

## **КІБЕРБЕЗПЕКА: ЯК БЕЗПЕЧНО ВИКОРИСТОВУВАТИ ОНЛАЙН-ПЛАТФОРМИ У НАВЧАННІ**

Під час онлайн-навчання і учні, і вчителі активно використовують такі платформи як Zoom, Google Classroom, Google Meet або Microsoft Teams для оптимізації роботи. Проте якщо не дотримуватися правил безпечного використання цих програм, можна натрапити на випадки несанкціонованого втручання у освітній процес як зловмисників, так і членів російських хакерських угруповань. Такі випадки ускладнюють здобуття якісних знань, зривають процес навчання та унеможливають використання повного потенціалу онлайн-платформ.

А якщо ви стикаєтеся з хакерськими втручаннями під час навчання, необхідно звертатися до кіберполіції. Телефонуйте на гарячу лінію:

**0 800 505 170.**

Кіберполіціанти готові реагувати на усі інциденти, пов'язані з несанкціонованим втручанням в інформаційно-комунікаційні системи та мережі закладів освіти.

### **Правила кібербезпеки під час війни**

Війна йде не лише безпосередньо на полі бою, вона йде і в інших просторах, зокрема — в інтернеті. Фейки, вкиди, збір інформації — це все знаряддя цієї війни. Тож дуже важливо навчитися самим та навчити дітей правильно реагувати на них.

Особливо вразливими до ворожих інформаційних атак зараз є діти та підлітки, що багато часу проводять в інтернет-просторі, але через свій вік ще не завжди можуть розпізнати загрозу. Тому дуже важливо донести до них кілька правил безпеки інтернет-спілкування у військовий час.

Краще за все спілкуватись в інтернеті лише з тими, кого дитина знає особисто — однокласниками, сусідами, друзями, знайомими. Пам'ятайте, що особа, яку ви знаєте виключно за фото на аватарці, може бути не тим, за кого вона себе видає. В першу чергу це стосується нових віртуальних знайомих.

Нагадайте дітям, що неможна через інтернет передавати будь-яку особисту інформацію, зокрема — номери телефону, адресу, інформацію щодо батьків. Якщо хтось ставить такі питання, краще, що може зробити дитина — це негайно припинити спілкування та сказати про це батькам.

Не переходьте самі за сумнівними посиланнями та забороняйте так робити дітям. Посилання від незнайомих контактів можуть містити віруси або вести на фішінгові сайти, мета яких — скопіювати важливі паролі. Періодично навіть знайомі контакти, сторінки яких зламали, можуть розсилати такі посилання. Якщо від когось із знайомих прийшло сумнівне посилання, краще за все зв'язатися з ним особисто та спитати, чи відправляв він вам щось.

Розмовляйте з дітьми про важливість критичного мислення та перевірки фактів. Вчить їх не піддаватися на емоційні маніпуляції. Ви можете разом пройти безкоштовні курси з критичного мислення та інформаційної гігієни

Ще раз нагадайте дітям, що не можна нікому відправляти свої інтимні фото або інтимні фото інших людей. Навіть отримавши одне таке фото шахраї

можуть почати шантажувати дитину, вимагаючи гроші, нові фото чи відео або якісь інші дії. Після першого ж прохання надіслати такі матеріали, слід негайно заблокувати контакт та сказати про це батькам. Корисно також передати цю інформацію кіберполіції.

Якщо дитина вже користується соціальними мережами, розкажіть їй про цифровий слід та про те, як важко видалити інформацію, що потрапила в інтернет. Вчіть її дуже прискіпливо відноситись до того, що вона публікує.

Розкажіть дитині про шахраїв, що пропонують легкий та швидкий заробіток в інтернеті за виконання різних завдань або ж ігри чи челенджі — щось кудись віднести, сфотографувати, намалювати. Попередьте, що за такими проханнями та завданнями можуть ховатися диверсії або злочини.

Не бійтесь розмовляти з дітьми на важкі теми, вони й без того бачать та чують більше, ніж здається батькам. Але задача вчителів — навчити їх безпечно користуватися інформацією та відповідально до неї ставитися.

### **Рекомендації використання гаджетів, які можуть надавати освітяни батькам та дітям.**

Не дозволяти дитині користуватися гаджетом у спальні та за годину до сну. Девайси можуть впливати на сон дитини через збудження нервової системи.

Не використовувати гаджети, коли дитина йде вулицею, переходить дорогу, грає на подвір'ї. Варто бути пильними і стежити за ситуацією навколо, особливо під час руху.

Проводити час і спілкування з родиною має відбуватися наживо, наскільки це можливо в наш час.

Не реєструвати дитину у соціальних мережах до настання мінімального віку (у різних соціальних мережах він різний, але не менше 13 років).

Не дозволяти використовувати соціальні мережі з ваших профілів. Пам'ятайте, що ваш профіль для системи — дорослий, отже, контент, який переглядає дитина, не фільтрується.

Пояснювати дитині, що не можна ділитися інтимними світлинами й особистою інформацією через інтернет та періодично нагадуйте про це.

Не користуватися девайсами за столом під час вживання їжі. Дуже важливо залишатися сконцентрованим на процесі й не відволікатися. Це важливо для системи травлення дитини, а також впливає на спілкування з близькими.

Контролювати, що саме дитина шукає в інтернеті та соціальних мережах.

Проводити з дитиною бесіди-дослідження про недоліки надмірного використання смартфонів, простежте, чим зазвичай зайнята ваша дитина в гаджеті, заохочуйте використання смартфона з користю.

Подумати про встановлення чітких часових обмежень для користування гаджетами, щоб не було суперечок, коли потрібно зупинитися.

Аргументувати свої дії без ультиматумів типу «Я сказав/-ла, тому буде саме так!» Можливо, варто використати «Сімейну угоду».

### **Безпечний Instagram для дітей.**

Instagram — це соціальна мережа компанії «Meta Platforms», що

базується на обміні світлинами та відео.

Яких правил варто дотримуватися:

Не створюйте профілі дітям молодшим 13 років, або використовуйте вікові позначки та «Сімейний нагляд».

Зробіть профіль дитини приватним — так він буде недоступним для сторонніх користувачів.

Встановіть ліміт часу на використання соціальної мережі.

Поясніть дитині, що не варто додавати у підписники невідомих користувачів.

Періодично переглядайте підписників дитини і видаляйте незнайомих.

Більше порад про безпечний Instagram шукайте у гайді.

### Як налаштувати Tik Tok?

Tik Tok — це застосунок для перегляду та створення коротких відео. Як і в будь-якій соцмережі, у Tik Tok є ризик натрапити на небажаний контент або користувача.

Діти до 13 років можуть користуватись мережею, але без створення профілю. Якщо дитині від 13 до 15 років, то акаунти автоматично створюються приватними. Для дітей 16-17 років акаунти автоматично створюються публічними.

### Правила безпечного Tik Tok:

Зробіть профіль дитини приватним.

Налаштуйте обмеження контенту, якщо бачите недоречні відео в Tik Tok дитини.

Поясніть дитині, як можна поскаржитися на відео, видалити небажані коментарі та заблокувати профілі, які їй не подобаються.

Налаштуйте систему «Сімейний зв'язок» — опція, яка дозволяє батькам з'єднати свій профіль у Tik Tok з обліковим записом дитини та отримати доступ до деяких налаштувань безпеки і конфіденційності дитячого акаунта.

Не давайте дитині використовувати Tik Tok з вашого профілю, бо ваш контент може їй не підходити.

Встановіть довірливі стосунки з дитиною. Якщо її щось засмутить або злякає у соціальних мережах, вона може звернутись до вас за порадою.

Ще більше про налаштування безпеки для дитини у Tik Tok читайте в гайдах.

Разом ми формуємо безпечний освітній простір!

# БУЛІНГ ТА КІБЕРБУЛІНГ

## ПОРАДИ ПЕДАГОГАМ, ЯК ДІЯТИ У ВИПАДКУ БУЛІНГУ І КІБЕРБУЛІНГУ

Нині серед учнівської молоді надзвичайно загострилася проблема насильства, здійснюваного самими дітьми одне до одного.

Останніми роками визнано поширення в освітній практиці такого явища, як шкільний булінг. Це соціальна проблема всього світу протягом останніх ста років, однак вона ще й досі не вивчена. Перші публікації в Україні з'явилися 2005 р.

Булінг (bullying, від англ. bully — хуліган, забіяка, задирака, грубіян, насильник) визначається як утиск, дискримінація, цькування. Цей термін означає тривалий процес свідомого жорстокого ставлення (фізичного і психічного) з боку дитини або групи до іншої дитини або інших дітей.

Мотивацією до булінгу стають заздрість, помста, відчуття неприязні, прагнення відновити справедливість; боротьба за владу; потреба підпорядкування лідерові, нейтралізації суперника, самоствердження тощо аж до задоволення садистських потреб окремих осіб.

Як показує практика, форми шкільного булінгу можуть бути різними:

систематичні кепкування з будь-якого приводу (від національності до зовнішнього вигляду дитини);

задирство;

фізичні і психічні приниження;

різного виду знущання;

бойкот та ігнорування;

псування особистих речей та ін.

Хулігани (булі) надзвичайно винахідливі. Новітній їхній “винахід” — кібербулінг, тобто знущання з використанням електронних засобів комунікації.

Дослідники пропонують таку найзагальнішу класифікацію всіх видів булінгу:

1-ша група — прояви, пов'язані переважно з активними формами приниження;

2-га група — прояви, пов'язані зі свідомою ізоляцією, обструкцією скривджених.

Соціальна структура булінгу, як правило, має три елементи, а саме:

переслідувач (булі);

жертва;

спостерігач.

У сучасній науці існує декілька підходів до вивчення булінгу. Одні дослідники зосереджують увагу на пошуку й визначенні особистісних рис, характерних для особи булі та його жертви. Інші намагаються розглядати булінг як соціально-психологічний процес.

Ось як визначає типові риси учнів, схильних ставати булі, норвезький психолог Д. Ольвеус:

вони відчують сильну потребу панувати й підпорядковувати собі інших учнів, переслідуючи власні цілі; вони імпульсивні й легко шаленіють;

вони часто зухвалі та агресивні в ставленні до дорослих (передусім батьків і вчителів);

вони не виявляють співчуття до своїх жертв;

якщо це хлопчики, вони зазвичай фізично сильніші за інших.

Типові жертви булінгу також мають свої характерні риси:

вони полохливі, вразливі, замкнуті й соромливі;

вони часто тривожні, невпевнені в собі, нещасній мають низьку самоповагу;

вони схильні до депресії й частіше за своїх ровесників думають про самогубство;

вони часто не мають жодного близького друга та успішніше спілкуються з дорослими, ніж із однолітками;

якщо це хлопчики, вони можуть бути фізичнослабшими за своїх ровесників.

Як зрозуміти, що дитина є жертвою боулінгу:

Діти, які страждають від булінгу, можуть не хотіти йти до школи або ж можуть плакати, вигадувати хворобу у шкільні дні.

Вони не беруть участь у спільній класній діяльності, соціальних заходах.

Часто у дитини змінюється поведінка: вона усамітнюється, поводить себе незвичайно.

Дитина починає губити гроші або речі, приходять додому у порваному одязі чи з поламаними речами. Коли ви її запитаете, що трапилося – не можуть реалістично пояснити.

Може почати говорити про те, що кине школу, пропускає заходи, в яких приймають участь інші учні.

Відсутність контакту з однолітками: немає друзів, зідзвонювань, не ведеться переписка у соцмережах, похід до школи і повернення звідти наодинці, немає у кого запитати домашнє завдання.

Психосоматичні ознаки: часті хвороби, наприклад, ломота в тілі, болі в животі, вірусні інфекції.

Обмальовані руки або специфічні малюнки на полях у зошиті.

Бажання іти до школи іншою дорогою, аніж та, якою йдуть усі інші діти.

Наслідки шкільного насильства

Жертви булінгу переживають важкі емоції – почуття приниження і сором, страх, розпач і злість. Булінг вкрай негативно впливає на соціалізацію жертви, спричиняючи:

неадекватне сприймання себе – занижене самооцінювання,

комплекс неповноцінності, беззахисність;

негативне сприймання однолітків – відсторонення від спілкування,

самотність, прогули у школі;

неадекватне сприймання реальності – підвищену тривожність,

різноманітні фобії, неврози;

девіантну поведінку – схильність до правопорушень, суїцидальні наміри, формування алкогольної, тютюнової чи наркотичної залежності.

Як реагувати на цькування

Як молодші школярі так і старшокласники мають неодмінно звертатися за

допомогою до дорослих – учителів і батьків. Допомога дорослих дуже потрібна особливо якщо дії кривдників можуть завдати серйозної шкоди фізичному та психічному здоров'ю.

Підлітки часто намагаються самостійно впоратись із деякими ситуаціями.

Психологами було розроблено такі поради для них.

## **КІБЕРБУЛІНГ ТА ЙОГО ТИПИ**

Безпечне і здорове освітнє середовище є сукупністю умов у закладі освіти, що унеможливають заподіяння учасникам освітнього процесу фізичної, майнової та/або моральної шкоди, зокрема внаслідок недотримання вимог законодавства щодо кібербезпеки, захисту персональних даних, шляхом фізичного та/або психологічного насильства, експлуатації, дискримінації за будь-якою ознакою, приниження честі, гідності, ділової репутації (булінг (цькування), поширення неправдивих відомостей тощо), пропаганди та/або агітації, у тому числі з використанням кіберпростору.

Кібербулінг - це один із різновидів булінгу (цькування), що передбачає жорстокі дії з метою дошкулити, нашкодити, принизити людину з використанням сучасних електронних технологій: Інтернету (електронної пошти, форумів, чатів, ICQ) та інших засобів електронної техніки – мобільних телефонів чи інших гаджетів.

Відмінності кібербулінгу від булінгу зумовлюються особливостями Інтернет-середовища: анонімністю, можливістю підмінити ідентичність, охоплювати велику аудиторію одночасно, (особливо дієво для поширення пліток), здатність тероризувати та тримати у напрузі жертву будь-де і будь-коли.

Кібербулінг являється формою психологічного насильства.

### **ТИПИ КІБЕРБУЛІНГУ:**

перепалка (флеймінг) - обмін короткими гнівними та запальними репліками між учасниками з використанням комунікаційних технологій (як правило, на форумах та в чатах);

нападки (домагання) – регулярні висловлювання образливого характеру на адресу жертви (багато СМС-повідомлень, постійні дзвінки), що переважantlyють персональні канали комунікації;

наклеп - поширення неправдивої, принизливої інформації;

самозванство - використання особистих даних жертви (логіни, паролі до акаунтів в мережах, блогах) з метою здійснення від її імені негативної комунікації;

публічне розголошення особистої інформації - поширення особистої інформації, наприклад шляхом публікування інтимних фотографій, фінансової інформації, роду діяльності з метою образи чи шантажу;

ошуканство - виманювання конфіденційної особистої інформації для власних цілей або передачі іншим особам;

відчуження (острокізм, ізоляція) - онлайн відчуження в будь-яких типах середовищ, де використовується захист пароллями, формується список небажаної пошти або список друзів;

кіберпереслідування - приховане вистежування жертви для скоєння нападу, побиття, зґвалтування;

хепіслепінг – реальні напади, які знімаються на відео для розміщення в Інтернеті, що можуть привести до летальних наслідків;

онлайн-грумінг – побудова в мережі інтернет дорослим або групою дорослих осіб довірливих стосунків із дитиною (підлітком) з метою отримання її інтимних фото/відео та подальшим її шантажуванням про розповсюдження цих фото, наприклад для отримання грошей, більш інтимних зображень чи навіть примушування до особистих зустрічей.

### **Ознаки кібербулінгу:**

- ◆ систематичність (повторюваність) діяння;
- ◆ наявність сторін – кривдник (булер), потерпілий (жертва булінгу), спостерігачі (за наявності);
- ◆ дії або бездіяльність кривдника, наслідком яких є заподіяння психічної та/або фізичної шкоди, приниження, страх, тривога, підпорядкування потерпілого інтересам кривдника та/або спричинення соціальної ізоляції потерпілого.

Якщо висловлювання, поширення картинок тощо в мережі Інтернет щодо певної особи сприймається нею як жарт, не мають систематичного характеру та не викликають негативних емоційних реакцій, такі дії не вважаються кібербулінгом.

## Сторони кібербулінгу та їхні ролі

Кривдник (булер) – учасник освітнього процесу, в тому числі малолітня чи неповнолітня особа, яка вчиняє булінг (цькування) щодо іншого учасника освітнього процесу.

Потерпілий (жертва) – учасник освітнього процесу, в тому числі малолітня чи неповнолітня особа, щодо якої було вчинено булінг (цькування).

Спостерігач – свідки та (або) безпосередні очевидці випадку булінгу (цькування).

Дії педагогічних працівників у випадку виявлення кібербулінгу

Норми Порядку реагування на випадки булінгу (цькування), затвердженого наказом Міністерством освіти і науки України від 28 грудня 2019 року № 1646 (далі - Порядок), поширюється у тому числі на випадки прояву кібербулінгу.

Так, у закладі освіти заяви або повідомлення про випадок булінгу (цькування) або підозру щодо його вчинення приймає керівник закладу (абзац другий пункту 1 розділу II Порядку).

Повідомлення можуть бути в усній та (або) письмовій формі, в тому числі із застосуванням засобів електронної комунікації.

Керівник закладу освіти у разі отримання заяви або повідомлення про випадок булінгу (цькування):

невідкладно у строк, що не перевищує однієї доби, повідомляє територіальний орган (підрозділ) Національної поліції України, принаймні одного з батьків або інших законних представників малолітньої чи неповнолітньої особи, яка стала стороною булінгу (цькування)

за потреби викликає бригаду екстреної (швидкої) медичної допомоги для надання екстреної медичної допомоги;

повідомляє службу у справах дітей з метою вирішення питання щодо соціального захисту малолітньої чи неповнолітньої особи, яка стала стороною булінгу (цькування), з'ясування причин, які призвели до випадку булінгу (цькування) та вжиття заходів для усунення таких причин;

повідомляє центр соціальних служб для сім'ї, дітей та молоді з метою здійснення оцінки потреб сторін булінгу (цькування), визначення соціальних послуг та методів соціальної роботи, забезпечення психологічної підтримки та надання соціальних послуг;

скликає засідання комісії з розгляду випадку булінгу (цькування) (далі - комісія) не пізніше ніж упродовж трьох робочих днів з дня отримання заяви або повідомлення.

Строк розгляду комісією заяви або повідомлення про випадок булінгу (цькування) в закладі освіти та виконання нею своїх завдань не має перевищувати десяти робочих днів із дня отримання заяви або повідомлення керівником закладу освіти (пункт 11 розділу IV Порядку).

### **Дії потерпілого**

щодо видалення інформації про нього в комп'ютерній мережі

З метою захисту від кібербулінгу потерпілий може вчиняти наступні дії:

→ На початковому етапі прояву кібербулінгу, якщо це можливо, емоційно не реагувати, оскільки "емоції породжуються емоції".

→ Фіксувати всі дії кривдника (наприклад, робити фото або скріншоти неправдивої інформації про себе; інформації, що містить персональні дані; інформації, що принижує честь та гідність (далі - інформація).

→ Звернутися за порадою щодо дій кривдника до батьків, вчителів, довіреної особи або зателефонувати на національну дитячу "гарячу" лінію (у будні: з 12.00 по 16.00 за номером 0 800 500 225 (безкоштовно зі стаціонарних та мобільних) та 116 111 (безкоштовно з мобільних).

→ Звернутися із заявою або повідомленням про вчинення кібербулінгу до керівника навчального закладу, якщо кібербулінг вчиняється щодо потерпілого в навчальному закладі і кривдником є учень (студент) або член педагогічного колективу.

→ Якщо кібербулінг відбувається в соціальній мережі (наприклад, Facebook, Telegram, Вконтакте, Twitter, Youtube тощо), потерпілий має можливість звернутися зі скаргою до адміністратора сторінки або групи, що створена у відповідній соціальній мережі, з метою видалення інформації про нього. У випадку відмови адміністратора виконати відповідні дії, потерпілий може звернутися безпосередньо до служби підтримки соціальної мережі (наприклад, у соціальній мережі Facebook міститься вкладка "Довідка та підтримка") або натиснути кнопку "Поскаржитися".

### **Важливо!**

Посилання на ресурси безпеки в популярних соціальних мережах

→ У випадку виявлення в мережі Інтернет, на вебсайті інформації, потерпілий має право вимагати видалення такої інформації з вебсайту, а також, з результатів видачі за відповідними запитами з пошукових систем, котрі скеровують на вказані вище сайти. З цією метою варто звернутися до власника вебсайту (дізнатися дані щодо адміністраторів або власників вебсайтів допоможе сервіс Whois).

→ Якщо в досудовому порядку з'ясувати питання не вдалося, потерпілий має право, керуючись статтями 277 та 278 Цивільного кодексу України, звернутися безпосередньо до суду для захисту або поновлення своїх порушених прав\*.

\*Наприклад, належними відповідачами у справі вказано власників вебсайтів, оскільки саме вони створили технологічну можливість та умови для поширення недостовірної інформації, а також, пошукова система, яка індексує ці вебсайти, а саме в Україні це, як правило, представник компанії Товариство з обмеженою відповідальністю "Гугл" (рішення Солом'янського районного суду м. Києва від 28 жовтня 2016 року у справі № 760/17173/16-ц).

→ Звернутися до органів Національної поліції із заявою про вчинення адміністративного правопорушення відповідно до статті 1734 Кодексу України про адміністративні правопорушення.

Крім того, якщо дитина стала жертвою кібербулінгу, варто звернутися до управління/відділу протидії кіберзлочинам Департаменту кіберполіції Національної поліції України у відповідній області або направити електронне повідомлення про вчинення кримінального правопорушення.

### **Відповідальність за вчинення кібербулінг**

За вчинення кібербулінгу до кривдника може застосовуватися цивільна, адміністративна або кримінальна відповідальність.

### **Судова практика**

Рішення Європейського суду з прав людини від 11 лютого 2020 року у справі "BUTURUGA v. ROMANIA" (кібербулінг визнається одним із видів насильства над жінками та дівчатами, і він може мати різні форми, включно з кіберпорушенням конфіденційності, зламом комп'ютеру жертви та вилученням, поширенням і маніпуляцією даними та фотографіями, включно з особистою інформацією)

Рішення Святошенського районного суду міста Києва від 07 травня 2019 року у справі № 759/5671/19 (булінг з використанням комп'ютерних технологій, а саме розповсюдження фотографій порнографічного характеру в додатку "Viber")

### **Корисні посилання**

- [Що таке булінг та як з ним боротися?](#)
- [Кібербулінг як соціально-педагогічна проблема](#)
  - [Кібербулінг що це та як це зупинити?](#)
- [Як ефективно захистити свої права від Інтернет-порушників](#)

- [Освітній серіал "Про кібербулінг для підлітків". Проєкт Міністерства цифрової трансформації України за підтримки ЮНІСЕФ в Україні](#)
- [Протидія булінгу в дитячому середовищі](#)
- [Звернення до суду: позовне провадження у цивільному процесі](#)
- [Запобігання та протидія домашньому насильству](#)
- [Права та обов'язки педагогічного працівника загальноосвітнього закладу. Порядок оскарження його дій чи бездіяльності](#)
- [Мобінг: поняття, різновиди, причини, відповідальність](#)