальних мережах, обміну інформацією з незнайомими людьми в Інтернеті, використання налаштувань конфіденційності, надання паролів друзям, усвідомленням важливості збереження конфіденційності .

Секстинг

Секстинг зазвичай визначається як надсилання, отримання власноруч створеного сексуального контенту, зокрема, зображення, повідомлення або відео, або обмін ними за допомогою мобільних телефонів та/або інтернету . У більшості країн створення,

поширення та зберігання зображень дітей сексуального характеру є незаконним. У разі

поширення зображень дітей сексуального характеру дорослі не повинні переглядати їх. Демонстрація зображень сексуального характеру дитині дорослим завжди є злочинним діянням; поширення таких зображень між дітьми може завдати шкоди; слід повідомляти про подібні інциденти; може знадобитися допомога для усунення поширених зображень.

Секс-вимагання, або сексуальне вимагання стосовно дітей

Сексуальне вимагання означає «шантаж особи за допомогою власноруч створених зображень цієї особи з метою вимагання у неї сексуальних послуг, грошей або інших благ під загрозою поширення матеріалу без згоди особи, яка в ньому фігурує (наприклад, за допомогою розміщення зображень в соціальних мережах)» .

Інтернет речей

Інтернет речей є наступним кроком у напрямку цифровізації суспільства та економіки, коли взаємозв’язок людей та об’єктів здійснюється через комунікаційні мережі, а також передаються відомості про їх стан та навколишнє оточення .

URL

Скорочення з англійської «uniform resource locator», тобто «універсальний покажчик ресурсу» – адреса сторінки в Інтернеті .

Віртуальна реальність

Віртуальна реальність – це створення за допомогою комп’ютерних технологій ефекту тривимірного світу, в якому об’єкти сприймаються як реально існуючі в просторі .

WI-FI

Wi-Fi (з англ. «Wireless Fidelity» – «висока точність бездротового передавання») – набір технічних стандартів, що забезпечують можливість передавання даних бездротовими мережами .