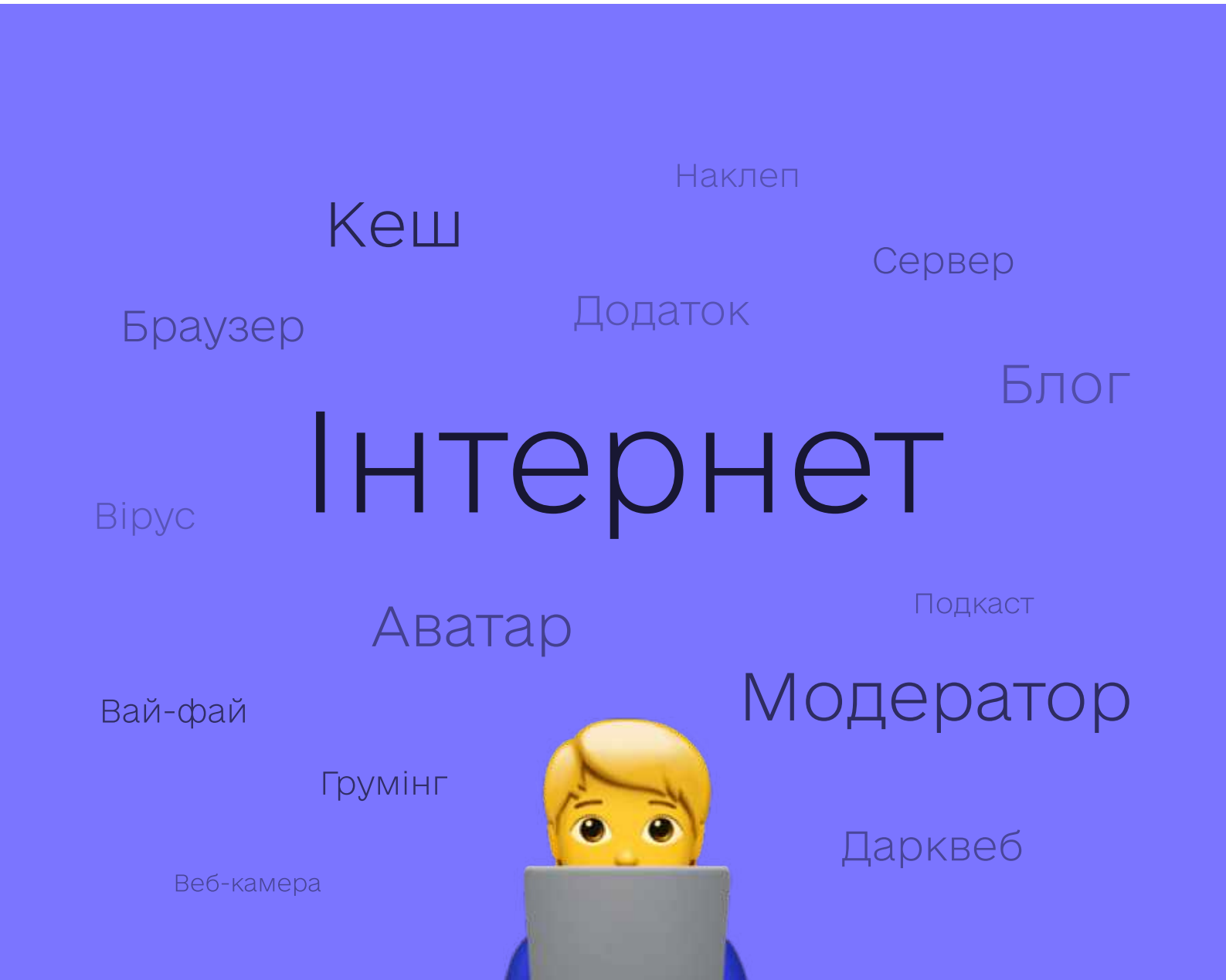
Міністерство
цифрової трансформації
України

Словник термінів з онлайн-безпеки



Україна на порозі цифрової трансформації. За динамічні зміни вболівають мільйони українців. Ми спільно будуємо країну, де можна буде отримати всі державні послуги онлайн. Країну зі швидким та безпечним Інтернетом. Державу, де можливості навчатися та розвивати власну справу, — рівні для всіх. Це сучасна омріяна Україна, де дбають про захист персональних даних та безпеку дітей в інтернеті.

В Україні інструменти захисту дитини онлайн ще недостатньо відповідають викликам часу та найкращим міжнародним практикам. Проте ми працюємо над погодженням Стратегії онлайн-захисту дітей, що допоможе попередити злочини або забезпечити швидке реагування на них у цифровому світі.

Актуальність проблеми підтверджують цифри

- 70% дітей та 35% батьків користуються соціальними мережами та месенджерами
- 67% дітей зізнались, що були чимось засмучені в Інтернеті, натомість лише 24% батьків знали про такі проблеми
- 29% дітей повідомили, що зустрічалися в реальному житті із тими, з ким вперше познайомились онлайн

Важливо, щоб державна політика була зрозумілою українцям, а чимало термінів та явищ цифрового світу є новими для громадян. Часто такі терміни є більш зрозумілими дітям, ніж їхнім батькам. Ми готові виправити цю ситуацію. Пропонуємо вашій увазі словник термінів, що допоможе говорити про безпеку онлайн уніфіковано.

Матеріал розроблено Міністерством цифрової трансформації з метою формування політики онлайн безпеки та інформування українців про Національну стратегію з безпеки для дітей в Інтернеті на 2020-2025 роки.

Щоб цифрове майбутнє для всіх нас настало швидше, запрошуємо вас приєднатися до руху за його створення. Зробити це нескладно — потрібно постійно навчатися нового й підвищувати свій рівень цифрової грамотності.

Аватар

це зображення, що візуально представляє учасників онлайн-чату, соціальної мережі, форумів, ігор тощо.

Безпека за дизайном

(англ. safety by design)

це заходи компанії або установи, які зосереджуються на безпеці та правах користувачів під час дизайну, розробки та впровадження онлайн-продуктів та послуг. Ініціативи мають на меті сприяти підвищенню стандартів безпеки користувачів.

Блог

(від комбінації слів web і log — з англ. “мережа” і “журнал”)

віртуальний журнал, створений користувачем(-ами) інтернету. Дописи блогу називаються «постами», вони містять текст і зображення та публікуються один за одним, у хронологічній послідовності. На сьогодні багато служб новин мають свої блоги та закликають читачів стежити за ними. Блог може мати головну тему, наприклад, «Поради з виховання дітей» або містити думки автора про події навколо.

Веб-камера

(webcam)

це камера, прикріплена до комп'ютера, яка може транслювати фото та відео зображення в режимі реального часу за допомогою Інтернету.

Веб-сайт або сайт

це місце в Інтернеті, де ви можете знайти інформацію, оплатити рахунки, пограти в ігри, поділитися фотографіями та історіями з іншими та ні. Компанії, уряди і окремі люди можуть мати веб-сайт. Кожен веб-сайт складається з веб-сторінок, на яких можуть відображатися текст, зображення, відео та звук.

Апаратне забезпечення/ комплектуючі

(англ. hardware)

це фізичні компоненти комп'ютера, такі як схема, екран або клавіатура та ін.

Біт-Торрент

це спосіб обміну інформацією, що дозволяє користувачам інтернету поширювати та завантажувати контент. Отримати необхідні файли можна від користувачів, що їх поширюють.

Блокування користувача

дія шляхом зміни налаштувань, завдяки якій один користувач забороняє іншому спілкуватися з ним/нею. Повідомлення від небажаної особи приховуються для користувача.

Браузер

(або веб-браузер)

це програма, яка дозволяє користувачам переглядати сторінки в інтернеті та взаємодіяти з інформацією онлайн. До найбільш популярних браузерів відносять: Google Chrome, Firefox, Opera, Safari, Internet Explorer та Edge.

Вай-фай

(безпровідна інтернет-мережа - wi-fi (wireless) internet access)

це мережева технологія, яка використовує радіохвилі для забезпечення високошвидкісного Інтернету та мережевих з'єднань без фізичного провідного з'єднання між відправником та одержувачем.

Веб-сторінка

це документ на веб-сайті, який можна побачити за допомогою веб-браузера. Веб-сторінка має індивідуальну веб-адресу або URL-адресу, наприклад, www.thedigital.gov.ua або www.google.com. Декілька веб-сторінок, які об'єднані однією темою, дизайном та пов'язані посиланнями, утворюють веб-сайт.

Вікі, вікіпедія

(wikis)

це група Інтернет-документів/веб-сторінок, які користувачі можуть вільно додавати та редагувати. Найвідомішою з них є Інтернет-енциклопедія — Вікіпедія. Усі вікі-сторінки створені групою осіб, а не одним автором. Під час перевірки фактів в Інтернеті багато людей звертаються до вікі-серверів, як до пріоритетної енциклопедії, оскільки вони можуть надати поточну інформацію про широкий спектр тем. Хороша вікі міститиме посилання на надійні веб-сайти. Користувачі повинні пам’ятати, що, оскільки вікі відкриті для публічного редагування, сторінки можуть бути вандалізовані та частина інформації може бути недостовірною через неякісне дослідження.

Вірус

це тип шкідливого програмного забезпечення, призначеного для копіювання та “зараження” комп'ютерних програм. Віруси можуть призвести до пошкодження даних та відмови системи. Віруси часто маскуються як щось інше, щоб їх можна було перенести з одного комп'ютера на інший без відома користувачів. Їх можна приховати в електронних листах, на компакт-дисках / USB-файлах або у файлах, якими можна ділитися через Інтернет. На комп’ютери можна встановити антивірусне програмне забезпечення, яке допоможе сканувати та видалити комп'ютерні віруси.

Дарквеб

(з англ. dark web — “темна павутина”)

це колекція веб-сайтів, навмисно прихована від пошукових систем. Ці сайти вимагають спеціального програмного забезпечення, конфігурації, шифрування або авторизації для доступу до них. Дарк-веб становить дуже маленьку частину діп-вебу (“глибокої павутини”) і зазвичай використовується для незаконної онлайн-діяльності.

Віртуальна реальність (virtual reality/VR)

Віртуальна реальність або VR — це програмне забезпечення, яке виробляє зображення та звуки для імітації реального тривимірного (3D) світу. Користувачі носять гарнітуру VR, яка створює середовище, з яким вони можуть взаємодіяти. Приклади містять 3D-тренажери польоту або ігри від першої особи, де можна досліджувати 3D-світ.

Вірус-вимагач

(англ. ransomware)

це тип шкідливого програмного забезпечення, яке блокує чи обмежує доступ до вашого комп’ютера або файлів і вимагає сплатити викуп шахраєві в обмін на розблокування.

Гіперпосилання

це будь-який текст або графік на сайті, який під час натисканн на нього переносить вас на інший ресурс або сторінку в інтернеті. Гіперпосилання часто з'являються у вигляді тексту іншого кольору або з підкресленням.

Грумінг

(від англ. groom — “доглядати”)

це коли доросла людина свідомо встановлює емоційний зв'язок з дитиною, щоб викликати у неї довіру задля сексуальних стосунків. Грумінгом можуть займатися дорослі, які видають себе за дітей у чатах або на сайтах соціальних мереж, щоб "подружитися" з дитиною і зустрітися з нею особисто. Грумінг може містити отримання інтимних зображень від дитини і є злочином згідно зі статтею 156 Кримінального кодексу України.

Дарксоушл

(з англ. dark social — “темна соцмережа”)

це обмін інформацією, який не може бути точно відстежений за допомогою веб-аналітики, тобто через збір і аналіз даних веб-сайту. Може містити посилання на веб-сайти у електронній пошті, текстові повідомлення, сервіси прямих повідомлень і додатки, які пропонує Facebook, Twitter, Snapchat і WhatsApp, а також внутрішньоігрові повідомлення, які можна знайти в таких іграх, як Minecraft і Roblox.

Діпфейк

(з англ. deep fake — “глибока підробка")

це надзвичайно реалістичне, хоча і фальшиве, зображення або відео, на якому реальна особа робить чи говорить щось, чого він/вона насправді не робили або не говорили. Діпфейки створюються за допомогою програмного забезпечення, яке спирається на велику кількість фотографій чи записів людини. Діпфейки використовуються для створення фальшивих новин, порнографічних відео знаменитостей та шахрайства.

Заборонений контент (prohibited content)

- зображення сексуального насильства над дітьми;
- просування або інструктаж з педофільної діяльності;
- вміст сексуального характеру;
- безкоштовні, деталізовані та вражаючі зображення реального насильства;
- вміст, який підтримує терористичний акт;
- вміст, що надає детальну інструкцію щодо злочину чи насильства або його сприяння.

Застосунок

це програма для смартфона або планшета, адаптована для роботи на екрані, меншому за комп’ютерний. Деяким мобільним додаткам для роботи необхідний постійний доступ до Інтернету.

Діпвеб

(з англ. deep web — “глибока павутина")

розміщений під "поверхнею" інтернету, до якого можна отримати доступ через пошукові системи. Вміст діпвебу невидимий для пошукових систем. Тут є вміст особистих поштових профілів, профілів у соціальних мережах та банківських рахунків в інтернеті.

Жертводорікання

(victim blaming)

це коли жертва злочину вважається відповідальною за шкоду, якої зазнала. Наприклад, той, хто зазнав насильства через зображення, можливо, ділився своїми інтимними зображеннями з іншою людиною, і це може ставитися особі за провину.

Завантаження

перенесення файлу, відео, документа або фотографії з веб-сайту на комп'ютер або інший цифровий пристрій.

Закладка/обрані

простір онлайн-закладок, які допомагають знайти потрібну сторінку або веб-сайт, коли це знадобиться знову. Веб-браузери дозволяють вам виділяти будь-яку сторінку і використовувати ці закладки для переходу на ресурс у будь-який час. Деякі браузери використовують термін "обране" замість терміну "закладка".

Згода

юридичне поняття, дія з явно визначеними правилами та наслідками за їх порушення, надається в усній чи письмовій формах. Згода може надаватися, наприклад, на отримання електронних листів та маркетингових матеріалів.

Інтернет

(або "всесвітня павутина")

це глобальна комп'ютерна мережа, яка дозволяє обмінюватися інформацією по всьому світу.

Інтернет-шахрайство

(англ. scam)

схема обману, за допомогою якої шахраї вимагають у користувачів гроші або доступ до персональних даних.

Кетфішинг

різновид обману, де людина створює в соціальних мережах фейкову (фальшиву) сторінку з метою романтичного знайомства, умисного шахрайства та ін.

Кібербулінг

цькування онлайн. Навмисна та неодноразова ворожа поведінка в онлайні з метою соціальної, психологічної чи фізичної шкоди. Зазвичай термін використовується для визначення жорстокої поведінки з дітьми та підлітками в інтернеті. Чи траплялося з тобою таке, коли хтось отримував доступ до твоїх акаунтів і надсилав твоїм друзям, рідним чи знайомим повідомлення з неприємним змістом? Це ще один прояв кібербулінгу, він називається самозванством (англ. impersonation).

Ім'я користувача

(username)

це ім'я, яке людина обирає в інтернеті. Коли ви реєструєтесь на сайті ігор або у чаті, вам потрібно створити унікальний ідентифікатор — "ім'я користувача", щоб ідентифікувати себе в цьому онлайн-середовищі. Вибір нікнейма замість власного повного імені, наприклад, "maz123", допоможе захистити вашу приватність.

Інтернет-провайдер

це компанія, яка надає доступ в інтернет приватним і бізнес-користувачам за абонентську плату.

Інформаційно-комунікаційні технології (ІКТ)

це термін, який використовується для опису всього обладнання і програмного забезпечення, що дозволяє обробляти, зберігати і передавати дані в цифровому форматі.

Кеш

веб-браузери зберігають копії нещодавно відвіданих веб-сайтів у пам'яті комп'ютера. Цей дисковий простір пам'яті називається “кешем”. Локальні файли завантажуються набагато швидше, аніж ті, що треба щоразу отримувати з Інтернету.

Кілоґер

(з англ. keylogger — “той, що веде журнал клавіш”)

це або апаратний пристрій, встановлений на клавіатурі, або шпигунське програмне забезпечення для запису кожного натискання (або послідовності натискань) на клавіатурі. Кілоґґер записує все, що користувач вводить, включаючи електронну пошту, імена користувачів, паролі, номери кредитних карт і/або банківських рахунків, з метою крадіжки інформації.

Кінцевий користувач

це особа, яка фактично використовує програмне забезпечення або онлайн-сервіс.

Користувач

(юзер)

особа, яка користується програмою на цифровому пристрої з або без підключення до інтернету.

Мережевий черв’як

(worm)

це програма, яка може копіюватись та поширюватись самостійно, без встручання людей. Черв'яки часто використовуються в комп’ютерних мережах, щоб скористатися вадами безпеки на вашому комп’ютері чи його операційній системі. Комп'ютерні черв'яки зазвичай трапляються у файлах, які додаються до електронних листів або миттєвих повідомлень. Як правило, їх можна уникати, не відкриваючи підозрілі електронні листи з вкладеннями або посиланнями, постійно оновлюючи комп'ютерну систему та використовуючи сучасне антивірусне програмне забезпечення.

Модем/роутер

це електронний пристрій, завдяки якому відбувається підключення комп’ютера до інтернету.

Наклеп

це поширення принизливої, образливої та неправдивої інформації про будь-кого. Наклеп може бути у вигляді текстових повідомлень, фото, мемів і є правопорушенням згідно з українським законодавством.

Насильство заради розваги

(англ. happy slapping)

коли будь-хто знімає сцени насильства (бійки, знущання) та поширює цей контент в інтернеті.

Ключові слова

це слова, що описують основний зміст веб-сторінки.

Мережа

це група комп'ютерів, які можуть взаємодіяти один з одним. Мережа може бути як невеликою (складатися з двох комп'ютерів), так і великою (складатися з мільярдів пристроїв).

Миттєвий обмін повідомленнями

відправлення повідомлень з одного комп'ютера або пристрою на інший за допомогою невеликих спливаючих вікон. Служби миттєвого обміну повідомленнями працюють, як і електронна пошта, — для спілкування двох або більшої кількості людей.

Міжнародний ідентифікатор мобільного обладнання

(IMEI)

це 15-значний номер, який ідентифікує бездротовий пристрій, наприклад, смартфон. IMEI-номер зазвичай розміщений на наклейці всередині пристрою або виводиться на екран після введення комбінації *#06#. Щоб не дозволити користування пристроєм у разі його втрати або крадіжки, можна попросити постачальника послуг заблокувати ваш IMEI.

Модератор

деякі соціальні мережі, а також онлайн-чати чи форуми використовують модераторів для перевірки змісту розмов, щоб переконатися, що користувачі дотримуються правил поведінки на сайті. Модератори часто можуть блокувати як окремі коментарі, так і користувачів, дописи яких не відповідають стандартам поведінки на сайті. Основна мета модераторів: не допускати образливих та принизливих коментарів.