Міжнародний союз електрозв'язку

Захист дітей у цифровому середовищі: рекомендації для органів державної влади

2020

Захист дітей у цифровому середовищі: рекомендації для органів державної влади

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.

Слова подяки

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

ECPAT International, мережа Global Kids Online, Глобальне партнерство з припинення насильства щодо дітей, проєкт HABLATAM, Мережа центрів безпечного Інтернету Insafe, Інтерпол, Міжнародний центр щодо зниклих безвісти та експлуатованих дітей (ICMEC), Міжнародний союз інвалідів, Міжнародний союз електрозв'язку (МСЕ), Фонд спостереження за інтернетом (IWF), Лондонська школа економіки, Канцелярія Спеціального представника Генерального секретаря з питання про насильство щодо дітей та Спеціальний доповідач з питання про торгівлю дітьми і сексуальної експлуатації дітей, Privately SA, RNW Media, Центр безпечного інтернету Сполученого Королівства, Глобальний альянс WePROTECT (WPGA) та Всесвітній фонд дитинства у США.

Робоча група проводила свою діяльність під головуванням Девіда Райта (Центр безпечного Інтернету Сполученого Королівства/ SWGfL) та при координувальній ролі Фанні Ротіно (МСЕ).

Ці Рекомендації не змогли б реалізуватися без витраченого авторами часу, властивого їм ентузіазму та самовідданості. Неоціненний внесок зробили також COFACE-Families Europe, Рада Європи, Комісаріат з електронної безпеки Австралії, Європейська комісія, Група e-Worldwide Group (e-WWG), OECP, Молодь та соціальні мережі/ Центр Беркмана Клейна з питань Інтернету та суспільства при Гарвардському університеті, а також уряди окремих країн та зацікавлені галузеві організації, об'єднані спільною метою — зробити Інтернет кращим та безпечнішим місцем для дітей та молоді.

Нижче перелічені партнери, яким МСЕ висловлює подяку за те, що вони присвятили свій час цій роботі та поділилися своїми знаннями (перелік наводиться в алфавітному порядку за назвою організації):

- Мартін Шмальцрід (COFACE-Families Europe)
- Лівія Стойка (Рада Європи)
- Джон Карр (ECPAT International)
- Джулія Фоссі та Елла Серрі (Комісаріат з питань електронної безпеки)
- Мануела Марта (Європейська комісія)
- Сальма Аббасі (e-WWG)
- Емі Крокер та Серена Томмасіно (Глобальне партнерство з припинення насильства щодо дітей)
- Ліонель Броссі (HABLATAM)
- Сандра Марченко (ICMEC)
- Карл Хопвуд (Insafe)
- Люсі Річардсон (Міжнародний союз інвалідів)
- Метью Домп'єр (Інтерпол)

- Фанні Ротіно (MCE)
- Тесс Лейленд (IWF)
- Соня Лівінгстон (Лондонська школа економіки та Global Kids Online)
- Елеттра Ронкі (OECP)
- Манус де Барра (Канцелярія Спеціального представника Генерального секретаря з питання про насильство щодо дітей
- Діпак Теварі (Privately SA)
- Павітра Рам (RNW Media)
- Мод де Бер-Букіккіо (Спеціальний доповідач з питання про торгівлю дітьми та сексуальну експлуатацію дітей)
- Девід Райт (Центр безпечного Інтернету Сполученого Королівства/ SWGfL)
- Іен Дреннан та Сюзанна Ричмонд (Глобальний альянс WePROTECT)
- Ліна Фернандес та д-р Джоанна Рубінштейн (Всесвітній фонд дитинства у США)
- Сандра Кортезі (Молодь та соціальні мережі)

Передмова

У сучасному світі, який характеризується проникненням Інтернету майже у всі сфери життя, забезпечення захисту молодих користувачів в цифровому середовищі стає дедалі нагальнішим завданням для кожної країни.

Свій перший комплект Керівних настанов щодо захисту дитини в цифровому середовищі МСЕ розробив ще у 2009 році. Відтоді Інтернет зазнав вражаючих змін. Він перетворився на нескінченно багате джерело ігор та знань для дітей, проте водночас він став для них набагато небезпечнішим місцем для занять без нагляду.

На сьогодні діти стикаються з численними ризиками: від проблем захисту конфіденційності до контенту з елементами насильства та іншого неналежного контенту, інтернет-шахрайства, а також загроз у вигляді грумінгу в цифровому середовищі, сексуальних зловживань та сексуальної експлуатації. Кількість загроз зростає, при цьому злочинці дедалі частіше діють одночасно у декількох юрисдикціях, що позначається на ефективності заходів реагування та відшкодування шкоди, що вживаються у межах окремих держав.

Крім того, у період глобальної пандемії COVID-19 відбулося різке збільшення кількості дітей, які вперше приєдналися до онлайн-світу, щоб одержувати допомогу в навчанні та підтримувати соціальну взаємодію. Запровадження обмежень у зв'язку з вірусом призвело не лише до того, що чимало дітей молодого віку почали спілкуватися в Інтернеті набагато раніше, аніж планували їхні батьки, а й до того, що чимало батьків, змушені виконувати свої посадові обов'язки, виявилися неспроможними наглядати за дітьми, що, своєю чергою, наражає останніх на небезпеку дістати доступ до неприйнятного контенту або стати мішенню злочинців, які займаються виробництвом матеріалів, пов'язаних із сексуальними зловживаннями стосовно дітей.

На сьогодні більше, ніж будь-коли раніше, для забезпечення безпеки дітей в цифровому середовищі необхідними є міжнародна співпраця та координація зусиль, які потребують активної участі й підтримки з боку широкого кола зацікавлених осіб: як представників галузі, включно з приватними платформами, постачальниками послуг та операторами мереж, так і урядових структур і громадянського суспільства.

Усвідомлюючи це, 2018 року держави-члени МСЕ попросили надати дещо більше, аніж чергове оновлення Керівних настанов з СОР, яке доти здійснювалося на періодичних засадах. Таким чином, ці нові переглянуті Рекомендації були переосмислені, переписані та повністю перероблені від початку і до кінця, щоб відобразити фундаментальні зміни, що сталися у цифровому середовищі, в якому перебувають діти.

Крім того, що в цьому новому виданні було відображено нові тенденції у цифрових технологіях та платформах, у ньому заповнено одну серйозну прогалину: становище, в якому перебувають діти з інвалідністю, яким онлайн-світ пропонує життєво важливий засіб комунікації, забезпечуючи їм можливість повноцінної участі у соціальному житті. У цьому документі також враховано особливі потреби дітей із середовища мігрантів та інших уразливих груп.

Ми сподіваємося, що ці Рекомендації стануть міцним фундаментом для розроблення директивними органами всеохопних національних стратегій за участі багатьох зацікавлених

сторін, включаючи відкриті консультації та діалог із дітьми, для вжиття більш адресних та ефективних заходів.

Працюючи над підготовкою нових керівних настанов, МСЕ та його партнери прагнули створити максимально практичну, гнучку та адаптовану платформу, що базується на міжнародних стандартах і спільній меті, включно з положеннями Конвенції про права дитини і Мети ООН у сфері сталого розвитку. У мене викликає почуття гордості той факт, що ці переглянуті Рекомендації були розроблені у межах глобальних спільних зусиль в істинному дусі МСЕ, його ролі як глобального організатора та координатора, та за активної участі міжнародних експертів із широкої багатосторонньої спільноти.

Я також рада представити вам наш новий талісман – Санго, доброзичливий, сміливий та безстрашний персонаж, повністю розроблений групою дітей у межах нової міжнародної програми МСЕ щодо підвищення обізнаності молоді.

В епоху, коли дедалі більше молоді залучаються до онлайн-технологій, ці Рекомендації із СОР є надважливими. Директивні органи, представники галузі, батьки, освітяни, а також самі діти – всі відіграють винятково важливу роль. Як завжди, я вдячна вам за підтримку та розраховую на подальшу тісну співпрацю з цього важливого питання.

Дорін Богдан-Мартін
Директор Бюро з розвитку електрозв'язку
Міжнародного союзу електрозв'язку

Вступ

Тридцять років тому уряди майже всіх держав узяли на себе зобов'язання дотримуватися, захищати і заохочувати права дітей. Конвенція ООН про права дитини (КПД) є найширшим ратифікованим міжнародним договором з прав людини за всю історію. Попри значний прогрес, досягнутий за ці три десятиліття, поряд із вже існуючими серйозними викликами з'являються нові джерела ризиків для безпеки дітей.

Року 2015-го всі держави знову заявили про свою відданість правам дитини, прийнявши порядок денний на період до 2030 року та 17 загальних цілей у сфері сталого розвитку (ЦСР). Наприклад, мета 16.2 полягає в тому, щоб до 2030 року покласти край нарузі, експлуатації та всім формам насильства і тортур щодо дітей. А загалом захист дітей – це єднальна тема для 11 із 17 ЦСР. ЮНІСЕФ ставить дітей у центр порядку денного на період до 2030 року, як показано на Рисунку 1.

Рисунок 1: Діти, ІКТ и ЦСР

У Порядку денному в сфері сталого розвитку на період до 2030 року визнається, що ІКТ можуть відігравати ключову роль у досягненні ЦСР. Поширення інформаційно-комунікаційних технологій (ІКТ) та глобальне взаємне підключення мереж відкривають можливості для прискорення людського прогресу, подолання цифрового розриву та формування спільнот, що базуються на знаннях. Також визначено конкретні завдання, пов'язані з використанням ІКТ для досягнення сталого розвитку в сфері освіти (ціль 4), гендерної рівності (ціль 5), інфраструктури (ціль 9 - загальний та недорогий доступ до Інтернету) і цілі 17 - партнерство та засоби здійснення . ІКТ спроможні повністю трансформувати економіку, позаяк вони є рушійною силою в досягненні кожної з 17 ЦСР. ІКТ вже демонструє свою ефективність, розширюючи права та можливості мільярдів людей у цілому світі за рахунок забезпечення доступу до освітніх ресурсів та охорони здоров'я, а також надання певних послуг, зокрема таких, як електронний уряд та соціальні мережі.

Отже, стрімке поширення інформаційно-комунікаційних технологій дало дітям та молоді безпрецедентні можливості для спілкування, під'єднання, обміну, навчання доступу до інформації та висловлювання своєї думки з питань, що стосуються їх власного життя та життя їхніх спільнот.

Проте розширення та спрощення доступу до Інтернету і технологій рухомого зв'язку також пов'язано із серйозними викликами для безпеки та благополуччя дітей як в цифровому середовищі, так і в реальному житті.

Щоб знизити ризики, які несе в собі цифровий світ, і водночас зробити так, аби більше дітей та молодих осіб могли користуватися його благами, уряди, представники громадянського суспільства, місцеві спільноти, міжнародні організації та галузеві підприємства повинні об'єднати свої зусилля задля спільної мети. Особливо важливу роль у виконанні загальносвітового завдання щодо забезпечення захисту дітей в цифровому середовищі відіграють директивні органи.

Для подолання викликів, пов'язаних із швидким розвитком ІКТ і захистом дітей від наслідків цього явища, в листопаді 2008 року Міжнародним союзом електрозв'язку (МСЕ) було запущено багатосторонню міжнародну ініціативу «Захист дитини в цифровому середовищі» (СОР). Ця ініціатива покликана об'єднати партнерів зі всіх секторів світової спільноти в інтересах створення безпечних і таких, що розширюють можливості, умов в цифровому середовищі для дітей у цілому світі.

Крім того, учасники Повноважної конференції Міжнародного союзу електрозв'язку 2018 року в Дубаї знову підтвердили важливість ініціативи СОР, визнавши її як ефективну платформу для підвищення поінформованості, обміну передовим досвідом, а також надання сприяння та підтримки державам-членам, особливо країнам, що розвиваються, в розробленні та реалізації дорожніх карт у сфері СОР. Також було визнано важливість забезпечення захисту дітей в цифровому середовищі в межах Конвенції ООН про права дитини й інших міжнародних договорів з прав людини шляхом заохочення співпраці між усіма зацікавленими сторонами, що займаються питаннями захисту дитини в цифровому середовищі.

Учасники Конференції визнали важливість Порядку денного у сфері сталого розвитку на період до 2030 року, який стосується різних аспектів захисту дитини в цифровому середовищі у межах Цілей сталого розвитку (ЦСР), в тому числі ЦСР 1, 3, 4, 5, 9, 10 і 16; також була прийнято до уваги Резолюцію 175 (Перегл. Дубай, 2018 р.) про доступ до електрозв'язку/інформаційно-комунікаційних технологій (ІКТ) для осіб з обмеженими можливостями та особливими потребами і Резолюція 67 (Перегл. Буенос-Айрес, 2017 р.) Всесвітньої конференції з розвитку електрозв'язку (ВКРЕ) про роль Сектору розвитку електрозв'язку МСЕ (МСЕ-D) в захисті дитини в цифровому середовищі.

Наприкінці 2019 року Комісія МСЕЭ/ЮНЕСКО з широкосмугового зв'язку в інтересах сталого розвитку звіт «Безпека дитини в цифровому середовищі», в якому містяться застосовні на практиці рекомендації щодо того, як зробити Інтернет безпечнішим для дітей.

Року 2009-го МСЕ випустив перший набір керівних настанов із захисту дитини в цифровому середовищі в межах ініціативи СОР. За останнє десятиріччя Рекомендації СОР були перекладені багатьма мовами та використовуються у багатьох країнах як довідковий ресурс під час розроблення дорожніх карт і національних стратегій із захисту дитини в цифровому середовищі. Вони стали підмогою для державних органів, організацій громадянського суспільства, установ з догляду за дітьми, галузевих організацій та багатьох інших зацікавлених сторін в їхніх зусиллях із захисту дитини в цифровому середовищі.

Зокрема, ці Рекомендації використовувалися під час складання, розроблення та втілення національних стратегій із захисту дитини в цифровому середовищі у багатьох державах-членах, таких як Камерун, Габон, Гамбія, Гана, Кенія, Сьєрра-Леоне, Уганда та Замбія в

Африканському регіоні; Бахрейн та Оман в Арабському регіоні; Бруней, Камбоджа, Кірибаті, Індонезія, Малайзія, М'янма і Вануату в Азійсько-Тихоокеанському регіоні; Боснія, Грузія, Молдова, Чорногорія, Польща та Україна в Європейському регіоні.

Крім того, ці Рекомендації лягли в основу регіональних заходів, таких як Регіональна конференція із захисту дитини в цифровому середовищі (АСОР) «Розширення прав та можливостей майбутніх цифрових громадян», яка пройшла в Кампалі (Уганда, 2014 р.), і Регіональна конференція АСЕАН із захисту дитини в цифровому середовищі, що відбулася в Бангкоку (Таїланд, 2020 р.)

Згідно з Резолюцією 179 (Перегл. Дубай, 2018 р.), МСЕ було доручено оновити чотири комплекти керівних настанов у співпраці з партнерами з ініціативи СОР та зацікавленими сторонами з урахуванням розвитку технологій в галузі електрозв'язку, в тому числі Рекомендації щодо дітей з інвалідністю та дітей з особливими потребами.

За підсумками цього процесу ці Рекомендації були значною мірою оновлені та переглянуті експертами і відповідними зацікавленими сторонами, які підготували широкий комплекс рекомендацій із забезпечення захисту дітей у цифровому світі. Вони є продуктом спільних багатосторонніх зусиль та підготовлені на основі знань, досвіду та експертної оцінки багатьох організацій і фахівців у галузі захисту дітей в цифровому середовищі з цілого світу. Ці Рекомендації покликані стати основою для створення безпечного та надійного кіберсвіту для майбутніх поколінь. Передбачається, що ці настанови стануть програмою, що може бути адаптована та використана відповідно до національних або місцевих традицій та законів. Крім того, ці Рекомендації присвячені питанням, які стосуються всіх дітей та молодих осіб до 18 років, з урахуванням відмінностей у потребах кожної вікової групи. Вони також спрямовані на задоволення потреб дітей, які живуть у різних умовах, дітей з інвалідністю та дітей з особливими потребами. Ці Рекомендації також розширюють охоплення заходів щодо захисту дітей в цифровому середовищі, враховуючи всі ризики, загрози та шкідливий вплив, на які можуть наражатися діти в цифровому середовищі, у співвідношенні з позитивними змінами, що їх цифровий світ може принести в їхнє життя.

Очікується, що ці Рекомендації не лише дозволять створити більш відкрите інформаційне суспільство, а й допоможуть державам-членам МСЕ виконати свої зобов'язання щодо захисту прав дітей, як передбачено в Конвенції ООН про права дитини, яка була прийнята Генеральною Асамблеєю ООН в резолюції 44/25 від 20 листопада 1989 року, і підсумковому документі Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства (ВВРІС).

Публікуючи ці Рекомендації, ініціатива СОР закликає всі зацікавлені сторони забезпечувати втілення правил та стратегій, яку захищатимуть дітей у кіберпросторі і сприятимуть безпечнішому доступу до всіх чудових можливостей, що їх можуть надати онлайн-ресурси.

Зміст

Список таблиць, рисунків та вставок

Таблиці

Зображення

Блоки

1. Огляд документа

1.1 Мета

Національні уряди зобов'язані забезпечувати захист дітей як у реальному, так і у віртуальному світі. Необхідно розуміти, що сьогодні, коли нові технології так міцно інтегровані в життя такої великої кількості дітей та молодих осіб в низці важливих сфер, більше немає сенсу намагатися зберігати чіткий розподіл між подіями реального світу й онлайн-подіями. Вони дедалі більше перетинаються і залежать один від одного.

Директивні органи1 і всі інші відповідні зацікавлені сторони відіграють надзвичайно важливу роль. В умовах стрімкого розвитку технологій багато традиційних методів розроблення політики виявляються непридатними. Для того щоб забезпечити захист дітей в цифровому середовищі, директивним органам необхідно розробити адаптивну та всеосяжну нормативно-правову базу, яка виконуватиме своє призначення в контексті швидкозмінного цифрового середовища.

Ці Рекомендації розроблені для того, щоб надати директивним органам держав-членів МСЕ зручну в користуванні та гнучку основу для розуміння та виконання ними своїх правових зобов'язань щодо забезпечення захисту дітей в реальному, тобто фізичному, та віртуальному світах.

З цією метою у цих керівних настановах висвітлюється низка важливих для директивних органів питань:

1) Що таке захист дитини в цифровому середовищі?
2) Чому директивні органи повинні дбати про захист дітей в цифровому середовищі?
3) Яка ситуація в моїй країні з погляду законодавства, соціально-політичних умов та розвитку?
4) Як директивним органам слід починати розгляд та визначення ефективної і послідовної політики щодо захисту дітей в цифровому середовищі в їхній країні?

При цьому ці Рекомендації розроблені на основі наявних моделей, механізмів та ресурсів, для того щоб розглянути конкретні приклади й отримати уявлення про передову практику, що застосовується у різних країнах світу.

1.2 Сфера застосування

Сфера застосування заходів щодо захисту дітей в цифровому середовищі поширюється на будь-яку шкоду, яка може бути заподіяна дитині в цифровому середовищі, включно з широким спектром чинників, що загрожують безпеці та добру дітей. Це комплексна проблема, до розв'язання якої слід підходити з різних сторін, в тому числі з погляду законодавства, управління, освіти, політики та суспільства.

Крім того, захист дитини в цифровому середовищі повинен ґрунтуватися на розумінні як загальних, так і конкретних для кожної країни ризиків, загроз та шкідливого впливу, на які наражаються діти в цифровому середовищі. Це потребує чіткого визначення понять та встановлення зрозумілих параметрів для втручання, в яких враховуються та розмежовуються дії, що є злочином, та дії, що не є протизаконними, проте загрожують благополуччю дитини.

З цією метою у керівних настановах надано огляд наявних загроз та шкідливого впливу, на які наражаються діти у цифровому середовищі. Разом з тим в умовах швидкого розвитку технологій та появи нових супутніх загроз і джерел шкідливого впливу традиційні терміни і методи розроблення політики виявляються неефективними. У цифрову епоху директивним органам необхідно створювати такі правові й політичні межі, які будуть досить адаптивними та відкритими для всіх, щоб розв'язувати наявні проблеми і по змозі передбачати майбутні виклики. Для цього потрібна співпраця з усіма зацікавленими сторонами, включно з галуззю

ІКТ, науковою спільнотою, громадянським суспільством, громадськістю та самими дітьми. Цей процес може бути підкріплений розглядом загальних принципів щодо захисту дитини в цифровому середовищі.

1.3 Загальні принципи

Одинадцять всеосяжних принципів, які наводяться нижче, у своїй сукупності є підмогою в розробленні перспективної цілісної національної стратегії щодо захисту дитини в цифровому середовищі.

Порядок, в якому подано ці принципи, продиктований не ступенем їх важливості, а радше логікою викладу.

Національна стратегія щодо захисту дітей в цифровому середовищі повинна:

1) базуватися на цілісному баченні, в якому враховується роль уряду, галузі та суспільства;
2) формуватися виходячи з всеосяжного розуміння та аналізу цифрового середовища загалом та коригуватися з урахуванням національних умов і пріоритетів конкретної країни;
3) узгоджуватися з основоположними правами дітей, як це закріплено в Конвенції ООН про права дитини, а також інших ключових міжнародних конвенціях та нормах, і гарантувати дотримання цих прав;
4) відповідати наявним аналогічним чи схожим внутрішнім законам та стратегіям, включно із законами про недопущення жорстокого поводження з дітьми і стратегією щодо захисту дітей, та гарантувати їх дотримання;
5) гарантувати дотримання громадянських прав та свобод дітей, якими не можна нехтувати задля забезпечення захисту;
6) розроблятися за активної участі всіх зацікавлених сторін, включно з дітьми, з урахуванням їхніх потреб та обов'язків, а також з огляду на потреби меншин та маргіналізованих груп;
7) розроблятися таким чином, щоб відповідати державним програмам більш загального характеру, спрямованим на досягнення економічного та соціального розквіту, і забезпечувати максимальний внесок ІКТ в досягнення сталого розвитку і соціальної інтеграції;
8) використовувати найбільш адекватні інструменти політики для досягнення поставленої мети з урахуванням специфічних умов відповідної країни;
9) здійснюватися на найвищому рівні в уряді, який відповідатиме за розподіл відповідних ролей та обов'язків, а також надання необхідних людських та фінансових ресурсів;
10) сприяти створенню такого цифрового середовища для дітей, батьків/опікунів та зацікавлених сторін, якому вони зможуть довіряти;

11) спрямовувати зусилля зацікавлених сторін з метою розширення прав та можливостей дітей, а також навчання дітей цифрової грамотності, для того щоб вони могли захистити себе в цифровому середовищі.

1.4 Використання цих керівних настанов

У цих керівних настановах розглядаються актуальні дослідження, наявні моделі та матеріали, а також даються чіткі рекомендації з розроблення національних стратегій щодо захисту дитини в цифровому середовищі.

- У розділі 2 надано вступну інформацію про захист дітей в цифровому середовищі та наводятьсядані останніх досліджень, в тому числі за аспектами, що стосуються нових технологій, основних загроз та шкідливого впливу, що з'являються і на які наражаються діти.
- У розділі 3 висвітлюються питання підготовки національної стратегії у сфері захисту дитини в цифровому середовищі, включаючи відповідні зацікавлені сторони, наявні приклади реагування на загрози та шкідливий вплив в цифровому середовищі, а також переваги прийняття національної стратегії.
- У розділі 4 наводяться рекомендації щодо відповідних механізмів та порядку втілення.
- У розділі 5 визначено перелік аспектів, які необхідно врахувати під час розроблення національної стратегії щодо захисту дітей в цифровому середовищі.
- У розділі 6 надано корисні довідкові матеріали.

2. Вступ

У 2019 році Інтернетом користувалася більше ніж половина населення світу. Найчисленніша група користувачів – це люди до 44 років, при цьому фіксується однакова активність серед користувачів віком від 16 до 24 років та від 35 до 44 років. Інтернетом користується кожна третя дитина (0-18 років) у цілому світі . У країнах, що розвиваються, користувачами Інтернету є переважно діти та молодь , і, за прогнозами, протягом наступних п'яти років їх кількість збільшиться більше ніж удвічі. Нові покоління користуються Інтернетом від самого дитинства, причому більшість людей під'єднується до мережі за допомогою технологій рухомого зв'язку, особливо у країнах глобального Півдня.

Попри те, що доступ до Інтернету має основоположне значення для здійснення прав дітей, як і раніше, спостерігаються серйозні регіональні, національні, гендерні та інші диспропорції в отриманні доступу, які обмежують можливості дівчат, дітей з інвалідністю, дітей із меншин та інших вразливих груп. Щодо цифрового гендерного розриву, то, як показують дослідження, у всіх регіонах світу, за винятком Сполучених Штатів Америки, серед користувачів Інтернету нараховується значно більше чоловіків, аніж жінок. У багатьох країнах дівчатка не мають рівних із хлопчиками можливостей щодо доступу до Інтернету, а в тих випадках, коли вони мають рівний доступ, їх контролюють та обмежують у використанні набагато більше, аніж хлопчиків, і вони можуть наражатися на ризики при спробах отримати доступ до інтернету . Очевидно, що дітям та молоді, які не мають достатніх цифрових навичок або розмовляють мовами меншин, непросто знайти потрібний їм контент в Інтернеті і що діти, які живуть у сільській місцевості, мають менш розвинуті цифрові навички, проводять більше часу в Інтернеті (особливо граючи в ігри) й отримують менше допомоги та контролю з боку батьків .

Проте неможливо говорити про ризики та загрози без розуміння того, наскільки величезними є переваги та можливості, що їх дають нам цифрові технології. Інтернет і цифрові технології змінюють наш спосіб життя і відкривають безліч нових можливостей для спілкування, ігор, прослуховування музики та участі в різноманітних культурних, освітніх заходах, заходах з розвитку навичок. Інтернет є засобом отримання доступу до послуг у галузі охорони здоров'я та освіти, а також до інформації на теми, що мають важливе значення для молодих осіб, але можуть розглядатися як табу в суспільстві, до якого вони належать.

Позаяк діти та молодь часто перебувають в авангарді застосування та опанування нових можливостей, які надаються Інтернетом, вони стикаються з різними явищами, що загрожують їхній безпеці та благополуччю; суспільство має усвідомлювати цю проблему й боротися з нею. Дуже важливо відкрито обговорювати ризики, на які наражаються діти та молодь в цифровому середовищі. Таке обговорення дає можливість навчити дітей та молодих осіб розпізнавати

ризики, запобігати шкідливому впливу або долати його, у разі якщо вони наразилися на нього, а також використовувати переваги, які може дати їм інтернет.

У багатьох країнах світу молодь добре обізнані з деякими ризиками, з якими вони можуть зіткнутися в цифровому середовищі7, . Наприклад, як показують дослідження, більшість дітей та молодих осіб спроможні відрізнити кібербулінг від жартів або глузування в Інтернеті. Вони розуміють, що кібербулінг має публічний характер і спрямоване на заподіяння шкоди, проте пошук балансу між можливостями та ризиками, що існують для дитини в цифровому середовищі, як і раніше, залишається складним завданням.

Держави-члени МСЕ і надалі приділяють першочергову увагу захисту дітей та молодих осіб в цифровому середовищі; при цьому необхідно дотримуватися належного балансу між вирішенням цього завдання та зусиллями щодо розширення можливостей дітей та молодих осіб в цифровому середовищі і забезпечувати захист дітей та молодих осіб таким чином, щоб не обмежувати їх доступ чи доступ ширших груп населення до інформації, а також можливість користуватися правом на свободу слова, висловлення думок та асоціації.

Є очевидна необхідність цілеспрямованої підтримки та вироблення нестандартних рішень для протидії ризикам, на які наражаються діти та молодь, в тому числі через цифровий розрив між дітьми та дорослими, який обмежує можливість батьків, учителів та опікунів давати дітям необхідні напучування. Водночас діти та молодь виростають і стають дорослими людьми, батьками й активними членами суспільства, що дає їм унікальну потенційну можливість скоротити цей цифровий розрив.

У зв'язку з цим зміцнення довіри до Інтернету мусить має першорядне значення і посідати центральне місце в державній політиці. Уряди та суспільство повинні провадити роботу з дітьми та молоддю, щоб розуміти їхню позицію й ініціювати справді суспільні дебати про ризики та можливості. Надання дітям та молоді сприяння в управлінні онлайн-ризиками може бути ефективне, проте уряди також повинні забезпечувати роботу компетентних служб підтримки для тих, кому задається шкода цифровому середовищі, а також інформувати дітей про те, як вони можуть звернутися до цих служб.

Деякі країни роблять усе можливе, щоб виділяти необхідні ресурси для вирішення проблеми цифрової грамотності та забезпечення безпеки дітей в цифровому середовищі. Проте самі діти кажуть про те, що важливу роль у розробленні рішень для підтримання їхньої безпеки в цифровому середовищі відіграють батьки, освітяни, технологічні компанії та уряди. Держави-члени МСЕ також зазначають, що такі заходи, як активізація обміну знаннями і координація зусиль з метою забезпечення захисту більшої кількості дітей в цифровому середовищі, мають значну підтримку.

Дітям та молоді доводиться орієнтуватися у дедалі складніших умовах цифрового середовища, а впровадження штучного інтелекту для машинного навчання, аналітика великих даних, роботизація, Інтернет речей, віртуальна та доповнена реальність повністю змінять досвід взаємодії дітей із медійним середовищем. У зв'язку з цим необхідні інвестиції та розроблення політики для підтримки дітей, батьків та спільнот як нині, так і в майбутньому.

2.1 Що таке захист дитини в онлайновому середовищі?

Завдяки онлайн-технологіям діти та молодь отримують величезні можливості для спілкування, набуття нових навичок, творчості та участі у створенні кращого суспільства. Проте ці технології також можуть створювати нові ризики, пов'язані з конфіденційністю, незаконним контентом, домаганнями, кібербулінгм, зловживанням особистою інформацією або грумінгом із сексуальною метою і навіть сексуальними зловживаннями щодо дітей.

Ці Рекомендації пропонують цілісний підхід до реагування на всі потенційні загрози та шкідливий вплив, на які можуть наражатися діти та молодь у процесі набуття цифрової грамотності. У них визнається, що всі відповідні зацікавлені сторони відіграють важливу роль у забезпеченні стійкості дітей та молодих осіб до впливу цифрового середовища, їх благополуччя та захисту при одночасному використанні ними можливостей, які надає Інтернет.

Захист дітей та молодих осіб є спільною відповідальністю, тому всі відповідні зацікавлені сторони повинні зробити свій внесок у досягнення сталого майбутнього для всіх. Для цього директивні органи, представники галузі, батьки, опікуни, освітяни та інші зацікавлені сторони повинні сприяти тому, аби діти та молодь могли реалізувати свій потенціал, як в цифровому середовищі, так і в реальному житті.

Поняття захисту дітей в цифровому середовищі не має універсального закріпленого визначення, проте воно передбачає цілісний підхід до створення безпечних, розрахованих на відповідний вік, відкритих і таких, що базуються на широкій участі, цифрових просторів для дітей та молодих осіб при забезпеченні:

- реагування, підтримки та самодопомоги за наявності загрози;
- запобігання шкідливому впливу;
- динамічної рівноваги між захистом та наданням дітям можливості бути цифровими громадянами;
- здійснення прав та обов'язків як дітей, так і суспільства.

Крім того, в умовах стрімкого розвитку технологій та суспільства, а також з огляду на безмежний характер Інтернету, для ефективного захисту дітей в цифровому середовищі потрібен гнучкий підхід. У цих керівних настановах докладно розглядаються основні ризики, на які наражаються діти та молодь в цифровому середовищі, включно зі шкідливим та незаконним контентом, домаганнями, кібербулінгм, зловживанням особистою інформацією чи грумінгом із сексуальною метою, сексуальними зловживаннями щодо дітей та їх сексуальною експлуатацією, проте у міру розвитку технічних інновацій виникатимуть нові виклики, які, як завжди, вирізнятимуться залежно від регіону. При цьому з новими викликами найкраще боротися спільними зусиллями в межах усього світового співтовариства, позаяк ці виклики потребуватимуть розробки нових рішень.

2.2 Діти в цифровому світі

Інтернет змінив наш спосіб життя, Він став невід'ємною складовою життя дітей та молодих осіб, унеможлививши сприйняття фізичної та цифрової реальності у відриві одне від

одного. На сьогодні діти та молодь становлять третину від загальної кількості користувачів Інтернету; за оцінками ЮНІСЕФ, 71% молодих осіб уже мають доступ до Інтернету.

Поширення доступу до Інтернету значно розширило можливості людей. Онлайн-світ дозволяє дітям та молоді долати обмеження, пов'язані з несприятливим становищем або інвалідністю, надає нові формати розваг, освіти, участі та вибудовування стосунків. На сьогодні цифрові платформи використовуються для різноманітних видів діяльності і часто мають мультимедійний характер.

Наявність доступу до цих технологій, вміння користуватися ними й орієнтуватися у цьому середовищі має велике значення для розвитку молодих осіб, тому ці технології використовуються ними з раннього віку. Директивні органи повинні розуміти, що часто діти та молодь починають користуватися різними платформами й послугами до того, як досягають установленого вікового мінімуму, тож навчання має починатися з малих літ.

Діти та молодь хочуть брати участь в обговоренні цієї проблеми; як представники цифрового покоління, вони мають цінний досвід і знання, якими вони можуть поділитися. Директивні органи та фахівці-практики повинні перебувати у безперервному діалозі з дітьми та молоддю з питань онлайн-середовища, щоб підтримати додержання їхніх прав.

Доступ до Інтернету

У 2019 році Інтернетом користувалася понад половина населення світу (53,6%): кількість користувачів становила близько 4,1 мільярда. Кожен третій користувач Інтернету в цілому світі – це дитина до 18 років . У деяких країнах з низьким рівнем доходу це співвідношення становить один до двох, а в країнах з більш високим рівнем доходу – приблизно один до п'яти. За даними ЮНІСЕФ, доступ до Інтернету має вже 71% молодих осіб у цілому світі . Таким чином, присутність дітей та молодих осіб в Інтернеті стає значною, постійною та незмінною . Інтернет використовується з різною соціальною, економічною та політичною метою, споживчий продукт або послугу і стає невід'ємним атрибутом життя родин, дітей та молодих осіб.

Дані за 2017 рік свідчать, що в різних регіонах доступ дітей та молодих осіб до Інтернету значною мірою залежить від рівня доходу. Як правило, у країнах з низьким рівнем доходу налічується менше дітей, які користуються Інтернетом, аніж у країнах із високим рівнем доходу.

У більшості країн діти та молодь проводять в Інтернеті більше часу у вихідні, аніж у будні, причому найбільше часу в мережі проводять підлітки (15-17 років) – в середньому від 2,5 до 5,3 годин, залежно від країни.

Використання Інтернету

Для виходу в Інтернет діти та молодь найчастіше використовують мобільний телефон, на другому та третьому місці – настільний комп'ютер та ноутбук відповідно. Діти та молодь проводять в Інтернеті в середньому близько двох годин на день протягом тижня і приблизно вдвічі більше часу у вихідні дні. Деякі залишаються під'єднаними безперервно. Проте чимало і тих, хто досі не має можливості виходу в Інтернет із дому.

На практиці більшість дітей та молодих осіб, які користуються Інтернетом, під'єднуються за допомогою кількох пристроїв: діти та молодь, які підключаються до Інтернету щонайменше раз на тиждень, можуть використовувати до трьох різних пристроїв. Діти старшого віку, а також діти у більш заможних країнах, як правило, використовують більше пристроїв, причому у всіх обстежених країнах хлопчики використовують більшу кількість пристроїв, аніж дівчатка. Найпоширеніший вид активності як серед дівчат, так і серед хлопчиків – це перегляд відеороликів. Понад три чверті дітей та молодих осіб, які користуються Інтернетом, кажуть, що дивляться відео в Інтернеті принаймні раз на тиждень разом з іншими членами родини або самостійно. Багатьох дітей та молодих осіб можна віднести до категорії соціально активних користувачів, позаяк вони зареєстровані відразу на декількох платформах, таких як Facebook, Twitter, TikTok і Instagram.

Діти та молодь також використовують Інтернет для участі в політиці та ведуть блоги для того, щоб висловлювати свою думку.

Загальний рівень участі в онлайн-іграх варіюється залежно від країни та приблизно відповідає ступеню доступності Інтернету для дітей та молодих осіб, при цьому 10-30% дітей та молодих осіб, які користуються інтернетом, щотижня займаються творчою діяльністю в онлайн-режимі.

Щодо освіти, то чимало дітей та молодих осіб різного віку користуються Інтернетом щотижня, аби зробити домашнє завдання, надолужити упущене після пропуску занять або знайти інформацію про здоров'я. Діти старшого віку, як видається, виявляють більшу зацікавленість до пошуку інформації, аніж діти молодші.

2.3 Вплив технологій на цифровий досвід дітей

Інтернет та цифрові технології можуть бути джерелами як можливостей, так і ризиків для дітей та молодих осіб. Наприклад, коли діти використовують соціальні мережі, перед ними відкриваються численні можливості для дослідження, навчання, спілкування та розвитку основних навичок. Зокрема, соціальні мережі сприймаються дітьми як платформи, що дозволяють їм розкривати власну ідентичність у безпечному середовищі. Володіння необхідними навичками та знаннями про те, як вирішувати проблеми, пов'язані з конфіденційністю та репутацією, має велике значення для молодих осіб.

«Я знаю, що все опубліковане нами в Інтернеті залишається там назавжди і може вплинути на наше життя у майбутньому» (хлопчик, 14 років, Чилі).

Проте, як було встановлено в процесі консультацій, більшість дітей використовують соціальні мережі до досягнення мінімально допустимого віку, який становить 13 років11, а служби перевірки віку, як правило, слаборозвинуті або їх немає взагалі, тому ризики, на які наражаються діти, можуть зростати. Попри те що діти прагнуть опанувати цифрові навички і бути добросовісними цифровими громадянами, дбаючи про недоторканність свого приватного життя, вони схильні замислюватися про цю проблему в стосунку до своїх друзів та знайомих: їх більше непокоїть, що можуть побачити їхні друзі, аніж незнайомі люди і треті особи. Усе це, у сукупності з притаманною дітям зацікавленістю та їх більшою схильністю до ризиків, може зробити їх більш вразливими до грумінгу, експлуатації, булінг або інших видів шкідливого контенту чи контакту.

Широка популярність обміну світлинами та відео за допомогою мобільних застосунків, зокрема використання дітьми платформ потокового контенту, також породжує занепокоєння стосовно недоторканності їхнього приватного життя та можливих ризиків. Деякі діти роблять світлини сексуального характеру за власної участі, участі своїх друзів, братів або сестер та діляться ними в Інтернеті. Для декого, особливо для дітей старшого віку, це може бути природним проявом сексуальності та пошуком сексуальної ідентичності, проте в інших випадках, зокрема це стосується дітей молодшого віку, йдеться про примус з боку дорослого чи іншої дитини. У будь-якому разі подібний контент є незаконним у багатьох країнах, він може стати причиною того що дитина наразиться на переслідування, або може бути використаний для подальшої експлуатації дитини.

Аналогічним чином онлайн-ігри дозволяють дітям реалізовувати свої основоположні права, в тому числі право грати, встановлювати контакти, проводити час із друзями, заводити нових друзів та розвивати важливі навички. У більшості випадків це може бути позитивний досвід. Проте з'являється дедалі більше свідчень, які вказують на те, що діти, які використовують онлайн-ігрові платформи без нагляду та без підтримки з боку відповідального дорослого, також можуть наражатися на ризики, такі як ігрові розлади, фінансові махінації, збір та монетизація особистих даних дітей, кібербулінг, агресивні висловлювання, насильство та неприйнятні контакти або контент, а також грумінг з використанням реальних світлин та відео або картинок та відео, які створені комп'ютером чи належать до віртуальної реальності, де зображуються або виставляються як норма сексуальні зловживання щодо дітей чи їх сексуальна експлуатація.

Крім того, розвиток технологій спричинився до появи Інтернету речей, який передбачає під'єднання дедалі більшої кількості різноманітних пристроїв один до одного, їх взаємодію та поєднання в мережі за допомогою Інтернету. До таких предметів належать іграшки, радіоняні та пристрої що працюють на основі штучного інтелекту, що може створювати ризики з погляду недоторканності приватного життя та небажаних контактів.

2.4 Основні загрози, на які наражаються діти в цифровому середовищі

Дорослі та діти наражаються на різноманітні ризики та загрози в цифровому середовищі. Проте діти є набагато вразливішою групою населення. Мало того, деякі категорії дітей перебувають в особливо вразливому становищі, наприклад діти з інвалідністю або діти в процесі транзиту. Директивні органи повинні робити все необхідне, щоб усі діти могли розвиватися та навчатися в безпечному цифровому середовищі. Думка про те, що діти вразливі і їх слід захищати від усіх форм експлуатації, визначена в Конвенції ООН про права дитини.

У деяких сферах цифрове середовище відкриває перед дітьми величезні можливості, які водночас можуть посилювати ризики, здатні завдати дитині серйозної шкоди та підірвати її благополуччя. Є побоювання як щодо дітей, так і щодо дорослих, що Інтернет, наприклад, може використовуватися для втручання у приватне життя, поширення дезінформації або, що ще гірше, доступу до порнографії.

Стосовно цього важливо проводити розмежування між ризиками та шкідливим впливом, на який наражаються діти. Не всі дії, які за певними ознаками можуть розцінюватися як ризик, є небезпечними, і не всі ризики обов'язково шкоди дітям – наприклад, секстинг, який може використовуватися молоддю для розкриття своє сексуальності й отримання досвіду стосунків, що аж ніяк не завжди завдає шкоди.

Рисунок 2: Класифікація загроз, на які наражаються діти в цифровому середовищі

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

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

З настанням цифрової епохи з'явилися нові виклики, пов'язані із захистом дитини. Діти повинні мати можливість почуватися захищеними в цифровому середовищі та користуватися численними благами, які воно надає.

Директивні органи повинні забезпечувати прийняття необхідного законодавства, надання гарантій та розроблення інструментів, для того щоб діти могли розвиватися й навчатися в безпечних умовах. Украй важливо, щоб діти мали всі необхідні навички для визначення загроз і повністю усвідомлювали наслідки своєї поведінки в цифровому середовищі.

В Інтернеті діти можуть наразитися на численні загрози, що виходять від організацій, дорослих та однолітків.

Контент і маніпуляція

- Зіткнувшись із неприйнятним або навіть злочинним контентом, діти можуть впадати в такі крайнощі, як заподіяння шкоди самим собі, руйнівна та жорстока поведінка. Вплив такого контенту може призвести до радикалізації дітей, а також розвитку у них зацікавленості до расистських або дискримінаційних ідей. Відомо, що чимало дітей не дотримуються вікових обмежень, установлених на вебсайтах.
- Отримання дітьми неточної або неповної інформації не дозволяє їм сформувати повноцінне уявлення про навколишній світ. Тенденція до персоналізації контенту залежно від поведінки користувача може призводити до утворення «інформаційної бульбашки», яка не дає дітям можливості розвиватися та споживати різноманітний контент.
- Вплив контенту, підданого алгоритмічній фільтрації з метою маніпуляції, може справити серйозний вплив на розвиток дитини, її погляди, цінності та звички. Ізоляція дітей у «відлуння-камері» чи «інформаційній бульбашці» обмежує їх доступ до всього розмаїття поглядів та ідей.

Контакти з дорослими та однолітками

Діти можуть стикатися з широким спектром загроз, вступаючи в контакт із дорослими або однолітками.

- Булінг в Інтернеті може мати ширші масштаби та поширюватися швидше, аніж в офлайн-середовищі. Булінг може здійснюватися у будь-який час - вдень чи вночі, порушуючи межі «простору», який донедавна вважався безпечним, і може мати анонімний характер.
- Діти, які стають жертвами в реальному житті, найімовірніше, зазнаватимуть віктимізації в цифровому середовищі. Таким чином, для дітей з інвалідністю є більша небезпека наражатися на ризики, адже, як показують дослідження, такі діти частіше стають жертвами різного типу зазіхань та особливо часто наражаються на сексуальну віктимізацію. Віктимізація може включати в себе булінг, домагання, ізоляцію та дискримінацію на ґрунті наявної чи можливої інвалідності дитини або аспектів, пов'язаних з її інвалідністю, таких як особливості поведінки чи мовлення, пристрої чи послуги, якими вона користується.
- Дифамація та заподіяння шкоди репутації: зображення та відео можуть редагуватися й поширюватися серед мільярдів людей. Невиправдано жорстокі коментарі можуть багато років залишатися доступними для перегляду.
- Діти можуть наражатися на переслідування, грумінг та наругу в Інтернеті з боку кривдників, які можуть перебувати як поблизу, так і в іншому кінці світу і які часто прикидаються тими, ким вони не є. Такий вплив може виявлятися в різним формах, включно з радикалізацією та примусом дітей до того, щоб вони самі надсилали контент сексуального характеру за власної участі.
- Здійснення покупок унаслідок тиску, обману чи примусу з дозволу платника чи без нього.
- У зв'язку з небажаною рекламою виникають запитання щодо згоди та продажу даних.

Поведінка дитини, яка може мати наслідки

- Булінг в цифровому середовищі може бути особливо неприємне чи руйнівне, тому що воно поширюється у ширших масштабах, з більшим ступенем публічності, а контент, що поширюється за допомогою електронних засобів, може в будь-який момент знову потрапити у фокус уваги, внаслідок чого людині, що стала жертвою булінг, може бути непросто забути про інцидент; такий контент може містити дискредитувальні візуальні зображення або образливі слова; він доступний 24 години на добу; булінг за допомогою електронних засобів зв'язку може відбуватися 24 години на добу 7 днів на тиждень, вдираючись у приватне життя жертви навіть там, де вона повинна почуватися в безпеці, наприклад удома; персональна інформація може бути спотворена, світлини змінені і потім передані іншим людям. Мало того, булінг може бути анонімне. Розкриття персональних даних може призвести до заподіяння фізичної шкоди, в тому числі до зустрічі в реальному житті після знайомства в Інтернеті, коли є небезпека фізичного насильства та/або сексуальних зловживань.
- Недотримання власних прав чи прав інших людей у процесі плагіату та завантаження в Інтернет контенту без дозволу, зокрема створення та розміщення в Інтернеті світлини неналежного змісту без дозволу.
- Порушення авторських прав інших людей, наприклад шляхом стягування з Інтернету музики, фільмів чи ТБ-програм, за які слід було б заплатити, позаяк це може завдати шкоди жертві крадіжки.
- Маніакальне чи надмірне використання Інтернету та/або онлайн-ігор на шкоду соціальним заходам та/або заняттям на свіжому повітрі, важливим для здоров'я, зміцнення довіри, соціального розвитку та загального добра.

- Спроби заподіяння шкоди, домагання чи булінг стосовно будь-кого, в тому числі коли зловмисник прикидається іншою людиною, часто іншою дитиною.
- Серед підлітків стає дедалі поширенішим таке явище, як «секстинг» (надсилання зображень або повідомлень сексуального характеру за допомогою мобільних телефонів). Як правило, люди надсилають такі зображення та повідомлення партнерам, з якими вони мають стосунки, або потенційним партнерам, проте іноді ці речі стають доступними для ширшої аудиторії. Малоймовірно, що підлітки повною мірою усвідомлюють наслідки подібної поведінки та потенційні ризики, які вона може потягти за собою.

2.5 Основні джерела шкоди для дітей в цифровому середовищі

У попередньому розділі йдеться про загрози, на які діти можуть наразитися онлайн. У цьому розділі висвітлюється шкода, що може стати наслідком цих загроз.

Джерела шкоди

Згідно з дослідженнями ЮНІСЕФ про використання Інтернету, до ризиків та джерел шкоди належать такі категорії:

- Заподіяння собі шкоди:
  - контент, що стосується самогубства;
  - дискримінація.
- Вплив неналежних матеріалів:
  - вплив екстремістського/насильницького контенту;
  - прихований маркетинг;
  - азартні онлайн-ігри.
- Близько 20 відсотків дітей, опитаних на цю тему, сказали, що за минулий рік бачили вебсайти або дискусії в мережі про те, як люди завдають собі фізичної шкоди чи болю.
- Радикалізація:
  - ідеологічна обробка;
  - агресивні висловлювання.
- Діти з великою ймовірністю повідомляли про те, що були засмучені агресивними висловлюваннями або контентом сексуального характеру в мережі, що з ними поводилися неналежним чином в цифровому середовищі чи в реальному світі, або тим, що вони зустрілися віч-на-віч з тим, з ким спочатку познайомилися в мережі.
- Сексуальні зловживання та сексуальна експлуатація:
  - власноручно створений контент;
  - грумінг із сексуальною метою;
  - матеріали, пов'язані із сексуальними зловживаннями щодо дітей (CSAM);
  - торгівля людьми;
  - сексуальна експлуатація дітей у подорожах і туризмі.

Проведене 2017 року дослідження становища дітей в Данії, Угорщині та Сполученому Королівстві показало, що у 6 відсотків дітей були відверті світлини, які передавалися без їхнього дозволу.

У 2019 році Фонд спостереження за Інтернетом (IWF) виявив понад 132 000 вебсторінок із підтвердженою наявністю зображень та відеоматеріалів, які містять сцени сексуальних зловживань щодо дітей. Кожна вебсторінка могла містити від одного до тисяч зображень цієї форми зловживань.

Ризики, пов'язані з насильством в цифровому середовищі, такі як поширення світлин оголеної натури без згоди та кібербулінг, характеризуються нерівномірною гендерною динамікою, за якої дівчатка, як правило, більшою мірою потерпають від гендерно обумовленого тиску щодо сексуальної поведінки, зазнають більш негативних наслідків, пов'язаних зі шкодою.

- Порушення щодо персональних даних та неправомірне їх використання:
  - злом;
  - шахрайство і крадіжка.

  Чимало людей знайомі з шахрайством та зломом, але люди вторгнення у приватне життя дитини в мережі розглядається як порушення іншого штибу. Дорослі часто діють неналежним чином стосовно молодих осіб, ретельно вивчаючи вміст їхніх мобільних телефонів та відстежуючи їхню діяльність у мережі; наприклад, опитування дітей у Бразилії показують, що як хлопчики, так і дівчатка з різних вікових груп вважають, що батьки більше схильні контролювати використання Інтернету дівчатками. Спроби пояснити це часто вказують на те, що подекуди дівчатка можуть бути більш уразливі через соціальні структури, в яких вони живуть, зокрема з погляду їхньої безпеки, в умовах коли межа між взаємодією в мережі та в реальному світі стає дедалі розмитішою.

- Кібербулінг, переслідування та домагання: ворожа та насильницька діяльність однолітків.

  Чати і сайти соцмереж можуть відкрити можливість для насильства та булінг, коли анонімні користувачі, в тому числі молодь, беруть участь в агресивному та образливому спілкуванні. У семи країнах Європи – Бельгії, Данії, Ірландії, Італії, Португалії, Румунії та Сполученому Королівстві – Лівінгстон, Маскероні, Олафссон та Хеддон1 виявили, що 2010 року в середньому 8 відсотків дітей стали жертвами кібербулінг, а 2014 року жертвами кібербулінг стали 12 відсотків дітей.

Важливо наголосити, що діти з найвразливіших груп з великою вірогідністю можуть стати жертвами кібербулінг.

У центрі уваги: посилення нерівності

У 2017 році в африканському регіоні не мали доступу до мережі близько 60 відсотків дітей, тимчасом як в Європі їх частка становила 4 відсотки. У всіх регіонах світу кількість чоловіків, які користуються Інтернетом, перевищує кількість жінок, а користування Інтернетом дівчатками часто контролюється й обмежується. З поширенням широкосмугового зв'язку на позбавлені з'єднання райони планети очікується значне посилення цієї нерівності .

Діти, які користуються мобільними телефонами, а не комп'ютерами, не можуть отримати кращий досвід перебування в цифровому середовищі. Діти, які говорять мовами меншин, часто не можуть знайти потрібний контент у мережі, а діти із сільських районів частіше наражаються на крадіжку паролів чи коштів.

Дослідження показують, що чимало підлітків у цілому світі змушені долати істотні бар'єри на шляху до участі в онлайн-житті. Для багатьох із них основними перешкодами залишаються проблеми доступу: поганий зв'язок, неприйнятно висока вартість тарифів підмикання та пристроїв, а також відсутність відповідного обладнання.

З поширенням доступного широкосмугового зв'язку в країнах, що розвиваються, необхідно в оперативному порядку вжити заходів щодо мінімізації ризиків та загроз для цих дітей, а також дати їм можливість скористатися всіма перевагами цифрового світу.

У центрі уваги: матеріали, пов'язані із сексуальними зловживаннями щодо дітей (CSAM)

Масштаб проблеми

Інтернет змінив масштаб та характер виробництва, поширення та доступності CSAM. У 2018 році технологічні компанії, які базуються у Сполучених Штатах Америки, повідомляли, що у цілому світі є понад 45 млн доступних онлайн-зображень та відеоматеріалів, в яких, як припускається, діти зазнають сексуальних зловживань. Це глобальна галузь, і масштаби та тяжкість цього зловживання зростають, попри зусилля щодо його припинення.

Історично склалося так, що в реальному світі пошук CSAM для злочинців був пов'язаний зі значними ризиками та великими затратами на доступ до матеріалів. Завдяки Інтернету злочинці тепер можуть відносно легко отримати доступ до цих матеріалів та поводитися ризикованіше. Відеокамери стали компактніші, вони дедалі більше інтегруються в кожен аспект нашого життя, що робить процес виробництва CSAM й отримання контенту від безконтактних зловживань легшим, аніж будь-коли.

Неможливо визначити точний масштаб чи форму цієї підпільної та незаконної діяльності. Проте зрозуміло, що кількість нелегальних зображень, що перебувають нині в обігу, може становити мільйони. Майже всі зображення з дітьми були скопійовані. У 2018 році IWF відстежив, як часто

з'являлися зображення дитини, яка була врятована в 2013 році. За три місяці аналітики IWF відстежили зображення 347 разів – 25 разів на тиждень.

Поточний стан справ

Щоразу, коли зображення дитини, яка зазнала насильства, з'являється у мережі або завантажується злочинцем, ця дитина знову зазнає експлуатації. Жертви змушені жити з фактом продовження існування й поширення цих зображень решту свого життя.

Щойно виявляється матеріал, що містить елементи сексуальних зловживань стосовно дітей, або вебхостинг, на якому розміщено подібні матеріали, важливо якомога швидше видалити чи заблокувати контент. Глобальна природа Інтернету ускладнює це завдання: порушники можуть виробляти матеріал в одній країні й розміщувати його в іншій для споживачів у третій. Практично неможливо діяти відповідно до національних ордерів або повідомлень без комплексної міжнародної співпраці.

Швидкість інновацій в цифровому світі означає, що середовище злочинної діяльності постійно змінюється.

Основні загрози, які з'явилися останнім часом, включають:

- Підвищення рівня шифрування ненавмисно дозволяє зловмисникам діяти й обмінюватися матеріалами прихованими каналами, тимчасом як виявлення та правоохоронна діяльність ускладнені.
- Форуми, присвячені грумінгу дітей, є в закритих куточках Інтернету, нормалізують та заохочують таку поведінку, часом вимагаючи завантажити новий контент для можливості приєднатися.

- Швидке поширення дозволяє користувачам виходити в мережу в тих регіонах, де ще тільки мають намір розробити/реалізувати комплексну стратегію захисту чи відповідну інфраструктуру.
- Діти користуються пристроями без нагляду у дедалі більш ранньому віці, а сексуальна поведінка в цифровому середовищі нормалізується. Кількість випадків зловживання власноруч створеними зображеннями зростає з кожним роком.

У центрі уваги: власноруч створений контент

Діти і підлітки можуть робити компрометуючі зображення або відеозаписи. Хоча така поведінка сама по собі не конче є протизаконною і може мати місце в межах нормального, здорового сексуального розвитку, є ризик, що будь-який подібний зміст може бути поширений в цифровому середовищі або в реальному світі з метою заподіяння шкоди дітям чи бути використаний для вимагання. Хоча деякі діти можуть ділитися своїми зображеннями сексуального характеру внаслідок тиску чи примусу, інші (зокрема, підлітки) можуть охоче створювати сексуальний контент. Це не означає, що вони погоджуються на виконання та/або поширення цих зображень з метою зловживання чи експлуатації або несуть за це відповідальність.

Секстинг визначається як «самостійне виробництво зображень сексуального характеру », «обмін повідомленнями або зображеннями сексуального характеру» чи «створення, пересилання або розсилання непристойних зображень, зображень, що містять оголену натуру, з використанням мобільного телефону та/або через Інтернет» . Секстинг є формою самостійно створеного контенту відвертого сексуального змісту , і ця практика «надзвичайно розмаїта з погляду контексту, значення та намірів» .

Хоча секстинг, можливо, є найпоширенішою формою відвертого сексуального контенту, що створюється самими дітьми, і часто відбувається за обопільною згодою підлітків, які отримують задоволення від досвіду, проте є також багато форм непроханого секстингу. Йдеться про аспекти цієї діяльності, які не містять елемента згоди, таких як обмін або отримання небажаних світлин, відеозаписів або повідомлень, наприклад, від відомих чи невідомих осіб, які намагаються вступити в контакт з дитиною, вчинити на неї тиск або зваблювати її. Секстинг також може бути формою булінг сексуального характеру, коли на дитину чинять тиск, щоб вона надіслала світлину хлопцю/подрузі/однолітку, які потім поширюють його серед ровесників без отримання згоди.

У центрі уваги: кібербулінг

Тимчасом як булінг як явище з’явилося задовго до Інтернету, збільшені масштаби, сфера охоплення та безперервність булінг, що здійснюється в цифровому середовищі, можуть ще більше посилити і так неприємний та часто шкідливий досвід жертв. Кібербулінг визначається як навмисне та неодноразове заподіяння шкоди шляхом використання комп’ютерів, мобільних телефонів та інших електронних пристроїв. Воно часто має місце паралельно з булінгм у реальному світі, що відбувається у школі чи будь-де іще, може мати додаткові расистські, релігійні чи сексистські аспекти, і є продовженням шкоди, якої завдають в цифровому середовищі, наприклад, шляхом злому облікового запису, поширення світлин та відео в мережі,а також безперервного характеру образливих повідомлень та доступності контенту. Як правило, це проблема соціального характеру, що не має елементів карного діяння, і стратегія боротьби з явищем кібербулінг потребує цілісного підходу, що охоплює школи, родини і насамперед самих дітей.

У центрі уваги: грумінг та секс-вимагання в цифровому середовищі

Зі швидким розвитком технологій та розширенням доступу до Інтернету і цифрових засобів зв'язку, що спостерігаються останніми роками, неминуче зростає ризик скоєння в Інтернеті злочинних діянь, спрямованих проти дітей. Серед цих нових форм сексуальної експлуатації дітей в мережі можна назвати грумінг та секс-вимагання стосовно дітей в цифровому середовищі. Грумінг в цифровому середовищі в широкому сенсі означає процес встановлення дружніх стосунків дорослого з дитиною (віком до 18 років) та справляння впливу на дитину шляхом використання Інтернету або інших цифрових технологій для полегшення контактної чи безконтактної сексуальної взаємодії з цією дитиною. У процесі грумінгу порушник намагається домогтися виконання дитиною інструкцій, щоб зберегти таємницю виявлення й уникнути покарання20. Важливо визнати, що є також випадки зловживань між однолітками.

Заданими Інтерполу, Інтернет полегшує грумінг завдяки наявності великої кількості легкодоступних потенційних цілей та можливостей для грумерів поставати у привабливому для дитини образі. Порушники, які займаються сексуальною експлуатацією дітей в цифровому середовищі, використовують маніпуляцію, примус та спокушання, щоб подолати стримувальні чинники і схилити дітей до участі в діях сексуального характеру. Грумер навмисне виявляє вразливу потенційну жертву, збирає інформацію про ситуацію в родині дитини й використовує тиск або почуття сорому/страху для сексуальної експлуатації дитини. Грумери можуть використовувати порнографічні матеріали для дорослих, а також контент, що містить елементи насильства над дітьми чи їх експлуатації, щоб подолати стримувальні чинники поведінки жертв, подаючи участь дитини в діях сексуального характеру як природну та нормальну. Інтернет змінив спосіб взаємодії людей один з одним і дав нове визначення поняття «друг». Грумер може дуже легко і швидко встановити дружбу з дитиною в цифровому середовищі, що змушує переглянути традиційні освітні повідомлення про небезпеки, які йдуть від незнайомців.

Грумінг в цифровому середовищі уперше був офіційно визнаний у Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуальних зловживань (Лансаротська конвенція) - міжнародному правовому документі 2007 року. Стаття 23 встановлює кримінальну відповідальність за «домагання стосовно дітей із сексуальною метою», яка передбачає наявність умисної пропозиції зустрітися з дитиною з метою скоєння злочину сексуального характеру, за якою ідуть «практичні дії, спрямовані на проведення такої зустрічі». У

багатьох випадках грумінгу діти зазнають сексуальних зловживань та сексуальної експлуатації в цифровому середовищі - «зустріч», передбачена Лансаротською конвенцією та багатьма наявними національними законами, є повністю віртуальною, але разом з тим завдає такої самої шкоди дитині, як і зустріч у реальному світі. Украй важливо, що кримінальна відповідальність за грумінг поширювалася «на випадки, коли сексуальні зловживання не є результатом особистої зустрічі, а скоюються в цифровому середовищі» .

Секс-вимагання може мати місце як частина грумінгу в цифровому середовищі або як самостійний злочин . Хоча секс-вимагання може відбуватися окремо від грумінгу в цифровому середовищі, в деяких випадках грумінг в цифровому середовищі може призвести до секс-вимагання . Секс-вимагання може відбуватися в контексті грумінгу в цифровому середовищі, тому що грумер маніпулює дитиною та справляє на неї вплив у процесі грумінгу, погрожуючи, залякуючи та змушуючи її пересилати свої зображення

сексуального характеру (власноруч створений контент) . Якщо жертва не надає запитані сексуальні послуги, додаткові інтимні зображення, гроші чи інші послуги, її зображення можуть бути розміщені в Інтернеті з метою принизити, викликати тривогу або змусити дитину до створення додаткового контенту відверто сексуального характеру .

Секс-вимагання класифікується як «віртуальна насильницька дія сексуального характеру» через схожі емоційні та психологічні наслідки для жертв . Подекуди дія настільки травмує, що жертви намагалися завдати собі шкоди або вчинити самогубство, щоб уникнути зловживань.

Європол зазначає, що збір інформації для оцінки масштабу секс-вимагання стосовно дітей є складним завданням і цей масштаб може бути сильно занижений . Крім того, відсутність загальної термінології та визначень для грумінгу і секс-вимагання в цифровому середовищі є перешкодою для збору точних даних та розуміння істинного масштабу проблем у цілому світі.

2.6 Діти, які перебувають у вразливому становищі

Діти та молодь можуть перебувати у вразливому становищі з цілої низки причин. Дослідженням, проведене у 2019 році, показало, що «життя в цифровому середовищі дітей та молодих осіб, які перебувають у вразливому становищі, не супроводжується тим особливим і уважним ставленням, яке в реальному житті обумовлюється їх несприятливою ситуацією». Мало того, у звіті сказано, що «в кращому разі вони [діти та молодь] отримують ті самі загальні рекомендації щодо безпеки в цифровому середовищі, що й усі інші діти та молодь, тимчасом як їм потрібна спеціалізована допомога».

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

Діти-мігранти

Діти та молодь із середовища мігрантів часто приїжджають до країни (або вже живуть там) із певним соціокультурним досвідом та очікуваннями. Незважаючи на те що технології зазвичай розглядаються як чинник, що сприяє налагодженню зв'язків та громадській участі, рівень онлайн-ризиків та можливостей може значно варіюватися залежно від умов. Крім того, отримані емпіричним шляхом дані та практичні дослідження свідчать про найважливішу роль цифрових засобів загалом:

- вони є важливими для орієнтування (у разі переїзду до нової країни).
- Це найважливіший засіб освоєння та ознайомлення із суспільством/культурою країни, що приймає.
- Соціальні мережі можуть відігравати ключову роль у підтриманні зв'язку з родиною та однолітками, а також в отриманні доступу до інформації загального характеру.

Поряд із багатьма позитивними аспектами цифрові засоби можуть також створювати для мігрантів труднощі:

- Інфраструктура: важливо замислюватися про створення безпечного онлайн-простору, для того щоб діти та молодь – мігранти могли користуватися Інтернетом безпечно та конфіденційно.
- Ресурси: мігранти витрачають більшу частину грошей на телефонні картки з попередньою оплатою.

- Інтеграція: поряд із доступом до технологій дітям та молоді – мігрантам також потрібна добра цифрова освіта.

Діти з розладами аутистичного спектру (ASD)

Аутистичний спектр охоплює дві основні сфери поведінкової діагностичної класифікації DSM-526:

- обмежена і повторювана поведінка («потреба в одноманітності»);
- труднощі спілкування та комунікації;
- часта у поєднанні з розумовою відсталістю, мовними й аналогічними проблемами.

Технології та Інтернет відкривають дітям та молоді безмежні можливості для навчання, спілкування та ігор. Проте поряд із перевагами є значна кількість ризиків, на які можуть більшою мірою наражатися діти та молодь з ASD:

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

Діти з інвалідністю

Діти з інвалідністю наражаються на ризики в цифровому середовищі багато в чому так само, як і діти без інвалідності, але попри це вони можуть наражатися на специфічні ризики, пов’язані з їхньою інвалідністю. Діти з інвалідністю часом стикаються з маргіналізацією, стигматизацією та бар’єрами (фізичними, економічними, соціальними, а також бар’єрами, що стосуються ставлення з боку інших людей) для участі в житті своїх спільнот. Подібний досвід може сприяти тому, що дитина з інвалідністю буде прагнути соціальної взаємодії та пошуку друзів в цифровому середовищі, що може мати позитивний результат, підвищити самооцінку та створити мережу підтримки. Проте це може призвести до підвищеного ризику таких дій щодо цих дітей та молодих осіб, як грумінг, схиляння в цифровому середовищі до дій сексуального характеру та/або сексуального домагання. Згідно з дослідженнями, діти та молодь, які мають труднощі в реальному світі, а також відчувають проблеми психологічного характеру, наражаються на підвищений ризик подібних інцидентів .

Загалом діти, які стають жертвами в реальному світі, найімовірніше, будуть жертвами в цифровому середовищі. Це означає, що дітям з інвалідністю загрожує більш високий ризик в цифровому середовищі, при тому що вони відчувають більшу потребу в ньому. Дослідження показують, що діти з інвалідністю частіше стають жертвами зловживань будь-якого виду і, зокрема, сексуальної віктимізації30. Віктимізація може включати в себе булінг, домагання, виключення та дискримінацію, що ґрунтується на фактичній або очікуваній інвалідності дитини чи на аспектах, пов’язаних з інвалідністю, наприклад, особливостями її поведінки або мовлення, обладнанням чи послугами, якими вона користується.

Серед осіб, які скоюють такі правопорушення, як грумінг, схиляння в цифровому середовищі до дій сексуального характеру та/або сексуальні домагання щодо дітей та молодих осіб 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 осіб 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 поліпшують мобільність), причому деякі з них самі прикидаються людьми з інвалідністю. Ці особи можуть вчиняти такі дії, як завантаження фото і відео дітей та молодих осіб 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.

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

Деякі діти з інвалідністю можуть наражатися на труднощі під час використання онлайн-майданчиків чи навіть на вилучення з мережевого середовища через недоступність дизайну (наприклад, застосунки, які не дозволяють збільшувати розмір тексту), відсутність спеціальних можливостей (наприклад, програмного забезпечення для читання з екрана чи адаптивного комп'ютерного управління) або необхідність у відповідній підтримці (наприклад, навчити користуватися обладнанням, допомогти з орієнтуванням у соціальних взаємодіях).

Щодо ризику, пов'язаного з укладанням договору чи підписанням умов, діти з інвалідністю більшою мірою ризикують прийняти юридичні умови, які іноді не можуть зрозуміти навіть дорослі.

2.7 Сприйняття дітьми ризиків в цифровому середовищі

Діти звертають увагу на такі ризики, як схильність до зазнавання насильства у цілому світі, доступ до неприйнятного контенту, товарів та послуг; занепокоєність щодо надмірно активного користування продуктами; питання захисту даних та недоторканності приватного життя.

Підлітки повідомляють про низку проблем, пов'язаних із їх взаємодією з цифровими технологіями. До них належать широко обговорювані проблеми безпеки в цифровому середовищі, такі як побоювання взаємодії з незнайомими людьми в мережі, доступ до невідповідного контенту або вплив шкідливих програм чи вірусів, тимчасом як інші проблеми пов'язані з надійністю їх доступу до технологій: втручання батьків у їхнє «приватне» життя в мережі, їхні навички цифрової грамотності.

Дослідження EU Kids Online показує, що порнографія і зміст, де є насильство, – це головні проблеми дітей в цифровому середовищі в Європі. Загалом хлопчиків більше непокоїть насильство, тимчасом як дівчаток більше непокоять ризики, пов'язані з контактами. Побоювання щодо ризиків є вищим серед дітей із країн з «активним користуванням, високим рівнем ризику».

У Латинській Америці консультації з дітьми показали, що основними проблемами, які спричинюють занепокоєння, є втрата недоторканності приватного життя, насильство та домагання. Діти повідомляють, що з ними зв'язувалися не знайомі їм люди – це особливо актуально в онлайн-іграх. У таких ситуаціях основна стратегія, імовірно, не реагувати на незнайомця та/або блокувати контакт. Дівчатка стикаються з домаганнями в соціальних мережах з раннього віку. Їм вдається самостійно орієнтуватися в цих формах насильства, блокуючи користувачів та змінюючи налаштування конфіденційності. Домагання виходять від користувачів, які іноді не розмовляють іспанською, але встигають надіслати їм зображення, попросити додати в друзі та прокоментувати їхні повідомлення. Деякі хлопчики також повідомляють про отримання таких запитів.

У багатьох частинах світу діти добре розуміють деякі ризики, на які вони наражаються у мережі38. Дослідження показали, що більшість дітей спроможні відрізнити кібербулінг від жартів та піддражнювання в цифровому середовищі, розуміючи, що кібербулінг стає публічним проявом жорстокості.

3. Підготовка національної стратегії захисту дитини в цифровому середовищі

Під час розроблення національної стратегії захисту дитини в цифровому середовищі для сприяння безпеці дітей та молодих осіб в цифровому середовищі національні уряди й директивні органи повинні виявляти передовий досвід та взаємодіяти з основними зацікавленими сторонами.

У наведених нижче розділах подано типових учасників та зацікавлених сторін, а також опис їх потенційної ролі та можливих обов'язків щодо захисту дітей в цифровому середовищі.

3.1 Учасники та зацікавлені сторони

Директивні органи можуть визначати відповідних осіб, групи та організації, які представляють кожну з цих структур та зацікавлених сторін у межах своєї компетенції. Для координації та організації діяльності на національному рівні у межах стратегій захисту дитини в цифровому середовищі важливо зробити оцінку поточних, запланованих та потенційних заходів.

Діти та молодь (молодь)

У цілому світі діти та молодь продемонстрували, що вони дуже легко можуть адаптуватися до нових технологій та використовувати їх. Важливість Інтернету для шкіл зростає, і він стає майданчиком де діти можуть грати, працювати і спілкуватися.

Згідно з останнім звітом Альянсу «ChildFund», тільки 18,1 відсотка опитаних дітей вважають, що директивні органи діють з метою їх захисту. Важливо, щоб директивні органи взаємодіяли з дітьми в цьому відношенні, визнаючи їхнє право бути вислуханими (стаття 12 КПД).

Для того щоб мати можливість захистити дітей, директивні органи повинні стандартизувати визначення поняття «дитина» у всіх правових документах. Під дитиною слід розуміти будь-яку особу віком до 18 років. Це відповідає статті 1 Конвенції ООН про права дитини (КПД ООН), яка зазначає, що «дитина означає будь-яку людську істоту, яка не досягла 18 років». Компаніям не слід вважати дорослою людиною кожну особу, яка за законом досягла віку, щоб дати згоду на обробку даних, але якій не виповнилося18 років. Таке вузьке визначення не підтверджено жодними доказами щодо етапів розвитку дитини. Воно підриває права дітей та загрожує їх безпеці.

Тимчасом як може здаватися, що чимало дітей впевнено використовують технології, багато хто з них не почувається у мережі в безпеці та має певні побоювання щодо інтернету.

Нерозвинений світогляд дітей та молодих осіб робить їх потенційно вразливими для різноманітних ризиків. Вони мають право чекати на допомогу та захист. Важливо також нагадати, що не всі діти та молодь однаково використовуватимуть Інтернет або нові технології. Деякі діти з особливими потребами, зумовленими обмеженнями фізичних чи інших можливостей, можуть виявитися особливо вразливими в цифровому середовищі і, отже, потребуватимуть додаткової підтримки.

Опитування показують, що здогадки дорослих про те, що діти та молодь роблять у мережі, і те, що там відбувається насправді, може цілковито відрізнятися. Половина всіх опитаних дітей сказали, що в їхній країні дорослі не дослухаються до їхньої думки з питань, що хвилюють їх . З цієї причини важливо, щоб незалежно від того, яких заходів вживають

на національному рівні для розроблення політики в цій сфері, було знайдено відповідні механізми, що дозволяють усім дітям та молоді бути почутими, і щоб було враховано їхній конкретний досвід використання технологій.

Батьки, опікуни та освітяни

Батьки, опікуни та освітяни проводять найбільше часу з дітьми. Вони повинні бути навчені цифрової грамотності, щоб розуміти цифрове середовище та вміти захищати дітей і навчити їх, як захистити себе.

Заклади освіти несуть особливу відповідальність за навчання дітей того, як бути у мережі у більшій безпеці, незалежно від того, чи використовують вони Інтернет у школі, вдома чи ще десь, а директивні органи повинні включати до національних навчальних програм питання цифрової грамотності з самого раннього віку (від 3 до 18 років). Це дозволило б дітям мати змогу захищати себе, знати свої права і, отже, використовувати Інтернет як засіб, що сприяє здобуванню знань .

Директивні органи повинні мати на увазі, що батьки й опікуни майже завжди будуть першою, останньою та найкращою лінією оборони і підтримки для власних дітей. Проте, коли йдеться про Інтернет, вони можуть почуватися дещо невпевнено. Знову-таки, школа може стати важливим каналом зв'язку з батьками й опікунами, щоб вони знали як про ризики, так і про чимало можливостей, що їх надають нові технології. Проте школи не повинні стати єдиним каналом інформування батьків та опікунів. Важливо використовувати чимало найрізноманітніших шляхів, щоб максимізувати можливість звернутися до максимально більшої кількості батьків та опікунів. Компанії галузі відіграють тут важливу роль, здійснюючи підтримку своїх користувачів або клієнтів. Батьки й опікуни можуть вибрати керування діяльністю своєї дитини в мережі і доступом до неї, поговорити з дитиною про правильну поведінку та використання технологій, зрозуміти, що дитина робить у мережі, щоб сімейна розмова поєднала в собі досвід онлайн-середовища та реального світу.

Батьки й опікуни також повинні подавати добрий приклад своїм дітям у тому, як користуватися своїми пристроями та правильно поводитися в Інтернеті.

Директивні органи повинні пам'ятати, що з батьками й опікунами слід консультуватися для з'ясування їхньої думки, досвіду та формування у них розуміння необхідності захисту їхніх дітей в цифровому середовищі.

Врешті-решт, директивні органи спільно з іншими державними установами можуть розробляти кампанії з інформування громадськості, в тому числі для батьків, опікунів та освітян. Публічні бібліотеки, медичні центри, навіть торговельні центри й інші великі центри роздрібної торгівлі можуть надати доступні приміщення для презентації інформації про електронну безпеку та цифрові навички. Виконуючи це завдання, уряди повинні забезпечити нейтральність наданих рекомендацій, свободу від будь-яких приватних інтересів, а також вони повинні охоплювати широкий спектр питань у межах цифрового простору.

Компанії галузі

Компанії галузі є однією з ключових зацікавлених сторін в екосистемі, позаяк вони мають технологічні знання, що їх директивні органи повинні враховувати і розуміти для розвитку

правової бази. Таким чином, по суті, директивні органи залучають компанії галузі до процесу розроблення законів про захист дитини в цифровому середовищі.

Крім того, під час розроблення нових технологій важливо заохочувати компанії галузі впроваджувати підходи, що базуються на врахуванні завдання забезпечення безпеки на етапі проєктування. Очевидно, що компанії, які розробляють або надають нові технологічні продукти й послуги, повинні допомагати своїм користувачам зрозуміти, як вони працюють і як безпечно та правильно використовувати їх.

Компанії галузі також несуть основну відповідальність за сприяння підвищенню обізнаності щодо програми дій з безпеки та онлайн-середовища, зокрема для дітей та їхніх батьків й опікунів, а також для спільноти загалом. Беручи участь у цій роботі, зацікавлені сторони галузі дізнаються більше про проблеми, що породжують занепокоєння інших зацікавлених сторін, а також про ризики та шкоду, на які наражаються кінцеві користувачі. Маючи такі знання, компанії галузі можуть коригувати наявні продукти й послуги та виявляти небезпеки на етапі розроблення.

Останні досягнення в галузі штучного інтелекту формують можливість для компаній галузі створювати надійнішу систему стримувань та противаг для ідентифікації користувача і забезпечення дітей сприятливим середовищем для конструктивної поведінки в цифровому середовищі. Ці досягнення також можуть містити нові ризики для дітей.

У деяких країнах Інтернет управляється в межах парадигми саморегулювання або спільного регулювання. Проте деякі країни розглядають або впровадили нормативно-правову базу, включно із зобов'язаннями компаній щодо виявлення, блокування та/або видалення джерел шкоди стосовно дітей із платформ або послуг, а також щодо надання чітких механізмів подання скарг та доступу до підтримки.

Академічна спільнота і неурядові організації

В університетах та академічній спільноті, найімовірніше, є чимало науковці та дослідників, які фахово цікавляться соціальним і технічним впливом Інтернету й мають вельми ґрунтовні знання в цій галузі. Вони є дуже цінним ресурсом з погляду надання допомоги національним урядам та директивним органам у формулюванні стратегій, що базуються на неспростовних фактах та переконливих доказах. Вони також можуть виступати як інтелектуальна противага бізнес-інтересам, які часом можуть бути надто короткотермінові й орієнтовані на прибуток.

Аналогічним чином у спільноті неурядових організацій (НУО) є чимало носіїв експертних знань та інформації, які можуть бути неоціненним ресурсом надання послуг дітям, батькам, опікунам та освітянам для сприяння просуванню порядку денного у сфері захисту дітей в цифровому середовищі та більш загально – захисту суспільних інтересів.

Органи охорони правопорядку

Дуже сумно, що така чудова технологія притягує також увагу кримінальних й антисоціальних елементів. Інтернет значно збільшив обсяги обігу CSAM та інших джерел шкоди в мережі. Сексуальні хижаки використовують Інтернет для першого контакту з дітьми, заманюючи їх у дуже шкідливі форми контакту, як в цифровому середовищі, так і в реальному світі.

Булінг й інші форми переслідування можуть завдати великої шкоди життю дітей, і Інтернет відкрив для цього новий шлях.

З цих причин важливо, щоб органи охорони правопорядку повністю займалися б діяльністю, пов'язаною з будь-якою загальною стратегією, з тим, щоб допомогти зробити Інтернет безпечнішим для дітей та молодих осіб. Працівники правоохоронних органів повинні пройти належну підготовку для проведення розслідування злочинів проти дітей та молодих осіб, пов'язаних з Інтернетом. Їм потрібен належний рівень технічних знань та доступ до інструментів криміналістики, щоб вони могли вилучати й інтерпретувати дані, отримані з комп'ютерів чи із мережі, за мінімальний час.

Крім того, дуже важливо, щоб органи охорони правопорядку сформували чіткі механізми, які дозволяють дітям та молоді чи будь-якому іншому громадянину повідомляти про будь-які випадки або побоювання, які можуть виникнути у них щодо безпеки дитини чи підлітка в цифровому середовищі. У багатьох країнах, наприклад, створено «гарячі лінії» для спрощення передавання повідомлень про CSAM, і є аналогічні спеціальні механізми для спрощення передавання повідомлень про інші види проблем, наприклад, про булінг. Директивним органам слід співпрацювати з Міжнародною асоціацією «гарячих ліній» Інтернету (INHOPE), надаючи їм підтримку в оцінці та опрацюванні звітів про CSAM, і мати користь від надання підтримки INHOPE організаціям у цілому світі у створенні «гарячої лінії» там, де її немає. Директивні органи повинні забезпечити наявність відкритих каналів зв'язку між правоохоронними органами й іншими зацікавленими сторонами. Правоохоронні органи є основним джерелом CSAM, що вилучається у межах національних кордонів. Необхідно організувати процес вивчення цих матеріалів, щоб установити, чи можна ідентифікувати місцевих жертв. Там, де це неможливо, матеріали слід передати до Інтерполу для включення до бази даних ICSE. Позаяк це загроза глобального масштабу, директивні органи повинні забезпечити міжнародну співпрацю між правоохоронними органами у цілому світі. Це скоротить час формальних процесів та дозволить агентам швидше реагувати.

Соціальні служби

Там, де діти або молодь зазнавали шкідливого впливу чи наражалися на зловживання в онлайн-режимі, наприклад, якщо в мережі були розміщені неприйнятні або незаконні їхні зображення, цілком імовірно, що їм потрібна спеціалізована й довготривала підтримка або консультація. Може також виникнути необхідність у комплексній психологічній допомозі та методах відновлення для правопорушників, особливо для неповнолітніх правопорушників, які, можливо, також стали жертвами зловживань у мережі чи в реальному світі. Фахівці, які працюють у соціальних службах, повинні бути відповідним чином навчені, для того щоб мати можливість надати підтримку такого виду. Підтримку слід надавати в онлайн-режимі та звичайними способами.

Служби охорони здоров'я

Медична допомога, необхідна після будь-якого випадку насильства щодо дитини, повинна бути включена до базового плану медичного обслуговування на національному рівні. Медичні установи повинні обов'язково повідомляти про випадки жорстокого поводження. Медичні працівники повинні бути належно оснащені та поінформовані, щоб мати можливість

надавати щодо цього підтримку дітям. Медичні послуги повинні поширюватися на підтримання психічного здоров'я та благополуччя дітей.

Урядові установи

Політика захисту дитини в цифровому середовищі перебуватиме у віданні низки урядових установ, і важливо залучити їх усі для успішної реалізації будь-якої національної стратегії та плану дій. Вони можуть включати:

- Міністерство внутрішніх справ;
- Міністерство охорони здоров'я;
- Міністерство освіти;
- Міністерство юстиції;
- Міністерство цифрового розвитку/інформації;
- Регуляторні органи.

Регуляторні органи мають найкращі можливості для того, щоб виконувати завдання контролю й обліку у співпраці з урядовими установами. Сюди можуть входити органи, що регулюють засоби масової інформації та захист даних.

Оператори широкосмугових, мобільних та Wi-Fi мереж

Оператори можуть виявляти, блокувати незаконний контент у своїй мережі та повідомляти про нього, а також надавати інструменти, послуги й конфігурації для використання родинами та батьками при виборі способу керування доступом своїх дітей. Важливо, щоб постачальники послуг однаковою мірою забезпечували дотримання громадянських свобод та недоторканність приватного життя.

Права дитини

Незалежні організації, що займаються захистом прав дитини, можуть відігравати вирішальну роль у забезпеченні захисту дітей в Інтернеті. Хоча їхні повноваження варіюються, такі установи вирішують, як правило, такі завдання:

- стежити за впливом законодавства, політики та правозастосування на захист прав дитини;
- сприяти реалізації міжнародних стандартів у сфері прав людини на національному рівні;
- розслідувати порушення прав дитини;
- представляти експертне знання у сфері прав дитини в судах;
- забезпечити заслуховування думок дітей з питань, що стосуються їхніх прав людини, включно з розробленням відповідних законів та політики;
- сприяти розумінню та усвідомленню громадськістю прав дитини; і
- втілювати ініціативи щодо навчання та підготовки фахівців у сфері прав людини.

Важливо включити прямі консультації з дітьми, позаяк це їхнє право відповідно до статті 12 КПД ООН. Консультативні, слідчі, інформаційні та освітні функції незалежних правозахисних установ для дітей мають важливе значення для запобігання шкоді в цифровому середовищі та реагування на нього. З цієї причини такі установи повинні брати активну участь у розробленні всеосяжного підходу, що базується на правах, до зміцнення правових, нормативних та політичних рамок, які регулюють захист дитини в цифровому середовищі, включно з прямими консультаціями з дітьми, адже це їхнє право відповідно до статті 12 КПД ООН.

Останнім часом також були приклади, коли у державах створювалися державні установи, наділені конкретними повноваженнями з підтримання прав дитини у мережі, включно з їх захистом від насильства або джерел шкоди, чи розглядалися можливості їх створення. Там, де є такі установи, вони також повинні бути тісно пов’язані із заходами посилення реагування з метою захисту дитини в цифровому середовищі на національному рівні.

3.2 Наявні заходи у відповідь щодо захисту дитини в цифровому середовищі

Було розроблено низку ініціатив, спрямованих на те, щоб діяти на національному та міжнародному рівнях з урахуванням дедалі більшого значення ІКТ в житті дітей у цілому світі та притаманних їм ризиків для наймолодших членів наших спільнот.

Національні моделі

На національному рівні слід виокремити декілька законодавчих ініціатив, що охоплюють важливі аспекти всеохопної рамкової основи захисту дитини в цифровому середовищі. Вони включають, серед інших, такі:

- Директива про аудіовізуальні медіа-послугах (AVMSD) (перегл. 2018 р., ЕС);
- Загальний регламент про захист даних (GDPR) (2018 р., ЄС).

У нормативно-правовому та інституційному реагуванні держав-членів на загрози безпеці та благополуччю дітей у мережі є інноваційні рішення. Єдиного способу реагування на CSAM, кібербулінг та інші джерела шкоди, з якими діти стикаються в цифровому середовищі, немає, проте слід зазначити, що за останні кілька років було випробувано нові підходи:

Кодекс проєктування з огляду на вік (2019 р., Сполучене Королівство)

На початку 2019 року Управління Комісару з інформації опублікувало пропозиції до свого «кодексу проєктування з огляду на вік» для зміцнення захисту дітей. У запропонованому кодексі основна увага приділяється найкращому забезпеченню інтересів дитини, як це передбачено в КПД ООН, і викладається низка очікувань, що покладаються на компанії галузі. До них належать надійні заходи з перевірки віку, відімкнення за замовчуванням послуги щодо визначення місця перебування для дітей, збір та зберігання компаніями лише мінімального обсягу персональних даних дітей, продумана безпечність продуктів, доступність і відповідність віку пояснень.

Закон про шкідливу цифрову комунікацію (перегл. 2017 р., Нова Зеландія)

У законі 2015 року запроваджується кримінальна відповідальність за зловживання ІКТ; основна увага приділена широкому діапазону видів шкоди, від кібербулінг до поширення матеріалів порнографічного змісту з міркувань помсти. Закон спрямовано на стримування, запобігання та зменшення шкідливого цифрового спілкування, забороняючи розміщення цифрового повідомлення з наміром завдати значних емоційних страждань будь-кому іншому, і встановлює 10 принципів спілкування. Він уповноважує користувачів подавати скарги до незалежної організації, якщо ці принципи порушуються, або клопотати про судову постанову щодо автора чи структури, що розмістила повідомлення, якщо питання не розв'язано.

Комісаріат електронної безпеки (2015 р., Австралія)

Комісаріат з питань електронної безпеки (eSafety) – це перша у світі урядова установа, що спеціалізується на безпеці в цифровому середовищі. Заснована у 2015 році структура має законодавчо закріплені функції щодо керівництва, координації, навчання та консультування з питань безпеки в цифровому середовищі, щоб забезпечити всім громадянам Австралії безпечний, позитивний досвід, що розширює їхні можливості роботи в мережі. eSafety проводить розслідування щодо значних джерел шкоди, включно із серйозним кібербулінгм дітей, жорстоким поводженням із використанням заборонених зображень та заборонений контент. Структура уповноважена проводити розслідування та вживати заходів для розгляду скарг чи повідомлень щодо такої шкоди, включно подекуди з повноваженнями надсилати повідомлення окремим особам та онлайн-службам для видалення матеріалів. Поряд із повноваженнями з проведення розслідувань, eSafety застосовує комплексний

підхід, що базується на соціальних, культурних і технологічних ініціативах та діях. Її зусилля з профілактики та захисту й активний підхід забезпечують комплексне розв'язання питання в цифровому середовищі.

Міжнародні моделі

На міжнародному і транснаціональному рівнях різні зацікавлені сторони розробили рекомендації та стандарти. Ці настанови базуються на результатах роботи, проведеної, у межах таких зусиль:

Рекомендації щодо здійснення Факультативного протоколу до Конвенції про права дитини, який стосується торгівлі дітьми, дитячої проституції та дитячої порнографії.

Рекомендації Ради Європи щодо поваги, захисту та реалізації прав дитини в цифровому середовищі . Рекомендації адресовані всім державам-членам Ради Європи з метою надання допомоги державам-членам та іншим відповідним зацікавленим сторонам в їхніх зусиллях з прийняття комплексного стратегічного підходу до максимального дотримання всього спектру прав дітей у цифровому середовищі. Серед багатьох тем, що розглядаються, є захист персональних даних, надання адаптованого до потреб та зростаючих здібностей дітей контенту, телефони довіри та «гарячі лінії», вразливість і адаптація, а також роль та відповідальність компаній. Крім того, в керівних настановах міститься заклик на адресу держав взаємодіяти з дітьми, в тому числі в процесі прийняття рішень, для належного відображення в національній політиці змін у цифровому середовищі. На сьогодні керівні принципи доступні 19 мовами. Вони супроводжуватимуться адаптованою для дітей версією документа, а також Настановою для директивних органів, в якій будуть викладені конкретні заходи щодо реалізації цих керівних настанов.

Рада Європи – Лансаротська конвенція

Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуальних зловживань (Лансаротська конвенція) вимагає від держав прийняття комплексних заходів щодо боротьби з сексуальним насильством стосовно дітей на основі підходу з такими елементами: запобігання, захист, судове переслідування й заохочення національної та міжнародної співпраці. Комітет учасників Конвенції про захист дітей від сексуальної експлуатації та сексуальних зловживань («Комітет Лансароте») уточнив дію Конвенції щодо цифрового середовища, прийнявши низку документів. До них належать такі: Думка про зображення та/або відеоматеріали непристойного чи явно сексуального характеру за участю дітей, які створюються, пересилаються та отримуються дітьми (6 червня 2019 р.); Думка про тлумачення застосовності Конвенції Лансароте до сексуальних злочинів щодо дітей, спрощених завдяки використанню ІКТ (12 травня 2017 р.); Декларація про вебадреси, що містять рекламу матеріалів або зображень, що пропагують сексуальну експлуатацію дітей чи будь-які інші злочини, визнані такими відповідно до Конвенції Лансароте (16 червня 2016 р.); і Думка щодо статті 23 Конвенції Лансароте – Грумінг дітей із сексуальною метою за допомогою інформаційно-комунікаційних технологій. Комітет Лансароте здійснює моніторинг реалізації положень Конвенції: його другий тематичний раунд моніторингу зосереджено на захисті дітей від сексуальної експлуатації та сексуального насильства за допомогою ІКТ: в 2020 році буде опубліковано доповідь про раунд моніторингу. Станом на 2019 рік до Конвенції приєдналися 46 держав, включно з Тунісом – першою державою, що не є членом Ради Європи.

Інші керівні принципи Ради Європи

Інші стандарти й інструменти Ради Європи сприяють розробці колективного зведення правил для створення всеосяжних рамок, орієнтованих на всі зацікавлені сторони. Конвенція Ради Європи про кіберзлочинність містить зобов'язання для учасників щодо запровадження кримінального переслідування за скоєння цілої низки злочинів, пов'язаних із матеріалами стосовно сексуальних зловживань щодо дітей: на сьогодні її ратифікували 64 держави-учасниці. Зокрема, Рада Європи особливу увагу приділяє розширенню можливостей дітей та їхніх близьких безпечно орієнтуватися у цифровій сфері. Цьому сприяють освітні інструменти, включно з повністю переглянутим Довідником з питань грамотності в Інтернеті (2017 г.), «Настанова з виховання цифрової громадянськості» (2019 р.) та посібниками, призначеними для батьків («Батьки в цифрову епоху» – Настанова для батьків щодо захисту дітей від сексуальної експлуатації та сексуальних зловживань в цифровому середовищі (2017 р.); «Цифрове громадянство... і ваша дитина» – те, що повинен знати і робити кожен із батьків (2019 р.). Нарешті, Рада Європи провела консультативне дослідження з дітьми щодо їхніх прав у цифровому середовищі – «Це наш світ: погляди дітей на те, як захистити їхні права в цифровому середовищі» (2017 р.), і розпочав проведення консультативних досліджень, присвячених досвіду дітей з інвалідністю у цифровому середовищі – «Два кліки вперед і один клік назад: доповідь про дітей з інвалідністю у цифровому середовищі» (2019 р.).

Звіт про безпеку дитини в цифровому середовищі

Безпека дитини в цифровому середовищі: мінімізація ризику насильства, жорстокого поводження й експлуатації в цифровому середовищі, а також Загальна декларація безпеки дитини в цифровому середовищі .

Рекомендації ОЄСР щодо захисту дитини в цифровому середовищі (2012 р./перегл. 2019-2020 рр.). Крім того, слід виокремити інші національні та міжнародні ініціативи, що сприяють зміцненню міжнародної співпраці, а також національних зусиль з розроблення стратегій захисту дитини в цифровому середовищі, наприклад:

Міжнародна база даних зображень, що містять елементи сексуальної експлуатації дітей Міжнародна база даних зображень, що містять елементи сексуальної експлуатації дітей (БД ICSE), ведеться Інтерполом і є потужним інструментом отримання інформації та ведення розслідувань, який дозволяє спеціалізованим слідчим обмінюватися даними з колегами у цілому світі. БД ICSE, доступ до якої здійснюється через захищену глобальну комунікаційну систему поліції Інтерполу (відому як I-247), використовує складне програмне забезпечення для порівняння зображень, щоб установити зв'язок між жертвами, зловмисниками та місцями. БД ICSE дозволяє сертифікованим користувачам у державах-членах отримувати доступ до бази даних у режимі реального часу – досліджувати наявні елементи, завантажувати нові дані, сортувати матеріали, проводити аналіз та спілкуватися з іншими експертами у цілому світі з питань, пов'язаних із розслідуванням випадків сексуальної експлуатації дітей.

Глобальний альянс WePROTECT

Глобальний альянс WePROTECT (WPGA) є глобальним рухом, в якому поєднані вплив, досвід та ресурси, необхідні для трансформації методів боротьби з сексуальною експлуатацією дітей в цифровому середовищі (OSCE) у цілому світі. Це союз урядових структур, глобальних технологічних компаній та організацій громадянського суспільства. Його багатосторонній характер є унікальним у цій галузі. Бачення Глобального альянсу WePROTECT полягає у

виявленні та захисті більшої кількості жертв, затриманні більшої кількості злочинців та припиненні сексуальної експлуатації дітей в цифровому середовищі.

Глобальний альянс WeProtect включає низку компонентів, зокрема, моделі національних заходів реагування та глобальної стратегічної відповіді. Докладніша інформація міститься у Додатку 3.

Індекс безпеки дитини в цифровому середовищі 2020 року

Розроблений інститутом DQ Індекс безпеки дитини цифровому середовищі (COSI) 2020 року є першою у світі аналітичною платформою, що працює в режимі реального часу, допомагає країнам відстежувати стан безпеки дітей онлайн.

COSI базується на шести аспектах, які утворюють межі COSI. Перший і другий аспекти – кіберризики й упорядкування використання цифрового середовища, стосуються розумного використання цифрових технологій. Третій і четвертий аспекти – цифрова компетентність та Рекомендації й навчання, пов'язані з розширенням прав та можливостей. Останні два аспекти пов'язані з інфраструктурою, це аспекти соціальної інфраструктури та встановлення з'єднань.

3.3 Приклади реагування на джерела шкоди в цифровому середовищі

У Доповненні 4 наведено низку прикладів реагування на джерела шкоди в цифровому середовищі. Ці приклади охоплюють заходи у відповідь у галузі освіти, законодавства та виявлення шкоди в Інтернеті.

3.4 Переваги національної стратегії захисту дитини в цифровому середовищі

Гармонізація законодавства

Прийняття всіма країнами належного законодавства проти неправомірного використання ІКТ зі злочинною метою чи з іншою метою має надзвичайно важливе значення для забезпечення глобальної кібербезпеки. Позаяк загрози можуть виникати в будь-якій точці світу, проблеми за своїм масштабом є міжнародними та потребують міжнародної співпраці, сприяння у розслідуванні загальних оперативних та процесуальних положень. Отже, важливо, щоб країни гармонізували своє законодавство щодо боротьби з кіберзлочинністю, дітей та спрощення міжнародної співпраці .

Розроблення належного національного законодавства, законодавства щодо боротьби з кіберзлочинністю і в межах цього підходу гармонізація на міжнародному рівні є головним кроком до успіху будь-якої національної стратегії щодо захисту дитини в цифровому середовищі. Це потребує насамперед прийняття необхідних положень кримінального законодавства для запровадження кримінального переслідування таких дій, як комп'ютерне шахрайство, незаконний доступ, втручання в дані, порушення авторських прав, CSAM, а також запобігання неналежному кримінальному переслідуванню дітей. Той факт, що в кримінальному кодексі є положення, застосовні до аналогічних діянь, що скоюються в реальному світі, не означає, що вони можуть бути також застосовані і до діянь, що скоюються в Інтернеті. Отже, для визначення можливих прогалин важливо провести ретельний аналіз наявних національних законів. Наступний крок – виявлення та визначення

законодавчих формулювань і довідкових матеріалів, які можуть допомогти країнам у розробленні узгоджених законів та процесуальних норм з проблематики кіберзлочинності. Такі практичні інструменти можуть бути використані країнами у розробленні законодавства проти кіберзлочинності та пов'язаних із ним законів. МСЕ працює в цьому напрямі з державами-членами та відповідними зацікавленими сторонами і робить великий внесок у просування вперед процесу узгодження законодавства щодо боротьби з кіберзлочинністю на глобальному рівні.

З урахуванням швидких темпів появи технологічних інновацій, як потенційні рішення проблеми старіння наявної системи регулювання та повільного процесу розроблення законодавчих норм було висунуто концепції саморегулювання та спільного регулювання. Разом з тим, для того щоб бути ефективними, регуляторним/директивним органам необхідно чітко визначити конкретні цілі та проблеми в сфері захисту дитини в цифровому середовищі, реалізувати чіткий процес огляду та методологію оцінки ефективності саморегулювання і спільного регулювання, а в разі якщо у процесі саморегулювання та спільного регулювання не вдається розв'язати виявлені проблеми, розпочати офіційний процес розроблення законодавства для розв'язання цих проблем. Крім того, успішні заходи саморегулювання можуть поступово переводитися в площину формального законодавства в межах законодавчого процесу, для того щоб стати правовим запобіжником та не допустити згортання чи припинення здійснення деяких ініціатив у сфері саморегулювання.

Координація

Цілком імовірно, що активні особи та зацікавлені сторони вже випрацювали чимало заходів та дій, спрямованих на захист дитини в цифровому середовищі, але які мають спорадичний характер. Важливо мати уявлення про таку діяльність, щоб врахувати зусилля, що вже робляться під час підготовки національної стратегії захисту дитини в цифровому середовищі. Така стратегія буде координувати та спрямовувати зусилля через організацію як наявних, так і нових видів діяльності.

4. Рекомендації щодо принципів та реалізації

Уряди повинні боротися з усіма проявами насильства щодо дітей у цифровому середовищі. Проте заходи, що вживаються для захисту дітей в цифровому середовищі, не повинні необґрунтовано обмежувати здійснення інших прав, таких як право на свободу висловлювання думок, право на доступ до інформації або право на свободу асоціацій. Замість того щоб обмежувати природну цікавість та здатність дітей до сприйняття інновацій через побоювання їх зіткнення з ризиками в цифровому середовищі, вкрай важливо використовувати винахідливість дітей та підвищувати їх пристосованість у процесі дослідження потенціалу цифрового середовища.

У багатьох випадках акти насильства щодо дітей скоюються іншими дітьми. У таких ситуаціях уряди повинні, наскільки це можливо, застосовувати відновлювальні підходи, за яких завдана шкода усувається, запобігаючи при цьому кримінальному переслідуванню дітей. Уряди повинні заохочувати використання ІКТ у запобіганні насильству та боротьбі з ним, наприклад, у розробленні технологій та ресурсів, що дозволяють дітям отримувати доступ до інформації, блокувати шкідливі матеріали та повідомляти про випадки насильства, коли вони відбуваються .

Щоб розв'язувати проблему глобальної ситуації з безпекою дитини онлайн, уряди повинні сприяти спілкуванню між відповідними організаціями й відкрито співпрацювати з метою усунення шкоди, що завдається дітям в цифровому середовищі.

4.1 Базові рекомендації

4.1.1 Правова база

Урядам слід переглянути і, за потреби, оновити свою правову базу з метою підтримання повноцінної реалізації прав дитини в цифровому середовищі. Всеосяжна правова база повинна стосуватися превентивних заходів; заборони всіх форм насильства щодо дітей в цифровому середовищі; надання ефективних засобів реагування, відновлення та реінтеграції для розв'язання проблем, пов'язаних з порушеннями прав дитини; створення механізмів консультування та повідомлення про проблеми і скарги, що враховують інтереси дітей; а також механізмів підзвітності для боротьби з безкарністю.

По змозі, законодавство має бути технологічно нейтральне, щоб його застосовність не знижувалася у світлі майбутніх технологічних розробок.

Ефективна реалізація законодавчих заходів потребує від урядових структур додаткових кроків, включно з ініціативами щодо підвищення обізнаності та соціальної мобілізації, зусиллями та кампаніями в сфері навчання і створення потенціалу фахівців, які працюють із дітьми та в їхніх інтересах.

Під час розроблення відповідного законодавства важливо також враховувати, що діти не є однорідною групою. Дітям різних вікових груп можуть бути потрібні різні заходи у відповідь,

так само як і дітям з особливими потребами чи дітям, яким з більшою імовірністю може бути завдано шкоди в цифровому середовищі або під час його використання.

Урядам слід створити чітку та передбачувану нормативно-правову базу, яка б допомагала компаніям та іншим третім сторонам виконувати свої обов'язки щодо захисту прав дитини у всіх аспектах діяльності, як на території країни, так і за кордоном.

Директивним органам під час дослідження сфери охоплення правових меж слід взяти до уваги наведені нижче моменти:

- грумінг або інші форми дистанційного спокушання, вимагання чи примушення дітей до неприйнятного сексуального контакту або сексуальної діяльності;
- володіння, виробництво та поширення CSAM, незалежно від наміру поширювати;
- домагання, булінг, образи чи риторика ненависті в цифровому середовищі;
- терористичні матеріали в цифровому середовищі;
- кібербезпека;
- відображення того факту, що те, що є незаконним офлайн, також є незаконним онлайн.

4.1.2 Політична та інституційна база

Гарантія реалізації прав дитини в цифровому середовищі вимагає від урядів дотримання балансу між максимізацією переваг, які отримуються дітьми від використання ІКТ, і мінімізацією пов'язаних із цим ризиків. Цього можна домогтися включенням заходів щодо захисту дітей в цифровому середовищі до національних планів з розвитку широкосмугової мережі та розробленням окремої багатосторонньої стратегії щодо захисту дітей онлайн. Такий порядок денний має бути повністю інтегрований з будь-якими наявними політичними принципами, що стосуються проблематики прав дітей чи захисту дітей, а також повинна доповнювати національну політику в сфері захисту дитини, пропонуючи конкретні основи для всіх ризиків та потенційних джерел шкоди для дітей, спрямовані на створення безпечного, цифрового середовища для всіх, яке сприяє розширенню прав та можливостей.

Урядам слід створити національну координаційну структуру з чітким мандатом та достатніми повноваженнями для координації всієї діяльності, пов'язаної з правами дітей і цифровими засобами масової інформації та ІКТ, на міжсекторальному, національному, регіональному й місцевому рівнях. Уряди повинні сформулювати цілі з конкретними термінами їх досягнення та організувати прозорий процес оцінки й моніторингу виконаної роботи, а також забезпечити надання необхідних людських, технічних та фінансових ресурсів для ефективного функціонування цієї структури.

Урядам слід створити багатосторонню платформу для керівництва розробленням, реалізацією та моніторингом національного цифрового порядку денного в інтересах дітей. Така платформа повинна включати представників найважливіших груп населення, включно з: дітьми та молоддю; асоціаціями батьків/опікунів; відповідними урядовими установами; сектором освіти, юстиції, охорони здоров'я та соціального забезпечення; національними правозахисними установами й відповідними регуляторними органами; громадянським суспільством; компаніями галузі; науковими колами; та відповідними асоціаціями фахівців.

4.1.3 Нормативна база

Урядові структури відповідальні за порушення прав дітей, що стали прямим чи опосередкованим наслідком дій компаній, якщо вони не вжили необхідних, належних та розумних заходів для запобігання та виправлення таких порушень чи іншим чином співпрацювали з такими підприємствами або ігнорували порушення, які ті скоювали54.

Керівні принципи підприємницької діяльності в аспекті прав людини передбачають забезпечення компаніями механізмів правового захисту та розгляду скарг, які є законними, доступними, передбачуваними, справедливими, сумісними з правами, прозорими, такими, що базуються на діалозі та участі, а також можуть бути джерелом постійного навчання. Механізми

розгляду скарг, створені компаніями, можуть забезпечувати гнучкі та сучасні альтернативні рішення, і їх використання під час розв'язання проблем, пов'язаних із поведінкою тієї чи іншої компанії, може дозволити враховувати інтереси дитини. У всіх випадках має бути забезпечено доступ до судів або судового перегляду адміністративних засобів захисту та інших процедур . Слід розглянути механізми, що створюють безпечні послуги для дітей, що відповідають віку, для того щоб користувачі могли повідомляти про свої проблеми.

Попри наявність внутрішніх механізмів розгляду скарг, уряди повинні створити механізми моніторингу для розслідування порушень прав дітей та відшкодування відповідного збитку в сенсі підвищення підзвітності компаній сфери ІКТ і суміжних галузей, а також посилення відповідальності регуляторних органів за розроблення стандартів щодо прав дітей та ІКТ . Це особливо важливо, позаяк інші засоби правового захисту, що є в розпорядженні потерпілих від дій компаній, такі як цивільний позов та інші засоби судового захисту, часто є складними та дорогими .

Комітет ООН з прав дитини наголосив на потенційній ролі національних правозахисних установ у цій сфері, охарактеризувавши роль, яку вони могли б відігравати в отриманні та розслідуванні скарг на порушення з боку галузевих структур, а також організації посередництва з цих питань; проведенні державних розслідувань великомасштабних зловживань; проведенні перегляду законодавства з метою забезпечення дотримання Конвенції про права дитини. Комітет зазначив, що, коли це необхідно, «державам слід розширити законодавчий мандат національних правозахисних установ, для того щоб він відповідав правам дітей та інтересам бізнесу». Особливо важливо, щоб будь-який механізм розгляду скарг враховував інтереси дітей, забезпечував недоторканність приватного життя і захист жертв, а також включав діяльність з моніторингу, подальших заходів та перевірки в інтересах дітей-жертв.

Одним із прикладів сфери, в якій національна правозахисна установа чи інший регуляторний орган могли б надати дітям ефективні засоби правового захисту, є кібербулінг. Внутрішні механізми правового захисту та розгляду скарг часом виявляються неефективними в таких випадках, адже попри те, що зміст викликає тривогу і завдає шкоди, він часто не розглядається національним законодавством, і немає чітких підстав для того, щоб домагатися його видалення структурою, яка розміщує контент. Наділення державного органу повноваженнями отримувати скарги у зв'язку з випадками кібербулінг та звертатися до структур, які розміщують контент, для видалення відповідних матеріалів буде важливим елементом захисту дітей . Переваги такого заходу полягатимуть в оперативності реагування,

яка має вирішальне значення в контексті кібербулінг, а також у створенні чіткої правової основи для розв'язання проблеми видалення матеріалів, пов'язаних із кібербулінгм.

Під час розроблення підходу до регулювання цифрового середовища уряди повинні також враховувати вплив такого регулювання на втілення всіх прав людини, включно зі свободою самовияву .

Урядам слід покласти на підприємства зобов'язання виявляти належну обачність у питаннях прав дитини. Це забезпечить роботу підприємств з виявлення, запобігання та пом'якшення свого впливу на права дітей, в тому числі в межах своїх ділових відносин та глобальної діяльності .

Крім того, уряди повинні розглянути додаткові заходи, такі як забезпечення дотримання галузевими організаціями, чия діяльність може справляти вплив на права дітей у цифровому середовищі, найвищих стандартів з погляду запобігання можливим порушенням прав та реагування на них, щоб мати право на отримання фінансування або укладення контрактів.

4.2 Рекомендації практичного характеру

Урядам слід забезпечити доступ до ефективних засобів правового захисту для дітей, які стали жертвами порушення їхніх прав, у тому числі допомагати їм оперативно отримати належне відшкодування завданої шкоди, виплачуючи компенсації в разі потреби. Урядам слід також надавати адекватну підтримку та допомогу дітям, які стали жертвами порушень, пов'язаних із цифровими засобами інформації та ІКТ, зокрема організувати роботу служб комплексної підтримки, для того щоб забезпечити повне одужання та реінтеграцію потерпілих дітей, а також запобігти їх повторній віктимізації .

Безпечні та легкодоступні механізми консультування, подання та розгляду скарг, з урахуванням інтересів дітей, такі як телефони довіри, мають бути передбачені і бути частиною національної системи захисту дітей. Важливо, щоб ці служби були пов'язані з якимись регуляторними органами, що допомогло б спростити взаємодію дитини з державними інституціями в той час, коли вона перебуває у важкому становищі. Телефони довіри особливо цінні з погляду дуже чутливих тем, таких як сексуальні зловживання, які дітям буває складно обговорити з однолітками, батьками, опікунами чи освітянами. Служби «Телефон довіри» також важливі, тому що вони можуть підказати дитині до кого звернутися, наприклад, до служби юридичної допомоги, притулків, правоохоронних органів чи служб реабілітації .

Крім того, уряди повинні розуміти і відстежувати поведінку правопорушників, щоб підвищити статистику виявлення зловмисників та знизити ризик повторного скоєння ними правопорушень. Рекомендується створити телефони довіри з безкоштовною та анонімною консультацією і підтримкою по телефону або в чаті громадянам, у яких виникають почуття або думки, пов'язані з сексуальним інтересом до дітей. Допомога таким потенційним правопорушникам у зміні їхньої поведінки зводить до мінімуму ризик повторного скоєння правопорушення.

Установлені на законодавчому рівні механізми розгляду скарг також є дуже важливою частиною системи ефективних засобів правового захисту.

Регуляторні органи повинні проводити незалежні вимірювання та дослідження для оцінки того, як платформи повідомляють і розв'язують проблеми, пов'язані із захистом дитини.

Є технологія, що дозволяє регуляторним органам самостійно проводити моніторинг платформ. Необхідно надавати допомогу постачальникам послуг з метою публікації звітів, що надаються для забезпечення транспарентності.

Державні органи разом із міжнародною спільнотою та галузевими компаніями повинні розробити універсальний набір показників, які могли б використовуватися зацікавленими сторонами для вимірювання всіх відповідних аспектів безпеки дитини в цифровому середовищі.

4.2.1 Сексуальна експлуатація

Нижче перелічені конкретні міркування, які слід узяти до уваги представникам директивних органів під час розгляду загроз, здатних завдати дітям шкоди, а саме матеріалів, пов'язаних із сексуальними зловживаннями щодо дітей, власноруч створеного контенту, грумінгу та секс-вимагання, а також інших онлайн-ризиків:

- Заходи з припинення або зменшення трафіку передавання матеріалів CSAM, наприклад, шляхом створення національної «гарячої лінії» чи використання порталу IWF для подання скарг та блокування доступу до онлайн-контенту, про який відомо, що він містить або рекламує наявність матеріалів CSAM.
- Забезпечити наявність національних процедур, що гарантувало б, що всі виявлені у країні матеріали CSAM надсилатимуться до централізованого національного ресурсу, який на законодавчому рівні наділений повноваженнями вимагати від компаній видалення контенту.
- Стратегії контролю попиту на матеріали CSAM, зокрема, для тих, хто вже був визнаний винним у скоєнні таких злочинів. Важливо підвищувати обізнаність із тим, що цей злочин не належить до злочинів без жертв: діти використовуються для створення матеріалу, який переглядається, і переглядаючи та завантажуючи матеріали CSAM у цілому світі, кожен безпосередньо сприяє зловживанням щодо зображеної там дитини, а також заохочує використання більшої кількості дітей для створення більшої кількості зображень.
- Підвищити обізнаність з тим, що дитина в принципі не може дати згоди на те, щоб вона зазнавала сексуальних зловживань, для виробництва матеріалів CSAM чи в будь-який інший спосіб. Рекомендуйте тим, хто використовує матеріали CSAM, звернутися за допомогою і водночас інформуйте їх про те, що вони нестимуть кримінальну відповідальність за незаконні дії, до яких вони залучені.
- Інші стратегії контролю попиту на матеріали CSAM. Наприклад, у деяких країнах ведеться реєстр засуджених сексуальних злочинців. Суди видають юридичні приписи, що або зовсім забороняють таким злочинцям користуватися Інтернетом, або дозволяють використовувати лише ті ділянки Інтернету, які часто відвідують діти та молодь. Проблема з цими приписами полягає в тому, як забезпечити їх виконання. Проте в деяких країнах розглядається питання об'єднання списку відомих сексуальних злочинців у список блокування, що унеможливлює їх відвідування певних вебсайтів або реєстрування на них, наприклад на вебсайтах, про які відомо, що їх відвідує чимало дітей та молодих осіб. Звичайно, якщо злочинець зареєструється на вебсайті, використовуючи інше ім'я чи фальшивий логін, ефективність таких заходів значно знизиться, проте оголошення такої поведінки протизаконною може стати ще одним стримувальним засобом.
- Забезпечити жертвам відповідну довготривалу підтримку У тих випадках, коли діти або молодь стали онлайн-жертвами, наприклад якщо в Інтернеті з'явилося їх незаконне зображення, вони цілком природно непокоїтимуться про те, хто може побачити його і які наслідки це матиме для них. Це може змушувати дитину або молоду людину почуватися вразливою щодо булінг чи подальшої сексуальної експлуатації та сексуальних зловживань. У цьому контексті важливо, щоб були доступні служби

підтримки для дітей та молодих осіб, які опинилися в такій ситуації. Така підтримка може потребуватися на довгостроковій основі.

- Забезпечити створення та широке просування механізму, що забезпечує зрозумілі та швидкі засоби для спілкування про незаконний контент або про незаконну чи підозрілу поведінку в онлайн-режимі, наприклад, системи, аналогічної до тієї, яка була створена Віртуальною глобальною цільовою групою та INHOPE. Слід заохочувати і використання системи INTERPOL i24/7.
- Забезпечити, щоб достатня кількість працівників органів охорони правопорядку пройшли відповідне навчання щодо розслідування злочинів, скоєних в Інтернеті або з використанням комп'ютерів, а також мали доступ до відповідних засобів криміналістики, які дозволяють їм виокремлювати та інтерпретувати відповідні цифрові дані.
- Інвестувати в навчання працівників органів охорони правопорядку, прокуратури та юстиції методів, що використовуються онлайн-злочинцями для скоєння таких злочинів. Інвестиції також потрібні на придбання й обслуговування обладнання, необхідного для отримання й інтерпретації криміналістичних доказів із цифрових пристроїв. На додаток буде важливо створити двосторонню та багатосторонню співпрацю й обмін інформацією з відповідними організаціями охорони правопорядку та слідчими органами в інших країнах.

4.2.2 Освіта

У межах стратегії необхідно забезпечити цифрову грамотність дітей, щоб гарантувати, що вони можуть отримувати вигоду від використання технологій, не наражаючись на небезпеку. Це дозволить дітям розвинути навички критичного мислення, які допоможуть їм визначити і зрозуміти добрі та погані сторони власної поведінки в цифровому просторі. Важливо показати дітям приклад шкоди, якої можна зазнати в цифровому середовищі, проте це буде ефективно лише в тому разі, якщо це буде зроблено в межах ширшої програми цифрової грамотності, яка має відповідати віку та фокусуватися на навичках і компетенціях. Важливо, щоб програма навчання безпеки в цифровому середовищі включала принципи соціального та емоційного навчання, позаяк вони допоможуть студентам зрозуміти емоції та керувати ними, а отже, мати здорові стосунки на основі поваги як в цифровому середовищі, так і в реальному світі.

Один з оптимальних способів забезпечити безпеку дітей, які користуються Інтернетом, полягає в наданні їм відповідних інструментів та знань. Як варіант, можна включати розвиток цифрової грамотності до шкільних програм. Інший підхід передбачає створення освітніх ресурсів за межами шкільної програми.

Ті, хто працює з дітьми, повинні мати відповідні знання та навички, щоб упевнено допомагати дітям реагувати на проблеми, пов'язані з їхнім захистом в цифровому середовищі, та вирішувати їх, а також забезпечувати набуття дітьми необхідних цифрових навичок для успішного використання технологій.

4.2.3 Галузеві компанії

Національні та міжнародні галузеві гравці повинні працювати над підвищенням обізнаності щодо проблем, пов'язаних із безпекою дитини в цифровому середовищі, та допомагати всім дорослим, відповідальним за благополуччя дитини, зокрема, батькам та опікунам, школам, молодіжним організаціям та спільнотам, розвивати знання та навички, необхідні їм для забезпечення безпеки дітей. Підхід галузевих компаній до розроблення своїх продуктів,

послуг та платформ повинен базуватися на принципі підвищення безпеки, а забезпечення безпеки має бути визнане основним завданням.

- Надати відповідні віку інструменти, що враховують інтереси родини, щоб допомогти своїм користувачам поліпшити управління захистом родини в цифровому середовищі.
- Надати своїм користувачам відповідні механізми для повідомлення про проблеми та речі, що викликають занепокоєння. Користувачі повинні очікувати своєчасної відповіді на ці повідомлення з інформацією про вжиті заходи і, якщо застосовно, про те, де вони можуть отримати додаткову підтримку.
- Крім того, забезпечити механізм попереджувального повідомлення про експлуатацію дітей, щоб виявити й усунути будь-які види зловживань (що класифікуються як злочинна діяльність) стосовно дітей. Ця практика показала, що якщо всі зацікавлені сторони роблять свій вклад у виявлення, блокування та повідомлення, то Інтернет буде чистіший та безпечніший для всіх. Галузеві компанії повинні розглянути можливість застосування всіх відповідних інструментів, таких як послуги IWF, для запобігання зловмисному використанню їхніх платформ.

Дуже важливо, щоб усі відповідні учасники екосистеми знали про ризики й можливості заподіяння шкоди в цифровому середовищі, щоб діти не наражалися на непотрібні ризики.

Необхідно розробити загальні показники безпеки дітей в цифровому середовищі, щоб виміряти всі відповідні аспекти. Наявність загальних стандартів та показників - це єдиний спосіб відстежування прогресу в країнах, визначення успішності проєктів та заходів, спрямованих на викорінення будь-якого насильства щодо дітей, та визнання ефективності екосистеми безпеки дитини в цифровому середовищі.

5. Розроблення національної стратегії захисту дитини в цифровому середовищі

5.1 Список для самоперевірки на національному рівні

Для того, щоб сформулювати національну стратегію, спрямовану на забезпечення безпеки дитини в цифровому середовищі, директивні органи повинні розглянути широкий комплекс заходів. У Таблиці 1 подані ключові сфери, що потребують розгляду.

Таблиця 1: Ключові сфери, що потребують розгляду

	#	Ключові сфери, що потребують розгляду	Додаткова інформація
Правові межі	1	Переглянути наявні правові межі, щоб встановити, що є всі необхідні юридичні права, для того, щоб правоохоронні органи й інші організації захищали людей віком до 18 років в цифровому середовищі на всіх платформах доступу до Інтернету.	Як правило, потрібно буде запровадити блок законів, які роз'яснюють, що будь-який злочин, який може бути скоєний проти дитини в реальному світі, може, з урахуванням відповідних поправок, також бути скоєним в Інтернеті чи будь-якій іншій електронній мережі. Крім того, можливо буде потрібно розробити нові чи переглянути наявні закони для того, щоб встановити незаконність певних видів поведінки, які можуть існувати лише в Інтернеті, наприклад, дистанційне заманювання дітей для виконання й перегляду сексуальних дій або «звваблення» дітей для зустрічі в реальному світі з сексуальною метою. На додаток до цих цілей, як правило, потрібно запровадити законодавство, яке встановить незаконність зловмисного використання комп'ютерів зі злочинною метою, незаконність хакерства й іншого шкідливого та невідповідного використання комп'ютерних програм, і визначить, що Інтернет є місцем, в якому можуть бути скоєні злочини.
	2	Встановити, з урахуванням необхідних змін , що будь-яка дія проти дитини, яка є незаконною в реальному світі, є незаконною в цифровому середовищі, і що правила захисту даних та конфіденційності в цифровому середовищі застосовні також і для дітей.	

	#	Ключові сфери, що потребують розгляду	Додаткова інформація
Регуляторні межі	3	Розглянути можливість розроблення політики регулювання. Вона може передбачати саморегулювання, спільне регулювання, а також повне регулювання. Модель саморегулювання чи спільного регулювання може включати розроблення й публікацію кодексів добросовісної практики або базових очікувань щодо безпеки в цифровому середовищі як у сенсі надання сприяння залученню, координації чи організації та збереженню залученості всіх зацікавлених учасників, так і в сенсі підвищення швидкості, з якою можуть бути розроблені та реалізовані дії у відповідь на технологічні зміни. Модель регулювання може визначати очікування та зобов'язання зацікавлених сторін і закріплювати їх у правовому полі. Також можуть бути розглянуті штрафи за недотримання політики.	Деякі країни для розроблення правил у цій сфері створили модель самостійного або спільного регулювання, і за допомогою таких моделей вони, наприклад, публікують кодекси добросовісної практики, для того, щоб спрямовувати галузь Інтернету, використовуючи ті заходи, які можуть якнайкраще працювати там, де справа стосується забезпечення безпеки дітей та молодих осіб в цифровому середовищі. Так, у межах Європейського Союзу опубліковано кодекси ЄС, як для сайтів спілкування в соціальних мережах, так і для мереж рухомого телефонного зв'язку, які стосуються надання контенту й послуг дітям та молоді через ці мережі. Саморегулювання або спільне регулювання може бути ефективніше в сенсі підвищення швидкості, з якою можуть бути сформульовані та введені в дію відповідні заходи на технологічні зміни. Зовсім нещодавно декілька країн підготували та/або прийняли регуляторні норми. У цих випадках регуляторні норми розроблені на основі моделей саморегулювання або спільного регулювання та в них визначені вимоги й очікування зацікавлених сторін, особливо галузевих постачальників, для кращого захисту своїх користувачів.

	#	Ключові сфери, що потребують розгляду	Додаткова інформація
Повідомлення про незаконний контент	4	Забезпечити створення і широку відомість механізму щодо надання зрозумілих способів повідомляти про різний незаконний контент, виявлений в Інтернеті. Наприклад, державна «гаряча лінія», що має можливість швидкого реагування й видалення незаконного матеріалу чи заборони доступу до нього. Галузь повинна мати механізми для виявлення, блокування та усунення зловживань щодо дітей в цифровому середовищі із залученням усіх послуг, що стосуються її організацій.	Механізми для повідомлення про зловживання під час використання онлайн-послуг або для повідомлення про негожу чи незаконну поведінку в цифровому середовищі, наприклад, національною «гарячою лінією», слід широко рекламувати і просувати як в Інтернеті, так і в інших засобах інформації. Якщо національна «гаряча лінія» недоступна, IWF як рішення пропонує використовувати портали для надсилання повідомлень. Посилання на механізми для повідомлення про зловживання повинні бути явно відображені на відповідних розділах кожного вебсайту, які дозволяють розміщувати контент, що створюється користувачами. Має бути також забезпечена можливість, щоб люди, які відчувають, що їм загрожує небезпека будь-якого виду, або люди, які помітили будь-які підозрілі дії в Інтернеті, могли б максимально швидко повідомити відповідні органи охорони правопорядку, які повинні бути навчені й готові зреагувати на це повідомлення. Віртуальна глобальна цільова група - це організація органів охорони правопорядку, яка надає механізм, що діє в режимі 24/7, для прийняття від громадян США, Канади, Австралії та Італії заяв про незаконну поведінку чи контент; очікується, що інші країни також невдовзі приєднаються. Див. www.virtualglobaltaskforce.com. Див. також INHOPE.
Повідомлення про потреби користувачів	5	Представники галузі повинні надати користувачам можливість повідомляти про свої питання, що виникають занепокоєння, та проблеми і реагувати на них відповідно.	На постачальників слід покласти обов'язок надавати і чітко вказувати своїм користувачам на можливість повідомляти про проблеми та речі, що викликають занепокоєння і стосуються їхніх послуг. Це має бути зручно й доступно для дітей.

	#	Ключові сфери, що потребують розгляду	Додаткова інформація
Учасники та зацікавлені сторони	6	Залучити всі відповідні сторони, ацікавлені в забезпеченні захисту дитини в цифровому середовищі, зокрема: • урядові організації; • органи охорони правопорядку; • організації соціального обслуговування; • постачальників послуг Інтернету й інших постачальників електронних послуг; • постачальників послуг рухомої телефонії; • постачальників громадських точок доступу Wi-Fi; • інші відповідні високотехнологічні компанії; • учительські організації; • батьківські організації; • дітей та молодих осіб; • НУО щодо захисту дітей та інші відповідні НУО; • академічні та дослідні організації; • власників інтернет-кафе та інших постачальників послуг колективного доступу, наприклад бібліотеки, центри електрозв'язку, комп'ютерні клуби63, центри онлайн-ігор тощо.	Деякі національні уряди вважають за корисне звести докупи всі зацікавлені сторони й учасників ринку для розроблення та реалізації національної ініціативи з метою зробити Інтернет безпечнішим місцем для дітей та молодих осіб, а також з метою підвищення поінформованості щодо проблем і щодо того, як їх розв'язувати на практиці. У межах цієї стратегії важливо буде розуміти, що чимало людей повсюдно й постійно під'єднані до Інтернету через різноманітні пристрої. Мають бути залучені оператори широкосмугового та рухомого зв'язку і Wi-Fi. Крім того, у багатьох країнам важливим джерелом доступу до Інтернету, особливо для дітей та молодих осіб, є мережа громадських бібліотек, центрів електрозв'язку та інтернет-кафе.
Дослідна робота	7	Провести дослідження всього спектру національних учасників та зацікавлених сторін для визначення їхніх думок, досвіду, речей, що спричиняють занепокоєння, а також можливостей про те, що стосується діяльності із захисту дитини в цифровому середовищі. Слід також оцінити зону відповідальності, а також заходи, яких вживають чи планують щодо захисту дитини в цифровому середовищі.	

	#	Ключові сфери, що потребують розгляду	Додаткова інформація
Освіта: цифрова грамотність і компетентність	8	Розроблення матеріалів із цифрової грамотності в межах будь-якої національної шкільної програми, яка б відповідала віку та могла б застосовуватися для навчання всіх дітей.	Школи та система освіти загалом будуть основою освіти і компонента цифрової грамотності в національній стратегії захисту дітей в цифровому середовищі. Будь-яка національна шкільна програма повинна включати аспекти захисту дітей в цифровому середовищі та бути націленою на те, щоб дати дітям різного віку навички, що відповідають їхньому віку, щоб вони могли вміло і для добра використовувати технології, а також усвідомлювати загрози та шкоду, яких слід уникати. У ній має визнаватися та заохочуватися позитивна й конструктивна поведінка в цифровому середовищі. У межах багатьох освітніх та інформаційних кампаній важливо обрати правильний тон. Слід уникати страшних повідомлень, і тому наголос треба робити на безліч позитивних та розважальних можливостей нових технологій. Інтернет має величезний потенціал як засіб допомоги дітям та молоді у дослідженні нових світів. Навчання їх позитивних та відповідальних форм онлайн-поведінки є головним завданням освітніх та інформаційних програм. Ті, хто працює з дітьми, особливо освітяни, повинні мати відповідну підготовку й оснащення, щоб успішно навчати дітей цих навичок. Вони повинні розуміти, що таке онлайн-загрози та шкода, а також уміти впевнено розпізнавати ознаки зловживань та шкоди, реагувати на них і повідомляти про свої побоювання, щоб захищати дітей.

	#	Ключові сфери, що потребують розгляду	Додаткова інформація
Освітні ресурси	9	Використовувати знання та досвід усіх зацікавлених сторін і підготувати повідомлення та матеріали про безпеку в Інтернеті, які відображають місцеві культурні норми та закони, і забезпечити, щоб вони були ефективно розподілені й відповідно представлені всім основним цільовим аудиторіям. Розглянути можливість залучення допомоги засобів масової інформації у поширенні повідомлень, які підвищують поінформованість. Розробити матеріали, які висвітлюють позитивні та дієві аспекти Інтернету для дітей та молодих осіб і дозволяють уникати повідомлень, надісланих через емоцію страху. Пропагувати позитивні та відповідальні форми поведінки в цифровому середовищі. Розглянути питання про розроблення ресурсів, щоб допомагати батькам оцінювати безпеку своїх дітей в цифровому середовищі й довідатися, як звести до мінімуму ризики та максимально збільшити потенціал власної родини за допомогою цілеспрямованого навчання.	При створенні навчальних матеріалів важливо враховувати, що чимало людей, які мало знають про технології, почуватимуться некомфортно, використовуючи її. З цієї причини важливо забезпечити, щоб матеріали про безпеку були доступні як у друкованому вигляді, так і в інших інформаційних форматах, які сприйматимуться новачками як щось більш знайоме, наприклад відеоролики. Безліч великих інтернет-компаній створюють вебсайти, що містять великий обсяг інформації про онлайн-загрози для дітей та молодих осіб. Проте дуже часто цей матеріал доступний лише англійською мовою або невеликою кількістю мов. Отже, дуже важливо, щоб матеріали створювалися на місцях та відображали національні закони й місцеві культурні норми. Це буде важливо для будь-якої кампанії з безпеки Інтернету та для розроблення будь-яких навчальних матеріалів.
Захист дитини	10	Гарантувати наявність універсальних системних механізмів захисту дитини, що зобов'язують усі сторони, які працюють з дітьми (служби соціального захисту, охорони здоров'я, школи тощо) виявляти випадки зловживань та заподіяння шкоди і Інтернеті, реагувати на них та повідомляти про такі інциденти.	Повинна існувати універсальна система захисту дитини, яка б застосовувалася до всіх, хто працює з дітьми, в якій вони були б зобов'язані повідомляти про зловживання щодо дітей або заподіяння їм шкоди, що дозволило б розслідувати проблемну ситуацію та знайти вирішення.

	#	Ключові сфери, що потребують розгляду	Додаткова інформація
Обізнаність на національному рівні	11	Організувати національні кампанії з підвищення обізнаності з метою привернення загальної уваги до проблем захисту дитини в цифровому середовищі. Для розроблення кампанії може бути корисно використовувати такі глобальні кампанії, як День безпечнішого Інтернету.	Батьки, опікуни та фахівці, як-от освітяни, відіграють надзвичайно важливу роль у тому, щоб допомагати дітям та молоді залишатися в безпеці, перебуваючи в мережі. Програми підтримки, які дозволять забезпечити обізнаність у цих проблемах, а також визначать стратегію боротьби з ними. Слід також розглянути питання допомоги з боку засобів масової інформації в поширенні даних та проведенні кампаній з метою підвищення обізнаності. Такі можливості, як День безпечнішого Інтернету, допоможуть стимулювати й заохочувати обговорення теми захисту дитини в цифровому середовищі. Чимало країн успішно організували національні кампанії з підвищення обізнаності в контексті Дня безпечнішого Інтернету, до яких були залучені різні учасники та зацікавлені сторони, з метою посилення універсального обміну повідомленнями у засобах інформації та соціальних мережах.

	#	Ключові сфери, що потребують розгляду	Додаткова інформація
Інструменти, послуги та налаштування	12	Розглянути корисну роль, яку здатні відігравати налаштування пристроїв, технічні інструменти (наприклад, програми фільтрації) та додатки, що забезпечують захист дитини. Закликати користувачів нести відповідальність за свої пристрої, регулярно оновлювати операційну систему, а також використовувати відповідне програмне забезпечення та додатки безпеки.	Є низка доступних послуг, які допомагають виявити небажані матеріали або заблокувати небажані контакти. Деякі з цих програм забезпечення безпеки дитини та програм-фільтрів можуть бути фактично безкоштовні, позаяк вони є частиною операційної системи комп'ютера або постачаються як частина пакета послуг постачальників послуг Інтернету чи постачальників електронних послуг. Виробники деяких ігрових консолей також надають аналогічні інструменти, якщо пристрій допускає вихід в Інтернет. Ці програми не є гарантією абсолютно надійного захисту, але вони можуть забезпечити належний рівень підтримки, особливо в родинах із маленькими дітьми. Більшість пристроїв мають налаштування, що допомагають захистити дітей, а також сприяють здоровому та збалансованому використанню. Також є механізми, що дозволяють батькам керувати пристроями своїх дітей за допомогою встановлення часу, вибору додатків та послуг, що їх діти можуть використовувати, і керування покупками. Останнім часом було підготовлено звіти і розроблено налаштування, що дозволяють користувачам та батькам краще відстежувати час роботи з пристроєм та доступ до нього й керувати ним. Ці технічні інструменти слід використовувати як частину більш широкого арсеналу. Дуже важливою є участь батьків та/або опікунів. Подорослішавши, діти зажадають більше конфіденційності і також відчують сильне бажання розпочати власні дослідження. Крім того, там, де між продавцем та споживачем є фінансові відносини, дуже корисними можуть виявитися способи підтвердження віку, які допомагають продавцям товарів та послуг, що мають вікові обмеження, а також видавцям матеріалів, призначених тільки для читачів після певного віку, мати доступ до цієї особливої аудиторії. Там, де фінансових відносин немає, використання технологій підтвердження віку може виявитися проблематичним, або у багатьох країнах воно може виявитися неможливим через відсутність.

5.2 Приклади запитань

Після визначення національних зацікавлених сторін та учасників, серед них можна поширити перелік таких запитань із проханням надати відповіді. Їхні відповіді допоможуть

визначити сферу політики, сильні сторони, а також розділи у списку для самоперевірки на національному рівні, на які слід звернути особливу увагу.

- Якою мірою ви відповідаєте за безпеку дітей в цифровому середовищі та їхні права?
- Як безпека в цифровому середовищі та права дитини інтегровані у ваші наявні політики та процеси?
- Якою мірою безпека в цифровому середовищі охоплюється чинним законодавством?
- Якими є ваші пріоритети у сфері безпеки в цифровому середовищі?
- Які види діяльності ви здійснюєте з метою підтримання безпеки в цифровому середовищі?
- Чи мають діти/батьки можливість повідомити вам про проблеми та питання, що викликають занепокоєння і стосуються безпеки в цифровому середовищі?
- Назвіть три основні виклики, що стоять перед вами в онлайн-світі.
- Назвіть три головні можливості, що відкриваються перед вами в онлайн-світі.

Крім того, було б корисно провести дослідження, щоб зрозуміти, як діти і їхні батьки уявляють собі захист дитини в цифровому середовищі та яким є їхній досвід.

6. Довідкові матеріали

Захист дитини в цифровому середовищі: основні документи і публікації

2020 рік

- ECPAT International, Sexual Exploitation Of Children In The Middle East And North Africa, DQ Institute, 2020 Child Online Safety Report, 2020
- EU Kids Online, EU Kids Online 2020: Survey results from 19 countries, 2020

2019

- Internet Watch Foundation (IWF), Annual Report, 2019
- WeProtect Global Alliance, Global Threat Assessment, 2019
- Broadband Commission / ITU, Child Online Safety. Universal Declaration, 2019
- Broadband Commission / ITU, Child Safety Online: Minimizing the Risk of Violence, Abuse and Exploitation Online, 2019
- Global Kids Online, Growing up in a connected world, 2019
- Rethinking the Detection of Child Sexual Abuse Imagery on the Internet, in Proceedings of the 2019 World Wide Web Conference, May 13–17, 2019, San Francisco, USA, 2019
- UK Home Office, Online Harms White Paper (UK only), 2019
- PA Consulting, A tangled web: rethinking the approach to online CSEA, 2019
- UK Information Commissioner Office, Consultation on Code of Practice to help protect children online (UK only), 2019
- Global Fund to End Violence against Children, Disrupting Harm: evidence to understand online child sexual exploitation and abuse, 2019
- Global Partnership to End Violence against Children, Safe to Learn Call for Action, Youth Manifesto, 2019
- UNESCO, Behind the numbers: Ending school violence and bullying, 2019 (includes data on online hurtful behaviour and cyber-bullying)
- United Nations Human Rights, children's rights in relation to the digital environment, 2019
- Australian eSafety Commissioner, Safety by Design Overview, 2019
- UNICEF, Why businesses should invest in digital child safety brief, 2019
- U.S. Department of State, Trafficking in Persons report, 2019

2018

- WeProtect Global Alliance, Global Threat Assessment, 2018
- Child Dignity on the Digital World, Technical Working Group Report, 2018 Council of Europe, Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment, 2018
- Global Fund to End Violence against Children, Two years of supporting solutions: results from the Fund's investments, 2018
- WeProtect Global Alliance, Country examples of Model of National Response capabilities and implementation, 2018
- INTERPOL and ECPAT International, Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material, 2018

- EUROPOL, Internet Organized Crime Threat Assessment (IOCTA), 2018
- NetClean, Report about Child Sexual Abuse Cybercrime, 2018
- International Centre for Missing & Exploited Children (ICMEC), Child Sexual Abuse Material: Model Legislation & Global Review, 9th Edition, 2018
- International Centre for Missing & Exploited Children (ICMEC), Studies in Child Protection: Sexual Extortion and Non-Consensual Pornography, 2018
- International Association of Internet Hotlines, INHOPE Report, 2018
- Internet Watch Foundation (IWF), Annual Report, 2018
- Thorn, Production and Active Trading of Child Sexual Exploitation Images, 2018
- ITU, Global Cybersecurity Index, 2018
- CSA Centre of Expertise, Interventions for perpetrators of online child sexual exploitation - a scoping review and gap analysis, 2018
- NatCen, Behaviour and Characteristics of Perpetrators of Online-facilitated CSEA - a rapid evidence assessment, 2018
- UNICEF, Policy guide on children and digital connectivity, 2018

2017

- The National Center for Missing & Exploited Children (NCMEC), The online enticement of children: an in-depth analysis of CyberTipline Reports, 2017
- 5Rights Foundation, Digital Childhood, development milestones in digital environment, 2017
- Childnet, DeShame Report, 2017
- Canadian Centre for Child Protection, Survivors' survey, 2017
- Internet Watch Foundation (IWF), Annual Report, 2017
- International Centre for Missing & Exploited Children (ICMEC), Annual Report, 2017
- International Centre for Missing & Exploited Children (ICMEC), Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review, 2017
- Thorn, Sextortion online survey with 2,097 victims of sextortion ages 13 to 25, 2017
- UNICEF, Children in a Digital World, 2017
- Western Sydney University, Young and Online: Children's Perspectives on Life in Digital Age, 2017
- ECPAT International, Sexual Exploitation of Children in South East Asia, 2017

2016

- UNICEF, Perils and possibilities: growing up online, 2016
- UNICEF, Child protection in the digital age: National responses to online CSEA in ASEAN, 2016
- Centre for Justice and Crime Prevention, Child Online Protection in the MENA Region, 2016
- ECPAT International, Interagency Working Group on Sexual Exploitation of Children, Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (The Luxembourg Guidelines), 2016

2015

- WeProtect Global Alliance, Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response, 2015
- NCMEC, A Global Landscape of Hotlines Combating CSAM, 2015
- ITU and UNICEF, Guidelines for Industry on Child Online Protection, 2015

Про права людини в цифровому світі

- Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment, 2018
- UNESCO, Internet Universality Indicators, 2019
- Ranking Digital Rights (RDR), 2019 RDR Corporate Accountability Index, 2019
- Broadband Commission for Sustainable Development, The State of the Broadband, 2019
- ITU, Measuring Digital Development, 2019
- ITU, Measuring Information Society Report, 2018
- UNICEF, Children and Digital Marketing Industry Toolkit, 2018
- Broadband Commission for Sustainable Development, Digital health, 2017
- Broadband Commission for Sustainable Development, Digital Skills for life and work, 2017
- Broadband Commission for Sustainable Development, Digital gender divide, 2017
- UNICEF, Privacy, protection of personal information and reputation, 2017
- UNICEF, Freedom of expression, association, access to information and participation, 2017
- UNICEF, Access to the Internet and digital literacy, 2017
- UN CRC, Guidelines on effective protection of children from sexual exploitation, 2019

Додаткові матеріали доступні у відповідному розділі на вебсайті: www.itu-cop -guidelines.com.

Доповнення 1: Термінологія

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

Підліток

Підлітки – це особи віком від 10 до 19 років. Важливо зазначити, що в міжнародному праві немає обов'язкового терміну підлітки, й особи до 18 років розглядаються як діти, тим часом як 19-річні особи вважаються дорослими, крім випадків, коли повноліття настає раніше, відповідно до Національного законодавства67.

Штучний інтелект (ШІ)

У найширшому сенсі цей термін розпливчасто визначає системи, що стосуються сфери чистої наукової фантастики (так званий «сильний» ШІ, що має форму самосвідомості), і системи, які вже діють та спроможні виконувати дуже складні завдання (розпізнавання голосу або осіб, кермування автомобілем: ці системи описуються як «слабкий» або «середній» ШІ).

Системи ШІ

Система ШІ - це система на основі машин, яка в межах установленого людиною певного набору цілей може складати прогнози, робити рекомендації або приймати рішення, що впливають на реальне чи віртуальне середовище, і призначена для функціонування з різним рівнем автономності.

Найкращі інтереси дитин

Описує всі елементи, необхідні для прийняття рішення в конкретній ситуації для конкретної дитини або групи

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 стосовно дітей (CSEA)

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

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

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

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

Діти та молодь (молодь)

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

Іграшки, що мають доступ до Інтернету

Іграшки з доступом до Інтернету під'єднуються до нього за допомогою таких технологій, як Wi-Fi та Bluetooth, і зазвичай працюють у поєднанні зі спеціальними додатками, забезпечуючи дітям можливість інтерактивної гри. Згідно з проведеним компанією Juniper Research дослідженням, 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 США. Ці іграшки збирають та зберігають персональну інформацію про дітей, зокрема, імена, дані геолокації, адреси, світлини, аудіо- та відеозаписи.

Кібербулінг, що також іменується булінгм в цифровому середовищі

Міжнародне право не містить визначення кібербулінг. Для потреб цього документу під кібербулінгм розуміють навмисну агресивну дію, що неодноразово вчиняється групою осіб або окремою особою за допомогою цифрових технологій та спрямована проти жертви, якій важко захиститися. Зазвичай воно передбачає «використання цифрових технологій та інтернету для розміщення чутливої інформації про будь-кого, навмисне поширення відомостей особистого характеру, небажаних світлин або відео, надсилання повідомлень із погрозами чи образами (електронною поштою, у форматі миттєвого обміну повідомленнями,

в чатах і текстових повідомленнях), поширення пліток та неправдивої інформації про жертву або навмисне виключення її з онлайн-спілкування». Воно може відбуватися безпосередньо (в чатах або текстових повідомленнях), у межах спільноти з обмеженим доступом (розсилання постів та дратівливих повідомлень за списком електронних адрес) або ж у громадському доступі (наприклад, створення сайтів навмисне для знущання з жертв).

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 стосується раси, сексуальної орієнтації, релігії національності або імміграційного статусу, статевої/гендерної належності і політичного аспекту».

Цифрове громадянство

Цифрове громадянство означає корисну, відповідальну та компетентну діяльність у цифровому середовищі із застосуванням навичок ефективної комунікації та творчого підходу для втілення форм соціальної участі, що ґрунтуються на повазі до прав людини та людської гідності, 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 безпосередньо комунікації, технічні навички та критичне мислення.

Стійкість до впливу цифрового середовища

Цей термін описує здатність дитини емоційно впоратися зі шкідливими факторами в цифровому середовищі. Стійкість до впливу цифрового середовища передбачає наявність емоційних ресурсів, необхідних для того, щоб розуміти, коли дитина наражається на ризик в інтернеті, знати, як звертатися за допомогою, здобувати практичні уроки та відновлюватися після невдалого досвіду.

Освітяни

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

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

Грумінг в цифровому середовищі

Грумінг в цифровому середовищі, згідно з Люксембурзькими керівними настановами, означає процес налагодження/побудови взаємин із дитиною особисто або за допомогою інтернету чи інших цифрових технологій, з метою домогтися сексуальних зв'язків із цією особою в цифровому середовищі або в реальному житті, схиливши дитину вступити в сексуальний

зв'язок. Процес, спрямований на заманювання дітей у дії чи бесіди сексуального характеру, як з їх відома, так і без нього, або процес, що передбачає спілкування та встановлення взаємин між порушником і дитиною, з метою зробити останню вразливішою перед сексуальними зловживаннями. Термін «грумінг» не передбачено у міжнародному праві; в деяких юридичних системах, зокрема в Канаді, використовується термін «заманювання».

Інформаційно-комунікаційні технології (ІКТ)

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

Інтернет і пов'язані з ним технології

Тепер можна під'єднатися до інтернету, використовуючи різноманітні пристрої, наприклад смартфони, планшети, ігрові приставки, телевізори та ноутбуки, а також звичайні комп'ютери. Таким чином, за винятком випадків, коли контекст передбачає інше, слід розуміти, що будь-яке посилання на інтернет охоплює все це розмаїття способів під'єднання. Щоб відобразити багатство та складність інтернету, вислови «інтернет і пов'язані з ним технології», «ІКТ й онлайн-індустрія» та «інтернет-послуги» використовуються як взаємозамінні.

Повідомлення та видалення

Оператори та постачальники послуг іноді отримують повідомлення про підозрілий контент в інтернеті від споживачів, представників громадськості, правоохоронних органів або організацій «гарячої лінії». Процедури повідомлення та видалення - дії, що їх вчиняє компанія, зі швидкого видалення («видалення») незаконного контенту (незаконний контент визначається згідно із законодавством), щойно компанії стає відомо про наявність такого в її послугах («повідомлення«).

Онлайнові ігри

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

«Екосистема онлайн-ігор», згідно з 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 чи спілкуватися з гравцями та іншими представниками аудиторії85.

Інструменти батьківського контролю

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

проміжки часу. Досконаліші версії дозволяють вести запис усіх текстових повідомлень, що надсилаються або отримуються через пристрій. Зазвичай такі програми захищаються паролями.

Батьки та опікуни

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

Персональна інформація

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

Конфіденційність

Конфіденційність нерідко оцінюється з погляду 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, усвідомлення важливості збереження конфіденційності.

Секстинг

Секстинг зазвичай визначається як надсилання, отримання власноруч створеного сексуального контенту, зокрема, зображення, повідомлення або відео, чи обмін ними за допомогою мобільних телефонів та/або Інтернету. У більшості країн створення, поширення та зберігання зображень дітей сексуального характеру є незаконним. У разі поширення зображень дітей сексуального характеру дорослі не повинні переглядати їх. Демонстрація зображень сексуального характеру дитині дорослим завжди є злочинним діянням; поширення таких зображень між дітьми може завдати шкоди; слід повідомляти про подібні інциденти; може знадобитися допомога для усунення поширених зображень.

Секс-вимагання, або сексуальне вимагання стосовно дітей

Секс-вимагання, або сексуальне вимагання (також називається «сексуальним примусом або вимаганням в цифровому середовищі» означає «шантаж особи за допомогою власноруч створених зображень цієї особи з метою вимагання у неї сексуальних послуг, грошей або інших благ під загрозою поширення матеріалу без згоди особи, що фігурує в ньому (наприклад, через публікування зображень у соціальних мережах)».

Інтернет речей (IoT)

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

URL

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

Віртуальна реальність

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

WI-FI

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

Доповнення 2: Контактні злочини проти дітей та молодих осіб

Діти та молодь можуть бути відкриті для численних небажаних та неналежних контактів в Інтернеті, які можуть мати для них фатальні наслідки. Деякі з цих контактів можуть мати сексуальну природу.

Згідно з дослідженнями, 22% зазнавали булінг , домагань або переслідування в мережі; 24% отримували небажані сексуальні коментарі ; 8% зустрічалися в реальному житті з людьми, з якими доти спілкувалися тільки в мережі . Хоча значення для різних країн та різних регіонів відрізняються, ці цифри показують, що ризики реальні . В одному дослідженні Інтернету, проведеному в Сполучених Штатах Америки , зазначено, що 32% підлітків спілкувалися з абсолютно незнайомою людиною, 23% з них сказали, що їм було страшно та ніяково під час розмови; і 4% наражалися на наполегливі та агресивні сексуальні чіпляння.

Сексуальні інтернет-хижаки використовують Інтернет для спілкування з дітьми та молоддю з сексуальною метою, часто користуючись способами, відомими під назвою «грумінг», за допомогою яких вони домагаються довіри дитини, звертаючись до її чи його зацікавлень. Вони часто порушують сексуальні теми, використовують сексуальні світлини та відверті мовні засоби, для того щоб зменшити вразливість, підвищити сексуальну обізнаність та послабити волю своїх маленьких жертв. Для переслідування та звабления дитини або молодої особи використовуються подарунки, гроші, навіть квитки на транспорт, щоб заманити її туди, де інтернет-хижак зможе скоїти сексуальне насильство над нею. Може навіть відбуватися фото- або відеознімання цих зустрічей. Дітям та молоді часто бракує емоційної зрілості та почуття власної гідності, що робить їх вразливими для маніпуляцій та булінг. Вони також бояться сказати дорослим про свої зустрічі, побоюючись втрапити в ніякове становище або втратити доступ до Інтернету. Подекуди вони зацьковані інтернет-хижаками і їм наказано тримати цей зв’язок у таємниці. Крім того, сексуальні інтернет-хижаки вчаться один в одного на інтернет-форумах та в чатах.

Доповнення 3: Глобальний альянс WeProtect

Модель типових національних заходів реагування WePROTECT

Стратегія Глобального альянсу WePROTECT допомагає країнам розробити скоординовані багатосторонні заходи реагування для боротьби із сексуальною експлуатацією дитини в онлайн-середовища, керуючись відповідною Моделлю типових національних заходів реагування. Модель типових національних заходів реагування Глобального альянсу WeProtect виступає як програми заходів, які повинні прийматися на національному рівні. Вона надає країнам фундамент для боротьби із сексуальною експлуатацією в цифровому середовищі. Ця Модель типових національних заходів реагування призначена для того, щоб допомогти країні:

- оцінити актуальні на сьогодні заходи реагування на проблему сексуальної експлуатації дитини в цифровому середовищі та виявити прогалини;
- визначити пріоритетність національних зусиль із заповнення прогалин;
- зміцнити розуміння та співпрацю на міжнародному рівні.

Модель не пропонує обов'язкового характеру певних дій і не передбачає лише один підхід. Мета моделі - описати можливості, необхідні для ефективного захисту дітей, та підтримати країни в розвитку або розширенні наявних можливостей. У ній також міститься перелік стимулювальних чинників, які в разі їх запровадження й ефективності прискорять досягнення результатів та поліпшать їх. Модель включає двадцять одну можливість, які згруповані в шість блоків: політика й управління, кримінальна юстиція, потерпілі, соціальні питання, галузь, а також засоби інформації та комунікації. На думку Глобального альянсу WePROTECT, вжиття заходів у всіх шести блоках забезпечить всебічне національне реагування на такого типу злочини.

Ця модель дозволить країні, незалежно від поточного стану справ, виявити будь-які прогалини у сфері можливостей та планування з метою усунення цих прогалин. Країни розроблятимуть власні індивідуальні підходи, проте роблячи це в контексті єдиних погоджених меж та розуміння можливостей, можна продовжувати розвиток зв'язків та співпрацю між зацікавленими сторонами як на національному, так і на міжнародному рівнях.

Глобальні стратегічні заходи реагування WePROTECT

Глобальні стратегічні заходи реагування Глобального альянсу WePROTECT - це скоординований підхід до боротьби із сексуальною експлуатацією дитини в цифровому середовищі, який включає глибше осмислення глобальних проблем, міжнародну гармонізацію національних підходів та глобальні рішення на доповнення до національних заходів реагування. Глобальні стратегічні заходи реагування, по суті, є супутнім компонентом Моделі типових національних заходів реагування; тим часом як Модель типових національних заходів реагування зосереджена на можливостях, необхідних для розв'язання проблеми сексуальної експлуатації дитини в цифровому середовищі на національному рівні, Глобальні стратегічні заходи реагування зосереджені на пріоритетних сферах міжнародної співпраці та створення потенціалу.

Глобальні стратегічні заходи реагування включають шість тематичних сфер, кожна з яких характеризується необхідними можливостями та очікуваними результатами, а також наявністю партнерів, які для їх досягнення повинні провадити спільну роботу в різних країнах.

Політика та законодавство

Розвиток як політичної волі до дії, так і законодавства для ефективного узгодження підходу до кримінальних злочинів спричинить відновлення на національному та міжнародному рівнях зобов'язань високого рівня щодо боротьби із сексуальною експлуатацією дитини в цифровому середовищі.

Кримінальна юстиція

Обмін інформацією, зокрема, спільний доступ до міжнародних баз даних через офіційні структури обміну даними в поєднанні зі спеціалізованими, навченими працівниками та прокурорами, які мають досвід роботи із сексуальною експлуатацією дитини в цифровому середовищі, є найкращим способом виявлення, переслідування та затримання правопорушників, зокрема, завдяки успішному проведенню спільних розслідувань та винесенню вироків.

Подання заяв потерпілими, служби надання допомоги

Ефективна та своєчасна підтримка жертв, зокрема, захист їх власної ідентичності та можливість сказати про те, що сталося, допомагає гарантувати жертвам доступ до необхідної підтримки, коли вона їм потрібна.

Технологія

Використання технічних рішень, зокрема, штучного інтелекту, для виявлення, блокування та запобігання поширенню матеріалів шкідливого змісту, потокового мовлення й онлайн-грумінгу, що потребує обов'язкового та послідовного залучення більшої кількості представників технологічного сектору, унеможливить використання платформ як інструменту для сексуальної експлуатації дитини в цифровому середовищі.

Соціальні питання

Є ціла низка заходів, що їх суспільство вживає загалом, які сукупно можуть дати дітям можливість захиститися від сексуальної експлуатації в цифровому середовищі, хай би де вони не жили. Забезпечення безпеки цифрової культури на рівні проєкту (коли функції безпеки вбудовані) та дотримання етичного й послідовного підходу до висвітлення у засобах масової інформації обмежать доступ до незаконного контенту в цифровому середовищі. При цьому освіта й інформаційна¬пропагандистська діяльність, орієнтована на дітей та батьків, опікунів та фахівців, а також точкові заходи щодо правопорушників - усе це має на меті запобігти випадкам сексуальної експлуатації дитини в цифровому середовищі або пом'якшити їхні наслідки.

Дослідження та розуміння питання

Нарешті, оцінка загроз (наприклад, Global Threat Assessment 2019) і дослідження, що присвячені правопорушникам та стосуються довгострокових травм жертв, - усе це забезпечить уряду, правоохоронним органам, громадянському суспільству, академічним колам та промисловості чітке розуміння актуальних загроз.

Доповнення 4: Заходи реагування на джерела шкоди в цифровому середовищі (приклади)

Збірник наведених тут прикладів укладений авторами вкладів та авторами керівних настанов МСЕ для директивних органів.

Роз'яснювальна робота з дітьми щодо джерел шкоди в цифровому середовищі

Застосунок Own It компанії BBC - додаток для забезпечення благополуччя дітей віком 8-13 років, які отримали перший смартфон. У цьому додатку поєднуються передові технології машинного навчання для відстежування дій дітей на їхніх смартфонах та можливість дітей самостійно повідомити про свій емоційний стан, при цьому ця інформація використовується для надання адаптованого контенту та вжиття заходів, що допомагає дітям залишатися щасливими в цифровому середовищі.

Завдяки наявності спеціального тематичного контенту, що готується в межах усієї компанії BBC, додаток робить доступними корисні матеріали та ресурси, що допомагає молоді максимально ефективно використовувати час в цифровому середовищі та формувати здорову поведінку і здорові звички в цифровому середовищі, а також сприяє тому, щоб молодь та батьки провадили конструктивніші розмови про власний онлайн-досвід. Додаток не збирає ані персональних даних, ані згенерованого користувачем контенту, тому що все машинне навчання відбувається в додатку/на пристрої користувача.

Project Evolve - бібліотека навчання цифровим компетенціям, яка повністю забезпечена відповідними ресурсами та містить опис цифрових навичок дітей різного віку; ці матеріали допомагають батькам та освітянам осмислити компетенції, що їх повинні мати діти; є також матеріали та завдання для розвитку певних навичок.

360 degree safe - онлайн-інструмент самоконтролю для шкіл, що дає можливість розглянути й дати всебічну оцінку своєї безпеки в цифровому середовищі, а також забезпечує керівництво й надає підтримку в розробленні чітких стандартів.

Інститут DQ: За 2017-2019 роки в 30 країнах світу були зібрані дані 145 426 дітей та підлітків у межах руху #DQEveryChild, що просувається інститутом DQ, - глобального руху за цифрове громадянство, який почався в Сінгапурі за підтримки компанії Singtel і швидко розрісся завдяки співпраці зі Всесвітнім економічним форумом, охопивши понад 100 партнерських організацій. Цей рух був спрямований на те, щоб діти мали широкі знання у сфері цифрового громадянства від самого початку свого цифрового життя за допомогою онлайн-програми освіти й оцінки DQ World. Дані цього руху були використані для створення Індексу безпеки дитини в цифровому середовищі в 2020 році. В Індексі зроблена оцінку та ранжування безпеки дитини в цифровому середовищі в 30 країнах із використанням 24 чинників впливу на безпеку дитини в цифровому середовищі, згрупованих у шість блоків.

Пакет DQ Pro Family Readiness та онлайн-програма DQ World надають батькам можливість оцінити цифрову готовність своєї дитини та з використанням навчальних матеріалів

поліпшити цифрові компетенції, як-от цифрове громадянство, керування часом, проведеним за екраном, боротьба з кібербулінгм, управління кібербезпекою, цифрове співчуття, управління цифровим слідом, критичне мислення й управління конфіденційністю.

Австралійський Комплект інструментів електронної безпеки для шкіл - це набір ресурсів для підтримки шкіл у створенні безпечнішого онлайн-середовища. Комплект інструментів відображає багатогранний підхід до навчання онлайн-безпеці та складається із чотирьох блоків із ресурсами, які:

- готують школи до оцінки їхньої готовності розв'язувати проблеми онлайн-безпеки та містять пропозиції щодо поліпшення поточної практики;
- залучають усю шкільну спільноту до участі у створенні безпечного онлайн-середовища;
- призначені для навчання онлайн-безпеки на базі прикладів передового досвіду, допомагаючи школам розвивати можливості шкільної спільноти у сфері безпеки в цифровому середовищі;
- дозволяють ефективно реагувати на інциденти, зберігаючи безпеку та благополуччя.

Освітня кампанія I Click Sensibly Управління електронними засобами зв'язку (UKE) Польщі розповідає дітям та їхнім батькам про те, як підвищити онлайн-безпеку, розпізнати ризики ними управляти.

ChildFund Вьетнаму виступив з ініціативою Swipe Safe. У цій програмі дітям розповідається про потенційні ризики в цифровому середовищі, як-от кібершахрайство, булінг або сексуальні зловживання, і даються поради, як залишатися в безпеці.

Доповідь Комісії з широкосмугового зв'язку, Технології, широкосмуговий зв'язок та освіта: прискорене виконання програми «Освіта для всіх», 2013 г.

Дослідження на тему «Досвід дітей в цифровому середовищі: забезпечення взаєморозуміння та вживання заходів на глобальному рівні», ЮНІСЕФ, 2019 г.

Дослідний проєкт Global Kids Online містить різнобічну інформацію про передову практику реагування на різні види онлайн-шкоди.

Приклади залучення галузевих компаній

Комісаріат з електронної безпеки Австралії вибудовує міцні партнерські стосунки та співпрацює з галузевими компаніями, щоб досвід усіх австралійців в цифровому середовищі був більш безпечний та позитивний. Прикладом може бути його ініціатива «Безпека на етапі проєктування». У межах цієї ініціативи Комісаріат з електронної безпеки провів докладні консультації з галузевими компаніями, торговельними органами й організаціями, що відповідають за захист користувачів, а також батьками, опікунами і молоддю. Ініціатива «Безпека на етапі проєктування» має на меті заохочувати галузеві компанії та допомагати їм у забезпеченні безпеки користувачів, починаючи з етапів проєктування, розроблення та розгортання онлайн-послуг і платформ. Комісаріат з електронної безпеки також адмініструє три програми надсилання повідомлень та подання скарг: програму щодо кібербулінг, програму щодо зловживань із використанням зображень та програму щодо онлайн-контенту. Комісаріат з електронної безпеки може офіційно надавати приписи певним постачальникам онлайн-послуг щодо видалення контенту. Попри те, що програми значною мірою діють як модель співпраці між урядом та компаніями галузі, наявні у Комісаріату з електронної безпеки повноваження з видалення матеріалів забезпечують критичну мережу

безпеки та спонукують компанії галузі бути ініціативними в боротьбі зі шкодою в цифровому середовищі.

Компанія Telia зобов'язалася проаналізувати негативні наслідки, пов'язані з під'єднанням, і забезпечити управління ними, а також домогтися повної прозорості та підзвітності на рівні ради директорів. Компанія також виявляє турботу про дітей та молодь, визнаючи їх активними користувачами послуг компанії.

Управління електронних засобів зв'язку (UKE) у Польщі залучає громадянське суспільство та дітей до участі в інформаційно-пропагандистських кампаніях, щоб ті розуміли, на яких документах в цифровому середовищі вони ставлять підпис.

Internet Watch Foundation (Фонд спостереження за інтернетом) - це партнерська організація, що об'єднує галузеві компанії, державні структури, правоохоронні органи та НУО з метою викорінення практики сексуальних зловживань щодо дітей. Станом на 2020 рік до складу IWF входить 152 члени з платформ та інфраструктурних служб; членам пропонується низка послуг із запобігання поширенню кримінальних зображень на своїх платформах.

Законодавче регулювання

Виявіть політичну волю, щоб надати пріоритетного значення захисту дитини в цифровому середовищі, - підпишіть Загальну декларацію про безпеку дитини в цифровому середовищі (Комісія з широкосмугового зв'язку).

Регулювання

Отчет Out of the Shadows: shining light on the response to child sexual abuse and exploitation («Вийти з тіні: висвітлюючи заходи проти сексуальних зловживань щодо дітей та їх сексуальної експлуатації») (Economist Intelligence Unit, 2019) - єдиний інструмент, в якому прописані контрольні показники реагування країн на сексуальні зловживання щодо дітей та їх сексуальну експлуатацію, включно з цифровим простором, та заходи реагування, що вживаються компаніями ІКТ.

Виявлення зловживань щодо дітей в цифровому середовищі

Нижче наведені приклади належної практики виявлення випадків зловживань щодо дітей в цифровому середовищі.

INHOPE: Мережа INHOPE була створена 1999 року для боротьби з матеріалами CSAM в цифровому середовищі у відповідь на єдине бачення інтернету як простору, вільного від матеріалів, пов'язаних із сексуальними зловживаннями щодо дітей. За минулі 20 років мережа INHOPE зросла, успішно протидіючи збільшенню кількості матеріалів CSAM у мережі, їх географічному поширенню та жорстокості. На сьогодні «гарячі лінії» INHOPE працюють на місцях на всіх континентах, отримують повідомлення та негайно видаляють матеріали CSAM з інтернету, а також обмінюються інформацією з правоохоронними органами.

Microsoft PhotoDNA створює хеші зображень та порівнює їх із базою даних хешів, які вже визначені й затверджені як матеріали CSAM. У разі виявлення збігу зображення блокуються. Але цей інструмент не використовує технологію розпізнавання облич і не може ідентифікувати людину чи об'єкт на зображенні. Усе змінилося із винаходом PhotoDNA for Video.

PhotoDNA for Video розбиває відео на ключові кадри і фактично створює хеші для таких знімків екрана. Так само як PhotoDNA може визначити зображення, яке було змінено, щоб уникнути виявлення, PhotoDNA for Video може знайти контент із сексуальною експлуатацією дітей, відредагований або включений до відео, яке в іншому випадку було б нешкідливе.

Компанія Microsoft випустила новий інструмент для виявлення інтернет-хижаків, які полюють на дітей і входять у довіру до них в онлайн-чатах. Project Artemis, розроблений у співпраці з The Meet Group, Roblox, Kik і Thorn, побудований на запатентованій технології Microsoft і вільно поширюватиметься організацією Thorn серед компаній, що надають онлайн-послуги та пропонують функцію чату. Project Artemis - це технічний інструмент, що допомагає попередити адміністраторів про необхідність будь-якого модерування чатів. Ця техніка виявлення грумінгу зможе виявити інтернет-хижаків, які намагаються звабити дітей із сексуальною метою, вжити щодо них заходів та повідомити про них:

Неурядова організація Thorn розробила рекламні оголошення, що мають на меті втримати людину від пошуку матеріалів, пов'язаних із сексуальними зловживаннями щодо дітей; протягом трьох років ці оголошення були розміщені у чотирьох пошукових системах мільйони разів. Так, в оголошеннях зазначено 3-відсотковий рейтинг кліків від людей, які звертаються за допомогою після пошуку матеріалу, пов'язаного з експлуатацією.

Thorn's Safer - інструмент, який можна використати безпосередньо на платформі приватної компанії для визначення та видалення матеріалів CSAM, а також надання повідомлень про такі матеріали.

Thorn Spotlight - програмне забезпечення, що дає правоохоронним органам у всіх 50 штатах Сполучених Штатів Америки та в Канаді можливість прискорити ідентифікацію жертв і скоротити час розслідування більш ніж на 60%.

На сайті оголошень Geebo, адміністратори якого взяли на себе зобов'язання не допускати сексуальної експлуатації на цій платформі, ніколи не було випадків сексуальної експлуатації дітей. Їм вдається зробити це завдяки наявності процедури попередньої перевірки.

Класифікатор Google AI можна використовувати для виявлення матеріалів, пов'язаних із сексуальними зловживаннями щодо дітей, у мережах, сервісах та на платформах. Цей інструмент доступний безкоштовно через **API безпеки контенту Google**, пакет програм, що розширює можливості перегляду контенту за участю меншої кількості людей. Цей інструмент допоможе експертам-особам переглядати матеріали ще більшого обсягу та не давати спокою порушникам, орієнтуючись на зображення, які раніше не були позначені як незаконні матеріали. Спільне використання цієї технології прискорить ідентифікацію зображень.

У 2015 році Google розширив свою роботу з хешами, надавши першу такого типу технологію зняття «відбитків пальців» та порівняння відео на YouTube, яка сканує та ідентифікує завантажені відео, що містять відомі матеріали, пов'язані із сексуальними зловживаннями щодо дітей.

Під час хакатону з безпеки дітей у 2019 роціFacebook оголосив про переведення на відкритий початковий код двох технологій, які виявляють ідентичні та майже ідентичні світлини і відео. Ці два алгоритми доступні на GitHub, що дозволяє системам обміну хешами спілкуватися одна з одною та робить системи набагато потужнішими.

«Гаряча лінія» організації IWF постійно функціонує і не лише стежить за тисячами повідомлень від представників громадськості, які наштовхнулися на онлайн-зображення, що містять елементи сексуальних зловживань щодо дітей, а й виконує унікальну ініціативну роль, здійснюючи пошук цього незаконного контенту в Інтернеті. Можливість використовувати інформацію «гарячих ліній» та фокусувати ресурси на ній дозволяє ідентифікувати й видалити більше контенту. Мало того, IWF незмінно працює з Google, Microsoft, Facebook та іншими компаніями, що є її членами, щоб постійно розширювати технічні межі. IWF пропонує як рішення портал для надсилання повідомлень, який дає можливість користувачам Інтернету в країнах без «гарячих ліній» повідомляти про зображення та відеоролики, що, вочевидь містять елементи сексуальних зловживань щодо дітей, безпосередньо у IWF через спеціальну сторінку онлайн-порталу.

IWF у співпраці з доброчинним Фондом Мері Коллінз, що спеціалізується на підтримці жертв, хоче запустити нову кампанію, в якій закликатиме молодь повідомляти про будь-які самостійно згенеровані сексуальні зображення або відеоролики дітей до 18 років, на які вони натрапляють під час навігації Інтернетом.

В **Інтерполі** створена Міжнародна база даних щодо сексуальної експлуатації дітей (ICSE), що містить зображення та відео, - інструмент розвідки та розслідування, який дозволяє спеціалізованим слідчим більш ніж із 50 країн обмінюватися даними про випадки сексуальних зловживань щодо дітей. Аналізуючи цифровий, візуальний та звуковий контент світлин та відео, що визначають жертв, фахівці можуть знаходити докази, виявляти будь-які збіги у справах та об'єднувати зусилля з пошуку жертв сексуальних зловживань щодо дітей. На сьогодні база даних Інтерполу щодо сексуальної експлуатації дітей містить понад 1,5 млн зображень так відео, і завдяки їй були знайдені 19 400 жертв у цілому світі.

NetClean ProActive - це програмне забезпечення, що базується на порівнянні сигнатур та інших алгоритмах виявлення, які автоматично виявляють зображення та відео, що містять елементи сексуальних зловживань щодо дітей, в корпоративному середовищі.

Компанія Griffeye Brain використовує штучний інтелект для сканування контенту, що раніше не належав до будь-якої категорії, порівнюючи його з атрибутами відомого контенту CSAM і позначення підозрілих елементів для перегляду агентом.

Організація RAINN створила Національну «гарячу лінію» боротьби з сексуальним насильством, керує її роботою у партнерстві з більш ніж із 1000 місцевих організацій у цілій країні, яким можна повідомити про випадки сексуального насильства, а також адмініструє службу Безпечного телефону довіри Міністерства оборони США. RAINN також втілює програми щодо запобігання сексуальному насильству, надання допомоги потерпілим та забезпечення притягнення винних до відповідальності.

Safehorizon - це некомерційна організація з надання допомоги жертвам насильства та зловживань, яка працює у Нью-Йорку з 1978 року. Safehorizon надає жертвам насильства послуги «гарячої лінії»

Project Arachnid - це інноваційний інструмент, який адмініструє в Канаді, призначений для боротьби зі зростанням поширення в Інтернеті матеріалів, пов'язаних із сексуальними зловживаннями щодо дітей (CSAM).

http://www.oecd.org/internet/bridging-the-digital-gender-divide.pdf

With the support of: