Міжнародний союз електрозв'язку

Захист дітей у цифровому середовищі: рекомендації для індустрій

2020

Захист дітей у цифровому середовищі: рекомендації для індустрій

МІНЗМІН

Міністерство
цифрової трансформації
України

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.

Передмова

Стрімкий розвиток цифрових технологій спричинив появу безпрецедентних можливостей для дітей і молоді стосовно спілкування, встановлення зв'язків, навчання, обміну інформацією та доступу до неї, а також висловлення своїх поглядів і думок з питань, що зачіпають їхні життя та спільноти. Але водночас більш широкий і легкий доступ до онлайнових послуг становить більшу загрозу для безпеки дітей як в цифровому середовищі, так і в реальному житті. Сучасні діти стикаються з безліччю серйозних ризиків - від питань недоторканності приватного життя, насильства між однолітками і жорстокого та/або невідповідного вікового контенту до інтернет-шахрайства та злочинів проти дітей, як-от грумінг в цифровому середовищі та сексуальні зловживання і сексуальна експлуатація. Кількість загроз зростає, а правопорушники все більше діють одночасно, перебуваючи до того ж у різних країнах, що ускладнює їх відстеження і притягнення до відповідальності.

Крім цього, Глобальна пандемія COVID-19 призвела до збільшення числа дітей, які вперше почали користуватися Інтернетом для продовження своєї освіти та підтримки соціальної взаємодії. Обмеження, обумовлені вірусом, означають не тільки те, що багато дітей молодшого віку починають спілкуватися в мережі набагато раніше, ніж, можливо, планували їх батьки, а й те, що з огляду на необхідність перегляду своїх робочих зобов'язань багато батьків виявилися не в змозі контролювати своїх дітей, піддаючи їх ризику доступу до неприйнятного контенту або перетворення на мішень для злочинців, які створюють матеріали, пов'язані із сексуальними зловживаннями щодо дітей (CSAM).

Злочинці отримують вигоду від технологічного прогресу, як-от застосунків та ігор, що забезпечують взаємодію, швидкого обміну файлами, потокового мовлення, криптовалюти, тіньового інтернету і програм сталого шифрування. Водночас вони також отримують вигоду від зазвичай нескоординованих і нерішучих дій з ефективного усунення проблеми зі сторони технологічного сектору.

Частково проблему можна вирішити завдяки новим технологіям, наприклад, з використанням бази даних Інтерполу стосовно сексуальних зловживань щодо дітей, яка обслуговується штучним інтелектом і де застосовується програмне забезпечення для порівняння зображень і відеоматеріалів, що дозволяє швидко встановити зв'язки між жертвами, насильниками та їхнім місцеперебуванням. Однак лише технологій недостатньо для вирішення проблеми.

Для зменшення ризиків, пов'язаних із цифровою революцією, при одночасному забезпеченні можливостей для використання її переваг дедалі більшою кількістю молодих осіб, як ніколи раніше важливою є спільна і скоординована реакція різних заінтересованих сторін. Уряди, громадянське суспільство, місцеві спільноти, міжнародні організації та заінтересовані сторони індустрії повинні об'єднати свої зусилля заради спільної мети.

Визнаючи цей факт, у 2018 році Держави - Члени МСЕ звернулися з проханням підготувати розгорнуте оновлення наших Керівних настанов щодо захисту дитини в цифровому середовищі. Ці нові Рекомендації МСЕ були заново усвідомлені, сформульовані й перебудовані з урахуванням значних змін, що відбулися в цифровому середовищі, в якому живе сьогоднішнє покоління дітей. Окрім додання нових розробок у сфері цифрових технологій та платформ, у цьому новому виданні була усунута значна прогалина: в ньому приділяється увага становищу дітей-інвалідів, для яких цифрове середовище відкриває особливо важливі можливості щодо забезпечення повноцінної участі в соціальному житті.

Індустрія електронних технологій відіграє вирішальну та ініціативну роль у формуванні основ більш безпечного і надійного використання інтернет-послуг та інших технологій для сучасних дітей і майбутніх поколінь.

Будь-яка підприємницька діяльність повинна активніше орієнтуватися на інтереси дітей з особливим акцентом на захист персональних даних юних користувачів, збереження їх права на свободу висловлення своєї думки, боротьбу зі зростанням обсягів CSAM і забезпечення систем ефективної протидії порушенню прав дітей та реагування на факти вчинення таких порушень.

У тих країнах, де норми місцевого законодавства поки що відстають від вимог міжнародного права, всі підприємства мають можливості й водночас обов'язки стосовно узгодження своїх власних методів роботи з високими стандартами і передовим досвідом.

Ми сподіваємося, що для індустрії ці Рекомендації стануть надійною основою для розробки правил ведення бізнесу та інноваційних рішень. 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 я рада представити новий талісман Захист дітей у цифровому середовищі - Санго - доброзичливого, непосидючого та відважного персонажа, створеного групою дітей у межах нової міжнародної програми МСЕ з охоплення молоді.

В епоху, коли все більше молодих осіб під'єднуються до інтернету, Рекомендації МСЕ щодо захисту дитини набувають особливої ваги. Індустрія, уряди, батьки і освітяни, а також самі діти - всі повинні відіграти свою важливу роль. Я, як завжди, дуже вдячна вам за підтримку і нетерпляче чекаю на продовження нашої тісної співпраці у вирішенні цих нагальних питань.

Дорін Богдан-Мартін

Директор

Бюро розвитку електрозв'язку, МСЕ

Таблиці

1. Огляд

Мета цього документу - задати напрямок для заінтересованих сторін індустрії ІКТ стосовно
створення їх власних ресурсів щодо захисту дітей в цифровому середовищі (Захист дітей у цифровому середовищі). Ці
Рекомендації щодо захисту дитини в цифровому середовищі призначені для індустрії й покликані скласти корисну, гнучку і зручну для застосування основу як для розробки концепцій різних компаній, так і для формування їхньої відповідальності у сфері захисту користувачів. Вони також спрямовані на формування засад більш безпечного і надійного використання інтернет-послуг та інших технологій для сучасних дітей і майбутніх поколінь.

Як набір інструментів, ці Рекомендації також мають на меті сприяти успішності бізнесу, допомагаючи великим і дрібним операторам і заінтересованим сторонам у створенні та підтримці привабливих і стійких бізнес-моделей, одночасно усвідомлюючи правову і моральну відповідальність перед дітьми та суспільством.

Реагуючи на значний прогрес у індустрії технологій та їх конвергенцію, МСЕ, ЮНІСЕФ та партнери щодо захисту дитини в цифровому середовищі розробили й оновили Керівні настанови для широкого кола компаній, що розробляють, надають або використовують технології електрозв'язку під час поширення своєї продукції та послуг.

Нові Рекомендації для індустрії щодо захисту дитини в цифровому середовищі є результатом консультацій з учасниками Ініціативи Захист дітей у цифровому середовищі, а також більш широкого
консультаційного процесу за участю громадянського суспільства, бізнесу, індустрії освіти,
державних органів, засобів масової інформації, міжнародних організацій та молоді.

Мета цього документу:

- визначити загальний еталон і Рекомендації для галузей, пов'язаних з ІКТ та інтернетом, а також для всіх заінтересованих сторін;
- надати компаніям Рекомендації щодо виявлення, запобігання і пом'якшення будь-якого негативного впливу їхньої продукції та послуг на права дітей;
- надати компаніям Рекомендації щодо виявлення способів сприяння реалізації прав дитини та формування відповідального цифрового громадянства серед дітей;
- запропонувати загальні принципи для формування засад національних або регіональних зобов'язань за всіма взаємопов'язаними галузями, водночас усвідомлюючи, що різні типи бізнесу використовують різні моделі їх виконання.

Сфера застосування

Захист дитини в цифровому середовищі - це комплексне завдання, що охоплює безліч управлінських, політичних, оперативних, технічних і правових аспектів. Ці Рекомендації є спробою проаналізувати, організувати і визначити пріоритети багатьох з-поміж таких аспектів на підставі визнаних моделей, схем та інших матеріалів.

Рекомендації спрямовані на захист дітей в усіх сферах і від усіх ризиків цифрового світу і, як такі, виділяють передовий досвід галузевих заінтересованих сторін, який можна враховувати в процесі проєктування, розробки та керування політиками захист дітей у цифровому середовищі на рівні компаній. Вони скеровують учасників індустрії не тільки в тому, як управляти і стримувати незаконну онлайнову діяльність, якій вони зобов'язані протидіяти (як-от CSAM в інтернеті) за допомогою своїх послуг, але і в тому, як вирішувати інші питання, які можуть не вважатися злочинами в різних юрисдикціях. До них належать насильство між однолітками, кібербулінг і домагання в інтернеті, а також питання, пов'язані з конфіденційністю або загальним добробутом, шахрайством або іншими загрозами, які можуть лише нашкодити дітям у певному контексті.

У зв'язку з цим до Керівних настанов унесено рекомендації щодо передових практичних підходів до усунення ризиків, з якими стикаються діти у цифровому світі, і того, як діяти з метою формування безпечного середовища для дітей в інтернеті. В них містяться поради стосовно методів роботи індустрії, що сприяє забезпеченню безпеки дітей, які користуються ІКТ, інтернетом і всіма супутніми технологіями або пристроями, що мають вихід в інтернет, зокрема бездротові телефони, ігрові консолі, іграшки, що мають вихід в інтернет, годинники, інтернет речей та системи, що керуються Штучним Інтелектом. Таким чином, вони містять огляд головних аспектів і завдань, пов'язаних із захистом дитини в цифровому середовищі та пропозиції щодо дій, які бізнес і заінтересовані особи можуть здійснити для розроблення місцевих і внутрішніх політик Захист дітей у цифровому середовищі. Ці Рекомендації не охоплюють такі моменти, як фактична розробка процесу або конкретний текст політик Захист дітей у цифровому середовищі для індустрії.

Структура

Розділ 1 - Огляд. У цьому розділі визначено мету, сферу застосування та цільову аудиторію цих Керівних настанов.

Розділ 2 - Передмова до теми захисту дитини в цифровому середовищі. У цьому розділі представлений огляд теми захисту дитини в цифровому середовищі та деяка базова інформація, зокрема особлива ситуація, в якій перебувають діти-інваліди. Окрім того, тут наводяться приклади чинних міжнародних та національних моделей щодо забезпечення безпеки дітей в цифровому середовищі як ймовірної сфери втручання для заінтересованих сторін у індустрії.

Розділ 3 - Основні царини у сфері захисту та сприяння реалізації прав дітей. Цей розділ присвячений опису п'яти основних варіантів дій компаній в напрямку забезпечення захисту дітей та позитивного застосування ІКТ.

Розділ 4 - Загальні Рекомендації. В цьому розділі містяться рекомендації для всіх заінтересованих сторін в індустрії щодо забезпечення безпеки дітей під час використання ІКТ і щодо сприяння позитивному застосуванню ІКТ, зокрема відповідальне цифрове громадянство серед дітей.

Розділ 5 - Контрольні переліки залежно від виконуваних функцій. Цей розділ містить окремі рекомендації для заінтересованих сторін стосовно конкретних дій щодо підтримки прав дітей з урахуванням таких функцій:

- функція А: надання послуг зі встановлення з'єднань, зберігання і публікування даних;
- функція В: пропозиція відібраного цифрового контенту;

- функція C: публікування створюваного користувачами контенту і встановлення зв'язків між користувачами;
- функція D: системи на основі штучного інтелекту.

Цільова аудиторія

В контексті розроблених ООН Керівних принципів підприємницької діяльності в аспекті прав людини1 документ "Права дітей та принципи підприємництва" закликає компанії виконувати свої зобов'язання стосовно поваги до прав дітей, уникаючи будь-яких негативних впливів через їх діяльність, продукцію чи послуги. Принципи встановлюють відмінність між "повагою" (мінімальною вимогою до компаній щодо недопущення спричинення шкоди дітям) і "підтримкою" (яка виражається, наприклад, у проведенні добровільних акцій, спрямованих на забезпечення реалізації прав дитини). Компанії повинні забезпечувати права дітей як на захист в цифровому середовищі, так і на доступ до інформації та свободу вираження, сприяючи водночас позитивному застосуванню ІКТ дітьми.

Традиційне розмежування між різними сферами галузей електрозв'язку та рухомого зв'язку, а також між інтернет-компаніями і радіомовними організаціями, стрімко руйнується або стає несуттєвим. Конвергенція призводить до об'єднання цих раніше чітко розмежованих цифрових потоків в одну течію, що охоплює мільярди людей у всіх куточках світу. Кооперація і партнерство є ключами до формування засад більш безпечного і надійного використання інтернету і супутніх технологій. Державні органи, приватний сектор, директивні органи, індустрія освіти, громадянське суспільство, батьки та опікуни - всі вони відіграють гранично важливу роль у досягненні поставленої мети. Індустрія може діяти в п'яти основних царинах, опис яких наводиться далі в розділі 3.

2. Що таке захист дитини в цифровому середовищі?

За останні 10 років характер використання і роль інтернету в житті людей значно змінилися. З огляду на переважання смартфонів і планшетів, доступність Wi-Fi і технологій 4G, а також розвиток платформ соціальних мереж і застосунків, все більше людей отримують доступ до інтернету з різних причин, кількість яких постійно зростає.

У 2019 році більш ніж половина всього населення Землі користувалася інтернетом. Найбільшу частину користувачів інтернету становлять особи віком до 44 років, водночас обсяги використання у вікових групах 16-24 роки і 35-44 роки однакові. На глобальному рівні кожний третій користувач інтернету є дитиною (0-18 років), і за оцінками ЮНІСЕФ 71 відсоток молоді вже перебуває в цифровому середовищі . Повсюдне поширення точок доступу до інтернету, рухливі технології та щораз більше розмаїття пристроїв на базі інтернет-технологій (у поєднанні з величезними ресурсами кіберпростору) створюють безпрецедентні можливості для навчання, обміну інформацією та спілкування.

До переваг використання ІКТ належать більш широкий доступ до інформації про соціальні служби, освітні ресурси та здоров'я. Оскільки діти, молодь і сім'ї користуються інтернетом і мобільними телефонами для пошуку інформації та допомоги, а також для повідомлення про випадки зловживань, такі технології здатні допомогти захистити дітей і молодь від насильства і експлуатації. Постачальники послуг захисту дітей також використовують ІКТ, серед іншого, для збирання і передавання даних, тим самим спрощуючи реєстрацію

народження, управління справами, відстеження сімей, збір даних і складання мап насильства.

Окрім того, інтернет забезпечив більш вільний доступ до інформації в усіх куточках земної кулі, надаючи дітям і молоді можливість вивчити практично будь-який предмет, що їх цікавить, отримати доступ до всесвітніх засобів масової інформації, відстежити пропоновані вакансії та осягти ідеї для майбутнього. Застосування ІКТ дає дітям і молоді можливість заявити про свої права і висловити свою думку, а також пропонує безліч способів встановлення контактів і спілкування з їхніми сім'ями та друзями. ІКТ також є першорядними засобами культурного обміну і джерелом розваг.

Незважаючи на серйозні переваги інтернету, користуючись ІКТ, діти і молодь також стикаються з безліччю ризиків. Вони можуть піддаватися впливу невідповідного для них вікового контенту або неприйнятних контактів, зокрема можливих винуватців сексуальних зловживань. Вони можуть страждати від порушення репутації внаслідок публікації персональної інформації інтимного характеру або в інтернеті, або через "секстинг", не вповні усвідомивши всі наслідки подібних контактів для самих себе та інших осіб в їх довгостроковій "цифровий географії". Вони також стикаються з ризиком порушення конфіденційності, пов'язаного зі збиранням та використанням даних, а також збиранням інформації про місцеперебування.

Конвенція про права дитини, яка є найбільш широко ратифікованим міжнародним документом з прав людини , дає визначення цивільних, політичних, економічних, соціальних і культурних прав дітей. У ній зафіксовано, що всі діти мають право на освіту; дозвілля, участь в іграх і культурному житті; отримання відповідної інформації; свободу думки і вираження; особисте життя і висловлення своїх поглядів стосовно питань, які їх турбують, відповідно до їхніх дедалі більших здібностей. Крім того, Конвенція захищає дітей від усіх форм насильства, експлуатації, зловживання і дискримінації будь-якого роду і гарантує вирішення всіх питань, що їх стосуються, з урахуванням найкращих інтересів дитини. Батьки, опікуни, освітяни та представники спільнот, зокрема лідери громад та різні громадські діячі, несуть відповідальність за виховання та підтримку дітей та молоді протягом їх дорослішання. Державні органи відіграють важливу роль у забезпеченні того, щоб усі заінтересовані сторони виконували свої завдання. Стосовно захисту прав дітей в цифровому середовищі бізнес має об'єднувати зусилля в пошуках точного балансу між правом дитини на захист та правами на доступ до інформації та свободу вираження поглядів. Компаніям слід поставити на одне з перших місць заходи щодо захисту дітей в цифровому середовищі, які мають бути цілеспрямованими та без надмірних обмежень як для дитини, так і для інших користувачів. Крім того, дедалі більше міцніє загальна думка про те, що сприяння цифровому громадянству серед дітей і молоді, а також створення продуктів і платформ, які сприяють позитивному застосуванню ІКТ дітьми, повинні стати пріоритетом для приватного сектору.

Притім, що інтернет-технології створюють безліч можливостей для дітей і молодих осіб в аспекті спілкування, вивчення нових навичок, творчості й внеску в поліпшення суспільства для всіх, вони також можуть являти нові ризики для безпеки дітей та молоді. Вони можуть піддавати дітей та молодь потенційним ризикам і завдавати шкоди в таких сферах, як-от конфіденційність, незаконний контент, домагання, кібербулінг, неправомірне використання персональних даних або грумінг в сексуальних цілях, ба навіть сексуальні зловживання щодо дітей та їх сексуальна експлуатація. Окрім того, вони можуть завдавати шкоди репутації, зокрема "порнопомста" у зв'язку з публікацією закритої персональної інформації

або в інтернеті, або із застосуванням "секстингу" як способу, через який користувачі можуть розсилати сексуально відверті повідомлення, фотографії або зображення між мобільними телефонами. Також є ризики, пов'язані з конфіденційністю під час використання інтернету. Діти через свій вік та недостатню зрілість часто не здатні повністю зрозуміти ризики, з якими пов'язаний онлайновий світ, і ймовірні негативні наслідки їхньої неприйнятної поведінки для інших та них самих.

Незважаючи на всі переваги, є також і зворотна сторона використання новітніх і більш просунутих технологій. Розробки у сфері Штучного Інтелекту і машинного навчання, віртуальної та доповненої реальності, великих даних, робототехніки та інтернету речей ще більше перетворять взаємодію дітей та молоді із засобами передавання. Притому, що такі технології розробляються, головним чином, з метою розширення обсягу послуг, що надаються, і збільшення зручності (за допомогою, наприклад, голосових асистентів, доступності й нових форм цифрового занурення), деякі з них можуть мати ненавмисний вплив і навіть неправомірно використовуватися особами, які вчиняють сексуальні злочини проти дітей, з метою задоволення їх потреб. Створення безпечного і надійного онлайнової середовища для дітей та молоді вимагає ефективної участі державних органів, приватного сектору та всіх заінтересованих осіб. Крім того, однією з першорядних цілей має бути розвиток цифрових навичок і грамотності у батьків та викладачів, і для її досягнення індустрія може відігравати життєво важливу і стійку роль.

Деякі діти можуть добре розуміти онлайн-ризики і знати, як реагувати на них. Проте цього не можна сказати про всіх дітей повсюдно, особливо серед уразливих груп. Згідно із завданням 16.2, поставленим у межах Цілей ООН у сфері сталого розвитку, яке спрямоване на усунення зловживань, експлуатації, торгівлі людьми та всіх форм насильства і катувань щодо дітей, захист дітей в цифровому середовищі має величезне значення.

Починаючи з 2009 року, організована МСЕ Ініціатива захист дітей у цифровому середовищі для безлічі заінтересованих сторін на міжнародному рівні служила меті підвищення поінформованості про безпеку дітей в цифровому середовищі та реагування на ці ризики. Вона спрямована на об'єднання зусиль партнерів з усіх секторів світової спільноти з метою забезпечення безпечного та надійного онлайнового досвіду для дітей будь-де у світі. У частині цієї Ініціативи в 2009 році МСЕ оприлюднила низку Керівних настанов Захист дітей у цифровому середовищі для чотирьох груп: дітей; батьків, опікунів і педагогів; індустрії; директивних органів. У цих

Керівних настановах захист дитини в цифровому середовищі розуміється як всеохопний підхід до реагування на всі потенційні загрози і шкоду, з якими діти та молодь можуть зіткнутися або в цифровому середовищі, або через онлайн-технології. У цьому документі захист дитини в цифровому середовищі також містить шкоду, що заподіяна дітям у реальному світі, але пов'язана з онлайновим насильством та зловживаннями. Крім розгляду поведінки та дій дітей в інтернеті, захист дитини в цифровому середовищі також містить неправомірне використання технологій іншими особами, крім самих дітей, з метою експлуатації дітей.

Всі відповідні заінтересовані сторони відіграють певні ролі в тому, щоб допомогти дітям та молоді скористатися можливостями, пропонованими інтернетом, водночас набуваючи цифрової грамотності та стійкості щодо онлайнової безпеки й захисту.

Захист дітей та молоді є загальним обов'язком всіх заінтересованих сторін. Для практичного вирішення цього завдання директивні органи, представники індустрії, батьки, опікуни,

освітяни та інші заінтересовані сторони повинні забезпечити дітям та молоді можливість реалізації свого потенціалу як в цифровому середовищі, так і в реальному житті.

За відсутності універсального визначення захист дитини в цифровому середовищі набуває форми цілісного підходу до створення безпечного, відповідного для віку, інклюзивного та такого, що передбачає участь, цифрового простору для дітей та молоді, яке має такі характеристики:

• реагування, підтримка і самодопомога перед наявними загрозами;

• запобігання шкоді;

• динамічний баланс між забезпеченням захисту і наданням дітям можливості стати цифровими громадянами;

• дотримання прав і обов'язків як з боку дітей, так і з боку суспільства.

Більш того, з огляду на стрімкий розвиток технологій і суспільства, а також відсутність кордонів в інтернеті, захист дітей в цифровому середовищі, щоби бути ефективним, має бути швидким і адаптивним. У процесі розвитку технологічних інновацій будуть з'являтися нові завдання, характер яких залежатиме від регіону. З огляду на необхідність пошуку нових підходів, поєднання зусиль в межах глобальної спільноти є найкращим способом їх успішного вирішення.

2.1 Базова інформація

Оскільки інтернет повністю інтегрований у життя дітей та молоді, не можна розглядати цифровий і фізичний світи окремо.

Така можливість установлення з'єднань дає неймовірні перспективи. Світ інтернету дозволяє дітям та молоді долати несприятливі обставини та обмеженість можливостей, а також служить новою ареною для розваг, навчання, участі та формування взаємин. Сучасні цифрові платформи використовуються для всіляких видів діяльності, і одержуваний досвід часто є мультимедійним.

Доступ і навчання використанню таких технологій, а також орієнтації в них, вважаються критично важливими навичками для розвитку молоді, і перше використання ІКТ відбувається в ранньому віці. Отже, дуже важливо, щоб усі дійові особи усвідомлювали, що діти та молодь часто починають користуватися платформами і послугами до того, як досягнуть певного мінімального віку, якому технологічна індустрія повинна відповідати, і тому навчання, поряд із заходами захисту, має бути інтегроване в усі онлайн-послуги, що використовуються дітьми.

2.1.1 Діти в цифровому світі

Доступ до інтернету

За даними за 2019 рік, більш ніж половина населення Землі користувалася інтернетом (53,6 відсотка), що за розрахунками становить 4,1 мільярда користувачів. На глобальному рівні щотретій користувач інтернету є дитиною віком до 18-ти років1. Згідно з даними ЮНІСЕФ, по всьому світові 71 відсоток молоді вже підключений до інтернету2. Незважаючи на встановлений мінімальний вік, Ofcom (регуляторний орган індустрії зв'язку Сполученого Королівства) вважає, що близько 50 відсотків дітей у віці від 10 до 12 років вже мають свій обліковий запис у соціальних мережах3. Діти та молодь сьогодні мають значну, постійну та стабільну присутність в інтернеті. Інтернет-послуги, орієнтовані на інші цілі, крім соціальних, економічних і політичних, стали сімейними або споживчим продуктом або послугою, що є невід'ємною частиною життя родин, дітей та молоді.

У 2017 році на регіональному рівні доступ дітей та молоді до інтернету був міцно пов'язаний з рівнем національного доходу. У країнах з низьким доходом спостерігався більш низький показник кількості дітей, які користуються інтернетом, порівняно з країнами з високим доходом. Діти та молодь в більшості країн проводять більше часу в мережі у вихідні, ніж у будні дні, водночас підлітки віком від 15 до 17 років витрачають на інтернет більше часу, ніж інші групи, перебуваючи в мережі близько 2,5 - 5,3 години залежно від країни.

Livingstone, S., Carr, J., and Byrne, J. (2015) One in three: The task for global internet governance in addressing children's rights. Global Commission on Internet Governance: Paper Series. London: CIGI and Chatham House, https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights.

Broadband Commission, "Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online (2019)," Broadband Commission for Sustainable Development, October 2019, 84, https:// broadbandcommission .org/Documents/working-groups/ChildOnlineSafety_Report.pdf.

BBC, "Under-age social media use 'on the rise', says Ofcom".

Використання інтернету

Найбільш популярним пристроєм для доступу до інтернету серед дітей та молоді є мобільний телефон. На другому місці стоять персональні комп'ютери і ноутбуки. В середньому діти та молодь проводять в мережі дві години на день протягом тижня і чотири години щодня у вихідні. Притому що частина з них вважає себе постійно з'єднаними, багато хто все ще не мають доступу до інтернету вдома. На практиці більшість дітей та молоді, які користуються інтернетом, отримують доступ через більш ніж один пристрій - ті, хто з'єднується принаймні щотижня, іноді користуються трьома різними пристроями. Діти старшого віку й ті, хто живе в багатших країнах, зазвичай користуються більшою кількістю пристроїв, водночас хлопчики використовують трохи більше пристроїв, ніж дівчатка, в усіх обстежених країнах.

Найбільш популярним видом діяльності як серед хлопчиків, так і серед дівчаток, є перегляд відеороликів. Понад три чверті дітей та молоді, які користуються інтернетом, повідомили про те, що переглядають відео в мережі як мінімум щотижня або самостійно, або з іншими членами родини. Багатьох дітей і молодих осіб можна назвати такими, що "активно спілкуються", оскільки вони користуються кількома соціальними мережами, як-от Facebook, Twitter, Tiktok або Instagram. Діти та молодь також беруть участь у політичному житті в інтернеті та діляться своєю думкою через блоги.

Загальний рівень участі в онлайнових іграх залежить від країни і грубо співвідноситься з показником легкості доступу до інтернету для дітей та молоді. Проте доступність онлайнових ігор та їхня прийнятність в ціновому аспекті швидко змінюються, і вік дітей, які вперше отримують доступ до онлайнових ігор, знижується.

Щотижня 10 - 30 відсотків дітей та молоді, що користуються інтернетом, з числа опитаних в ряді країн беруть участь у творчій діяльності в цифровому середовищі1. З метою освіти багато дітей і молодих осіб різного віку щотижня користуються інтернетом для виконання домашніх завдань або навіть для надолуження пропущених уроків, або у пошуках інформації про здоров'я. Схоже, що старші діти більше цікавляться інформацією, ніж діти молодші.

Livingstone, S., Kardefelt Winther, D., and Hussein, M. (2019). Global Kids Online Comparative Report, Innocenti Research Report. UNICEF Office of Research - Innocenti, Florence, https://www.unicef-irc.org/publications/1059 -global-kids-online-comparative-report.html.

Сексуальна експлуатація та сексуальні зловживання щодо дітей в цифровому середовищі

Сексуальна експлуатація та сексуальні зловживання щодо дітей (СЕНД) в цифровому середовищі зростають приголомшливими темпами. Десять років тому повідомлялося про менш ніж один мільйон файлів, що містять матеріали, пов'язані зі зловживаннями щодо дітей. У 2019 році їхня кількість зросла до 70 мільйонів, причому цей показник виріс майже на 50 відсотків за один лише 2018 рік. Крім того, вперше кількість відеоматеріалів перевищила кількість світ

лин згідно з даними, отриманими владою, що свідчить про необхідність пошуку нових інструментів для стримування цієї тенденції. Жертви СЕНД в інтернеті належать до різних вікових груп, але дедалі молодшають. У 2018 році аналітики мережі гарячих ліній INHOPE відзначили зміщення в профілях жертв від підліткового до передпідліткового віку. Крім того, за даними дослідження, проведеного ECPAT International та Інтерполом у 2018 році, діти молодшого віку ймовірно піддаються більш серйозним зловживанням, зокрема тортури, жорстке зґвалтування або садизм. Також це стосується немовлят віком лише у кілька днів, тижнів або місяців. Притому, що найчастіше жертвами стають дівчинки, хлопчики можуть піддаватися більш жорстокому насильству. У тому ж звіті відзначено, що 80 відсотків жертв, про які повідомлялося, були дівчатками, а 17 відсотків - хлопчиками. Діти обох статей згадувалися у 3 відсотках повідомлень.

Зріз даних:

- Щотретій користувач інтернету в усьому світі є дитиною.
- Кожні півсекунди одна дитина під'єднується до інтернету вперше.
- 800 мільйонів дітей користуються соціальними мережами.
- За наявними оцінками у будь-який момент часу 750 000 чоловік, що перебувають в мережі, шукають з'єднання з дітьми в сексуальних цілях.
- У сховищі Європолу міститься більш ніж 46 мільйонів унікальних зображень або відеороликів зі CSAM.
- Вік більш ніж 89 відсотків жертв становить від 3 до 13 років.

Більш детальна інформація про масштаби і методи реагування на СЕНД в інтернеті наводиться на сайті Глобального альянсу WePROTECT.

Сайт Фонду припинення насильства щодо дітей (End Violence Against Children), "Safe Online".

2.1.2 Вплив різних платформ на цифровий досвід дітей

Інтернет та цифрові технології являють собою як можливості, так і ризики для дітей та молоді. Деякі з них наведені нижче.

Коли діти користуються соціальними мережами, вони отримують переваги, пов'язані з безліччю можливостей досліджувати, вчитися, спілкуватися і розвивати основні навички. Для дітей соціальні мережі є платформою, що дозволяє їм досліджувати власну особистість у безпечному середовищі. Для молоді вкрай важливо володіти відповідними навичками та знати, як вирішувати питання, пов'язані з конфіденційністю і репутацією. "Я знаю - все, що ти постиш в інтернеті, залишається там назавжди і може в

майбутньому вплинути на твоє життя", - 14-річний хлопчик із Чилі.

Але з огляду на те, що за даними багатьох обстежень більшість дітей починають користуватися соціальними мережами, не досягнувши мінімального віку у 13 років, а засоби перевірки віку загалом або слабкі, або відсутні, діти стикаються з дуже серйозними ризиками. Крім того, якщо діти хочуть освоювати цифрові навички, ставати цифровими громадянами і контролювати параметри конфіденційності, вони схильні розглядати конфіденційність виключно щодо своїх друзів і знайомих - "що можуть побачити мої друзі", - але без урахування незнайомих осіб і третіх сторін. Це, в поєднанні з природною цікавістю дітей і закономірно більш низькими порогами сприйняття ризику, здатне зробити їх вразливими для грумінгу, експлуатації, булінг та інших типів шкідливого контенту і контактів.

Велика популярність обміну зображеннями і відеоматеріалами через мобільні застосунки та, особливо, через використання платформ прямого потокового мовлення, створює додаткові приводи для занепокоєння стосовно конфіденційності та ризиків. Деякі діти роблять сексуальні фотографії самих себе, своїх друзів і братів або сестер, і діляться ними в інтернеті. У 2019 році майже третина (29 відсотків) всіх веб-сторінок, підписаних IWF, містила самостійно виконані зображення. На 76 відсотках таких зображень були представлені дівчатка у віці 11-13 років, причому більшість з них фотографувалися у своїй ванній кімнаті або в іншій кімнаті свого будинку. Для одних, особливо старших дітей, це може бути проявом природного дослідження сексуальності та сексуальної ідентичності, тоді як для інших, особливо дітей молодшого віку, це часто пов'язано з примусом з боку дорослих або інших дітей. Хай там що, підсумковий контент в багатьох країнах є незаконним і може піддавати дитину ризику кримінального переслідування або використання для подальшої експлуатації, грумінгу або примусу.

Аналогічно, онлайн-ігри дозволяють дітям реалізувати своє фундаментальне право на гру, а також створювати комунікаційні мережі, проводити час із друзями та спілкуватися з ними, розвиваючи важливі навички. Попри всю переважну позитивність, подекуди ігрові платформи, якщо їх використання дітьми не контролюється відповідальними дорослими, які не надають дітям необхідної підтримки, можуть також становити ризик.

До нього належать надмірна кількість часу, що витрачається на ігри, фінансові ризики, пов'язані з великими покупками всередині гри, збирання і монетизація персональних даних дитини учасниками індустрії, кібербулінг, мова ненависті, насилля та вплив неприйнятної поведінки або контенту, грумінг, використання реальних, створених комп'ютером або навіть віртуальною реальністю зображень, а також відеоролики, що зображують і стверджують СЕНД як норму. Ці ризики не є унікальними для ігрового середовища, і також застосовуються до інших цифрових середовищ, в яких діти можуть проводити час.

Крім того, технологічні розробки призвели до появи "інтернету речей", що дозволяє будь-яким пристроям, які під'єднані до інтернету, кількість яких постійно зростає, з'єднуватися між собою і формувати мережі в інтернеті. До них, зокрема, належать іграшки, радіо-няні та пристрої, керовані Штучним Інтелектом, які можуть становити ризик стосовно конфіденційності та небажаних контактів.

Передовий досвід: дослідження

Стосовно питання булінг в цифровому середовищі або кібербулінг компанія Microsoft провела дослідження з цифрової безпеки та кібербулінг. У 2012 році дослідники опитали дітей з 25 країн віком від 8 до 17 років про їх негативний досвід в інтернеті. Отримані результати показали, що в середньому 54 відсотки учасників відзначили, що їх турбувала ймовірність булінг в цифровому середовищі, 37 відсотків заявили, що піддавалися кіберцькуванню і 24 відсотки зізналися, що самі дражнили когось іншого. В межах того ж дослідження з'ясувалося, що менш ніж 3 з 10 батьків обговорювали булінг в цифровому середовищі зі своїми дітьми. Починаючи з 2016 року Microsoft проводить **регулярні дослідження** у темі онлайнових ризиків, щороку складаючи звіти за Індексом цифрової культури.

FACES є мультимедійної програмою, що випускається каналом NHK, Японія, і конзахист дітей у цифровому середовищіціумом різних компаній суспільного мовлення, в межах якої розповідаються історії жертв булінг в цифровому середовищі та в реальному житті у всьому світі. Це серія особистих історій підлітків, в яких головні герої перед камерою діляться тим, як вони реагували на чіпляння в інтернеті. Таку ж серію, що випускається у формі двохвилинних кліпів, запустили Facebook, ЮНЕСКО та Рада Європи. Ці ролики можна подивитися кількома мовами.

У 2019 році ЮНІСЕФ опублікував дискусійний документ під назвою Child Rights and Online Gaming: Opportunities & Challenges for Children and the Industry ("Права дитини і онлайн-ігри: можливості та труднощі для дітей і індустрії"), щоб обговорити можливості й труднощі, що виникають перед дітьми в одній із галузей розваг, яка дуже стрімко розвивається. У документі висвітлюються такі теми:

- право дітей на гру і свободу вираження (час, що витрачається на гру, і наслідки для здоров'я);
- відсутність дискримінації, участь і захист від насильства (соціальна взаємодія і повноправне залучення, токсичне середовище, вікові обмеження та їх перевірка, захист від грумінгу та сексуальних зловживань);
- право на конфіденційність і свободу від економічної експлуатації (бізнес-моделі надання доступу за дані, безкоштовні ігри та монетизація, відсутність прозорості у комерційному контенті).

Передовий досвід: технологія

The Google Virtual Reality Action Lab вивчає, як віртуальна реальність може сприяти залученню молоді на сторону супротивників булінг в реальному житті та цифровому середовищі.

У вересні 2019 року BBC запустила мобільний застосунок під назвою Own IT, присвячений добробуту дітей віком 8-13 років, які отримали свій перший смартфон. Застосунок є частиною зобов'язання BBC стосовно підтримки молоді в сучасному мінливому медійному середовищі і наступним кроком після успішного запуску веб-сайту Own IT у 2018 році. Застосунок є поєднанням сучасної технології машинного навчання, що відстежує дії дитини на його смартфоні, з наданою дитині можливістю самостійно позначати свій емоційний стан. У ньому використовується інформація для надання індивідуально підібраного контенту і втручання з тим, щоб допомогти дитині залишатися щасливою і здоровою в цифровому середовищі, пропонуючи дружні підказки для підтримки, коли їх поведінка виходить за межі норми. Користувачі можуть звертатися до застосунку по допомогу, водночас його також зручно використовувати для виведення на екран миттєвих порад і підказок у разі необхідності через спеціально розроблену клавіатуру. До функцій програми належать:

- нагадування користувачам поміркувати двічі, перш ніж ділитися персональними даними, як-от номером мобільного телефону, в соціальних мережах;
- допомога в розумінні того, як повідомлення можуть сприйматися іншими людьми, перш ніж надсилати їх;
- відстеження настрою у часі та поради про те, як змінити ситуацію за необхідності;
- надання інформації з таких тем, як використання телефону пізно вночі та вплив на самопочуття користувача.

Більш детальну інформацію можна знайти в публікації Alexa Hasse et al., "Youth and Cyberbullying: Another Look", Berkman Klein Centerfor Internet & Society, 2019.

У застосунку використовується спеціально підібраний контент з різних архівів BBC. У ньому зібрані корисні матеріали та ресурси, що допомагають молоді отримати максимум від часу, проведеного в цифровому середовищі, і виробити здоровий стиль поведінки і звички роботи в інтернеті. Він допомагає молоді та батькам вести більш конструктивну розмову про їх онлайновий досвід, не надаючи звітів або зворотного зв'язку батькам і зберігаючи всі дані виключно на пристрої користувача. Застосунок не збирає ніяких персональних даних або контенту, створеного користувачем, оскільки весь процес машинного навчання відбувається всередині програми, не полишаючи пристрою, на якому він встановлений. Пристрої навчаються відокремлено на основі даних навчання, щоб гарантувати відсутність порушень конфіденційності.

2.1.3 Особлива ситуація, в якій перебувають діти з інвалідністю

Діти та молоді люди з інвалідністю піддаються ризикам в цифровому середовищі так само, як діти та молодь без інвалідності, проте вони також можуть піддаватися і конкретним ризикам, що обумовлені їхньою інвалідністю. Вони часто стикаються з неприйняттям, забобонами і бар'єрами (фізичними, економічними, соціальними та оцінковими), що перешкоджають їх участі в житті спільнот. Такий досвід може чинити негативний вплив на дитину з інвалідністю і призводити до того, що вона починає шукати соціальної взаємодії та дружби в онлайновому просторі. Притому, що такі взаємодії можуть позитивно впливати на

формування самооцінки і створювати підтримувальні мережі контактів, вони також здатні піддавати дітей вищому ризику випадків грумінгу, 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 проблеми психологічного характеру, піддаються підвищеному ризику подібних інцидентів.

Загалом діти, які стають жертвами в реальному світі, найімовірніше опиняться в тому ж становищі в онлайновому просторі. Це ставить дітей з інвалідністю під загрозу більшого ризику в інтернеті, водночас що вони мають велику потребу бути онлайн. Є дані дослідження, згідно з якими діти з інвалідністю більш імовірно зазнають насильства будь-якого роду , зокрема переслідувань сексуального характеру . 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 його інвалідністю, - це можуть бути особливості мови і поведінки, або обладнання, або послуги, якими він користується.

Серед осіб, які скоюють такі правопорушення, як грумінг, схиляння в онлайн-середовищі до дій сексуального характеру та/або сексуальні домагання щодо дітей та молодих людей з інвалідністю, можуть бути не лише порушники, які обирають своїми жертвами саме дітей та молодь, а й також ті, котрі обирають саме дітей і молодих людей 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 деякі з них самі прикидаються людьми з інвалідністю . Такі особи можуть вчиняти такі дії, як завантаження фото і відео дітей та молодих людей з інвалідністю (які самі по собі нешкідливі) та/або їх поширення через спеціально створювані форуми й облікові записи в соціальних мережах. Механізми інформування в межах форумів і соціальних мереж часто не передбачають можливостей припинення таких дій. Є побоювання щодо того, що "шерентинг" (публікування батьками інформації та світлин своїх дітей і молодих осіб в інтернеті) може порушити право дитини на недоторканність приватного життя, призвести до булінг і до виникнення незручних ситуацій, або негативно позначитися на дальшому житті . Деякі батьки дітей з інвалідністю можуть ділитися інформацією чи даними своїх дітей в пошуках підтримки або поради, тим самим ставлячи свою дитину під загрозу порушення конфіденційності як сьогодні, так і в майбутньому. Такі батьки також ризикують стати мішенню для неосвічених або безпринципних людей, що пропонують лікування або "зцілення" для їхньої дитини. Також деякі батьки дітей або молодих людей з інвалідністю можуть демонструвати гіперпіклування в силу нестачі знань про те, як найкраще направляти свою дитину під час використання інтернету або як захистити її від булінг або домагання.

Деякі діти та молоді люди з інвалідністю можуть стикатися з труднощами під час використання або навіть з відчуженням до онлайнового середовища через недоступність його структури (як-от застосунки, що не передбачають можливості збільшення шрифту), з відмовою від запитаних зручностей (наприклад, програм зчитування з екрана або адаптивних засобів керування) або з необхідністю прийнятної підтримки (наприклад, навчання тому, як

користуватися обладнанням, індивідуальна підтримка щодо навігації під час соціальних взаємодій).

2.2 Чинні національні й транснаціональні моделі захисту дитини в цифровому середовищі

На глобальному рівні ухвалено декілька моделей збереження безпеки дітей та молоді в цифровому середовищі. Заінтересованим сторонам в індустрії слід враховувати ці Рекомендації в межах міжнародних ініціатив, а також як основу забезпечення того, що вони доклали всіх зусиль для захисту дітей та молоді в інтернеті. Інтернет-індустрія - це різнопланова і заплутана сфера, що складається з компаній різного розміру та функцій. Дуже важливо, щоб захисту дітей приділяли увагу не лише платформи і служби, що працюють з контентом, але й ті, хто підтримує інфраструктуру інтернету.

Необхідно відзначити, що потенціал індустрії в аспекті введення всебічної політики захисту дітей обмежений наявними ресурсами. У зв'язку з цим у цих Керівних настановах міститься рекомендація щодо об'єднання зусиль різних галузевих організацій для розгортання послуг із захисту користувачів. Спільно використовуючи ресурси і технічний досвід, вони зможуть більш ефективно створювати "безпечні простори" з метою запобігання насильству.

Співпраця індустрії

Технологічна коаліція є прикладом успішної співпраці між заінтересованими сторонами в індустрії з метою боротьби із СЕНД.

Транснаціональні моделі

Галузевим організаціям слід уносити відповідні міжнародні Рекомендації до своїх структурних програм, а також дотримуватися всіх відповідних національних і транснаціональних законодавчих норм, що діють в тих країнах, де вони працюють. Їм необхідно враховувати не лише ті дії, які вони зобов'язані вчиняти на встановленому законом рівні, але й ті дії, які вони можуть виконати, та по змозі прагнути до реалізації ініціатив у всьому світі. Серед моделей, що містять принципи для таких ініціатив, можна назвати такі:

- Урядові Добровільні принципи протидії СЕНД в інтернеті п'яти країн (2020 рік);
- Комісія із широкосмугового зв'язку в інтересах сталого розвитку "Безпека дитини в цифровому середовищі: зменшення ризику насильства, жорстокого поводження та експлуатації в цифровому середовищі (2019 рік)";
- Глобальний альянс WePROTECT "Глобальна стратегічна відповідь на сексуальну експлуатацію та сексуальні зловживання щодо дітей в цифровому середовищі" (2019 рік);
- Глобальне партнерство з припинення насильства щодо дітей "Навчатися безпечно: заклик до дії";
- Гідність дитини у цифровому світі "Альянс за гідність дитини: звіт робочої технологічної групи (2018 рік");
- Директива (ЄС) 2018/1808 Європейського Парламенту і Ради Європейського Союзу про аудіовізуальні медіа-послуги;
- Загальний регламент Європейської комісії про захист персональних даних (2018 рік);
- Рекомендації ОЕСР щодо захисту дитини в цифровому середовищі (2012 рік).

Національні моделі

Є ціла низка національних та міжнародних моделей, що встановлюють чіткі ролі та обов'язки технологічної індустрії в питаннях захисту дітей в цифровому середовищі. Деякі з них не є специфічними саме для дітей, однак можуть застосовуватися до них як до користувачів інтернету. Вони містять всеосяжні Рекомендації для індустрії щодо регуляторної політики, стандартів і співпраці з іншими секторами. Для цілей цього документа виділимо основні принципи таких моделей у межах їх застосування до індустрії ІКТ.

Кодекс проєктування з огляду на вік, Сполучене Королівство

На початку 2019 року Управління Комісару з інформації опублікувало пропозиції до кодексу проєктування з з огляду на вік з метою захисту даних дітей. Пропонований кодекс складений, виходячи з кращих інтересів дитини, описаних у Конвенції ООН про права дитини, і встановлює низку вимог до індустрії. Кодекс складається з п'ятнадцяти стандартів, серед яких є вимикання послуг визначення розташування за замовчуванням для дітей, збирання й зберігання якнайменшої кількості персональних даних дітей для індустрії, проєктована конфіденційність для продуктів, а також доступні пояснення, що відповідають віку.

Закон про шкідливу цифрову комунікацію, Нова Зеландія

Законом, ухваленим у 2015 році, зловживання у кіберпросторі виділені як окремий вид злочину і розглядається великий спектр типів завданої шкоди - від кібербулінг до порнографії як помсти. Він спрямований на стримування, запобігання і зменшення цифрової комунікації, що є шкідливою, роблячи незаконною публікацію цифрових матеріалів з наміром заподіяння серйозного емоційного розладу комусь іншому і встановлюючи 10 принципів комунікації. Закон створює можливості для подання скарг до незалежної організації в разі порушення зазначених принципів або для подання судового позову проти автора або вузла зв'язку, якщо проблема не вирішується.

Комісаріат електронної безпеки, Австралія

Заснований у 2015 році в Австралії Комісаріат електронної безпеки є першим у світі державним органом, створеним з метою вирішення питань зловживань в інтернеті та забезпечення безпеки громадян в цифровому середовищі. Як незалежний національний регулятор з питань безпеки в цифровому середовищі, Комісаріат має повноваження щодо цілої низки функцій в діапазоні від профілактики (через підвищення обізнаності, навчання, дослідження і публікації керівних настанов про передові методи) до раннього втручання й усунення шкоди за допомогою різних законодавчих норм, що дають йому повноваження для швидкого припинення кібербулінг, зловживань з використанням зображень і незаконного онлайнового контенту. Настільки широке коло обов'язків забезпечує Комісаріату можливість працювати над безпекою в інтернеті на засадах багатогранного, цілісного підходу на випередження.

У 2018 році Комісаріат електронної безпеки розробив ініціативу щодо проєктованої безпеки (Safety by Design, SbD), яка ставить безпеку і права користувачів у центр роботи з проєктування, розроблення і розгортання онлайнових продуктів і послуг. Ініціатива спирається на низку принципів проєктування, що встановлюють реалістичні, дієві та досяжні критерії для індустрії, забезпечуючи більш якісний захист для громадян. Трьома всеосяжними принципами є:

1) Відповідальність постачальника послуг: тягар забезпечення безпеки не повинний цілком покладатися на кінцевого користувача. Вже на етапі проєктування можна зробити низку профілактичних кроків, які забезпечують оцінку відомої прогнозованої шкоди, і врахувати їх під час надання онлайнової послуги поряд із кроками, що знижують вірогідність того, що послуга буде сприяти, підштовхувати або заохочувати до незаконних неприйнятних дій.

2) Надання прав і можливостей користувачу та його автономність: гідність користувачів

та їхні кращі інтереси мають першорядну важливість. Необхідно підтримувати вибір і автономність людини, підкріплюючи і посилюючи їх за рахунок проєктування послуги, так, щоби дати користувачам можливість більшого контролю, керування і регулювання їхнього власного досвіду.

3) Прозорість і підзвітність: це відмітні ознаки надійного підходу до безпеки, який гарантує, що послуги надаються відповідно до заявлених цілей з безпеки, водночас навчаючи і надаючи громадськості можливості щодо кроків, які можна зробити для усунення проблем у цій індустрії.

Глобальний альянс WePROTECT

В основі стратегії, прийнятої Глобальним альянсом WePROTECT, є підтримка країн в процесі розробки скоординованих заходів реагування на випадки сексуальної експлуатації дітей в цифровому середовищі в межах пропонованої Альянсом моделі національного реагування, яка служить проєктом національних програм. Стратегія дає країнам схему, що допомагає вирішити проблему сексуальної експлуатації дітей в цифровому середовищі. У структурі моделі національного реагування WePROTECT вирізняється чіткий набір зобов'язань зі сторони компаній сфери ІКТ щодо:

- процедур оповіщення і вимикання;
- повідомлення про сексуальну експлуатацію та сексуальні зловживання щодо дітей (СЕНД) в цифровому середовищі;
- розроблення технологічних рішень; а також
- інвестування в ефективні програми по захисту дітей у цифровому середовищі і служби реагування.

Глобальне партнерство і фонд з припинення насильства щодо дітей

Глобальне партнерство і фонд з припинення насильства щодо дітей були започатковані Генеральним Секретарем ООН у 2016 році з єдиною метою: активізувати і підтримати дії з припинення всіх форм насильства щодо дітей до 2030 року завдяки унікальній співпраці більш ніж 400 партнерів з усіх секторів.

Ця робота орієнтована на порятунок і підтримку жертв, технологічні ідеї щодо виявлення та запобігання злочинам, підтримку правоохоронних органів, проведення законодавчих та політичних реформ, а також на генерування даних і доказів про масштаби й характер СЕНД в інтернеті та розуміння ситуації з позиції дітей.

3 Основні царини у сфері захисту та сприяння реалізації прав дітей

У цьому розділі наводиться опис п'яти основних варіантів дій компаній стосовно забезпечення захисту дітей та молоді під час використання ІКТ та сприяння позитивному застосуванню ІКТ.

3.1 Долучення положень про права дитини до усіх відповідних корпоративних політик та процесів управління

Необхідність враховувати права дитини вимагає від компаній відповідних заходів щодо виявлення, запобігання, пом'якшення та, по змозі, усунення потенційного або фактичного негативного впливу на права дитини. Рекомендації ООН щодо підприємницької діяльності в аспекті прав людини закликають всі підприємства і індустрії запровадити відповідні політики та процедури, спрямовані на виконання їхніх обов'язків щодо поваги до прав людини.

Галузевим організаціям слід приділяти особливу увагу дітям та молоді як вразливій групі в аспекті захисту їх персональних даних та свободи вираження поглядів. Резолюція Генеральної Асамблеї ООН 68/167 про право на недоторканність особистого життя в цифровому столітті закріплює право на недоторканність особистого життя та вільне висловлення своєї думки без незаконного втручання. Крім того, Резолюцією Ради з прав людини 32/13 про заохочення, захист і реалізування прав людини в інтернеті визнається глобальний та відкритий характер інтернету як однієї з рушійних сил прискорення прогресу на шляху розвитку в його різних формах і підтверджується, що ті самі права, які людина має в реальному світі, мають також захищатися і в цифровому середовищі. У державах з недостатньо визначеними законодавчими межами у сфері захисту прав дітей та молоді на особисте життя і вільне висловлення своєї думки компаніям слід дотримуватися більш суворих правил належного виконання, щоб забезпечити відповідність своїх політик і процедур міжнародним законам. У зв'язку з дедалі більшим зростанням участі молоді в житті громадянського суспільства завдяки онлайновим комунікаціям, компанії несуть відповідальність за повагу до прав дітей та молоді навіть якщо місцеве законодавство ще не досягло рівня міжнародних стандартів.

Компанії повинні на оперативному рівні розробити механізм розгляду скарг, який визначає формат поставлення питань про потенційні порушення особами, що зазнали негативного впливу. Механізми оперативного рівня мають бути доступними для дітей, їхніх родин та осіб, які представляють їх інтереси. Згідно з роз'ясненнями, наведеними у Принципі 31 Керівних принципів ООН щодо підприємницької діяльності в аспекті прав людини, такі механізми мають бути легітимними, доступними, передбачуваними, справедливими, прозорими, відповідати нормам у сфері прав людини, повинні служити джерелом безперервного навчання і ґрунтуватися на взаємодії та діалозі. Поряд з внутрішніми процесами контролю негативного впливу, механізми розгляду скарг мають гарантувати наявність в компаніях певних рам, що забезпечують необхідні засоби захисту прав дітей та молоді в ситуаціях, які становлять для них загрозу.

Прагнучи нормативної відповідності у сфері безпеки ІКТ, сфокусованій на дотриманні національного законодавства, дотриманні міжнародних керівних настанов за відсутності національних законів і недопущення несприятливого впливу на права дітей та молоді, компанії здійснюють запобіжні заходи для сприяння розвитку і добробуту дітей та молоді через проведення добровільних акцій, спрямованих на сприяння реалізації прав дитини на доступ до інформації, вільне вираження своїх поглядів та участь, а також освітніх та культурних прав.

Передовий досвід: політика і проектування з огляду на вік

Розробник застосунків Toca Boca виготовляє цифрові іграшки з огляду на перспективи дитини. Політика конфіденційності компанії складена таким чином, щоб пояснити, яку інформацію компанія збирає і як її використовує. Toca Boca, Inc є членом Програми сертифікації "безпечного простору" PRIVO Kids Privacy Assured COPPA.

LEGO® Life є прикладом безпечної платформи соціальних мереж для дітей, молодших за 13 років, де вони можуть обмінюватися своїми виробами з LEGO, отримувати натхнення та безпечно взаємодіяти один з одним. У дітей не запитують ніякої персональної інформації для створення облікового запису, для реєстрації якого досить лише адреси електронної пошти одного з батьків або опікуна. Застосунок створює для дітей і родин можливість обговорити питання безпеки та конфіденційності в мережі у позитивно налаштованому середовищі.

До прикладів проєктування з огляду на вік належать спеціальні пропозиції деяких великих компаній суспільного мовлення для певних вікових груп. Так в Німеччині ARD (Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland - Das Erste) та ZDF (Zweites Deutsches Fernsehen) налаштовані на аудиторію дітей від 14 років, пропонуючи спеціально підібраний контент через онлайновий канал funk.net. BBC (British Broadcasting Corporation) запустила проєкт CBeebies, призначений для дітей, молодших за 6 років. Контент веб-сайту підібраний спеціально для відповідних вікових груп.

Передовий досвід: політика і технології

Twitter безперервно інвестує у власні технології, що сприяють стабільному позбавленню людей від тягаря відповідальності за повідомлення про порушення1. Зокрема, понад 50 відсотків твітів (порівняно з 20 відсотками у 2018 році), які Twitter відстежує, зважаючи на їх образливий характер, наразі виявляються превентивно за допомогою технологій, а не лише покладаючись на повідомлення від користувачів. Нова технологія використовується в таких аспектах політики про контент, як-от конфіденційна інформація, вразливі засоби передавання, дії, що розпалюють ненависть, насильство та знеособлення.

3.2 Розроблення стандартних методів поводження з CSAM

У 2019 році IWF вжив заходів проти 132 676 веб-сторінок, що містять підтверджені матеріали, пов'язані із сексуальними зловживаннями щодо дітей . Будь-який URL може містити сотні, якщо не тисячі зображень і відеоматеріалів. З усіх зображень, блокованих IWF, на 45 відсотках були діти віком 10 років і молодші, і на 1609 веб-сторінках демонструвалися діти віком від 0 до 2 років, причому 71 відсоток з них містив сцени найбільш серйозних сексуальних зловживань, як-от зґвалтування і сексуальні тортури. Ці тривожні факти

підкреслюють важливість спільних дій між галузями, урядовими та правоохоронними органами, а також громадянським суспільством в аспекті боротьби з CSAM.

Водночас як уряди багатьох країн здійснюють активні дії у боротьбі з розповсюдженням CSAM, посилюючи законодавство, переслідуючи і караючи правопорушників, підвищуючи рівень обізнаності та підтримуючи дітей та молодь в процесі їхньої реабілітації після зазнаного насильства або експлуатації, багато країн поки що не мають у себе прийнятних систем. У кожній країні повинні діяти механізми, завдяки яким широкий загал може повідомляти про подібний контент насильницького та експлуатаційного характеру. Індустрія, правоохоронні та урядові органи, а також громадянське суспільство повинні тісно співпрацювати, гарантуючи належні правові межі відповідно до чинних міжнародних стандартів. Такі межі мають передбачати кримінальне переслідування за все форми СЕНД, зокрема за CSAM, захищати дітей, що стали жертвами такого насильства або експлуатації, а також забезпечувати максимально ефективне функціонування системи повідомлення, розслідування й видалення такого контенту.

Підприємства індустрії повинні зазначати на своїх веб-сайтах посилання на національні гарячі лінії, як-от портали IWF у деяких країнах і, за відсутності місцевих можливостей для повідомлення, зазначати посилання на інші відповідні міжнародні гарячі лінії, як-от в США Національний центр з питань дітей, які зникли або експлуатуються (NCMEC) або Міжнародна асоціація гарячих ліній в інтернеті (INHOPE), через яку можна звернутися з повідомленням на будь-яку міжнародну гарячу лінію.

Відповідальні компанії роблять цілий ряд кроків щодо попередження неналежного використання їхніх мереж і послуг з метою поширення CSAM. До таких кроків належить унесення до ухвалених компаніями положень, умов або кодексів поведінки пунктів, що беззаперечно забороняють подібний контент або дії , розроблення дієвих процесів оповіщення і вимикання, а також співпраця з національними гарячими лініями і підтримка їхньої роботи.

Водночас деякі компанії здійснюють технічні заходи щодо запобігання неналежного використання своїх послуг і мереж для обміну відомим CSAM. Наприклад, деякі постачальники послуг інтернету також блокують доступ до URL, на яких, згідно з підтвердженими даними відповідних органів, містяться CSAM, якщо головний вузол цього веб-сайту розташований на території країни, де відсутні необхідні процеси, що гарантують його швидке видалення. Інші застосовують технології гешування для автоматичного виявлення і видалення зображень, пов’язаних із сексуальними зловживаннями щодо дітей, про яких правоохоронні органи або гарячі лінії вже отримали інформацію. Членам індустрії слід розглянути і впровадити у свою роботу всі відповідні служби для запобігання поширенню сексуальних зловживань щодо дітей.

Учасники індустрії мають взяти зобов’язання щодо пропорційного розподілу ресурсів і продовжити розроблення й обмін технологічними рішеннями переважно з відкритим кодом для виявлення і видалення CSAM.

Передовий досвід: технологія

Microsoft застосовує чотиристоронній підхід для сприяння відповідальному і безпечному використанню технології з основною увагою до самої технології, самоврядування, партнерств, а також до навчання й охоплення споживачів. Компанія Microsoft також впровадила функції, які сприяють наданню окремим особам можливості більш ефективно керувати своєю безпекою в інтернеті. Однією з таких функцій є "безпека родини", що дозволяє батькам і опікунам контролювати використання інтернету їхньою дитиною.

На своїх платформах Microsoft дотримується політики, спрямованої проти домагань, і облікові записи користувачів, які порушують цю вимогу, закриваються або, в разі більш серйозних порушень, компанія звертається до правоохоронних органів.

Microsoft PhotoDNA - це інструмент, який створює геші зображень і порівнює їх з базою даних гешів, які вже виявлені та підтверджені як CSAM. Якщо він знаходить збіг, зображення блокується. Цей інструмент дав постачальникам контенту можливість видалити мільйони неправомірних фотографій з інтернету, допоміг притягнути до відповідальності сексуальних насильників над дітьми і подекуди допоміг правоохоронним органам врятувати потенційних жертв до того, як їм було завдано фізичної шкоди. Microsoft вже давно дотримується зобов'язання захищати своїх клієнтів від незаконного контенту у своїх продуктах та послугах, і застосування технології, вже розробленої компанією, для боротьби зі зростанням кількості таких незаконних відеоматеріалів стало логічним наступним кроком. Однак цей інструмент не використовує технологію розпізнавання особи і не в змозі ідентифікувати особу людини або об'єкт за зображенням. Проте з винаходом PhotoDNA for Video ситуація отримала новий напрямок розвитку. PhotoDNA for Video поділяє відеоролик на ключові кадри і створює геші для таких знімків екрану. Як PhotoDNA вміє зіставляти зображення, змінені задля уникнення виявлення, PhotoDNA for Video здатний знаходити контент з елементами сексуальної експлуатації дітей, що був відредагований або поділений на ролики, що в іншому випадку здавалися б нешкідливими.

Ба навіть більше, нещодавно Microsoft випустила новий інструмент для ідентифікації ґвалтівників над дітьми, які здійснюють грумінг з метою зловживань в онлайнових чатах. Проект Artemis, розроблений спільно із The Meet Group, Roblox, Kik і Thorn, ґрунтується на запатентованої технології Microsoft і буде переданий у вільний доступ через Thorn для кваліфікованих компаній інтернет-послуг, які пропонують функції чатів. Проект Artemis - це технологічний інструмент, який показує "червоні прапорці" адміністраторам у разі необхідності модерування в кімнатах чату. Завдяки цьому засобу виявлення грумінгу стає можливо ідентифікувати, вживати заходів і повідомляти про злочинців, які намагаються спокусити дітей у сексуальних цілях.

IWF пропонує низку послуг для представників індустрії, що допомагають захистити їхніх користувачів від контакту з CSAM. До них, попри інше, належать:

- якісні динамічні списки блокування URL, що містять матеріали прямих трансляцій;
- списки гешів відомого кримінального контенту, пов'язаного з CSAM;
- унікальні списки ключових слів шифрованих понять, що, як відомо, пов'язані з CSAM;
- список деталей доменних імен, під якими, як відомо, опублікований контент, що містить елементи сексуальних зловживань щодо дітей, який дозволяє швидко видаляти домени, на яких є незаконний контент.

3.3 Створення більш безпечного онлайнового середовища, що відповідає віку

Вкрай мало речей у нашому житті можна вважати абсолютно безпечними і такими, що не несуть ніякого ризику. Навіть у містах з максимально розвиненою системою регулювання дорожнього руху все одно стаються аварії. Так само кіберпростір не позбавлений ризиків, особливо для дітей та молоді. Діти та молодь можуть розглядатися як одержувачі, учасники та дійові особи в їхньому онлайновому оточенні. Ризики, з якими вони стикаються, можна поділити на чотири категорії:

- **Неприйнятний контент** - діти та молодь можуть стикатися з неприйнятним і незаконним контентом в процесі пошуку інших матеріалів, натискаючи на нібито безвинне посилання в отриманому повідомленні, блозі або під час обміну файлами. Водночас діти можуть шукати матеріали, що є неприйнятними або не відповідають віку, та обмінюватися ними. Уявлення про те, що саме слід вважати шкідливим контентом, залежить від конкретної країни, водночас до прикладів належать матеріали, що підтримують зловживання забороненими речовинами, пропаганду расової ненависті, ризикової або суїцидальної поведінки, анорексії або насильства.
- **Неприйнятна поведінка** - діти й дорослі можуть користуватися інтернетом з метою переслідування або навіть експлуатації інших людей. Діти інколи можуть поширювати образливі коментарі або зображення, що зачіпають чиюсь гордість, а також можуть красти контент або порушувати авторські права.
- **Неприйнятний контакт** - як дорослі, так і молодь можуть користуватися інтернетом з метою пошуку вразливих дітей або інших молодих осіб. Часто їх мета полягає в тому, аби переконати об'єкт пошуку у формуванні між ними значущих відносин, хоча в основі такої мети лежить прагнення маніпулювати своїм контактом. Вони можуть намагатися схилити дитину до дій сексуального або іншого образливого характеру в цифровому середовищі з використанням веб-камери або іншого записного пристрою, або ж вони можуть вдатися до спроб організувати особисту зустріч із фізичним контактом. Такий процес часто називають "грумінгом".
- **Комерційні ризики** - до цієї категорії належать ризики, пов'язані з конфіденційністю під час збирання і використання даних дитини, а також із цифровим маркетингом. Безпека в цифровому середовищі - це виклик для суспільства і можливість для індустрії, уряду та громадянського суспільства завдяки спільним зусиллям розробити відповідні принципи і методи їх забезпечення. Індустрія може запропонувати цілу низку технічних підходів, інструментів і послуг для партнерів, а також для дітей та молодих осіб і, перш за все, повинна створювати продукти, які є простими у використанні, спроектовані безпечно і відповідають віку їхньої основної категорії користувачів. Додатковими підходами є інструменти для розробки нових систем перевірки віку без порушення прав дитини на недоторканність приватного життя та доступ або встановлення обмежень у доступі до невідповідного віку контенту для дітей та молоді, а також обмеження доступу для осіб, з якими діти можуть контактувати, або часу, протягом якого вони можуть виходити в інтернет. І найголовніше - схеми "проєктованої безпеки" , які враховують потребу у конфіденційності в процесі інновацій та проєктування продукції. Безпека дітей і відповідальне використання технологій мають бути ретельно проаналізовані заздалегідь, не відкладаючи їх на потім.

Деякі програми дають батькам можливість контролювати тексти та іншу інформацію, яку отримують і надсилають їхні діти та молодь. У разі використання програм такого типу важливо відверто обговорити це з дитиною, інакше дитина може сприйняти таку поведінку як "шпигунство", що підриває довіру в сім'ї.

Для компаній одним із способів визначення, якого типу поведінки дотримуються і дорослі, і діти, які типи дій є неприйнятними та якими можуть бути їхні наслідки, є розроблення правил прийнятного використання. Чіткі та прозорі механізми зворотного зв'язку мають бути доступними для користувачів, у яких є сумніви щодо контенту та поведінки. До того ж всі повідомлення потребують належного контролю зі своєчасним наданням відомостей про статус повідомлення. Незважаючи на те, що в компаніях можуть застосовуватися різні механізми подальшого контролю залежно від конкретного випадку, важливо встановити чіткі часові межі для відповіді, надати інформацію про ухвалене рішення і запропонувати спосіб майбутніх дій, якщо користувач не задоволений отриманою відповіддю.

Передовий досвід: повідомлення про проблеми

Facebook, прагнучи до стримування сексуальних домагань на цифрових платформах, взяла участь у фінансуванні Проєкту deSHAME в Європейському Союзі спільно з Childnet, Save the Children, Kek Vonal і UCLan. Цей проєкт спрямований на активізацію повідомлень про проблеми, пов'язані із сексуальними домаганнями в інтернеті, серед неповнолітніх і розширення міжгалузевої співпраці з метою запобігання подібній поведінці та реагування на неї.

Оскільки однією з головних цілей проєкту є заохочення користувачів до повідомляння про контент, який їх засмучує або є неприйнятним, з ним також можна співвіднести Стандарти спільноти Facebook як Рекомендації про те, що дозволено, а що ні у Facebook. В них також визначені типи користувачів, яким заборонено робити публікації. Facebook також розробила функції безпеки, як-от "Чи знаєте ви цю людину?", скринька вхідних повідомлень "інші", до якої потрапляють нові повідомлення від осіб, не відомих користувачеві, та спливаюче вікно, яке з'являється у стрічці новин, якщо виникає підозра, що до неповнолітнього звертається доросла особа, яку ця дитина не знає.

Постачальники онлайнового контенту і послуг також можуть наводити опис характеру матеріалів, що ними надаються, і зазначати вікову групу, якій вони призначені. Такі описи слід узгоджувати з чинними національними та міжнародними стандартами, відповідними нормами та рекомендаціями щодо методів маркетингу і реклами для дітей, які розповсюджуються відповідними класифікаційними органами. Проте цей процес помітно ускладнюється з огляду на дедалі більшу кількість інтерактивних послуг, які допускають публікацію створеного користувачами контенту, як-от на електронних дошках оголошень, у тематичних чатах і соціальних мережах. Якщо цільовою аудиторією компанії є діти та молодь, або якщо послуги орієнтовані переважно на молодь, очікування щодо **дружнього до користувача, зрозумілого і доступного контенту** і безпеки будуть значно більшими.

Водночас заохочується прийняття компаніями найсуворіших стандартів захисту конфіденційності в ситуаціях, що вимагають збирання, оброблення та збереження даних, отриманих від дітей і молодих осіб або стосуються їх, оскільки діти та молодь можуть бути недостатньо зрілими, щоб оцінити широкі соціальні та особисті наслідки розкриття або згоди на надання їхньої персональної інформації в інтернеті, або на використання їхніх персональних даних у комерційних цілях. Послуги, спрямовані виключно або головним чином на дитячу та юнацьку аудиторію, повинні враховувати ризики, яким вони піддаються у зв'язку з доступом до таких послуг або збиранням і використанням їхніх персональних даних (зокрема відомості про місцеперебування), і гарантувати відповідні дії стосовно таких ризиків та інформування користувачів. Зокрема компанії повинні гарантувати, що мова і стиль всіх матеріалів та інформації, що використовуються для просування послуг, надання доступу до послуг або для доступу до особистої інформації, її збирання та використання, сприяють розумінню і допомагають користувачам контролювати власну конфіденційність чіткими і прозорими способами, а також чітко і зрозуміло пояснюють, на що саме погоджуються користувачі.

Передовий досвід: інновації

У 2018-2019 роках Регіональне відділення для Східної Азії і Тихого океану ЮНІСЕФ організувало п'ять круглих столів для багатьох заінтересованих сторін з метою обміну перспективним передовим досвідом у сфері СЕНД. Учасниками круглих столів стали представники провідних компаній приватного сектору, як-от Google, Facebook, Microsoft, Telenor, Ericsson, MobiCom (Монголія), Mobifone+ (В'єтнам), Globe Telecom (Філіппіни), True (Таїланд), Асоціація GSM, а також партнери, що представляють громадянське суспільство, зокрема INHOPE, ECPAT International та Міжнародна лінія допомоги дітям.

В частині того ж проєкту в лютому 2020 року ЮНІСЕФ запустив "мозковий центр" для прискорення виходу індустрії на лідерські позиції в Східній Азії та Тихоокеанському регіоні з метою запобігання насильству проти дітей в онлайновому світі. Мозковий центр - це інкубатор ідей та інновацій, який ґрунтується на унікальній перспективі учасників індустрії (виробництво товарів, маркетинг тощо) стосовно розроблення результативних навчальних матеріалів і виявлення найбільш ефективних платформ доставляння, а також для розроблення схем розвитку, що дозволяють вимірювати вплив таких навчальних матеріалів і повідомлень, спрямованих на дітей. До складу мозкового центру увійшли фахівці Facebook, Telenor, експерти академічних організацій, установи ООН, як-от МСЕ, UNESCO та UNODC, а також інші представники від таких організацій як Комісаріат електронної безпеки Австралії, ECPAT International, ICMEC, Інтерпол і Глобальний фонд з припинення насильства щодо дітей. Мозковий центр скликав збори, проведені паралельно з Регіональною конференцією АСЕАН щодо захисту дитини в цифровому середовищі, зібравши фахівців, зокрема з Microsoft, для вивчення технологій і дослідження можливостей для кращого відстеження змін в онлайновій поведінці на підставі показників використання матеріалів та повідомлень щодо безпеки в цифровому середовищі.

3.4 Навчання дітей, опікунів та педагогів правилам дитячої безпеки та відповідального використання ними ІКТ

Технічні заходи можуть бути важливим засобом забезпечення гарантії захисту дітей та молоді від потенційних ризиків, з якими вони стикаються в цифровому середовищі, але це лише одна складова рівняння. Інструменти батьківського контролю, посилення обізнаності й навчання також є вагомим компонентом, що сприяє розширенню прав, можливостей та інформування дітей і молодих осіб різних вікових груп, а також їхніх батьків, опікунів і педагогів. Хоча компанії відіграють важливу роль у забезпеченні відповідального і безпечного способу використання ІКТ дітьми і молодими особами, батьки, школа й самі діти та молодь поділяють з ними цю відповідальність.

Багато компаній інвестують в освітні програми, спрямовані на те, щоб у користувачів могли бути поінформовані рішення щодо контенту та послуг. Компанії допомагають батькам, опікунам та педагогам направляти дітей і молодь в аспекті більш безпечної, більш відповідальної та прийнятної поведінки в цифровому середовищі та в мережах телефонного зв'язку.

До такої роботи належить маркування контенту, що класифікується за віком, і чітке подання інформації з таких питань, як вартість контенту, умови передплати та способи

скасування підписки. Підтримка дотримання вимог щодо мінімального віку в соціальних мережах у всіх країнах, де є можливість здійснювати таку перевірку, також допоможе захистити дітей, дозволяючи надавати їм послуги доступу в прийнятному віці. Важливим моментом, який слід брати до уваги поряд із цією рекомендацією, є неминуче збирання додаткових даних для виконання цієї вимоги і необхідність обмеження збирання, збереження та оброблення такої інформації.

Також важливо надавати інформацію безпосередньо дітям та молоді про більш безпечне використання ІКТ, про позитивну і відповідальну поведінку. Крім підвищення рівня обізнаності про безпеку, компанії можуть сприяти розвитку позитивного досвіду, розроблюючи контент для дітей та молоді, який інформує про те, що, користуючись ІКТ, необхідно вести себе шанобливо, доброзичливо і неприховано, а також стежити за поведінкою своїх друзів. Вони можуть надавати інформацію про ті дії, які необхідно вчинити у разі негативного досвіду, як-от булінг або грумінгу в цифровому середовищі, і які спрощують повідомлення про такі інциденти та надають можливість отримання анонімних повідомлень.

Батьки іноді набагато менше знаються на інтернет-технологіях і мобільних пристроях, ніж діти та молодь. Також поєднання мобільних пристроїв та інтернет-послуг значно ускладнює нагляд з боку батьків. Індустрія може співпрацювати з державними та освітніми установами з метою посилення можливостей батьків стосовно підтримки їхніх дітей у формуванні їхньої власної стійкості до впливу цифрового середовища та моделей поведінки, властивих відповідальним цифровим громадянам. Мета полягає не в тому, щоб перекласти відповідальність за використання ІКТ дітьми лише на батьків, а у визнанні того, що батьки перебувають у більш вигідному становищі для вибору прийнятного матеріалу для своїх дітей і повинні усвідомлювати всі ризики, щоб захистити їх і дати їм можливість діяти.

Інформація може передаватися різними каналами передання інформації як у мережі, так і поза нею, зважаючи на той факт, що деякі батьки не користуються інтернетом. Важливою є співпраця з відділами шкільної освіти в тому, що стосується унесення тем безпеки в цифровому середовищі та відповідального користування ІКТ до навчального плану для дітей та молодих осіб і до суспільних дисциплін для батьків.

Як приклад можна привести роз'яснення, які є доступні типи послуг і можливості для здійснення контролю, які дії можна вчинити, якщо дитина піддається цькуванню або грумінгу в цифровому середовищі, як уникнути спаму і регулювати налаштування конфіденційності, а також як розмовляти з хлопчиками і дівчатками різного віку на делікатні теми. Спілкування - це двосторонній процес, і багато компаній пропонують своїм клієнтам можливість зв'язатися з ними і повідомити про наявні проблеми або обговорити сумніви.

Оскільки обсяги контенту і послуг незмінно збільшуються, рекомендації та нагадування про характер певної послуги і про те, як безпечно нею користуватися, будуть залишатися корисними для всіх користувачів.

Незважаючи на всю важливість навчання дітей способам відповідального використання інтернету, ми знаємо, що діти люблять експериментувати, ризикувати, володіють природною цікавістю і не завжди можуть приходити до кращих рішень. Надаючи їм шанс реалізувати цю потребу, ми сприяємо їхньому зростанню і забезпечуємо здоровий спосіб розвитку самостійності та стійкості до впливів, доки наслідки таких експериментів не є занадто жорсткими. Притому, що дітям необхідно дозволяти приймати певний ризик в цифровому середовищі, вкрай важливо, щоби батьки і компанії надавали їм підтримку в ситуаціях, які стали розвиватися неправильно, пом'якшуючи негативний вплив на неприємний досвід і перетворюючи його на корисний урок на майбутнє.

Передовий досвід: освіта

В Японії канал NHK проводить у Twitter кампанію із запобігання самогубствам серед молоді. Кількість самогубств досягає тут найвищих показників у період, коли діти повертаються до школи після літніх канікул. Причиною цього є повернення до реальності. Продюсерська група NHK Heart Net TV (NHK, Япония) випускає мультимедійну програму #On the Night of August 31st. Об'єднавши телебачення, пряме потокове мовлення і соціальні мережі, NHK успішно створив "місце", де підлітки можуть поділитися своїми почуттями без будь-яких побоювань.

Передовий досвід: освіта

Twitter також опублікувала посібник з медійної грамотності для педагогів. Складений за підтримки ЮНЕСКО, цей підручник, перш за все, призначений допомагати викладачам формувати у молодих поколінь навички медійної грамотності. Ще один аспект роботи Twitter у сфері безпеки пов'язаний з розкриттям інформаційних операцій. Це архів підтримуваних державою інформаційних операцій, до якого Twitter надає відкритий доступ. Ініціатива була започаткована з метою підвищення в академічному і суспільному середовищі рівня розуміння кампаній, пов'язаних із цим питанням, у всьому світі та для забезпечення можливості незалежного стороннього критичного аналізу цих тактик на платформі Twitter.

Проєкт deSHAME, що спільно фінансується Facebook і Європейським Союзом, а також сприяє створенню ресурсів для широкого спектру вікових груп з особливим акцентом на дітях 9-13 років. У межах проєкту було розроблено низку інструментів "Step Up, Speak Up!", що пропонує ряд навчальних матеріалів для підвищення обізнаності, а також практичні інструменти для профілактичної роботи і стратегій реагування в різних секторах. Навчальні матеріали проєкту будуть передаватися до інших країн Європи і партнерам у всьому світі з метою сприяння розумінню своїх цифрових прав серед молоді.

Компанія Google створила низку освітніх ініціатив, ресурсів та інструментів для сприяння підвищенню безпеки молоді в цифровому середовищі. Однією з них є кампанія Be Internet Awesome, присвячена цифровому громадянству і створена у співпраці з такими організаціями, як ConnectSafely, Інститут безпеки сім'ї в цифровому середовищі та Internet Keep Safe Coalition. Ця кампанія спрямована на молодих осіб віком від 8 до 11 років. Вона містить інтернет-гру для молоді (Interland), що навчає їх основам цифрової безпеки і надає ресурси для педагогів за такими темами, як цифрове громадянство і навчальний план з питань безпеки. Навчальний план з питань безпеки пропонує плани уроків за п'ятьма основними тематичними напрямами кампанії, один з яких присвячений кіберцькуванню. Водночас компанія Google створила онлайновий курс щодо цифрового громадянства і безпеки для педагогів, які викладають учням різного віку, надаючи подальшу підтримку для проведення занять із цифрового громадянства і заходів з безпеки в класах. Google також пропонує низку програм для допомоги безпосередньо молоді у сфері безпеки в цифровому середовищі та цифрового громадянства. Глобальна ініціатива Web Rangers є однією з таких програм, що навчають молодь безпеці в цифровому середовищі та сприяють їм у створенні власних кампаній щодо позитивного і безпечного використання інтернету. Є також спеціалізовані країнові програми для молоді, як-от Internet Citizens та Internet Legends у Сполученому Королівстві, створені Google.

У рамах молодіжного обміну новинами "Євробачення" Європейський радіомовний союз поєднує 15 європейських телекомпаній, які обмінюються програмами, форматами та рішеннями в мережі та за її межами. За останні роки навчання цифровій грамотності та попередження дітей про ризики в інтернеті стало основним у цих програмах. Серед найуспішніших ініціатив останніх років є програми реклами і новин у соціальних мережах, прийнятні для дітей, що випускаються Super і Ultra nytt на каналі норвезької громадської радіомовної організації NRK.

Передовий досвід: стратегічні партнерства

У межах проєкту, що підтримується Глобальним фондом із припинення насильства щодо дітей, у 2018 році Capital Humano y Social Alternativo уклав партнерську угоду з Telefónica - найбільшим постачальником послуг інтернету, кабельного мовлення і телефонії з Перу, що обслуговує 14,4 мільйона клієнтів, зокрема понад 8 мільйонів користувачів послуг мобільного зв'язку Movistar.

В рамах цього плідного партнерства було проведено кілька заходів:

- **Віртуальний курс із захисту дитини в цифровому середовищі** був розроблений Telefónica за технічної підтримки Capital Humano y Social Alternativo. Цей курс тепер відкритий для загального доступу на веб-сайті Telefónica, і компанія відстежує кількість осіб, які зареєструвалися та успішно його закінчили. Міністерство освіти Перу погодилося опублікувати посилання на цей курс на своєму офіційному веб-сайті.
- **Буклет щодо безпеки в інтернеті** був розроблений Capital Humano y Social Alternativo і поширений Telefónica через більш ніж 300 центрів продажів послуг мобільного зв'язку компанії з метою підвищення обізнаності про безпеку в цифровому середовищі та про ризики, пов'язані з СЕНД в інтернеті, серед клієнтів Telefónica.
- **Інтерактивна гра про СЕНД в цифровому середовищі** була створена Telefónica за технічної підтримки Capital Humano y Social Alternativo для того, щоб клієнти могли грати в неї, чекаючи своєї черги в точках продажу компанії.

Услід за успішним досвідом співпраці з Telefónica, Capital Humano y Social Alternativo уклало партнерську угоду з постачальником послуг інтернету і кабельного телебачення **Econocable**, що обслуговує клієнтів у віддалених районах Перу і районах з низьким рівнем доходу.

3.5 Сприяння розвитку цифрових технологій як засобу посилення участі в житті громадянського суспільства

Стаття 13 Конвенції ООН про права дитини говорить: "Дитина має право вільно висловлювати свою думку; це право охоплює свободу шукати, отримувати і передавати будь-яку інформацію та ідеї, незалежно від кордонів, в усній, письмовій чи друкованій формі, у формі творів мистецтва чи за допомогою інших засобів на вибір дитини". Компанії можуть висловити свою повагу до громадянських і політичних прав дітей, створивши умови, в яких технології та реалізація законодавчих і політичних норм, розроблені з метою захисту дітей та молоді від шкоди в цифровому середовищі, не мають непередбачуваних наслідків, що ведуть до придушення їх права на участь і висловлення своєї думки або позбавляють їх доступу до інформації, важливої для їхнього добробуту. У системах перевірки віку дуже важливо забезпечити відсутність урізання природних потреб певних вікових груп у доступі до контенту, що відповідає їхньому розвитку.

Водночас бізнес і індустрія можуть підтримувати права дітей та молоді, пропонуючи механізми та інструменти, що спрощують їхню участь. Вони можуть зробити наголос на можливості інтернету стосовно спрощення позитивної участі в житті громадянського суспільства, стимулювання соціального прогресу та впливу на сталий розвиток і життєздатність спільнот, наприклад, через участь в соціальних кампаніях і кампаніях щодо захисту довкілля, а також за допомогою забезпечення підзвітності всіх відповідальних осіб. Маючи у себе правильні інструменти та інформацію, діти та молодь опиняються у більш вигідній ситуації стосовно доступу до можливостей охорони здоров'я, освіти і працевлаштування, а також в аспекті вираження своєї думки і потреб у школі, суспільстві та країні. Вони отримують можливості доступу до інформації про свої права і можуть шукати інформацію з питань, що зачіпають їх особисто, як-от їхнє сексуальне здоров'я або відповідальність політиків та уряду.

Компанії також можуть вкладати кошти у створення онлайнового досвіду, прийнятного для дітей та молодих осіб з їхніми родинами. Вони можуть підтримувати розвиток технології та контенту, що заохочує і дає дітям та молоді можливість вчитися, творити і пропонувати рішення. Їхня продукція завжди має створюватися з огляду на принцип проєктованої безпеки.

Водночас компанії можуть вжити запобіжних заходів для підтримки прав дітей та молоді через роботу над усуненням цифрового розриву. Участь дітей та молоді вимагає цифрової грамотності - здатності розуміти та вміння взаємодіяти у цифровому світі. Без такої здатності громадяни не зможуть брати участь у безлічі соціальних функцій, які перейшли до цифрової площини, як-от подання податкових декларацій, підтримка політичних кандидатів, підписання онлайнових петицій, реєстрація народження дітей або простий доступ до комерційної, освітньої, культурної інформації або інформації, що стосується власного здоров'я. Через загальну бездіяльність прірва між громадянами, здатними користуватися такими форумами, і тими, у кого немає такої можливості через відсутність доступу до інтернету або цифрову безграмотність, буде дедалі збільшуватися, ставлячи останню групу в дедалі більш невигідне становище. Компанії можуть підтримувати мультимедійні ініціативи з розвитку цифрових навичок, необхідних дітям та молоді для того, щоб почуватися впевнено, відчувати свою причетність і проявляти активну позицію в житті громадянського суспільства . У багатьох країнах за останні роки підвищення цифрової та медійної грамотності та зусилля щодо усунення цифрового розриву стали частиною місії громадських засобів масової інформації. Так, парламент Італії запропонував національним

радіомовним організаціям поставити усунення цифрового розриву і забезпечення захисту дитини як в цифровому середовищі, так і в реальному світі на одне з перших місць - приклад, який варто запозичити іншим країнам.

Передовий досвід: міжустановче співробітництво

Нещодавно компанія Microsoft приєдналася до глобальної кампанії Power of ZERO, що проводиться організацією No Bully з метою допомоги дітям і дорослим, які про них піклуються, навчитися користуватися цифровими технологіями і висловлювати свою думку, співчуття та інклюзивність, що становлять основу цифрового громадянства. Ініціатива пропонує педагогам, які працюють з дітьми молодшого віку (кампанія спрямована на дітей, молодших за 8 років), і родинам безкоштовні навчальні матеріали для допомоги під час формування "12 здібностей добра" (визначених Power of Zero 12 життєво важливих навичок або "здібностей", що дозволяють дітям успішно орієнтуватися як в цифровому середовищі, так і реальному світі, зокрема навички стійкості, поваги, інклюзивності та творчості) і створення міцної основи, починаючи з молодого віку.

4. Загальні Рекомендації для індустрії

У Таблиці 1 наведені загальні Рекомендації для індустрії стосовно виявлення, запобігання і пом'якшення будь-яких несприятливих впливів продуктів і послуг на права дітей та молоді, а також щодо сприяння позитивному використанню ІКТ дітьми та молодими особами.

Зауважте, що всі кроки, наведені в Таблиці 1, можна застосувати до всіх компаній та послуг, і вони не є обов'язковими кроками для кожної окремої послуги, згаданої у цій Таблиці. Загальні Рекомендації для індустрії доповнюються контрольними переліками за окремими функціями (див. розділ 5) і навпаки. Контрольні переліки за окремими функціями, наведені у Таблицях 2-5, висвітлюють додаткові кроки, що є найбільш прийнятними для окремих послуг. Слід зазначити, що контрольні переліки за окремими функціями можуть перетинатися у певних аспектах і що одна і та сама послуга може зіставлятися відразу з декількома списками.

Таблиця 1 - Загальні Рекомендації для індустрії

Унесення положень про права дитини до всіх відповідних корпоративних політик та процесів управління (продовження)	Індустрія може виявляти, запобігати і послаблювати несприятливий вплив ІКТ на права дітей та молоді, а також визначати можливості для сприяння реалізації прав дітей та молодих осіб, вчиняючи такі дії:
	Призначити конкретну особу та/або групу, відповідальну за проведення цього процесу та що має доступ до всіх необхідних внутрішніх і зовнішніх заінтересованих сторін. Надати такій особі та/або групі повноваження з управління покращенням профілю захисту дитини в цифровому середовищі в межах компанії.
	Розробити політику захисту та охорони дітей та/або додати конкретні пункти про ризики та можливості, пов'язані з правами дітей та молоді, до документів, що визначають загальнокорпоративні зобов'язання (наприклад, з прав людини, конфіденційності, маркетингу або відповідних кодексів поведінки).
	Увести процедури належного виконання з питань захист дітей у цифровому середовищі у чинні межі забезпечення прав людини і оцінення ризику (наприклад, на корпоративному рівні, на рівні продукції та технологій та/або на рівні країни) з метою виявлення можливого несприятливого впливу або сприяння такому впливу з боку діяльності компанії або індустрії, або встановлення можливого прямого зв'язку між несприятливим впливом та діями компанії, її продукцією, послугами або діловими стосунками.
	Визначити вплив на права дитини в різних вікових групах, обумовлений діяльністю компанії, проєктуванням, розробленням та впровадженням продукції та послуг, а також встановити можливості щодо підтримки прав дітей та молоді.

Унесення положень про права дитини до всіх відповідних корпоративних політик та процесів управління (продовження)	Прийняти такий підхід до захисту дитини, що ґрунтується на розширенні прав і можливостей та навчанні. Враховувати права дітей на захист даних, їхні права на конфіденційність і свободу висловлювань, водночас пропонуючи навчання та інструкції стосовно послуг компанії.
	Спираючись на рекомендації внутрішніх та зовнішніх експертів і консультуючись з головними заінтересованими особами, зокрема з дітьми та молоддю, з питання механізмів забезпечення безпеки дитини в цифровому середовищі, встановити способи отримання постійного зворотного зв'язку та інструкцій стосовно підходів, які використовуються компанією.
	У державах з недостатньо визначеними законодавчими рамами у сфері захисту прав дітей та молоді на конфіденційність і вільне висловлення своєї думки компаніям слід дотримуватися більш суворих правил належного виконання, щоб забезпечити відповідність своїх політик і процедур міжнародним стандартам. Див. Резолюцію Генеральної Асамблеї ООН 68/167 про право на недоторканість особистого життя у цифровому столітті.
	Забезпечити доступ до засобів захисту, запровадивши на оперативному рівні механізми розгляду скарг та зворотного зв'язку стосовно всіх випадків порушень прав дитини (наприклад, щодо CSAM, неприйнятного контенту або контактів, втручання в особисте життя). Призначити менеджера з питань політики захисту дітей або іншу відповідальну особу, до якої можна буде звертатися стосовно проблем захист дітей у цифровому середовищі . Якщо дитина перебуває під загрозою заподіяння йому шкоди, менеджер з питань політики захисту дітей повинний негайно повідомити відповідні органи. Наприклад, в редакторських керівних настановах BBC (2019 р.) зазначено, що призначення менеджера з питань політики захисту дітей є обов'язковим у сфері громадських засобів масової інформації.

Розроблення галузевих стандартів захисту дітей в онлайновому середовищі	Створити і впровадити стандарти компанії та індустрії щодо захисту дітей та молоді з огляду на галузеву специфіку та характеристики.
Розроблення стандартних методів CSAM	Спільно з державними та правоохоронними органами, представниками громадянського суспільства та "гарячих ліній" індустрія відіграє важливу роль у боротьбі з матеріалами, що містять СЕНД, вчиняючи такі дії:
	Заборонити завантаження, публікацію, передачу, обмін або надання відкритого доступу до контенту, що порушує права будь-якої зі сторін або вимоги місцевого, регіонального, національного або міжнародного законодавства.
	Поширити серед національних правоохоронних органів або національних "гарячих ліній" інформацію про передачу повідомлень про CSAM негайно, щойно про них стає відомо передавальному. Забезпечити наявність внутрішніх процедур, спрямованих на виконання передбачених місцевим та міжнародним законодавством вимог щодо передання таких повідомлень. Якщо компанія працює на ринку з менш розвиненою системою регуляторного і правоохоронного нагляду в цій індустрії, вона може подавати свою інформацію до Міжнародної асоціації гарячих ліній в інтернеті (INHOPE), через яку можна передавати повідомлення на будь-яку міжнародну гарячу лінію.

Розроблення стандартних методів поводження з CSAM (продовження)	Встановити внутрішні процедури, що забезпечують відповідність місцевому та міжнародному законодавству з боротьби з CSAM. Створити вищу керівну посаду або відділ із впровадження таких процедур в структурі організації. Після чого члени індустрії зобов'язані будуть уносити відомості про вжиті заходи та досягнуті результати роботи такого відділу до своїх щорічних корпоративних звітів та звітів зі сталого розвитку. За відсутності достатнього захисту на рівні національних законодавчих норм, компанії повинні, шануючи національне законодавство, дотримуватися більш суворих вимог і використовувати власні важелі впливу для лобіювання змін у структурі законодавства, що дозволять індустрії ефективно боротися з CSAM. Необхідно створити вищу керівну посаду або відділ в структурі організації з інтегрування таких процесів і контролю за їх виконанням. Їхня робота має бути прозоро відображена у щорічних корпоративних звітах та звіті зі сталого розвитку, і відповідна інформація має бути відкритою для широкого загалу. Закріпити всебічне співробітництво з правоохоронними органами під час розслідування випадків виявлення або повідомлення про незаконний контент і визначити деталі відповідних заходів відповідальності, як-от штрафів або скасування пільгової оплати послуг.
	Закріпити всебічне співробітництво з правоохоронними органами під час розслідування випадків виявлення або повідомлення про незаконний контент і визначити деталі відповідних заходів відповідальності, як-от штрафів або скасування пільгової оплати послуг.
	Використовувати норми та умови для клієнтів та/або відповідні правила користування, аби беззаперечно визначити позицію компанії щодо невірного використання її послуг з метою збереження або обміну CSAM і наслідків таких зловживань.
	Створити систему оповіщення та вимикання, а також процеси зворотного зв'язку, що дозволяють користувачам повідомляти про CSAM або неприйнятний контакт і зазначати конкретний профіль/розташування, де був виявлений такий контент. Затвердити процеси подальшого контролю повідомлень, узгодити процедури збирання доказів і негайного видалення або блокування доступу до CSAM. Забезпечити, за необхідності, звернення постачальників послуг за консультацією до фахівців (наприклад, до національних органів захист дітей у цифровому середовищі) перед знищенням незаконного контенту. Переконатися, що відповідні треті особи, з якими компанія встановила договірні відносини, застосовують аналогічні надійні процедури оповіщення і вимкнення.
	Бути готовими вживати заходів щодо CSAM і повідомляти про них відповідним органам влади. Якщо стосунки між правоохоронними органами та національною "гарячою лінією" ще не налагоджені, працювати з ними щодо спільного розроблення відповідних процесів.
	Працювати з внутрішніми службами, зокрема з відділом із роботи з клієнтами, відділом з профілактики шахрайства та службою охорони з метою забезпечення можливості повідомляти про ймовірний незаконний контент безпосередньо правоохоронним органам і на "гарячі лінії". В ідеалі така процедура не повинна піддавати виконавчий персонал впливу шкідливого контенту, а також не повинна сприяти повторному насильству над потерпілою дитиною/потерпілими дітьми і молодими особами. Для тих ситуацій, коли співробітники можуть піддаватися впливу образливого матеріалу, встановити правила або впровадити програму підтримки для відновлення їхнього морального здоров'я, безпеки і добробуту.

Розроблення стандартних методів поводження з CSAM (продовження)	Увести правила утримування і збереження даних з метою надання підтримки правоохоронним органам такими діями як збирання доказів у розслідуванні кримінальних справ. Документально оформити політики компанії щодо поводження з CSAM, починаючи з моніторингу та закінчуючи остаточним перенесенням і знищенням контенту. Додати до складу документів перелік працівників, відповідальних за виконання різних операцій з матеріалами.
	Сприяти впровадженню механізмів зворотного зв'язку щодо CSAM і переконатися, що клієнти знають, як повідомити про факт виявлення таких матеріалів. За наявності національної гарячої лінії, зазначити посилання на неї на корпоративному веб-сайті та в усьому відповідному контенті, що поширюється компанією.
	Використовувати всі відповідні служби/дані для запобігання поширенню відомого контенту, пов'язаного із сексуальними зловживаннями щодо дітей, в межах їхніх послуг або платформ.
	Регулярно і активно проводити оцінювання всього контенту, що міститься на серверах компанії, зокрема комерційний контент (як такий, що має оригінальний фірмовий вміст, так і отриманий за договорами з третіми сторонами-постачальниками). Обміркувати застосування таких інструментів, як сканування геш-індексів зображень, пов'язаних із сексуальними зловживаннями щодо дітей, програм розпізнавання зображень або блокування URL з метою вжиття заходів щодо поводження з CSAM.
Створення більш безпечного онлайнового середовища, що відповідає віку	Індустрія може надати допомогу у створенні більш безпечного, більш захопливого цифрового середовища для дітей та молоді будь-якого віку такими діями:
	Запровадити принципи безпеки і проєктованої конфіденційності в технологіях і послугах компанії та вирізнити як пріоритетні ті рішення, що дозволяють зменшити обсяг даних, пов'язаних з дітьми, до мінімуму.
	Застосовувати проєктування з огляду на вік у пропонованих послугах. Надавати дітям інформацію про правила сайту в доступній і відповідній віку формі, зазначаючи прийнятну кількість подробиць. Крім відповідних віку і зрозумілих положень і умов, підприємствам індустрії слід так само в зрозумілій формі повідомляти різну інформацію, як-от правила і основні політики. В них слід робити наголос на прийнятній і неприйнятній поведінці в межах послуги, наслідки порушення правил, на специфіці послуги і на тому, на що саме дає згоду користувач, реєструючись у системі. Така інформація має бути, зокрема, спрямована на молодих користувачів, а також на їхніх батьків та опікунів.
	Використовувати умови обслуговування або правила і умови, щоб привернути увагу користувачів до контенту в онлайнових послугах компанії, які можуть бути прийнятними не для всіх вікових груп. Правила та умови також повинні визначати чіткі механізми зворотного зв'язку і розгляду випадків порушення встановлених правил.

Створення більш безпечного онлайнового середовища, що відповідає віку (продовження)	Розглягути надання механізмів, наприклад, програм батьківського контролю та інших інструментів, що дають батькам і опікунам можливість керувати доступом дітей до інтернет-ресурсів, водночас інструктуючи їх про правильне використання таких засобів, щоб уникнути порушення прав дітей. До них належать чорні/білі списки, фільтри контенту, моніторинг використання, керування контактами і обмеження часу/програм.
	Пропонувати прості у використанні інструменти батьківського контролю, що дозволяють батькам і опікунам обмежувати певні послуги і контент, до яких діти можуть мати доступ через електронні пристрої. Такі обмеження можуть охоплювати керування на рівні мережі та пристрою, а також керування застосунками. З огляду на те, що це має великий вплив на здатність дитини розвивати свої цифрові навички і погіршує їхні можливості в цифровому середовищі, такі засоби керування слід розробляти для дітей наймолодшого віку відповідно до рівня їхнього розвитку і за умови правильного інструктування батьків.
	По змозі сприяти розвитку національних служб підтримки, куди батьки та опікуни можуть повідомити про порушення і звернутися по допомогу у разі насильства та експлуатації.
	Уникати шкідливого або неприйнятного рекламного контенту в інтернеті й встановити зобов'язання повідомляти клієнтам інформацію про послуги, контент яких призначений для дорослої аудиторії та може виявитися шкідливим для дітей і молодих осіб. Шкідливою рекламою, зокрема, можна вважати рекламу продуктів харчування та напоїв з високим вмістом жирів, цукру або солі. Узгодити методи ведення бізнесу з нормами та рекомендаціями щодо методів маркетингу і реклами для дітей та молоді. Контролювати, де, коли і як діти та молодь можуть зіткнутися з потенційно шкідливими рекламними повідомленнями, призначеними для іншого сегменту ринку.
	Забезпечити відповідність політики збирання даних із чинними законами, що стосуються особистого життя дітей та молоді, зокрема розгляд необхідності отримання згоди батьків на збирання комерційними підприємствами інформації від дитини або про неї.
	Адаптувати і впровадити посилені параметри конфіденційності за замовчуванням під час збирання, оброблення, збереження, продажу та публікації персональних даних, зокрема інформацію про місцеперебування і найбільш часті перегляди в інтернеті, що стосуються осіб віком до 18 років. Налаштування конфіденційності за замовчуванням та інформація про важливість параметрів конфіденційності повинні відповідати віку користувачів і характеру послуги.
	Застосовувати технічні заходи, як-от відповідні інструменти батьківського контролю, проєктовану конфіденційність, розподіл робочого середовища за віковими групами із захистом контенту паролями, чорні/білі списки, контроль покупок/часу користування, функції за згодою, фільтри і модерування, щоб запобігти доступу малолітніх дітей та впливу на них неприйнятного контенту або послуг. Впроваджувати технології, що можуть визначати вік користувачів і пропонувати їм відповідну версію програми. Для контенту або послуг з віковими обмеженнями, заінтересовані сторони індустрії повинні вживати заходів з перевірки віку користувачів. По змозі використовувати функції перевірки віку для обмеження доступу до контенту або матеріалів, які відповідно до закону або політики компанії призначені лише для осіб певного віку. Також компанії повинні визнавати можливість неправильного використання таких технологій з метою обмеження права дітей та молодих осіб на вільне вираження своїх поглядів і на доступ до інформації, або для загрози їхній конфіденційності.

Створення більш безпечного онлайнового середовища, що відповідає віку (продовження)	Забезпечити стосовно контенту і послуг, які за віком є прийнятними не для всіх користувачів: • класифікацію згідно з національними стандартами та культурними нормами; • відповідність чинним стандартам в еквівалентних засобах інформації; • чітке і добре видиме відображення з метою контролю доступу; • пропозиція (по змозі - разом з підтвердженням віку) чітких умов, що стосуються видалення даних, що ідентифікують особу та одержуються в процесі такої перевірки. Наприклад, стосовно стандартів засобів масової інформації всі органи, що регулюють їхню діяльність, надають низку вимог щодо пов'язаного з віком контенту, і постачальники послуг інтернету зобов'язані адаптувати свої сховища даних і застосовувати такі Рекомендації під час пропонування свого контенту. Див. вимоги Ofcom в Сполученому Королівстві, CSA у Франції та AGCOM в Італії.
	Запропонувати чіткі інструменти зворотного зв'язку і розробити процес подальшого контролю повідомлень про неприйнятний контент, контакт або неправильне використання, а також надати користувачам послуги докладну інформацію про процес зворотного зв'язку.
	Забезпечити попереднє модерування інтерактивних просторів для дітей та молоді методами, що узгоджуються з правами дітей на особисте життя та з їхніми можливостями, що розвиваються. Активне модерування може сприяти формуванню атмосфери, де булінг і домагання є неприйнятними. Прикладами неприйнятної поведінки є: • публікація неприємних або загрозливих коментарів до чийогось профілю; • створення підставних профілів або "сайтів ненависті" для приниження жертви; • розсилання ланцюжків повідомлень і вкладень з наміром завдати шкоди; • злом чужих облікових записів з метою надсилання образливих повідомлень іншим.
	Вжити особливих заходів обережності стосовно штатних або позаштатних співробітників, які працюють з дітьми та молодими особами, і щодо яких може вимагатися попередня перевірка їхнього кримінального минулого у правоохоронних органах.
	Негайно передавати всі ймовірні випадки грумінгу на розгляд онлайновим або інтерактивним групам виконавчого керівництва, що відповідає за повідомлення про них відповідним органам: • повідомляти, по змозі, про грумінг у групу виконавчого керівництва і призначеному менеджеру з питань захисту дітей; • забезпечити користувачам можливість повідомляти про ймовірні випадки грумінгу безпосередньо органам влади; • надати можливість прямого контакту з метою попередження або повідомлення через адреси електронної пошти.
	За будь-яких обставин вважати безпеку і добробут дітей пріоритетом своєї роботи. Завжди діяти професійно і забезпечити відповідність будь-якого контакту з дітьми послузі, програмі, події, заходу або проєкту, що є активними. Ніколи не брати одноособову відповідальність за дитину. Якщо дитині необхідна турбота, попередити про це батьків, опікуна або супровідного. Завжди слухати й поважати дітей. Якщо хтось поводить себе неприйнятно з дітьми - повідомити про таку поведінку місцеве представництво з питань захисту дітей.

Створення більш безпечного онлайнового середовища, що відповідає віку (продовження)	Встановити чіткі правила, що розташовуються на видному місці і, загалом, містять найважливіші моменти положень і умов обслуговування та прийнятних керівних настанов з використання. Правила, складені зрозумілою для користувача мовою, повинні визначати: • характер послуги та очікування стосовно її користувачів; • що є і що не є прийнятним з боку контенту, поведінки та мови, а також заборона незаконного використання; • наслідки відповідно до ступеню вчиненого порушення, як-от повідомлення у правоохоронні органи або призупинення обслуговування облікового запису користувача.
	Спростити для клієнтів процес повідомлення про свої сумніви в зв'язку з неправильним використанням контенту співробітникам відділу з роботи з клієнтами, встановивши стандартний і доступний порядок розгляду різних проблем, як-от отримання небажаних відправлень (наприклад, SMS зі спамом).
	Бути щирими і надавати клієнтам чітку інформацію про характер пропонованих послуг, наприклад, про: • тип контенту/послуги та вартість; • мінімальні вікові вимоги для отримання доступу; • наявність інструментів батьківського контролю, зокрема вказівки про те, які сфери охоплюють (наприклад, мережа) або не охоплюють (наприклад, Wi-Fi) такі засоби контролю, і як навчитися працювати з ними; • тип інформації, що збирається про користувача, і характер її використання.
	Сприяти розвитку національних служб підтримки, що надають дітям та молоді можливість повідомити або звернутися по допомогу в разі, якщо вони піддаються насильству або експлуатації (як-от Міжнародній лінії допомоги дітям).
Навчання дітей, батьків і педагогів правилам дитячої безпеки та відповідального використання ними ІКТ	Індустрія може доповнювати технічні методи діями, спрямованими на підвищення рівня освіти та розширення прав і можливостей, як-от:
	Чітко описати доступний контент і відповідні налаштування батьківського контролю або родинної безпеки. Мова і термінологія, що використовуються, повинні бути доступними, наочними, зрозумілими та значущими для всіх користувачів, зокрема дітей, батьків і опікунів, особливо в тому, що стосується положень і умов, вартості користування контентом або послугами, політики конфіденційності та механізмів зворотного зв'язку.
	Навчити клієнтів, що слід робити в разі сумнівів, пов'язаних з використанням інтернету, зокрема спам, викрадення даних і неприйнятні контакти, як-от булінг та грумінг, і описати, які дії можуть зробити клієнти, і як їм висловити свої сумніви про неприйнятне використання.
	Встановити механізми і навчити батьків, як брати участь у пов'язаних з ІКТ діях дітей та молоді, особливо в наймолодшому віці, наприклад, надати батькам можливість перевіряти налаштування конфіденційності дітей та молодих осіб.
	Співпрацювати с державними та освітніми органами стосовно формування батьківського потенціалу з підтримки дітей та молодих осіб і проведення з ними бесід на тему необхідності бути відповідальними громадянами цифрового суспільства і користувачами ІКТ.

Навчання дітей, батьків і педагогів правилам дитячої безпеки та відповідального використання ними ІКТ	З огляду на місцевий контекст, надати матеріали для шкільного і домашнього використання, спрямовані на підвищення якості використання ІКТ дітьми та молодими особами і розвинення у них критичного мислення, що дозволяє діяти безпечно і відповідально під час користування послугами ІКТ.
	Підтримувати клієнтів через розповсюдження доступних інструкцій з безпеки родини в цифровому середовищі, заохочуючи батьків та опікунів: • знайомитися з продуктами і послугами, якими користуються діти та молодь; • забезпечувати помірне використання електронних пристроїв дітьми та молодими особами, піклуючись про їхній здоровий і збалансований спосіб життя; • приділяти пильну увагу поведінці дітей та молодих осіб, аби своєчасно виявляти зміни, що можуть свідчити про кібербулінг або домагання щодо них.
	Надати батькам необхідну інформацію, що допомагає зрозуміти, як діти та молодь користуються послугами ІКТ, як врегулювати питання, пов'язані зі шкідливим контентом і поведінкою, і як спрямувати дітей та молодих осіб на відповідальне використання. Це завдання можна спростити через використання інструментів і завдяки взаємодії з відділами шкільної освіти у сфері розроблення навчальних програм з безпеки в цифровому середовищі та освітніх матеріалів для батьків.
Використання технологічних досягнень для захисту і навчання дітей	Засоби Штучного Інтелекту для збереження конфіденційності, що розпізнають тексти, зображення, розмови та контекст, здатні виявити і вжити заходів щодо цілої низки шкідливих ситуацій і загроз в інтернеті, використовуючи цю інформацію для розширення можливостей та навчання дітей правилам дій у таких ситуаціях. У разі виконання в середовищі розумного пристрою це може захистити дані та конфіденційність молодих осіб, водночас надаючи їм підтримку.
	Суспільні послуги та національні засоби масової інформації можуть відігравати важливу роль завдяки запропонованим ними програмам (в реальному світі та в цифровому середовищі) з навчання батьків та дітей і доведення до їхнього відома ризиків і можливостей онлайнового світу.
Сприяння просуванню цифрових технологій як засобу збільшення участі в житті громадянського суспільства	Індустрія може заохочувати дітей та молодь і надавати їм відповідні можливості, підтримуючи їхнє право на участь, такими діями:
	Надати інформацію про послугу, підкреслюючи переваги, які діти можуть отримати, якщо будуть вести себе правильно і відповідально, наприклад, будуть використовувати послугу з метою творчості.
	Розробити письмові процедури, що гарантують послідовне впровадження політик і процедур, які захищають свободу вираження поглядів для всіх користувачів, зокрема дітей та молодих осіб, а також документацію відповідно до цих політик.

Сприяння просуванню цифрових технологій як засобу збільшення участі в житті громадянського суспільства	Уникати надмірного блокування законного і відповідним чином створеного контенту. Щоб не допустити неправильного використання запитів та інструментів фільтрації для обмеження доступу дітей та молодих осіб до інформації, забезпечити прозорість інформації про заблокований контент і встановити для користувачів порядок повідомлення про випадкове блокування. Такий порядок має бути доступним для всіх споживачів, зокрема адміністраторів сайтів. Всі процедури зворотного зв'язку повинні забезпечувати встановлення чітких, відповідальних і визнаних умов обслуговування.
	Створити онлайнові платформи, що сприяють реалізації прав дітей та молоді на висловлення своєї думки, спростити їхню участь у суспільному житті та заохочувати співпрацю, підприємництво й громадську участь.
	Розробити освітній контент для дітей та молоді, який заохочує вчитися, творити, думати і вирішувати завдання.
	Сприяти підвищенню цифрової грамотності, створенню потенціалу та розвитку навичок ІКТ у дітей і молодих осіб, особливо у дітей в сільських і недостатньо обслуговуваних районах, аби сприяти використанню ресурсів ІКТ і повноцінній безпечній участі в цифровому світі.
	Співпрацювати з місцевим громадянським суспільством і державними органами з питань національних і місцевих пріоритетів у сфері розширення універсального і рівноправного доступу до ІКТ, платформ і пристроїв, а також розширення інфраструктури, що є їхньою основою.
	Інформувати клієнтів, зокрема батьків, опікунів, дітей та молодих осіб, про пропоновані послуги, залучаючи їх до роботи з ними, наприклад, повідомляти про: • тип контенту та відповідні інструменти батьківського контролю; • механізми зворотного зв'язку у разі прояву насильства, неправомірного використання і неприйнятного або незаконного контенту; • процедури подальшого контролю повідомлень; • типи послуг з віковими обмеженнями; • безпечне й відповідальне використання "власних" інтерактивних послуг компанії.
	Працювати над більш широкими питаннями стосовно безпечного та відповідального цифрового громадянства, як-от питання репутації в цифровому середовищі та цифрової географії, шкідливого контенту та грумінгу. Обміркувати можливість партнерських стосунків з експертами місцевого рівня, зокрема з НДО, благодійними організаціями та виховними групами, що здатні допомогти у створенні звернень та розсилань компанії та охопленні цільової аудиторії.
	Якщо компанія вже працює з дітьми або школами, наприклад, в межах корпоративних програм соціальної відповідальності, з'ясувати, чи можна розширити таку діяльність, додавши до неї навчання дітей та молоді, а також педагогів , методам захист дітей у цифровому середовищі .
Інвестування в дослідження	Інвестувати в побудовані на доказах дослідження і поглиблений аналіз цифрових технологій, впливу технологій на дітей, захисту дітей та прав дитини щодо цифрового оточення, щоб інтегрувати онлайнові системи захисту в послуги, які використовуються дітьми та молодими особами, і краще зрозуміти, які типи втручання є найбільш ефективними з огляду на поліпшення дитячого досвіду в інтернеті.

Типологія компаній ІКТ

Притому, що ці Рекомендації МСЕ призначені для індустрії ІКТ в цілому, важливо визнати, що послуги, пропоновані компаніями ІКТ, способи здійснення їхньої діяльності, регуляторні схеми, в межах яких вони функціонують, обсяг і масштаби пропозиції значно різняться. Всі технологічні компанії, чиї продукти та послуги спрямовані безпосередньо або опосередковано на дітей, можуть отримати користь із загальних принципів, викладених вище, адаптуючи їх залежно від своєї конкретної сфери діяльності. Основна ідея полягає у підтримці та спрямуванні індустрії ІКТ в аспекті здійснення правильних заходів для поліпшення захисту дітей в цифровому середовищі від ризиків завдання шкоди, водночас наділяючи їх правами та можливостями для навігації по інтернет-простору найбільш прийнятними способами. Наведена нижче типологія допоможе краще зрозуміти деякі цільові аудиторії й те, як вони зіставляються з контрольними переліками, що містяться в наступному розділі. Необхідно відзначити, що це лише деякі конкретні приклади категорій, перелік яких не є вичерпним:

a) постачальники послуг інтернету, зокрема послуг фіксованих наземних широкосмугових мереж або послуг передання даних стільниковими мережами операторів мобільного зв'язку: зважаючи на те, що, як правило, такі послуги пропонуються на відносно довгострокових засадах за абонентськими угодами, вони також можуть поширюватися на компанії, що надають послуги безкоштовних або платних громадських точок доступу Wi-Fi;
b) соціальні мережі/платформи обміну повідомленнями та онлайнових ігор;
c) виробники апаратного та програмного забезпечення, як-от постачальники портативних пристроїв, зокрема мобільних телефонів, ігрових консолей, побутових приладів з голосовими помічниками, дитячих іграшок із вбудованими пристроями інтернету речей і розумного з'єднання з інтернетом.
d) компанії, що надають цифрові засоби (створюють або публікують контент, надають доступ);
e) компанії, що надають послуги потокового передання даних, зокрема пряме потокове мовлення;
f) компанії, що пропонують послуги цифрового сховища файлів, постачальники хмарних послуг.

5. Контрольні переліки за окремими функціями

У цьому розділі наведений раніше загальний контрольний перелік для індустрії доповнюється рекомендаціями щодо поваги та підтримки прав дитини в цифровому середовищі для компаній, що надають послуги з певними функціями. У цих контрольних списках за окремими функціями визначені засоби, що доповнюють загальні принципи та підходи, наведені в Таблиці 1, в їх прив'язці до різноманітних послуг. Тому їх слід вважати додатком до дій, які наведені в Таблиці 1.

Приведені тут функції накладаються одна на одну, і може бути так, що до однієї компанії застосовуються відразу кілька переліків.

Наступні переліки за функціями організовані за тими самими основними сферами, що і загальні Рекомендації в Таблиці 1. Кожний з контрольних переліків за функціями розроблений у співпраці з основними співавторами, через що в таблицях відзначаються лише незначні варіації.

5.1 Функція А: надання послуг встановлення з’єднань, збереження і публікування даних

Доступ до інтернету є основою реалізації прав дітей, і можливість встановлення з’єднань може відрити для дитини цілий світ. Постачальники послуг встановлення з’єднань, збереження і публікування даних мають величезні можливості щодо забезпечення безпеки та конфіденційності в межах своїх пропозицій для дітей та молоді. Послуги цієї категорії охоплюють, зокрема, операторів мобільного зв’язку, постачальників послуг інтернету, системи збереження даних і служби публікування даних.

Оператори мобільного зв’язку надають доступ до інтернету та цілу низку послуг, пов’язаних зі стільниковими технологіями передавання даних. Багато операторів вже затвердили кодекси захист дітей у цифровому середовищі і пропонують цілу низку інструментів та інформаційних ресурсів на підтримку виконання своїх зобов’язань.

Більшість постачальників послуг інтернету є водночас посередниками, що надають доступ до інтернету та з інтернету, і репозиторієм, який надає послуги головного вузла, а також послуги з гешування та збереження даних. Отже, вони несуть основну відповідальність стосовно захисту дітей в цифровому середовищі.

Доступ до інтернету в громадських місцях

Дедалі частіше муніципальні служби, роздрібні підприємства, транспортні компанії, мережеві готелі та інші комерційні підприємства і організації надають доступ до інтернету через бездротові точки доступу Wi-Fi. Такий доступ зазвичай надається безкоштовно або за незначну плату та іноді - з мінімальними вимогами щодо реєстрації, і використовується громадськими організаціями або компаніями для принадження клієнтів до своїх помешкань або для переконання більшого числа людей користуватися їхніми послугами.

Просування Wi-Fi - це ефективний спосіб забезпечення доступності інтернету в певному регіоні. Проте в громадських місцях, які часто відвідують діти, слід вживати певних запобіжних заходів. Користувачі повинні пам'ятати, що сигнали Wi-Fi можуть бути відкритими для всіх, хто йде повз, наражаючи на ризик їхні особисті дані. Отже, постачальники послуг Wi-Fi не завжди мають можливість підтримувати або контролювати використання наданого ними інтернет-з'єднання, і користувачі самі повинні вживати заходів, щоб уникнути обміну важливою інформацією через загальнодоступні точки Wi-Fi.

Постачальники послуг Wi-Fi в громадських місцях можуть розглянути можливість застосування додаткових заходів захисту дітей та молоді, зокрема:

- окрім зусиль щодо блокування доступу до CSAM, здійснювати запобіжні заходи з метою блокування доступу до веб-адрес, які, згідно з наявною інформацією, містять контент, неприйнятний для широкої аудиторії;
- унести до положень та умов обслуговування пункти, що забороняють використання послуги Wi-Fi для доступу або демонстрації матеріалів, які можуть бути неприйнятними в середовищі, де є діти. Положення та умови також повинні визначати чіткі механізми дії стосовно ліквідації наслідків порушення таких правил;
- вжити всіх заходів щодо захисту від несанкціонованого доступу, який може призвести до маніпуляцій або втрати персональних даних;
- встановити фільтри в системі Wi-Fi, щоб посилити дію правил стосовно неприйнятних матеріалів;
- розробити процедури і програмне забезпечення для позначення і пропонування додаткових інструментів батьківського контролю стосовно доступу дітей та молодих осіб до контенту в інтернеті.

Передовий досвід: Система регулювання електрозв'язку в багатьох країнах - членах Європейського Союзу зокрема передбачає, що доступ до мереж має ідентифікуватися за допомогою окремої SIM-карти або інших інструментів ідентифікації.

У Таблиці 2 наводяться Рекомендації для постачальників послуг встановлення з'єднань, збереження і публікування даних щодо дій, спрямованих на посилення захисту та участі дитини в цифровому середовищі.

Таблиця 2 - Контрольний перелік щодо захист дітей у цифровому середовищі для функції А: надання послуг встановлення з'єднань, збереження і публікування даних

Унесення положень про права дитини до всіх відповідних корпоративних політик та процесів управління	Постачальники послуг встановлення з'єднань, збереження і публікування даних можуть виявляти, запобігати й послаблювати несприятливий вплив ІКТ на права дітей та молоді, а також визначати можливості для сприяння реалізації прав дітей та молодих осіб.
	Див. загальні Рекомендації в Таблиці 1.
Розроблення стандартних методів поводження з CSAM	Співпрацювати з державними та правоохоронними органами, представниками громадянського суспільства та гарячими лініями з метою ефективного врегулювання питань, спричинених CSAM, і повідомлення про факти їхньої появи відповідним органам. Якщо стосунки між правоохоронними органами та гарячою лінією ще не налагоджені, працювати з ними щодо спільного створення відповідних процесів. Постачальники послуг встановлення з'єднань, збереження і публікування даних також можуть проводити навчання щодо ІКТ для правоохоронних органів.
	Якщо компанія працює на ринку з менш розвиненою системою регуляторного і правоохоронного нагляду в цій індустрії, вона може подавати свою інформацію до Міжнародної асоціації гарячих ліній в інтернеті (INHOPE), через яку можна передавати повідомлення на будь-яку міжнародну гарячу лінію.
	Обміркувати можливість застосування визнаних на міжнародному рівні чорних списків URL або веб-сайтів, складених відповідними органами (наприклад, національними правоохоронними органами або гарячими лініями, Cybertip Canada, Інтерполом, IWF), щоб ускладнити користувачам доступ до вже встановлених CSAM.
	Розробити процеси оповіщення, вимикання і повідомлення, і зв'язати повідомлення про зловживання з цими процесами відповідно до відкритої угоди про процедури реагування і часу вимкнення контенту. Див., наприклад, Посібник ЮНІСЕФ та Асоціації GSM щодо політик і методів оповіщення і вимикання.
	Встановити механізм зворотного зв'язку з чіткими інструкціями щодо його використання, наприклад, надати інструкції щодо незаконного контенту і поведінки, про які необхідно повідомляти, і роз'яснювати, які матеріали не можна додавати до повідомлення, щоб не допустити їх подальшого поширення в мережі.

Розроблення стандартних методів поводження з CSAM	Підтримувати правоохоронні органи у проведенні кримінальних розслідувань такими діями, як-от збирання доказів. Встановити в правилах і умовах обслуговування заборону на використання послуг для збереження/обміну або поширення CSAM. Переконатися, що в таких правилах недвозначно визначена абсолютна неприйнятність CSAM. Чітко зазначити у правилах і умовах обслуговування, що компанія буде повністю співпрацювати з правоохоронними органами під час проведення розслідувань у разі виявлення CSAM або повідомлення про нього.
	Наразі є два рішення для зворотного зв'язку щодо онлайнових CSAM на національному рівні: гарячі лінії та портали повідомлень. Повний актуальний перелік усіх наявних гарячих ліній та порталів можна знайти на сайті INHOPE. Гарячі лінії: За відсутності національної гарячої лінії, обміркувати методів поводження з CSAM можливості для її створення. Всю інформацію про варіанти можна знайти (продовження) у Практичному посібнику Асоціації GSM щодо гарячих ліній INHOPE, зокрема співпрацю з INHOPE і Фондом INHOPE. Є також інтерактивна версія посібника Асоціації GSM INHOPE, що містить інструкції, як розробити внутрішні процеси для персоналу служби підтримки клієнтів стосовно повідомлень про сумнівний контент у правоохоронні органи та INHOPE. Портали повідомлень: IWF пропонує рішення, що дає можливість користувачам інтернету в країнах і державах, які не мають власних гарячих ліній, повідомляти про зображення і відеоматеріали, що можуть бути пов'язані із сексуальними зловживаннями щодо дітей, в IWF через спеціалізовану сторінку онлайнового порталу.
	Постачальникам послуг встановлення з'єднань, збереження і публікування даних, чиї послуги припускають публікування певного типу контенту (багатьох це не стосується), необхідно запровадити процеси оповіщення і вимикання.
Створення більш безпечного, відповідного віку цифрового середовища	Постачальники послуг встановлення з'єднань, збереження і публікування даних можуть надати допомогу у створенні більш безпечної, більш захопливої цифрового середовища для дітей різного віку такими діями:
	Постачальники послуг збереження/публікування даних повинні обміркувати можливість надання функції зворотного зв'язку на всіх сторінках сайту і в межах відповідних послуг, та розробити і оформити документально чіткі процеси швидкого оброблення повідомлень про зловживання або інші порушеннях правил і умов.
	Постачальники послуг встановлення з'єднань повинні пропонувати власні технічні засоби контролю і позначення наявних інструментів, які створені спеціалізованими постачальниками, відповідають пропонованим послугам і є зручними для користувачів, а також пропонувати можливість блокування або фільтрації доступу до інтернету через мережі компанії. Встановити прийнятні механізми перевірки віку, якщо компанія пропонує контент або послуги (зокрема власні послуги або послуги третіх сторін, що рекламуються компанією), які є правомірними або прийнятними лише для дорослих користувачів (як-от певні види ігор, лотереї).

Навчання дітей, батьків і педагогів правилам дитячої безпеки та відповідального використання ними ІКТ	Постачальники послуг встановлення з'єднань, збереження і публікування даних повинні дублювати основні моменти своїх правил і умов у керівних настановах для спільноти, написаних зрозумілою користувачам мовою, з метою підтримки дітей та їхніх батьків або опікунів. У межах самої послуги в місці завантаження контенту розмістити нагадування про те, які типи контенту можуть вважатися неприйнятними.
	Забезпечити дітей та молодих осіб інформацією щодо більш безпечного використання інтернету. Творчо підходити до поширення важливої інформації, користуючись, наприклад, такими формулюваннями: "Ніколи не надавай контактну інформацію, зокрема відомості про своє фізичне місцеперебування та свій номер телефону, людям, яких ти особисто не знаєш". "Ніколи не погоджуйся на зустріч із людиною, з якою ти знайомишся в інтернеті, попередньо не порадившись із дорослим. Обов'язково скажи своєму другові, якому ти віриш, куди саме ти йдеш ". "Не відповідай на залякувальні, непристойні або образливі повідомлення, але збережи доказ - не видаляй такі повідомлення". "Якщо ти почуваєшся стурбовано або ніяково через щось або когось, розкажи про це дорослому або другові, якому віриш". "Ніколи нікому не називай свій пароль до облікового запису або ім'я користувача! Пам'ятай, що інші люди в інтернеті можуть шельмувати, аби переконати тебе поділитися своєю персональною інформацією".
	Постачальники послуг можуть об'єднувати зусилля з організаціями, що мають необхідні ресурси для навчання і підтримки дітей стосовно більш безпечного використання інтернету та інших пов'язаних з цим питань. Приклади див. у практичному посібнику Міжнародної лінії допомоги дітям і Асоціації GSM для гарячих ліній допомоги дітям і операторів мобільного зв'язку: спільна робота заради захисту прав дітей.
Сприяння просуванню цифрових технологій як засобу посилення участі у житті громадянського суспільства	Див. загальні Рекомендації в Таблиці 1.

5.2 Функція B: пропонування відібраного цифрового контенту

Інтернет пропонує найрізноманітніші варіанти контенту і діяльності, багато з яких призначені для дітей та молоді. Компанії, що надають спеціально підібраний контент, мають величезні можливості щодо забезпечення безпеки та конфіденційності в межах своїх пропозицій для дітей та молоді.

До цієї категорії належать як компанії, що створюють власний контент, так і ті, що надають доступ до цифрового контенту. Її складають, зокрема, послуги новин і мультимедійного потокового мовлення, національні та суспільні радіомовні організації, а також представники ігрової індустрії.

У Таблиці 3 наводяться Рекомендації для компаній, що пропонують спеціально підібраний контент, стосовно політик і дій, спрямованих на підвищення захисту та участі дитини в цифровому середовищі.

Таблиця 3 - Контрольний перелік щодо захист дітей у цифровому середовищі для функції B: пропонування відібраного цифрового контенту

Унесення положень про права дитини до всіх відповідних корпоративних політик та процесів управління	Компанії, що пропонують спеціально підібраний контент, можуть виявляти, запобігати і послаблювати несприятливий вплив ІКТ на права дітей та молоді, а також визначати можливості для сприяння реалізації прав дітей та молодих осіб такими діями:
	Розробити політики, що оберігають добробут дітей та молоді, які поповнюють онлайновий контент, враховуючи фізичний та емоційний добробут і гідність молодих осіб віком до 18 років, які беруть участь у програмах, фільмах, іграх, новинах тощо незалежно від згоди, яка може надаватися одним із батьків або іншим дорослим.
Розроблення стандартних методів поводження з CSAM	Спільно з державними та правоохоронними органами, представниками громадянського суспільства та гарячих ліній компанії, що пропонують спеціально підібраний контент, можуть відігравати важливу роль у боротьбі з CSAM такими діями: У випадках CSAM, які зокрема передаються через функції "коментарів" або "оглядів", де користувачі можуть вивантажувати свій контент, персонал повинний зв'язуватися з виконавчим керівництвом, що відповідає за повідомлення про такі матеріали до відповідних органів. Окрім того, необхідно: • негайно сповістити національні правоохоронні органи; сповістити свого керівника і повідомити про такі матеріали менеджеру з питань політики захисту дітей; • звернутися до служби внутрішніх розслідувань по телефону або електронною поштою, зазначивши подробиці інциденту, та спитати поради; • дочекатися рекомендацій відповідного органу, перш ніж видаляти матеріал, зберігати його в середовищі, відкритому для загального доступу, або пересилати його.

Розроблення стандартних методів поводження з CSAM	Якщо матеріал вже ідентифікований, про нього необхідно повідомити безпосередньо в організацію, що спеціалізується на питаннях безпеки в інтернеті та в обслуговчу систему зворотного зв'язку гарячої лінії, куди члени громадських організацій та професіонали у сфері інформаційних технологій можуть повідомляти про особливі форми потенційно незаконного онлайнового контенту. Так, наприклад, на основі своєї Політики захисту та охорони інтересів дітей компанія BBC випустила редакторські Рекомендації щодо взаємодії з дітьми та молодими особами в інтернеті. Компанія також розробила контрольні переліки та кодекси поведінки стосовно роботи з дітьми та молодими особами в інтернеті, які, зокрема, поширюються на субпідрядників та зовнішніх постачальників. У політиці Ofcom щодо захисту дітей для Сполученого Королівства питання онлайнового контенту, мобільних пристроїв та ігрових консолей розглядаються окремо. Впровадити стратегію швидкого та надійного передання справи до інстанцій у випадках, що стосуються публікації CSAM або незаконної поведінки. З огляду на це: • запропонувати користувачам простий та доступний спосіб попередження виробника контенту про порушення будь-яких правил в онлайновій спільноті; • видаляти контент, що порушує правила; • запропонувати користувачам простий та доступний спосіб попередження виробника контенту про порушення будь-яких правил в онлайновій спільноті; • видаляти контент, що порушує правила; Перед вивантаженням спеціально підібраного з огляду на вік контенту на сайт соціальної мережі необхідно ознайомитися з правилами та умовами роботи сайту. Уважно ставитися до вимог щодо мінімального віку доступу на різних сайтах соціальних мереж. Правила та умови роботи кожного онлайнового простору, зокрема, повинні містити чіткі механізми повідомлення про порушення цих правил.

Створення більш безпечного, онлайнового середовища, що відповідає віку	Компанії, що пропонують спеціально підібраний контент, можуть надати допомогу у створенні більш безпечного, більш захопливого цифрового середовища для дітей та молодих осіб будь-якого віку такими діями:
	Працювати з іншими представниками індустрії стосовно розроблення класифікації контенту/систем оцінки віку на основі прийнятних національних і міжнародних стандартів та відповідно до підходів, що застосовуються у схожих засобах інформації. По змозі класифікація контенту має бути узгодженою в межах різних медійних платформ, наприклад, рекламний ролик про фільм у кінотеатрі та на смартфоні слід залічувати до одного класу.
	Розробити дружні до дитини та відповідні віку продукти для дітей і молодих осіб на основі проєктованої безпеки, що доповнюються надійними системами перевірки віку.
	Допомогти батькам та іншим особам визначитися стосовно відповідності контенту віку дітей та молодих осіб, створити програми та послуги в усіх засобах інформації для узгодження із системами оцінювання контенту. Застосувати відповідні методи підтвердження віку, щоб запобігти доступу дітей та молоді до контенту, сайтів або онлайн-послуг, неприйнятних для певного віку. Передбачити рекомендації та нагадування про характер і вікову класифікацію контенту, що використовується.
	Компанія, що пропонує аудіовізуальні та мультимедійні послуги, може встановити власну систему персональних ідентифікаційних номерів для користувачів, які хочуть отримувати доступ до контенту, потенційно шкідливого для дітей.
	Забезпечити прозорість ціноутворення для продуктів і послуг, а також збирання інформації про користувачів. Забезпечити відповідність політики збирання даних із чинними законами, що стосуються особистого життя дітей та молоді, зокрема розгляд необхідності отримання згоди батьків на збирання комерційними підприємствами інформації від дитини або про неї.
	Забезпечити чітке розпізнавання повідомлень рекламного та комерційного характеру. Контролювати наявний в інтернеті контент і адаптувати його для різних груп користувачів, які найімовірніше будуть переглядати його, зокрема встановивши прийнятні правила онлайнової реклами для дітей та молоді. Якщо запропонований контент містить інтерактивні елементи, як-от коментування, онлайнові форуми, соціальні мережі, ігрові платформи, чати або дошки повідомлень, додати до умов обслуговування та інструкцій для користувачів чіткий набір "внутрішніх правил", викладених зрозумілою клієнтам мовою.
	Перед запуском онлайнової послуги вирішити, який саме рівень участі є бажаним. Послуги, спрямовані на дітей, повинні містити лише той контент, що є прийнятним для юнацької аудиторії. У разі сумнівів можна звернутися по консультацію до національних органів з питань захисту дітей.
	Надати чітке маркування контенту, що спирається на факти. Слід пам'ятати, що користувачі можуть зіткнутися з неприйнятним контентом, переходячи через посилання на сайти третіх сторін в обхід контекстних сторінок.

Навчання дітей, батьків і педагогів правилам дитячої безпеки та відповідального використання ними ІКТ	Компанії, що пропонують спеціально підібраний цифровий контент, можуть доповнити технічні знаряддя навчальними заходами, які розширюють можливості дітей, такими діями:
	Надати клієнтам конкретну й чітку інформацію про контент, зокрема зазначити його тип, вікові оцінки/обмеження, правила щодо грубіянства і насильства поряд із доступними інструментами батьківського контролю, а також про способи повідомлення про неправомірне використання і неприйнятний або незаконний контент, і про порядок опрацювання таких повідомлень. В інтерактивному світі таку інформацію слід надавати у формі маркування контенту за кожною програмою.
	Заохочувати до участі дорослих, особливо батьків, опікунів та педагогів, щодо споживання онлайнового контенту дітьми та молодими особами, щоб допомагати і направляти їх у виборі контенту під час його придбання, а також сприяти формуванню певних правил поведінки. Допомогти дітям (а також батькам та опікунам) навчитися керувати часом, який вони проводять біля екрану монітора, і зрозуміти, як користуватися технологіями, щоб не зашкодити своєму добробуту, зокрема знати, коли слід зупинитися і перемкнутися на щось інше.
	Розробити правила користування, складені зрозумілою і доступною мовою, щоб стимулювати дітей та молодь бути більш пильними і відповідальними під час навігації по інтернету.
	Створити відповідні віку інструменти, як-от навчальні програми та центри допомоги. По змозі співпрацювати з онлайновими або персональними профілактичними програмами та консультаційними клініками. Наприклад, за наявності ризику надмірного залучення дітей та молодих осіб до певних технологій, зокрема ігор, виникнення у них труднощів у формуванні взаємин або участі в корисних для здоров'я фізичних видах діяльності, на сайті можна розмістити посилання на службу допомоги або консультаційний центр. Всю інформацію про безпеку, зокрема посилання на рекомендації, зробити помітною, легкодоступною і зрозумілою в тому разі, якщо досить велика частка онлайнового контенту адресована дітям та юнацтву.
	Запропонувати інструменти батьківського керування, зокрема функцію "блокування" для контролю контенту, доступ до якого можливий через певний браузер.
	Співпрацювати з батьками, щоб гарантувати, що оприлюднена в інтернеті інформація про дітей не несе для них ніякого ризику. Способи ідентифікації дітей в межах спеціально підібраного контенту мають бути продуманими та обумовленими контекстом. По змозі отримувати інформовану згоду дітей у разі їхньої появи у програмах, фільмах, відеоматеріалах, тощо, і поважати їхнє право на відмову від участі.
Сприяння просуванню цифрових технологій як засобу збільшення участі в житті громадянського суспільства	Компанії, що пропонують спеціально підібраний цифровий контент, можуть заохочувати дітей та молодих осіб і надавати їм відповідні можливості, підтримуючи їхнє право на участь, такими діями:
	Створити та/або запропонувати вибір освітнього, захопливого та цікавого контенту високої якості відповідно до віку, який змушує думати, допомагає дітям та молоді і наповнює їхній довколишній світ сенсом. Окрім своєї привабливості та корисності, надійності та безпеки, такий контент може сприяти фізичному, розумовому і соціальному розвитку дітей та юнацтва, надаючи нові можливості для розваг і навчання. Особливо вітається контент, який дає дітям можливість зрозуміти різноманітність навколишнього світу, вибудовуючи позитивні рольові моделі.

5.3 Функція C: публікування створюваного користувачами контенту і встановлення зв'язків між користувачами

Були часи, коли в цифровому середовищі домінували дорослі, але наразі зрозуміло, що основними учасниками стають діти та молодь, які, користуючись безліччю платформ, створюють і обмінюються просто гігантськими обсягами користувацького контенту. Ця група зокрема охоплює послуги соціальних мереж, застосунків та веб-сайтів, пов'язаних із творчою реалізацією.

Послуги, що з'єднують користувачів між собою, можна поділити на три категорії:

- застосунки, що переважно використовуються для обміну повідомленнями (Facebook Messenger, Groupme, Line, Tinder, Telegram, Viber, WhatsApp);

- послуги переважно соціальних мереж, які ґрунтуються на генерованому користувачами контенті, що дозволяють їм обмінюватися контентом і бути на зв'язку як усередині, так і поза межами своїх мереж (Instagram, Facebook, SnapChat, TikTok);

- застосунки, що переважно використовуються для прямого потокового мовлення (Periscope, BiGo Live, Facebook Live, Houseparty, YouTube Live, Twitch, GoLive).

Постачальники послуг запитують мінімальний вік для реєстрації на своїх платформах, однак контролювати його дотримання складно, оскільки перевірка віку покладається на відомості, що надаються. Більшість послуг, що з'єднують нових користувачів між собою, також допускають функції обміну місцем розташування, що робить дітей та молодих осіб, які користуються такими послугами, більш уразливими до небезпек реального світу.

У Таблиці 4, основою якої є правила, прийняті однією з найбільш великих соціальних мереж, викладені Рекомендації для постачальників послуг, пов'язаних з публікуванням створюваного користувачами контенту і з'єднанням нових користувачів, стосовно політики та дій, які вони можуть вчинити, з метою посилення захисту та участі дитини в цифровому середовищі.

Таблиця 4 - Контрольний перелік щодо захист дітей у цифровому середовищі для функції C: публікування створюваного користувачами контенту і встановлення зв'язків між користувачами

Унесення положень про права дитини до всіх відповідних корпоративних політик та процесів управління	Постачальники послуг публікування створюваного користувачами контенту і з'єднання користувачів можуть виявляти, запобігати й послаблювати несприятливий вплив ІКТ на права дітей та молодих осіб, а також визначати можливості для сприяння реалізації прав дітей та юнацтва.
	Див. загальні Рекомендації в Таблиці 1.
Розроблення стандартних методів поводження з CSAM	Спільно з державними та правоохоронними органами, представниками громадянського суспільства та гарячих ліній компанії, що надають послуги публікування створюваного користувачами контенту і з'єднання користувачів, можуть відігравати важливу роль у боротьбі з CSAM такими діями:
	Встановити для всіх сайтів процедури надання негайної допомоги правоохоронним органам у надзвичайних ситуаціях і під час виконання звичайних запитів.
	Закріпити всебічну співпрацю з правоохоронними органами під час розслідування випадків виявлення або повідомлення про незаконний контент і визначити деталі відповідних засобів контролю відповідальності, як-от штрафів або скасування пільгової оплати послуг.
	Працювати з внутрішніми службами, зокрема з відділом із роботи з клієнтами, відділом з профілактики шахрайства та службою охорони з метою забезпечення можливості повідомляти про можливий незаконний контент безпосередньо правоохоронним органам і на гарячі лінії. В ідеалі така процедура не повинна піддавати виконавчий персонал впливу шкідливого контенту або сприяти повторному насильству над потерпілою дитиною/потерпілими дітьми та молодими особами. Для тих ситуацій, коли співробітники можуть піддаватися впливу образливого матеріалу, встановити правила або впровадити програму підтримки для відновлення їхнього морального здоров'я, безпеки і добробуту.
	Унести до правил та умов обслуговування пункти, які забороняють незаконний контент і поведінку, особливо наголошуючи на таких моментах: • шкідливий контент, зокрема можливі випадки грумінгу дітей з наміром застосування насильства із встановленням контакту або без контакту, не допускається; • незаконний контент, зокрема вивантаження і подальше поширення CSAM, не допускається; • компанія буде звертатися і всебічно співпрацювати з правоохоронними органами у розслідуванні випадків повідомлення або виявлення незаконного контенту або порушення політики захисту дітей.
	Документально оформити політики компанії щодо поводження з CSAM, починаючи з моніторингу та закінчуючи остаточним перенесенням і знищенням контенту. Додати до складу документів перелік працівників, відповідальних за виконання різних операцій з матеріалами.
	Запровадити правила, що регулюють питання прав власності на створюваний користувачами контент, зокрема можливість видалення такого контенту на прохання користувача. Видаляти контент, що порушує правила постачальника послуг, і попереджати користувачів, що його опублікували, про порушення.

Розроблення стандартних методів поводження з CSAM	Наголосити, що до користувачів, які не змогли виконати вимоги правил прийнятного використання, будуть застосовуватися певні заходи, зокрема: • видалення контенту, призупинення обслуговування облікових записів або їх закриття; • блокування можливості обмінюватися певними типами контенту або використовувати певні функції; • запобігання їхній можливості контактувати з дітьми; • повідомлення у правоохоронні органи.
Розроблення стандартних методів поводження з матеріалами, пов'язаними із сексуальними зловживаннями щодо дітей	Сприяти використанню механізмів зворотного зв'язку щодо CSAM або щодо будь-якого іншого незаконного контенту і переконатися, що клієнти знають, як саме повідомити про факт виявлення таких матеріалів. Створити системи та призначити спеціально навчених співробітників для оцінення конкретних випадків та вжиття відповідних заходів. Організувати повноцінні та забезпечені необхідними ресурсами оперативні групи підтримки користувачів. В ідеалі такі групи повинні пройти навчання щодо правил вирішення інцидентів різних типів, щоб гарантувати достатнє реагування та вжиття прийнятних заходів. Подана користувачем скарга передається відповідному працівнику залежно від типу інциденту. Також компанія може організувати спеціальні групи з розгляду клопотань користувачів у разі, якщо повідомлення надсилаються помилково.
	Також компанія може організувати спеціальні групи з розгляду клопотань користувачів у разі, якщо повідомлення надсилаються помилково.
	Затвердити порядок негайного видалення або блокування доступу до CSAM, зокрема процедури оповіщення і вимикання, спрямовані на видалення незаконного контенту відразу після його виявлення. Переконатися, що треті особи, з якими компанія встановила договірні відносини, застосовують аналогічні надійні процедури оповіщення і вимкнення. Якщо це дозволено законодавством, матеріал може зберігатися як доказ скоєного злочину під час його розслідування.
	Розробити технічні системи виявлення напевне незаконного контенту і запобігання його вивантаження в мережу, зокрема у приватних групах, або маркування такого контенту для негайного аналізу службою безпеки компанії. Вжити всіх відповідних заходів для захисту послуг від неправомірного використання з метою публікування, розповсюдження або створення CSAM.

Створення більш безпечного онлайнового середовища, що відповідає віку	По змозі створити запобіжні технічні засоби для аналізу пов'язаних із профілем об'єктів та метаданих з метою виявлення поведінки або схем, що переслідуються законом, і вжиття відповідних заходів.
	Якщо застосунок або послуга дозволяють клієнтам завантажувати або зберігати фотографії на серверах, що належать компанії або обслуговуються нею, встановити процеси та інструменти для розпізнавання зображень, які потенційно можуть містити CSAM. Впровадити запобіжні засоби ідентифікації, як-от технології сканування або перевірки людини.
	Найважливіші питання безпеки і законності мають бути подані у форматі, що відповідає віку (тобто з використанням інтуїтивних значків та символів), як під час входу до системи, так і своєчасно під час виконання різних дій на сайті.
	Спростити для клієнтів процес повідомлення про свої сумніви стосовно неправомірного використання контенту співробітникам відділу з роботи з клієнтами, встановивши стандартний і доступний порядок розгляду різних проблем, зокрема отримання небажаних матеріалів (спам, булінг) або перегляд неприйнятного контенту.
	Встановити відповідні віку налаштування обміну контентом та видимості. Наприклад, запровадити більш суворі обмеження у налаштуваннях конфіденційності та видимості для дітей та молодих осіб порівняно з налаштуваннями за замовчуванням для дорослих.
	Запровадити мінімальні вікові вимоги та сприяти проведенню досліджень і розроблень у сфері нових систем перевірки віку (зокрема біометрії), використовуючи у розробленні таких інструментів відомі міжнародні стандарти. Вжити заходів щодо виявлення і видалення облікових записів малолітніх користувачів, які неправильно зазначили свій вік з метою отримання доступу. Водночас треба враховувати неминучість збирання додаткових даних для виконання цієї вимоги і необхідність обмеження збирання, збереження та оброблення такої інформації. Якщо такі заходи ще не застосовуються, встановити прийнятні процеси реєстрації, що дозволяють визначити, чи достатньо зрілими є користувачі, щоб отримувати доступ до контенту або послуги, водночас такі процеси не повинні ставити під загрозу ідентичність, місцеперебування та персональні дані. Використовувати затверджені на національному рівні функціональні системи перевірки віку з огляду на застосовність та за умови наявності достатніх інструментів забезпечення конфіденційності даних дітей. Забезпечити наявність функції зворотного зв’язку або довідкової служби/центру, заохочуючи користувачів повідомляти про осіб, що фальсифікують відомості про свій вік.

Створення більш безпечного онлайнового середовища, що відповідає віку	Захистити молодих користувачів від отримання небажаних повідомлень і гарантувати дотримання встановлених правил конфіденційності та збирання інформації.
	Віднайти способи перевірки зображень і відеоматеріалів, що публікуються на сайтах, і видаляти неприйнятний контент у разі його виявлення. Корисними в цьому аспекті можуть виявитися такі інструменти, як сканування геш-індексів відомих зображень і програми розпізнавання зображень. Стосовно послуг, пов'язаних із дітьми, світлини та відеоматеріали можуть проходити попередню перевірку, щоб не допустити публікування дітьми вразливої персональної інформації про них самих та про інших осіб.
	Є ціла низка засобів контролю доступу до створюваного користувачами контенту й захисту дітей та молоді від неприйнятного або незаконного контенту в цифровому середовищі. З огляду на це важливо встановити перевірку надійності паролів як крок уперед на шляху захисту дітей та юнацтва у просторі ігрових та інших соціальних мереж. Іншими засобами є: • перевірка дискусійних груп з метою виявлення небезпечних тем для обговорення, агресивних висловлювань і протиправної поведінки, а також видалення подібного контенту в разі виявлення порушення правил користування; • створення інструментів активного пошуку і видалення контенту, що є незаконним або таким, що порушує правила та умови обслуговування компанії, а також інструментів, що запобігають вивантаженню на сайт напевне незаконного контенту; • попереднє модерування на дошках повідомлень силами спеціальної команди модераторів контенту для дітей та молоді, яка стежить за контентом, що суперечить опублікованим "внутрішнім правилам". Кожне повідомлення може перевірятися до його публікації, водночас модератори виявляють і відзначають підозрілих користувачів, а також користувачів, які потрапили в біду; • організацію групи провідних членів спільноти, яка служить вихідною точкою контакту для модераторів тоді, коли у них виникають сумніви щодо будь-якого користувача.
	Відповідально ставитися до перевірки контенту комерційного характеру, зокрема форуми, соціальні мережі та ігрові сайти. Впровадити прийнятні стандарти й правила захисту дітей від реклами, що що не відповідає віку, та встановити чіткі обмеження щодо онлайнової реклами для дітей та молодих осіб.

Навчання дітей, батьків і педагогів правилам дитячої безпеки та відповідального використання ними ІКТ	Постачальники послуг публікування створюваного користувачами контенту та з'єднання користувачів можуть вчиняти такі дії, спрямовані на підвищення рівню освіти та розширення прав і можливостей, на додаток до технічних інструментів:
	Створити розділ, в якому будуть публікуватися пов'язані з безпекою поради, статті, замітки та обговорення на теми цифрового громадянства, а також посилання на корисний контент сторонніх експертів. Поради щодо безпеки мають бути помітними і викладеними доступною для розуміння мовою. Постачальникам платформ також рекомендується встановити однотипні принципи навігації на різних пристроях, як-от комп'ютери, планшети або мобільні телефони.
	Запропонувати батькам чітку інформацію про доступні типи контенту та послуг, зокрема надати роз'яснення про сайти соціальних мереж і послуги, що надаються з огляду на місцеперебування користувача, про те, як здійснюється доступ до інтернету з мобільних пристроїв, а також про можливі варіанти застосування батьківського контролю.
	Інформувати батьків про те, як саме можна повідомити про зловживання, неправомірне використання та неприйнятний або незаконний контент, і як такі повідомлення будуть опрацьовуватися. Надати їм відомості про те, які саме послуги обмежуються за віком, а також про інші способи безпечної та відповідальної поведінки під час користування інтерактивними послугами.
	Встановити систему, яка ґрунтується на принципі "довіри і репутації" та заохочує до хорошої поведінки, що дозволить одноліткам передавати один одному досвід на власному прикладі. Сприяти розвитку розуміння важливості соціального зворотного зв'язку, сприяючи тому, щоб люди йшли назустріч іншим користувачам або друзям, яким вони довіряють, допомагаючи вирішити конфлікт або почати розмову про контент, що спричиняє занепокоєння.
	Зазначити рекомендації та нагадування про характер послуги або контенту, що надається, а також про те, як користуватися ним безпечно. Унести в структуру інтерактивних послуг інструкції для спільноти, наприклад у формі спливаючих підказок стосовно безпеки, що будуть нагадувати користувачам про прийнятну та безпечну поведінку, зокрема про те, що не слід розголошувати свої контактні дані.
	Співпрацювати з батьками і надавати їм інструкції, щоб гарантувати, що інформація про дітей, яка публікується в інтернеті, не становить для них ніякого ризику. По змозі отримувати інформовану згоду дітей у разі їхньої появи у створеному ними самими контенті та поважати їхнє право на відмову.
Сприяння просуванню цифрових технологій як засобу збільшення участі в житті громадянського суспільства	Постачальники послуг публікування створюваного користувачами контенту і з'єднання користувачів можуть заохочувати дітей та молодих осіб і надавати їм відповідні можливості, підтримуючи їхнє право на участь.
	Див. загальні Рекомендації в Таблиці 1.

5.4 Функція D: системи зі штучним інтелектом

На тлі посиленої уваги до технологій глибокого навчання терміни "штучний інтелект", "машинне навчання" та "глибоке навчання" серед широкого загалу є у певному сенсі взаємозамінними, відбиваючи концепцію копіювання "розумної" поведінки машинами. У цьому розділі ми зосередимося на тому, яким чином машинне навчання і глибоке навчання впливають на життя дітей і, зрештою, на їхні права.

"З огляду на експоненціальне просування технологій зі штучним інтелектом за останні кілька років сьогоднішні міжнародні схеми захисту прав дітей не охоплюють беззаперечно багато питань, що постали внаслідок розвитку і використання штучного інтелекту. Проте, вочевидь вирізняються деякі права, які можуть опинитися під впливом таких технологій, що є початком для аналізування того, яким чином, позитивно або негативно, ці нові технології можуть впливати на права дітей, зокрема на право на особисте життя, освіту, гру та відсутність дискримінації".

Застосування Штучного Інтелекту може змінити вплив, який чиниться на дітей різними послугами, що використовуються соціальними мережами, зокрема на платформах потокового мовлення. Алгоритми машинного навчання, служби рекомендацій, що застосовуються, перш за все, на популярних платформах обміну відеоматеріалами, оптимізуються для максимального збільшення кількості переглядів певних роликів протягом заданого часу. Технології сензахист дітей у цифровому середовищіних екранів та проєктування таких платформ дозволяють дітям навіть наймолодшого віку мандрувати цим контентом. Особливе турбує те, що алгоритми, які використовують рекомендовані відеоматеріали, можуть завести дітей у пастку "бульбашки фільтрів" з неякісним або неприйнятним контентом. Оскільки діти особливо сприйнятливі до рекомендацій контенту, шокувальні "пов'язані відео" можуть привернути їхню увагу і відвести вбік від більш дружніх до дитини алгоритмів.

Штучний інтелект також впливає на захист дитини в цифровому середовищі через розумні іграшки. Чіткі процеси, використовувані в роботі розумних іграшок, пов'язані зі своїми труднощами, тобто іграшка (що контактує з дитиною), мобільний застосунок, що діє як точка доступу для з'єднання Wi-Fi, та персоналізований обліковий запис іграшки/споживача, де зберігаються дані. Такі іграшки обмінюються інформацією з хмарними серверами, де зберігаються і обробляються дані, що надані дітьми, які взаємодіють з іграшками. Така модель спричинює побоювання стосовно конфіденційності в разі недостатньої безпеки на будь-якому з рівнів, що підтверджується численними випадками злому, що призводили до витоку персональних даних. Також деякі зламані пристрої (зокрема розумні пристрої, з'єднані з інтернетом, як-от радіо-няні, голосові помічники тощо) можуть використовуватися для відстеження користувачів без їхнього відома або згоди.

У впровадженні механізмів реагування на виявлені загрози для дітей, що користуються такими пристроями, зокрема через надання порад і рекомендацій на основі встановленої поведінки (як згадувалося раніше в описі програми BBC Own It), вкрай важливо, щоб компанії, які розробляють розумні пристрої, складали такі рекомендації, спираючись на об'єктивні дані, і розробляли їх на основі консультацій з фахівцями із захисту дітей та охорони їхніх інтересів.

Притому, що деякі компанії пропагують принципи етичного використання Штучного Інтелекту, не зовсім зрозуміло, чи існують будь-які суспільні правила у сфері Штучного Інтелекту та дітей Низка технологічних і галузевих асоціацій та наукових груп з інформатики склали проєкт переліку етичних принципів стосовно Штучного Інтелекту. Однак ці принципи не мають чіткого зв'язку з правами дитини, способами, в межах яких технології Штучного Інтелекту можуть становити ризик для дітей, або із запобіжними планами щодо пом'якшення таких ризиків.

"Як і корпорації, уряди у всьому світі запроваджують стратегії, що дозволяють первувати у сфері розроблення і використання Штучного Інтелекту, формування середовища, сприятливого для новаторів і корпорацій". Проте не цілком зрозуміло, яким чином такі національні стратегії зіставляються з правами дитини.

Покращення роботи Facebook із контентом, пов'язаним із самогубством і нанесенням собі тілесних ушкоджень

У 2019 році компанія Facebook започаткувала серію регулярних консультацій із фахівцями з різних країн світу стосовно низки найбільш складних тем, пов'язаних із самогубством та самоушкодженням. Зокрема розглядалися питання реагування на записки про самогубство, ризики, пов'язані з депресивним контентом в інтернеті та освітленням суїциду в новинах. Додаткові подробиці цих зустрічей наводяться на новій сторінці "Запобігання самогубствам" Facebook у розділі "Центр безпеки". Ці консультації дозволили зробити кілька поліпшень у способах поводження Facebook із таким контентом. Зокрема, політика щодо нанесення собі тілесних ушкоджень була посилена забороною на зображення з пораненнями, щоб уникнути ненавмисного сприяння самоушкодженню або його ініціювання. Навіть якщо хтось звертається по допомогу або демонструє себе в пошуках допомоги для лікування, Facebook тепер маскує загоєні рани на зображеннях. Такий контент наразі виявляється за допомогою Штучного Інтелекту, водночас дії стосовно потенційно шкідливого контенту, зокрема його видалення або додавання масок, можуть робитися автоматично. З квітня по червень 2019 року Facebook вжила заходів стосовно більш ніж 1,5 мільйону одиниць контенту про суїцид і самоушкодження на своєму сайті, причому більш ніж 95 відсотків з них були виявлені до моменту повідомлення про них користувачами. За той самий період часу Instagram розглянула понад 800 тисяч одиниць аналогічного контенту, з яких понад 77 відсотків були виявлені до моменту отримання повідомлень про них від користувачів.

Виявлення потенційного булінг або насильства між однолітками в реальному часі та інформування користувачів

Instagram впроваджує Штучний інтелект задля викорінення такої поведінки як образи, публічне висміювання і неповагу. Використовуючи високотехнологічні інструменти зворотного зв'язку, модератори можуть швидко закривати облікові записи, що належать особам, які здійснюють булінг в інтернеті.

60

Передовий досвід: використання штучного інтелекту для виявлення матеріалів, пов'язаних із сексуальними зловживаннями щодо дітей

Спираючись на щедрий внесок Microsoft у боротьбу з дитячою експлуатацією у формі PhotoDNA і нещодавній запуск Google Content Safety API, Facebook розробила технології для виявлення контенту, пов'язаного із сексуальними зловживаннями щодо дітей.

Ці технології, що отримали назву PDQ і TMK+PDQF, є частиною набору інструментів, які Facebook використовує для виявлення шкідливого контенту. До інших алгоритмів та інструментів, наявних в арсеналі індустрії, належать pHash, aHash і dHash. Застосовуваний Facebook алгоритм порівняння фотографій PDQ багато в чому перегукується з pHash, проте він був розроблений окремо й з нуля на основі незалежного програмного забезпечення.

Технологія порівняння відеоматеріалів TMK+PDQF була розроблена спільно групою дослідження Штучного Інтелекту Facebook і вченими-фахівцями з Університету Модени та Реджо-Емілія в Італії.

Ця технологія забезпечує ефективний спосіб зберігання файлів у вигляді коротких цифрових гешів, що дозволяють визначити, чи є два файли однаковими або схожими навіть за відсутності первинного зображення або відеоролика. Такими гешами також можна легко обмінюватися з іншими компаніями і неприбутковим організаціями.

PDQ і TMK+PDQF були розроблені для широкого застосування з підтримкою гешування відеокадрів і застосунків у реальному часі.

Деякі рекомендації для компаній щодо узгодження їхніх принципів під час проєктування та впровадження рішень на основі Штучного Інтелекту, спрямованих на дітей, наведені в Таблиці 5.

Рекомендації ґрунтуються на роботі ЮНІСЕФ із розроблення глобальних керівних настанов щодо Штучного Інтелекту та дітей, які будуть призначені для державних органів та галузевих підприємств. Більш докладну інформацію про проєкт можна знайти за адресою https://www.unicef.org/globalinsight/featured -projects/ai-children. У цих рекомендаціях також враховані положення звіту ЮНІСЕФ і UC Berkeley щодо Штучного Інтелекту і прав дитини.

61

Таблиця 5 - Контрольний перелік щодо захисту дітей у цифровому середовищі для функції D: системи зі Штучним Інтелектом

Унесення положень про права дитини до всіх відповідних корпоративних політик та процесів управління	Постачальники послуг на основі систем, керованих Штучним Інтелектом, можуть виявляти, запобігати і послаблювати несприятливий вплив ІКТ на права дітей та молодих осіб, а також визначати можливості для сприяння реалізації прав дітей та молоді.
	Системи Штучного Інтелекту необхідно проєктувати, розробляти, впроваджувати і досліджувати, поважаючи, сприяючи і дотримуючись прав дітей, що записані у Конвенції про права дитини. Дитинство, яке дедалі більше проходить у цифровому середовищі, - це час, що вимагає особливої турботи і допомоги. Системи Штучного Інтелекту слід використовувати таким чином, щоб реалізувати повний потенціал такої підтримки.
	Слід застосовувати всеосяжний підхід до проєктування під час створення продуктів, призначених для дітей, щоб максимально розширити гендерне, географічне і культурне розмаїття, залучаючи великий спектр заінтересованих сторін, зокрема батьків, освітянив, дитячих психологів і, по змозі, самих дітей.
	Необхідно встановити рамкові засади управління, зокрема етичні норми, закони, стандарти і регуляторні органи, що передбачають процеси, які забезпечують застосування систем Штучного Інтелекту без порушення прав дитини.
Розроблення стандартних методів поводження з CSAM	Спільно з державними та правоохоронними органами, представниками громадянського суспільства та гарячих ліній постачальники послуг на основі систем зі Штучним Інтелектом можуть відігравати важливу роль у боротьбі з CSAM такими діями:
	Див. загальні Рекомендації в Таблиці 1.

62

Створення більш безпечного онлайнового середовища, що відповідає віку	Постачальники послуг на основі систем зі Штучним Інтелектом можуть надати допомогу у створенні більш безпечного, більш захопливого цифрового середовища для дітей різного віку такими діями:
	Запровадити міждисциплінарний підхід у розробленні технологій, що впливають на дітей, і консультуватися з громадянським суспільством, зокрема освітніми установами, щоб визначити можливий вплив таких технологій на права різних груп потенційних кінцевих користувачів.
	Застосовувати принципи проєктованої безпеки і проєктованої конфіденційності для продуктів і послуг, призначених для дітей або таких, що ними часто використовуються.
	Оскільки системи Штучного Інтелекту вимагають великих обсягів даних, компанії, які застосовують Штучний інтелект у своїх послугах, повинні бути особливо пильними стосовно збирання, опрацювання, збереження, продажу та публікації персональних даних дітей. Системи Штучного Інтелекту мають бути прозорими, тобто необхідно забезпечити можливість встановити, як і чому система дійшла певного рішення або, якщо це робот, чому він виконав саме цю дію. Така прозорість є вкрай важливою для формування довіри та забезпечення перевірки, розслідування та звернення по допомогу в імовірних випадках заподіяння шкоди дітям. Забезпечити наявність функціональних і правових механізмів для звернення по допомогу, якщо дітям було завдано шкоди через систему Штучного Інтелекту або в разі надходження такої претензії. Необхідно встановити процеси для своєчасного виправлення всіх наслідків, що дискримінують, і створити наглядові органи для подання звернень і безперервного моніторингу безпеки та захисту дітей. Підзвітність та механізми виправлення є тісно пов'язаними між собою.
	Розробити плани щодо поводження з особливо чутливими даними, зокрема порядок розкриття зловживань або інших шкідливих матеріалів, які можуть використовуватися у внутрішньому середовищі компанії через її продукцію. Збирання даних про дітей на цифрових платформах і в системах Штучного Інтелекту має бути мінімальним та з наданням дітям максимальної можливості контролювати дані, які вони створюють. Умови використання повинні бути зрозумілими для дітей та сприяти підвищенню їхньої обізнаності та свободи вибору.
Навчання дітей, батьків і педагогів правилам дитячої безпеки та відповідального використання ними ІКТ	Постачальники послуг на основі систем зі Штучним Інтелектом додатково до технічних заходів можуть сприяти підвищенню рівня освіти й розширенню прав і можливостей.
	Необхідно забезпечити можливість роз'яснення мети систем Штучного Інтелекту користувачам-дітям та їхнім батькам або опікунам, аби розширити їхні можливості для визначення щодо використання цієї платформи або відмови від нього.
Сприяння просуванню цифрових технологій як засобу збільшення участі в житті громадянського суспільства	Постачальники послуг на основі систем зі Штучним Інтелектом можуть заохочувати дітей та молодь і надавати їм відповідні можливості, підтримуючи їхнє право на участь, такими діями:
	Див. загальні Рекомендації в Таблиці 1.
Використання технологічних досягнень для захисту та навчання дітей	Системи, керовані Штучним Інтелектом, необхідно розробляти з огляду на підтримку розвитку та добробуту дітей у всіх елементах проєктування, розроблення та впровадження. Вихідною точкою мають служити кращі з наявних і повсюдно визнані показники розвитку та добробуту. Компаніям слід вкладати кошти у дослідження і розроблення етичних інструментів на основі Штучного Інтелекту з метою виявлення фактів CSAE в інтернеті, а також домагань і булінг в цифровому середовищі, у співпраці з провідними фахівцями з прав дитини та самими дітьми. Необхідно застосовувати досягнення в технологіях Штучного Інтелекту з метою надання дітям інформації, що відповідає віку, без обмеження їхньої ідентичності, без розкриття їхнього місця перебування і персональних даних.

63

Довідкові матеріали

Текст GDPR (Регламент (ЄС) 2016/679 Європейського Парламенту та Ради Європейського Союзу від 27 квітня 2016 року про захист фізичних осіб під час опрацювання персональних даних і про вільний обіг таких даних, а також про скасування Директиви 95/46/ЄС (Загальний регламент про захист персональних даних) і текст, опублікований в Офіційному бюлетені ЄС.

Переглянена Директива AVMS (про аудіовізуальні медіа-послуги), яка вносить поправки до Директиви 2010/13/ЄС про координування деяких положень закону, норм і адміністративних актів у Державах-членах щодо положень про аудіовізуальні медіа-послуги (Директива про аудіовізуальні медіа-послуги) з огляду на зміни, що відбуваються на ринку, а також текст, опублікований в Офіційному бюлетені ЄС.

Політика BBC:

- Політика щодо захисту та охорони дитини, редакція 2017 року, переглянена у 2018 році, та оновлена редакція 2019 року
- Робота з юнацтвом та дітьми в BBC;
- Загальні принципи для незалежних продюсерських компаній, що працюють у проєктах BBC, стосовно розроблення правил зовнішніх постачальників щодо захисту дітей;
- Рекомендації: Взаємодія з дітьми та молодими особами в цифровому середовищі стосовно редакторських керівних настанов щодо діяльності в цифровому середовищі.

Розслідування, яке підтверджує недотримання правил перевірки віку в соціальних мережах у Сполученому Королівстві: 2016 р., 2017 р.; 2020 р.

Глосарій

Викладені нижче визначення наводяться, переважно, на підставі чинної термінології, закріпленої Конвенцією про права дитини 1989 року, а також розробленої Міжвідомчою робочою групою щодо сексуальної експлуатації дітей у Керівних настановах щодо термінології у сфері захисту дітей від сексуальної експлуатації та сексуальних зловживань, 2016 рік (Люксембурзькі Рекомендації), Радою Європи у Конвенції про захист дітей від сексуальної експлуатації та сексуальних зловживань, 2007 рік, та ЮНІСЕФ у доповіді Global Kids Online, 2019 рік.

Підліток

Підлітки - це особи віком від 10 до 19 років. Важливо наголосити, що у міжнародному праві відсутній обов'язковий термін "підлітки", і особи, молодші за 18 років, вважаються дітьми, водночас 19-річні особи вважаються дорослими, крім випадків, коли повноліття настає раніше згідно з національним законодавством .

Штучний інтелект

У найширшому сенсі термін "штучний інтелект (ШІ)" розпливчасто визначає системи, що належать до сфери суто наукової фантастики (так званий "сильний" ШІ, який має форму самосвідомості), і системи, що вже діють і здатні виконувати дуже складні завдання (ці системи описуються як "слабкий" або "середній" ШІ, як-от системи розпізнавання осіб або голосу та системи керування автомобілем) .

Системи штучного інтелекту

Система ШІ - це система на основі машин, яка в межах заданого набору визначених людиною цілей може складати прогнози, виносити рекомендації або ухвалювати рішення, що впливають на реальне або віртуальне середовище. Системи ШІ призначені для функціонування з різними рівнями автономності .

Alexa

Amazon Alexa, відома як просто Alexa, є системою ШІ - віртуального помічника, розробленою Amazon. Вона підтримує такі функції, як голосова взаємодія, відтворення музики, складання списку справ, установлення будильнику, відтворення подкастів та аудіокниг, повідомлення прогнозу погоди, даних про ситуацію на дорогах, спортивні події та іншої інформації в реальному часі, зокрема новин. Alexa також може контролювати декілька «розумних» пристроїв, функціонуючи як система побутової автоматизації. Користувачі можуть розширювати функціонал Alexa через встановлення "вмінь" (додаткових функціональних можливостей, що розробляються сторонніми постачальниками, які в інших випадках зазвичай іменуються застосунками, як-от програм відстеження погоди і аудіофункцій).

Найкращі інтереси дитини

Поняття, що описує всі елементи, необхідні для ухвалення рішення в конкретній ситуації щодо конкретної дитини або групи дітей .

Дитина

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

Сексуальна експлуатація та сексуальні зловживання щодо дітей

Це поняття описує всі форми сексуальної експлуатації та сексуальних зловживань, як-от "a) схиляння або примушування дитини до будь-якої незаконної сексуальної діяльності; b) використання з метою експлуатації дітей у проституції або в іншій незаконній сексуальній практиці; c) використання з метою експлуатації дітей у порнографії та порнографічних матеріалах " , а також "статевий контакт, переважно із застосуванням сили до особи без її згоди" . Сексуальна експлуатація та сексуальні зловживання щодо дітей (СЕНД) дедалі частіше відбуваються з використанням інтернету або так чи інакше пов'язані з онлайнової середовищем.

Матеріали, пов'язані із сексуальною експлуатацією та сексуальними зловживаннями щодо дітей

Стрімкий розвиток ІКТ призвів до появи нових форм сексуальної експлуатації та сексуальних зловживань щодо дітей в цифровому середовищі, які можуть відбуватися у віртуальній формі та не обов'язково значать особисту зустріч з дитиною . Хоча в багатьох юридичних системах зображення та відеоматеріали, пов'язані із сексуальними зловживаннями щодо дітей, як і раніше, вважають "дитячою порнографією" або "непристойними зображеннями дітей", в цих Керівних настановах вони будуть сукупно іменуватися "матеріалами, пов'язаними із сексуальними зловживаннями щодо дітей "(CSAM). Цей термін узгоджується з Керівними настановами Комісії із широкосмугового зв'язку та Моделлю реагування на національному рівні, розробленої Глобальним альянсом WePROTECT , і точніше описує відповідний контент. Порнографією вважається правомірна комерційна індустрія, і, як зазначається в Люксембурзьких керівних настановах, використання такого терміну: "може (самочинно або мимоволі) сприяти полегшенню ступеня тяжкості, зменшенню значущості або навіть легітимізації того, що за суттю є сексуальними зловживаннями щодо дітей та/або їх сексуальним експлуатуванням. Термін "дитяча порнографія" створює небезпеку його тлумачення таким чином, ніби дії відбуваються за згодою дитини і є законним матеріалом сексуального характеру ". Використовуючи термін CSAM, ми маємо на думці матеріали, що являють собою діяння, які є сексуальними зловживаннями щодо дітей та/або їх сексуальним експлуатуванням. Це 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 для цілей сексуального характеру.

Визначення таких понять, як "матеріали, пов'язані із сексуальними зловживаннями щодо дітей, створені комп'ютером або цифровими засобами", див. у Люксембурзьких керівних настановах.

Діти та молодь

Поняття, яке описує всіх осіб віком до 18 років, водночас "дітьми" (або "дітьми молодшого віку" в цих Керівних настановах МСЕ) вважаються всі особи молодші за 15 років, а "молодими особами" - всі особи вікової групи 15-18 років.

Іграшки, що мають вихід в Інтернет

Іграшки, що мають вихід в інтернет, з'єднуються з ним за допомогою таких технологій, як Wi Fi та Bluetooth, і зазвичай працюють у поєднанні зі спеціальними застосунками, забезпечуючи дітям можливість інтерактивної гри. Згідно з проведеним компанією Juniper Research дослідженням, у 2015 році обсяг ринку іграшок, що мають вихід в інтернет, сягнув 2,8 млрд. доларів США та, за прогнозами, до 2020 року збільшиться до 11 млрд. доларів . Ці іграшки збирають та зберігають персональну інформацію про дітей, у тому числі імена, дані геолокації, адреси, світлини, аудіо- та відеозаписи .

Кібербулінг

Кібербулінг - це навмисно агресивна дія, неодноразово здійснювана колом осіб або окремою особою за допомогою цифрових технологій, і спрямована проти жертви, якій важко себе захистити . Зазвичай вона значить "використання цифрових технологій та Інтернету для публікування 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 або текстових повідомленнях), поширення пліток і неправдивої інформації про жертву або навмисне вилучення її з онлайнового спілкування" .

Кіберненависть, дискримінація та насильницький екстремізм

"Кіберненависть, дискримінація та насильницький екстремізм є виразною формою кібернасильства, яка спрямована проти колективної ідентичності, а не проти окремих людей, ... і нерідко зачіпає расу, сексуальну орієнтацію, релігію, національність або імміграційний статус, статеву/гендерну приналежність і політичний аспект" .

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, через відповідальне 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 у собі 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. Він також пов'язаний з емоційним інтелектом, необхідним для того, щоб розуміти, коли дитина наражається на ризик в інтернеті, знати, як звертатися по допомогу, здобувати практичний досвід і відновлюватися після досвіду невдалого .

Керівники

Стосується всіх осіб, що обіймають посади у шкільному керівництві або керівних структурах.

Грумінг/грумінг в цифровому середовищі

Грумінг/грумінг в цифровому середовищі, згідно з Люксембурзькими керівними настановами, означає "процес налагодження/побудови стосунків з дитиною особисто або за допомогою інтернету або інших цифрових технологій з метою домогтися сексуальних зв'язків із цією особою в цифровому середовищі або в реальному житті". Це кримінальне діяння, в межах якого започатковується дружба з дитиною ... з метою схилити її до сексуальних стосунків.

Інформаційно-комунікаційні технології

Інформаційно-комунікаційні технології (ІКТ) - це всі інформаційні технології, де основний наголос припадає на комунікацію. До них належать всі послуги та пристрої, які використовують з'єднання з інтернетом, як-от комп'ютери, ноутбуки, планшети, смартфони, ігрові консолі та "розумні" годинники . Того ж стосуються послуги, зокрема радіо і телебачення, 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 вихід в Інтернет, 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 або усі функції комп'ютера чи іншого пристрою, здатного підтримувати зв'язок з Інтернетом. Зазвичай такі програми дозволяють обмежувати Інтернет-доступ до певних видів або категорій веб-сайтів або онлайнових послуг. Деякі також мають налаштування часу, тобто пристрій можна налаштувати таким чином, щоб він під'єднувався до Інтернету лише у певні проміжки часу. Більш досконалі версії дозволяють вести запис усіх текстових повідомлень, що надсилаються або отримуються через пристрій. Зазвичай такі програми захищаються паролями .

Персональна інформація

Термін означає індивідуально визначену інформацію про особу, яка збирається в онлайновому 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 або будь-які інші відомості, що дозволяють вступити у фізичний або віртуальний контакт або визначити місце перебування особи. У цьому контексті персональна інформація також значить будь-яку інформацію про дитину та її оточення, яка збирається в онлайновому режимі постачальниками послуг інтернету, зокрема іграшками з виходом в інтернет та інтернетом речей, а також будь-якими іншими технологіями, що використовують з'єднання з інтернетом.

Конфіденційність

Конфіденційність нерідко оцінюється під кутом 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 та усвідомлення важливості збереження конфіденційності .

Громадські засоби масової інформації

До них належать національні радіомовні організації або засоби масової інформації, які отримали ліцензію на радіомовлення на підставі низки договірних зобов'язань, узгоджених із державою або парламентом. Останнім часом у багатьох країнах такі зобов'язання були доповнені з огляду на необхідність реагувати на наслідки цифрової трансформації через засоби масової інформації та цифрові програми посилення грамотності, а також з огляду на обов'язки щодо усунення цифрового розриву.

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 власноруч створених зображень дітей сексуального характеру дорослі не повинні їх переглядати. Демонстрація зображень сексуального характеру дитині дорослим завжди є злочинним діянням, здатним завдати шкоди, і, можливо, буде потрібно повідомити про такі зображення або знищити їх.

Секс-вимагання або сексуальне вимагання стосовно дітей

Сексуальне вимагання - це "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, що фігурує в ньому (наприклад, через публікування зображень у соціальних мережах)" .

Інтернет речей

"Інтернет речей (IoT) є наступним кроком до цифровізації нашого суспільства та економіки, коли взаємозв'язок людей та об'єктів здійснюється через комунікаційні мережі, а також передаються відомості про їхній стан і оточення" .

URL

Скорочення, що значить "універсальний вказівник ресурсу" ("Uniform Resource Locator"), тобто адреса сторінки в інтернеті .

Віртуальна реальність

"Віртуальна реальність - це створення за допомогою комп'ютерних технологій ефекту тривимірного світу, в якому об'єкти сприймаються як такі, що реально існують у просторі" .

WI-FI

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

With the support of:

Міжнародна спілка
електрозв'язку

ISBN: 978-92-61-30414-0

Place des Nations
CH-1211 Geneva 20
Switzerland

Опубліковано у Швейцарії
Женева, 2020 р.
Світлини надані: Shutterstock