Міністерство освіти і науки України

Науково-методичний центр
професійно-технічної освіти
у Запорізькій області

Марина ТАРАН

ОСНОВИ ЦИФРОВОЇ ГІГІЄНИ

Методичні рекомендації

Розглянуто і схвалено:
Науково-методичною радою
НМЦ ПТО у Запорізькій області
як рекомендації для педагогічних
працівників закладів професійної
(професійно-технічної) освіти
Протокол № 2 від 27.04.2023

Запоріжжя
2023

УДК 004.738

Укладач:
Таран М.В., методист Науково-методичного центру професійно-технічної освіти у Запорізькій області

Рецензент:
Шумада Р.Я., завідувач обласного науково-методичного центру моніторингових досліджень якості освіти Комунального закладу «Запорізький обласний інститут післядипломної педагогічної освіти» Запорізької обласної ради.

Відповідальний за випуск:
Паржницький О.В., директор Науково-методичного центру професійно-технічної освіти у Запорізькій області, канд. пед. наук.

Методичні рекомендації містять принципи цифрової гігієни, що допоможе педагогічним працівникам дотримуватись правил цифрової безпеки та швидко, правильно реагувати на кібербулінг в освітньому процесі.

ЗМІСТ

ВСТУП

У сучасному світі високий рівень досягнення у сфері комп’ютерних технологій особливо вимагає дотримання певних правил поведінки для убезпечення себе та оточення від кіберзагроз у цій сфері. Інформаційний потік стає все доступнішим, а особиста інформація може бути, як на долоні. Тому постає питання, як захистити себе та близьких в епоху, коли цифровий простір стрімко розвивається, а світ навколо нас невпинно діджиталізується.

Зі стрімким розвитком технологій ми все більш часу проводимо у цифровому середовищі та потрапляємо у пастку відкритого доступу до інтернет-сервісів, залишаючи все дедалі більше особистої інформації, яка зберігається на персональних комп’ютерах та мобільних пристроях. Гаджетам та різноманітним вебсередовищам (соцмережі, ігри, онлайн-кінотеатри тощо) доручаємо знати все більше приватної інформації про нас, тому ризикуємо зустрітися у цифровому світі зі злочинцями або шахраями та загрозою стати їх «жертвою».

На жаль у повсякденному житті кібершахрайство стало поширеною проблемою, тому необхідно вміти попередити можливу кібератаку або мінімізувати її наслідки, у випадку якщо вони все ж таки сталися.

1. Правила цифрової безпеки

У світі, який постійно діджиталізується, існують свої правила, що можуть вберегти від кіберзагроз наш цифровий простір. Саме ці правила і є цифровою гігієною.

Тобто цифрова гігієна – це грамотне споживання інтернет-інформації, а також дотримання базових правил безпеки.

Зі збільшенням досягнень у сфері комп'ютерних технологій та кількості віддалених працівників більш актуально постає питання збереження особистих і корпоративних даних від зловмисників. Нище наведено перелік найвідоміших цифрових атак в Україні за останні роки.

Квітень 2017 року – «вірус Петя», один із наймасштабніших вірусів у нашій державі. Petya.A – шкідливе програмне забезпечення, яке було спрямоване на мережу державних підприємств, установ, банків та медіа. Цей вірус, потрапивши до системи, безповоротно знищував оригінальні файли і примусово перезавантажував комп'ютер, після чого користувачеві виводився екран напис з вимогою перерахувати певну грошову суму в біткоїнах на криптогаманець. Вірус розповсюджувався через популярну та широко використовувану серед бухгалтерів програму M.E.Doc. Зокрема, цій атаці було піддано такі підприємства, як аеропорт «Бориспіль», ЧАЕС, «Укртелеком», Ощадбанк, «Укрзалізниця», а також офіційний сайт Кабінету міністрів України та численні комерційні підприємства.

Березень 2019-го – фішингова розсилка на тему виборів проводилася нібито від імені Центру соціальних і маркетингових досліджень (SOCIS). Як приманка використовувалися «інформаційні матеріали» про соціально-політичну ситуацію в Україні. А також користувачеві важливо вміти відрізняти фішингові листи від справжніх. Фішинг – це спроба оманливим шляхом отримати особисту інформацію суб'єктів в інтернет-середовищі насамперед, це підроблені електронні листи, оголошення або сайти.

Березень 2020 року – фішингові листи на тему коронавірусу, що приховували у собі шкідливе програмне забезпечення.

Жовтень 2020-го – фішингові розсилки працівникам державних установ України з метою компрометації облікових записів електронної пошти.

Січень 2021 року – відбулася масова розсилка фішингових електронних листів на державні установи України. Листи були відправлені начебто від імені адміністрації Держспецзв'язку з поштової скриньки zapros@dsszzi.gov.ua та містили вкладення зі шкідливим програмним забезпеченням.

Лютий 2021-го – хакерське втручання в нову популярну соціальну мережу Clubhouse. Хакер-«благодійник» перенаправляв аудіопотоки розмов, що велись у Clubhouse, на інший вебсайт, щоб інші користувачі могли слухати розмови.

Але цей перелік кібератак, як ми розуміємо, тільки «краплина в морі», і для того, щоб їх уникнути, необхідно бути обережним у цифровому просторі та обов'язково дотримуватись певних правил. То ж познайомимось із цими правилами.

1. Встановлювати антивірус та регулярно оновлювати бази вірусних сигнатур. На кожному пристрої обов'язково має бути антивірус для забезпечення безпечної роботи та безперебійного його використання.

2. Використовувати ліцензійні програми та слідкувати за програмами, які відправляють запити про доступ до геолокації, камери, мікрофона тощо. Необхідно постійно оновлювати програми та операційні системи на всіх гаджетах, тому що розробники в оновленнях виправляють помилки та посилюють захист.

3. Особиста інформація у соцмережах – особиста та персональна. Необхідно максимально скоротити кількість особистих даних у соціальних мережах, через них злочинці можуть багато про вас дізнатися та застосувати їх для здійснення кібератак.

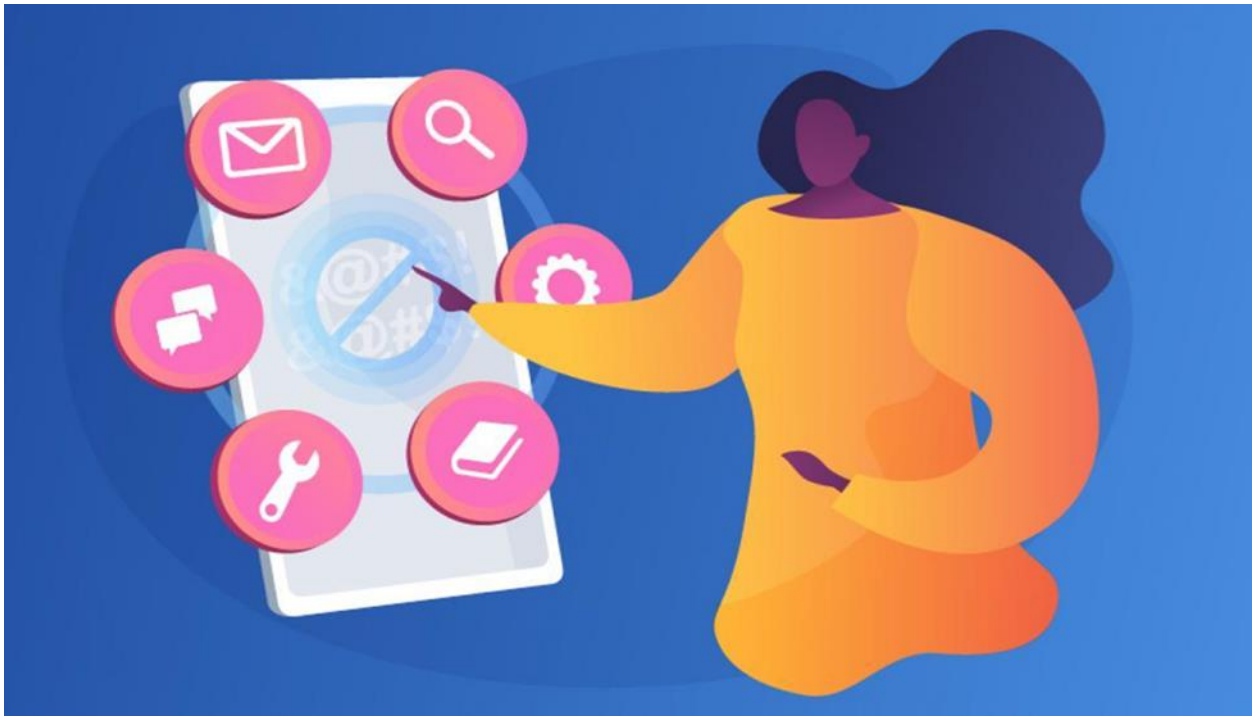
4. Робити резервне копіювання. Для того, щоб попередити втрати важливої інформації можна налаштувати резервне копіювання в хмарні сховища

в щоденний режим і не хвилюватися щодо загубленого телефона або видалення даних з комп’ютера.

5. Робити періодичну відписку від поштових розсилок. Тому що серед зайвих розсилок можна не помітити дійсно важливі повідомлення.

6. Не переходити за підозрілими посиланням в електронних листах – вони можуть бути вірусними або фішинговими. При отриманні такого листа, необхідно бути обережними – не «клікати» на посилання, не надавати особисті дані та не завантажувати файли, що мають невідоме або потенційно небезпечне розширення.

Шахраї у фішингових листах або на сайтах найчастіше запитують таку інформацію: імена користувачів і паролі, зокрема прохання змінити пароль; номери банківських рахунків та кредитних карток; PIN-коди; особисту іншу персональну інформацію користувача тощо.



7. Не зберігати дані банківських карток на сайтах або у браузері. Дуже часто на сайтах налаштоване автоматичне списання коштів.

8. Перевіряти фінансові операції. Бажано раз на рік робити запити про кредитну історію, аби переконатися, чи не відкриті на ваше ім’я чужі позики.

9. Встановити у налаштуваннях банківського додатка двофакторну аутентифікацію. Тоді потрібно буде вводити не лише пароль, а, наприклад, і код з СМС – така додаткова безпека ніколи не завадить.

10. Відключити автоматичний запуск зовнішніх носіїв інформації та забезпечити їх перевірку на наявність шкідливого програмного забезпечення.

Для захисту даних про дітей в інтернет-просторі необхідно:

- чистити цифровий слід месенджерів, соцмереж тощо – пройтися налаштуваннями приватності, зняти або поставити потрібні галочки;
- відписатись від спільнот із загрозливим чи сумнівним контентом;
- стежити за оновленнями безпеки гаджетів;
- перевіряти паролі на складність та пояснити дітям, що розповідати паролі друзям не потрібно;
- встановлювати правила користування пристроями, бажано завести традицію здавати телефони на ніч на підзарядку;
- стежити за поведінкою дитини;
- вчити пильності щодо запобігання загрозам цифрової атаки під час користування не тільки гаджетами, а й банкоматами, кредитними картками тощо.

Кібербулінг – нова форма прояву цькування. І якщо дитина раптово перестала використовувати гаджет – це має бути тривожним сигналом для батьків.

2. Інформаційна гігієна у соціальних мережах

Зазвичай люди проводять у соцмережах дуже багато часу. У середньому ми витрачаємо щодня 3,25 години в інтернеті. Дорослі перевіряють смартфони приблизно 47 разів в день, а молодь – 86 разів на день. Використання смартфонів викликають симптоми, схожі на синдром дефіциту уваги. А у тих, хто постійно чекає на повідомлення, знижується концентрація уваги та зростає рівень тривоги.

Наразі ми маємо великий вибір соцмереж, а також і джерел інформації. Але алгоритми соціальних мереж влаштовані таким чином, щоб захопити увагу користувачів для споживання, як можна більше контенту – таке завдання було поставлене розробникам додатків. Під час знаходження на сайтах працюють наші біологічні механізми – тяга до дофаміну та бажання отримати схвалення. Розробники Інтернет-мережі використовують соціальні медіа, копіюючи методи азартних ігор з метою створення психологічної тяги до перебування якомога більше часу у додатку. При цьому відбувається активація таких самих механізмів мозку, як і при вживанні кокаїну.

Соцмережі негативно впливають на психіку людини – більшість стає нервовими, дратівливими та заздрісними. Використання мережі Facebook протягом 10 хвилин можуть привести до погіршення настрою користувача, внаслідок заздрості або під час зустрічі у стрічці дійсно страшних речей (стосовно війни, катастроф) – до відчуття безвиході.

Під час перебування в інтернеті ми працюємо, відпочиваємо, отримуємо нові знання тощо…і тут наша стрічка перетворюється в нескінченний потік «необхідної інформації», так ми потрапляємо у бульбашку фільтрів. Бульбашка фільтрів (або інформаційна бульбашка) – це негативна сторона персоналізованого пошуку. Коли вебсайти визначають, яку інформацію користувач хотів би побачити, спираючись на його місцеперебування, історію кліків та пошуку. У результаті сайти показують лише ту інформацію, яка збігається з точкою зору та інтересами користувача. Інша інформація, як

правило, не виводиться. Тому бажано звільнитися від влади соціальних мереж над нами та подумати про такі речі:

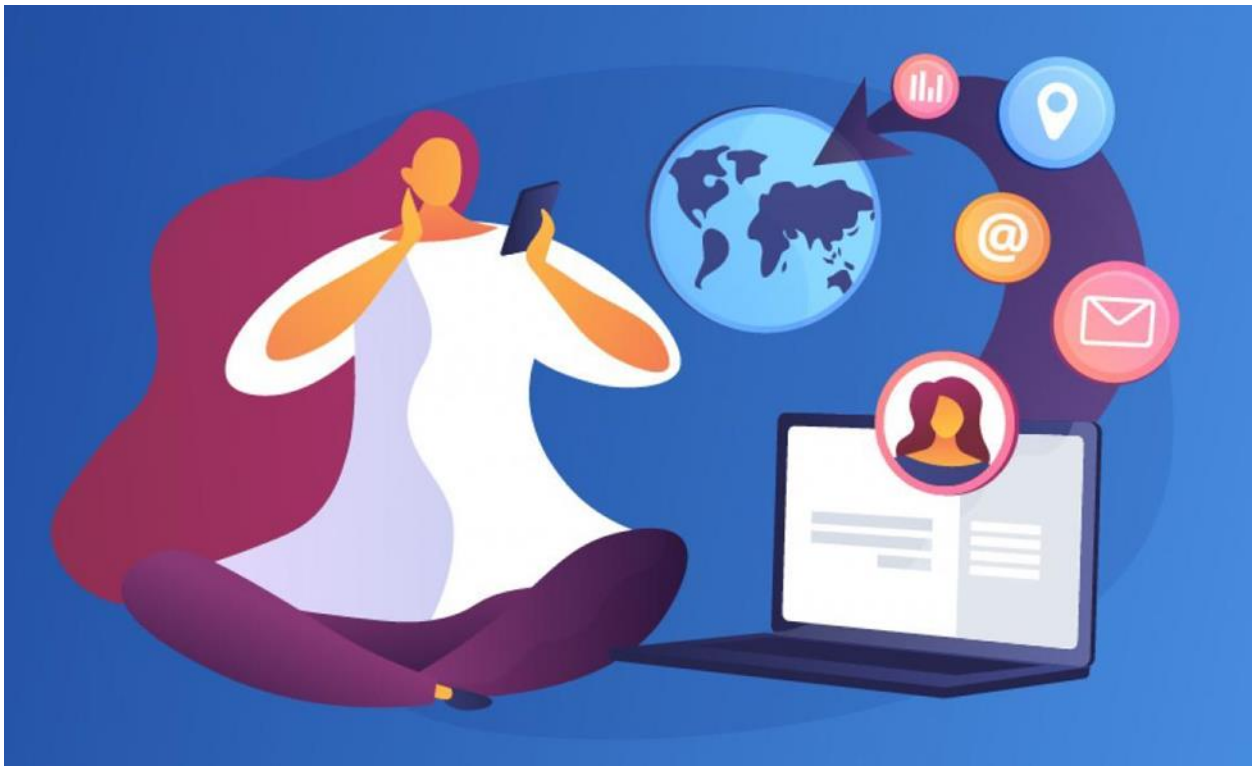
- кількість отриманої інформації, рівноцінно затраченому часу;
- корисність контенту;
- постійний аналіз інформації;
- за не необхідності відписатись від непотрібного контенту.

Зазвичай люди оцінюють новини лише по заголовках, тому фейкові повідомлення поширюються у 6 разів швидше ніж справжні. Більша частина користувачів вважає, що вміє розпізнати брехню з огляду на освіту та життєвий досвід, проте тільки 3% насправді можуть це зробити. Наразі у суспільства збільшується кількість інформації і, як наслідок і дезінформації. Людям важко розпізнати справжню інформацію від фейкової. Тому користувачеві вкрай важливо дотримуватись інформаційної гігієни, а також розвивати критичне мислення та інфомедіаграмотність.

Перелік основних правил інформаційної гігієни:

1. Уникання повторюваної інформації.
2. Зниження інформаційного навантаження.
3. Вивчення різних точок зору на одну проблему.
4. Насторожуватись, коли починаються емоції.
5. Ставити собі питання та шукати, кому вигідно, щоб дізналися новину й повірили в неї.

У сучасному інтернет-середовищі знайти необхідну інформацію дуже просто, і нам здається, що безплатно. Але ми за неї платимо, тільки не грошима, а іншою цифровою валютою – часом, який проводимо на певній платформі, переглядом реклами для подальшого придбання нами товару, а також проводиться аналіз персоналізованого пошуку та збираються емоційні гачки. Якщо ж ці дані збирають платформи, то для захисту користувача їх дуже узагальнюють, а якщо шахраї для подальших маніпуляцій – то це і є найважливішою загрозою, що наразі існує у цифровому просторі.



Також існує ще одна загроза цифрового світу, яка може поширювати дезінформацію – це боти, які працюють так, щоб увімкнути стадний інстинкт. Коли люди бачать допис в якому є велика кількість коментарів та/або вподобайок, мозок буде сприймати таку інформацію, як правдиву.

Найпоширеніший алгоритм загрози інфовірусом у соцмережах:

- мати доступ;
- знати емоційні гачки;
- відповідно до емоційних гачків створити інфовірус;
- запустити;
- користувачі самі поширять.

Додаткові способи збору даних, які наразі розповсюдженні у соцмережах:

- флешмоби, де необхідно скопіювати та вставити якусь інформацію;
- тести, опитування у вигляді ігор;
- фейкові додатки тощо.

Правила безпеки поводження у соцмережах:

- переглядати дописи на наявність ботів у коментарях, якщо є – перевіряти інформацію;

- перед взаємодією із дописом – обов’язково повністю читати;
- проводити аудит, на які сторінки підписаний автор;
- подавати в друзі тільки після перевірки акаунту;
- не додавати у друзі ботів;
- не проходити опитування та тестів у вигляді ігор;
- не брати участь у флешмобах по принципу «скопіюй та встав інформацію».

Вважається, що під час знаходження на платформах соціальних мереж здійснюється і позитивний вплив на людину. Гаджети можуть виконувати безліч позитивних функцій: дарувати емоції, розширювати контакти та знайомства, знаходити інформацію, служити органайзером, допомагати у роботі тощо. А коли самореалізація людини пов’язана із знаходженням у соціальних мережах, то відмова від них може призвести до стресу. Цифрова гігієна полягає у грамотному та вибірковому споживанні інформації, із вибором того, що корисно, а не шкідливо для людини. Тобто при дотриманні так званої «інформаційної дієти», можна із користю проводити час у соціальних мережах та отримувати від них тільки переваги для себе.

Основні аспекти «інформаційної дієти»:

- фокусування – вибирати для роботи конкретний час та фокусуватися на виконанні завдання;
- баланс – балансувати між дефіцитом та перебором інформації;
- відновлення – приділяти собі час для відновлення енергії, а не «зависати» годинами у соцмережах;
- етика – встановити правила, коли і в який час вас непотрібно турбувати у месенджерах тощо, повідомити про це друзів, знайомих;
- вибір – вміти визначати та робити для себе вибір, яка інформація корисна, а яка зайва й непотрібна.

3. Кібергігієна під час дії воєнного стану

У зв'язку із ситуацією, яка склалася в Україні, а саме із повномасштабним вторгненням РФ – є небезпека використання мобільних застосунків, розроблених спецслужбами країни-агресора. Вони використовують їх для отримання інформації про розташування військових об'єктів та критичної інфраструктури. Через такі застосунки ворог схиляє громадян несвідомо допомагати окупантам. Зазвичай мова йде про вимогу здійснити фотофіксацію місцевості, поділитися геолокацією чи нанести «малюнок» на локацію.

Кіберполіція нашої держави пропонує:

- завантажувати додатки з офіційних джерел;
- перевіряти усі доступні дані. Інформацію про розробників, доступи, відгуки користувачів.

А також, наразі дуже почастішали кібератаки країни-агресора з метою збору інформації, один із прикладів наведений нижче.

Кіберфахівці Служби безпеки України нейтралізували російську хакерську атаку на електронні системи житлової інфраструктури в одному із прикордонних регіонів країни. Через Wi-Fi мережу багатоквартирних будинків хакери хотіли дистанційно долучитись до системи відеоспостереження за територією житлових комплексів, прилеглими автомобільними дорогами тощо. Таким чином вони планували мати прихований канал для збору інформації щодо ситуації у місті. Також агресора цікавили відомості щодо адрес проживання українських правоохоронців.

Воєнний стан у своїх корисливих цілях використовують і шахраї. Один із таких випадків наведено нижче.

Шахраї видали себе за благодійну організацію. Вони спочатку сповіщали людям, що доступна виплата грошової допомоги та пропонували авторизуватися через банківський застосунок. Переходячи за посиланням, людина опинялася на фейковому сайті, дуже схожому на сайт-оригінал, далі пропонували вказати номер картки, пароль та пін-код…і як наслідок – грошей на картці не

залишалося. Необхідно пам’ятати, що міжнародні організації ніколи не вимагають паролів, пін-кодів, чи іншої особистої інформації!

І також потрібно пам’ятати, що «Мовчання - надійний тил захисників!»

4. Кібербулінг

Одним із типів кібергігієни є запобігання кібербулінгу. Кібербулінг – це цькування людини із використанням цифрових платформ та сервісів. І являє собою жорстокі неодноразові дії, спрямовані на приниження, залякування та дошкулювання особистості. Тобто являється формою психологічного насильства. Зазвичай він відбувається за участю електронної пошти, соціальних мереж, месенджерів, форумів, чатів, ігрових сервісів, мобільних телефонів та інших гаджетів.

Особисте цькування та кібербулінг часто пов’язані між собою, але відмінністю є: анонімність або підміна особистості, охоплення великої аудиторії одночасно та можливість тримати у напрузі «жертв», коли заманеться.

Типи кібербулінгу:

- флеймінг – обмін короткими гнівними та запальними репліками між учасниками, зазвичай використовуються форуми, чати тощо;
- домагання – часті або регулярні висловлювання образливого характеру на адресу «жертви»;
- наклеп – поширення неправдивої, принизливої інформації;
- самозванство – використання особистих даних жертви (логіни, паролі до акаунтів в мережах, блогах тощо) 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 – онлайн відчуження в будь-яких типах середовищ, де використовується захист паролями, формується список небажаної пошти або список друзів;

- кіберпереслідування – приховане вистежування жертви для скоєння нападу, побиття, зґвалтування тощо;
- 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;
- наявність сторін – булер, потерпілий, спостерігач (за наявності);
- дії або бездіяльність кривдника, наслідком яких є заподіяння психічної та/або фізичної шкоди, приниження, страху, тривоги, підпорядкування потерпілого інтересам кривдника та/або спричинення соціальної ізоляції потерпілого.

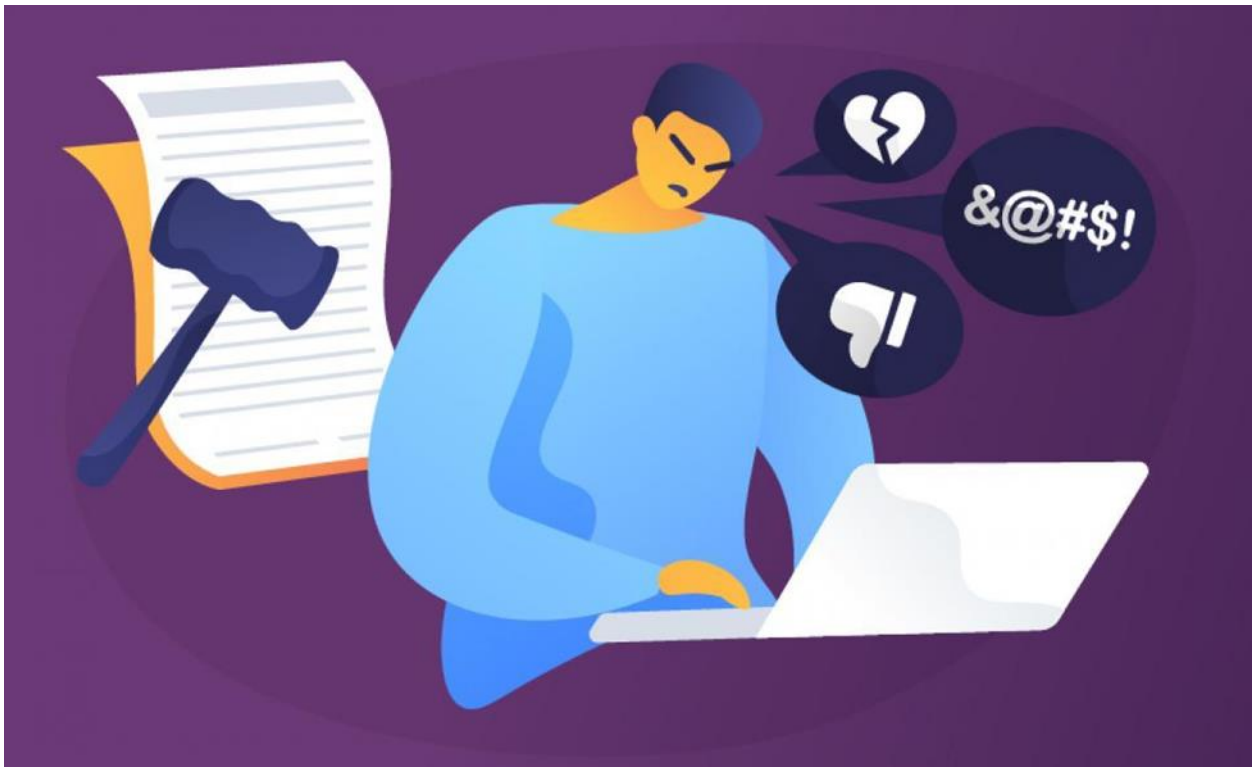
Сторони кібербулінгу та їхні ролі:

- кривдник – особа, яка вчиняє булінг (цькування) щодо іншої людини;
- потерпілий – особа, щодо якої було вчинено булінг (цькування);
- спостерігач(і) – свідки та/або безпосередні очевидці випадку булінгу (цькування).

Наслідки кібербулінгу можуть впливати на людину довгий час і вона може відчувати себе постійно у небезпеці, навіть вдома. Способи впливу булінгу на особистість:

- ментальний – відчуття смутку, пригніченості, злості, відчуття себе в безглуздому становищі;
- емоційний – відчуття сорому, страху, втрата зацікавленостей;

- фізичний – відчуття втоми, втрата сну або таких симптомів, як біль у животі та мігрень. А також, у крайніх випадках кібербулінг може призвести навіть до скоєння самогубства.



Поради протидії кібербулінгу:

1. якщо вам не зручно спілкуватися з кимось, знайомим, необхідно пошукати гарячу лінію у своїй країні, щоб поговорити з професійним консультантом;
2. якщо булінг трапляється на соціальній платформі, необхідно заблокувати цькувальника та офіційно повідомити про його/її поведінку на самій платформі. Соціальні мережі зобов'язані підтримувати безпеку своїх користувачів.

Для того, щоб булінг припинився, його потрібно ідентифікувати і обов'язково повідомити про нього.

У випадку загрози небезпеки, слід звернутися до поліції чи служб швидкої допомоги у країні.

5. Кібербулінг в освіті

Зазвичай від кібербулінгу страждають малолітні діти або підлітки. Перший крок дитини – це звернутися за допомогою до когось, кому вона довіряє, наприклад, до батьків, близького члена сім'ї чи іншого дорослого. Якщо це відбувається у закладі освіти, тоді необхідно обов'язково звернутися до педагогічного працівника або психолога/соціального робітника.

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):

1. 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);
2. за потреби викликає бригаду екстреної (швидкої) медичної допомоги для надання екстреної медичної допомоги;
3. повідомляє службу у справах дітей з метою розв'язання 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;

4. 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;
5. 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).

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 скриншот 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 (безплатно зі стаціонарних та мобільних) та 116 111 (безплатно з мобільних);
- звернутися із заявою або повідомленням про вчинення кібербулінгу до керівника навчального закладу, якщо кібербулінг вчиняється щодо потерпілого у закладі освіти і кривдником є здобувач освіти або член педагогічного колективу;
- якщо кібербулінг відбувається в соціальній мережі (наприклад, Facebook, Telegram, 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»;

- 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;
- 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.

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

Список використаних джерел

1. Закон України «Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню)».
   URL: https://zakon.rada.gov.ua/laws/show/2657-19#Text
   (дата звернення: 16.02.2023).
2. Закон України «Про освіту».
   URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text
   (дата звернення: 16.02.2023).
3. Кібербулінг. Вікіпедія: вебсайт.
   URL: https://uk.wikipedia.org/wiki/Кібербулінг
   (дата звернення: 16.02.2023).
4. Кібербулінг в освітньому середовищі. Вікіпедія: вебсайт.
   URL:https://wiki.legalaid.gov.ua/index.php/Кібербулінг_в_освітньому_середовищі
   (дата звернення: 16.02.2023).
5. Кодекс України про адміністративні правопорушення.
   URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text
   (дата звернення: 16.02.2023).
6. Конвенція про права дитини від 20 листопада 1989 року.
   URL: https://zakon.rada.gov.ua/laws/show/995_021#Text
   (дата звернення: 16.02.2023).
7. Лист Міністерства освіти і науки України від 18 травня 2018 року № 1/11-5480 «Методичні рекомендації щодо запобігання та протидії насильству». Закон онлайн: вебсайт.
   URL: https://zakononline.com.ua/documents/show/439414___439479
   (дата звернення: 16.02.2023).
8. Лист Міністерства освіти і науки України від 08 квітня 2020 року № 1/9-201 «Щодо нагальних питань впровадження Закону України «Про повну загальну середню освіту». Міністерство освіти і науки: вебсайт.
   URL: https://mon.gov.ua/ua/npa/shodo-nagalnih-pitan-vprovadzhennya-zakonu-ukrayini-pro-povnu-zagalnu-serednyu-osvitu
   (дата звернення: 16.02.2023).
9. Порядок реагування на випадки булінгу (цькування), затверджений наказом Міністерством освіти і науки України від 28 грудня 2019 року № 1646.
   URL: https://zakon.rada.gov.ua/laws/show/z0111-20#Text
   (дата звернення: 16.02.2023).

10. Про затвердження плану заходів, спрямованих на запобігання та протидію булінгу в закладах освіти. Міністерство освіти і науки: вебсайт. URL: https://mon.gov.ua/ua/npa/pro-zatverdzhennya-planu-zahodiv-spryamovanih-na-zapobigannya-ta-protidiyu-bulingu-ckuvannyu-v-zakladah-osviti (дата звернення: 16.02.2023).