Комунальний заклад «Кіровоградський обласний інститут післядипломної педагогічної освіти імені Василя Сухомлинського»
Комунальний заклад «Житомирський обласний інститут післядипломної педагогічної освіти» Житомирської обласної ради
Комунальний заклад вищої освіти «Вінницька академія безперервної освіти»
Комунальний заклад «Запорізький обласний інститут післядипломної педагогічної освіти» Запорізької обласної ради
Тернопільський національний педагогічний університет імені Володимира Гнатюка
Центральноукраїнський національний технічний університет
Центральноукраїнський інститут розвитку людини Університету «Україна»
Донецький державний університет внутрішніх справ
Кіровоградський науково-дослідний експертно-криміналістичний центр МВС України
Центр «Адвокат дитини» Вищої школи адвокатури Національної асоціації адвокатів України

III Всеукраїнська науково-практична конференція

«БЕЗПЕКА ДІТЕЙ В ІНТЕРНЕТІ: ПОПЕРЕДЖЕННЯ, ОСВІТА, ВЗАЄМОДІЯ»

05-09 лютого 2024 року

Сайт конференції

Сторінка матеріалів учасників конференції

Відеозапис пленарного засідання конференції

Кропивницький
2024

УДК 004 (06)

Безпека дітей в Інтернеті: попередження, освіта, взаємодія: збірник матеріалів ІІІ Всеукраїнської науково-практичної конференції, м. Кропивницький, 05-09 лютого 2024 року / уклад. С.М. Єфіменко; за заг. ред. Г.В.Скрипки. Кропивницький: КЗ «КОІППО імені Василя Сухомлинського», 2024. 140 с.

Друкується за рішенням вченої ради
комунального *закладу «Кіровоградський обласний інститут післядипломної педагогічної освіти імені Василя Сухомлинського»*
(від 14 лютого 2024 року, протокол №2)

Рецензенти:
Сергій БУРТОВИЙ, кандидат педагогічних наук, заступник директора з науково-дослідної діяльності та міжнародного співробітництва комунального закладу «Кіровоградський обласний інститут післядипломної педагогічної освіти імені Василя Сухомлинського»;
Олександр УЛІЧЕВ – кандидат технічних наук, старший викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

Відповідальний за випуск – Віталій ДМИТРУК

Збірник матеріалів конференції містить основні результати науково-практичних пошуків освітян, правоохоронців, представників громадських організацій та державних органів різних областей України щодо осмислення, виявлення та поширення ефективних практик, які сприяють забезпеченню безпеки дітей в Інтернеті, а також розвитку кіберграмотності педагогічної спільноти.

Матеріали опубліковані в авторській редакції.

ЗМІСТ

СОЦІАЛЬНО-ПЕДАГОГІЧНИЙ ВИМІР ПОНЯТТЯ «ПРАВА ДИТИНИ В ІНТЕРНЕТІ»

ПРАВОПОРУШЕННЯ В ІНТЕРНЕТІ: ВПЛИВ ВІКОВОГО ФАКТОРУ НА ВИЯВЛЕННЯ ТА ФІКСАЦІЮ

Єлизавета ШАЄЦ

У контексті сучасного інформаційного суспільства виникає нагальна необхідність розглядати явище правопорушень в Інтернеті з призми впливу вікового фактору на процеси виявлення та фіксації подібних порушень. Перед нами виникає завдання дослідити взаємозв'язок між віковими особливостями суб'єктів інтернет-комунікацій та ефективністю механізмів виявлення правопорушень, а також удосконалити процедури їх фіксації з урахуванням психологічних та поведінкових відмінностей різних вікових груп. Розгляд цього аспекту є критично важливим для подальшого розвитку ефективних стратегій кібербезпеки та правозахисту в онлайн-середовищі.

Правопорушення в Інтернеті становлять серйозну загрозу як для індивідуальної безпеки, так і для суспільства в цілому. Ці порушення включають різноманітні види злочинності, такі як наркозлочинність, терористична діяльність, інтернет-шахрайство, розповсюдження порнографії, спам, кібербулінг, кібергонки, порушення авторських прав, використання античних програм, атаки на кібербезпеку та конфіденційність даних, ідентифікаційна крадіжка, а також злочини проти дітей в онлайн-середовищі.

Для ефективної боротьби з цими загрозами необхідно проводити науковий аналіз та дослідження їхніх причин, механізмів виявлення та фіксації, а також розробляти ефективні стратегії превентивних дій та захисту. Врахування вікового фактору у цьому контексті є ключовим, оскільки вікові особливості можуть впливати на способи виявлення та реакцію на правопорушення в Інтернеті. Подальший розвиток наукових досліджень у цій області є важливим для забезпечення безпеки та захисту користувачів Інтернету.

Вивчення впливу вікового фактору на процеси виявлення та фіксації правопорушень в Інтернеті також допоможе розробити персоналізовані підходи до кібербезпеки та правозахисту, враховуючи психологічні та поведінкові відмінності різних вікових груп. Це сприятиме підвищенню ефективності заходів захисту в Інтернеті та зменшенню ризиків від цифрових загроз. Такий підхід може стати важливим кроком у забезпеченні безпеки та захисту інтернет-середовища для всіх його користувачів.

Дослідження впливу вікового фактору на процеси виявлення та фіксації правопорушень є необхідним для розуміння та подальшого вдосконалення стратегій кібербезпеки та правозахисту. Вік як основний фактор може впливати на способи сприйняття та реакції на цифрові загрози. Наприклад, молодші користувачі Інтернету можуть мати менше досвіду у розпізнаванні шахрайства або обману в мережі порівняно з дорослими, що може збільшити їхню вразливість перед певними видами кіберзлочинності.

Однак, науковий аналіз виявляє, що велике значення має не лише вік сам по собі, а й пов'язані з ним психологічні та поведінкові особливості. Наприклад, підлітки можуть бути більш схильні до ризикованих онлайн-поведінок через свою вибухливу натуру та бажання експериментувати. З іншого боку, старші люди можуть бути менш технологічно освіченими та відчувати певну неспроможність у розумінні складних кіберзагроз.

Отже, важливо розробляти стратегії кібербезпеки, які враховують ці вікові та психологічні відмінності. Наприклад, освітня програма може бути націленою на різні вікові групи, забезпечуючи їх інформацією та навичками, які відповідають їхнім потребам та рівню розуміння. Також важливо розробляти інструменти та технології, які спрощують виявлення та фіксацію цифрових порушень для різних вікових груп.

Подальші дослідження у цій області допоможуть розробити більш ефективні та персоналізовані стратегії кібербезпеки та правозахисту, що стане кроком до підвищення загальної безпеки в Інтернеті. Розуміння впливу вікового фактору на цифрові загрози дозволить створити більш адаптовані та ефективні заходи захисту для всіх категорій користувачів, зменшуючи загрози для їхньої безпеки та конфіденційності в онлайн-середовищі.

ПРОТИДІЯ ДЕЗІНФОРМАЦІЇ В КОНТЕКСТІ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Інна ВІДІБОРЕНКО

Основна мета інформаційної війни — маніпулювання свідомістю суспільства, прагнення викликати дії противника, що суперечили б його інтересам.

Інформаційна війна росії проти України (ворожі меседжі, наративи) випередила фізичне вторгнення агресора на територію нашої країни. Окупації наших територій танками і російськими військовими передувала окупація мізків українців російськими серіалами на телевізійних екранах, російськими наративами в медіаполі, російською псевдоісторією в книжках і пабліках.

У відеоматеріалі наведено приклади інструментів інформаційної війни росії проти України та охарактеризовано шляхи підвищення рівня критичного мислення й медіаграмотності. Відеоматеріал буде актуальним як підліткам, так і дорослим.

Ключові слова: критичне мислення, медіаграмотність, факт, фейк, офіційні джерела інформації, дезінформація, інформаційна війна, маніпуляція, ворожі меседжі, наративи, Ефект Мандели.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Центр протидії дезінформації : вебсторінка. URL: https://cpd.gov.ua/warnin/fejk-pro-pohovannya-zagyblyh-ukrayinskyh-vijskovyh/.
2. НотаЄнота : вебсторінка. URL: https://www.facebook.com/notaenota1/.
3. По той бік новин : вебсторінка. URL: https://behindthenews.ua/.
4. Вивчай та розрізняй: інфомедійна грамотність : вебсторінка. URL: https://l2d.in.ua/#meta.
5. У кремлі затвердили тематику нового етапу інформаційної війни проти України. Головне управління розвідки МО України // URL: https://t.me/DIUkraine/2746 (дата звернення 06.02.2024 р.).

ІНФОРМАЦІЙНА ГРАМОТНІСТЬ У СОЦІАЛЬНИХ МЕРЕЖАХ ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУЧАСНИХ ДІТЕЙ

Наталія ДУНЯШЕНКО

Інформаційна безпека передбачає належний рівень інформаційної культури, тобто теоретичну і практичну підготовку особистості, що забезпечує захист і реалізацію її життєво важливих інтересів і гармонійний розвиток в умовах інформаційного суспільства, незалежно від наявності інформаційних загроз; здатність держави створити умови для гармонійного розвитку та задоволення інформаційних потреб особи незалежно від наявності інформаційних загроз; забезпечення, розвиток і використання інформаційного середовища в інтересах особи; захист від різноманітних інформаційних загроз [3, с.121].

Досліджуючи тему «Інформаційна безпека дітей в умовах воєнного стану», варто звернути увагу і на поняття інформаційної грамотності людини і суспільства вцілому. Адже дезінформація – це простий та невід'ємний компонент інформаційної війни, яку часто ведуть держави, організації чи приватні компанії. Дезінформацію можна визначити як свідомо подану неправдиву інформацію, яка поширюється, щоб заподіяти шкоду особі, організації або державі. Отже, дезінформація має чітко визначений намір – обслуговувати ті чи інші політичні цілі за допомогою негативного впливу.

Зважаючи на деструктивні наміри поширення дезінформації, з нею слід боротися, спростовувати її. *Спростування – це комунікаційний інструмент, який викриває неправдиву інформацію та наводить правдиві контраргументи.*

«Спростування. Навіщо воно потрібне?» Спростування використовують уже після того, як дезінформація була поширена, тобто це реактивний комунікаційний метод. Основна мета – знешкодження дезінформації через викриття її неправдивості та інформування про реальний стан справ.

«Чи варто спростовувати? Якщо так, то коли?» Зазначимо, що цей інструмент потрібно використовувати лише в окремих випадках, оскільки в сучасному інформаційному просторі дезінформація поширюється швидко та масово. Це, так само, робить неможливим спростування всієї дезінформації, яка існує у світі. Для того, щоб визначити, чи потрібно спростовувати певну дезінформацію, слід спершу оцінити її вплив на цілі певної організації та масштаб її поширення. Якщо дезінформація шкодить політичним та комунікаційним цілям організації, то її слід спростовувати. Ключовим показником необхідності спростування виступає масштаб дезінформації. Якщо дезінформація спорадична та малопоширена, то її не слід спростовувати, щоб уникнути так званого «ефекту зворотного результату». «Ефект зворотного результату» означає явище, коли спростування малопоширеної дезінформації лише сприяє ще більшому її поширенню та закріпленню у свідомості цільової аудиторії як правдивої інформації.

Для того, щоб спростування було ефективним, воно має бути структурованим:

- Факт. Текст повинен починатися з чіткого, простого та зрозумілого факту, щоб визначити стійке уявлення про проблему у потенційного/-ої споживача/-чки інформації?
- Попередження про міф. Потрібно розповісти, яку дезінформацію поширюють зловмисники? Хто? Описати неправдиву інформацію лише раз і доволі коротко.
- Обґрунтування хибності. Навести сильні аргументи, які доводять неправдивість та маніпулятивність поширеної дезінформації.
- Факт. Повторити факт як підсумок.

Під час війни росія масовано ширить дезінформацію. Можемо виділити такі ознаки, за якими можна розпізнати дезінформацію:

- використання готових, беззаперечних тверджень без надання аргументації («українці завжди незадоволені владою»);
- відсутність покликання на будь-яке джерело чи узагальнене покликання/апелювання до авторитетів – авторитетних особистостей чи організацій, вагомих джерел (експерти ООН, британські вчені);
- заклики до очевидного («усім відомо», «абсолютно зрозуміло», «очевидно»);
- конспірологічні версії («ви ніде про це не прочитаєте», «всесвітня змова», «від нас приховують інформацію»);
- «розмитість» трактувань, оцінок («більшою мірою», «по суті», «як правило»);
- шокуючий характер новини, потужна емоційність повідомлення.

Дезінформація сьогодні найбільш активно поширюється через соціальні мережі та месенджери. Кількість вподобайок і поширень не є ознакою правдивості чи актуальності інформації, часто – навпаки, це може свідчити про спеціальну інформаційну чи інформаційно-психологічну операцію ворога з навмисного поширення дезінформації. А велика кількість коментарів під постами може бути навмисно спровокована ботами й тролями.

Тому перед репостами (поширенням) інформації завжди варто перевірити, чи має вона достовірні джерела, чи не містить ознаки дезінформації.

Актуальними правилами поведінки дітей в інформаційному просторі під час воєнного стану можемо назвати такі:

Перевірка інформації: враховуючи підвищений рівень дезінформації під час воєнного стану, діти повинні уважно перевіряти джерела інформації перед її поширенням або використанням.

Дотримання законів та правил: зважаючи на виняткову ситуацію, важливо дотримуватися законів та правил, навіть у віртуальному просторі. Будь-яка дія, що порушує закон, може мати серйозні наслідки.

Виявлення та повідомлення про дезінформацію: діти мають активно виявляти та повідомляти про випадки дезінформації, сприяючи збереженню правдивої інформації та запобіганню паніці.

Обережне обговорення тем: у соціальних мережах та інших платформах діти повинні застерігатися обговорення тем, які можуть бути чутливими або сприяти соціальній напрузі.

Безпека особистої інформації: оскільки інформаційний простір може бути об'єктом кібератак, важливо оберігати особисті дані та уникаюти їх непередбаченого розголошення.

Готовність до екстрених ситуацій: діти повинні мати інформацію про екстрені процедури та контакти для негайного повідомлення про надзвичайні події чи випадки.

Розуміння психологічного впливу: з урахуванням можливого стресу та напруженості важливо розуміти, як інформація впливає на психіку та вміти керувати емоціями.

Сприяння єднанню громади: важливо дотримуватися єдності та підтримувати один одного, а не створювати атмосферу конфліктів чи недовіри.

Ці правила сприяють створенню інформаційного простору, що сприяє безпеці та доброчесності під час воєнного стану.

Отже, важливість інформаційної безпеки для дітей у воєнний час не може бути переоцінена. Під впливом воєнних конфліктів діти можуть опинитися в екстремальних ситуаціях, які вимагають особливого захисту їхньої психологічної та фізичної безпеки. Забезпечення надійної інформаційної ізоляції, перевірка інформації на достовірність та розуміння психологічних аспектів допомагають створити для дітей безпечне і емоційно стабільне середовище. Запровадження ефективних систем інформаційної освіти для дітей та їх батьків у воєнний час є необхідним елементом, спрямованим на підтримку їхнього фізичного та психологічного благополуччя. Взаємодія між громадськістю, урядовими структурами та непереборним бажанням забезпечити безпеку дітей є ключем до успішного забезпечення їхньої інформаційної безпеки в умовах воєнного стану.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року № 47/2017. URL: https://zakon.rada.gov.ua/go/47/2017 (дата звернення: 06.02.2024).

2. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»: Указ Президента України від 19 березня 2022 року № 152/2022. URL: https://zakon.rada.gov.ua/go/152/2022 (дата звернення: 02.02.2024).

3. Смотрич Д.В., Браілко Л. Інформаційна безпека в умовах воєнного стану. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/284104/278250 (дата звернення: 01.02.2024).

БЕЗПЕКА НЕПОВНОЛІТНІХ ІНТЕРНЕТ-КОРИСТУВАЧІВ В УМОВАХ ВОЄННОГО СТАНУ

Світлана ЄФІМЕНКО

В умовах воєнного стану Всесвітня мережа збагатилась низкою потенційних небезпек, спрямованих на неповнолітнього інтернет-користувача. А саме: фейковою інформацією, небезпечним контентом, небезпечною взаємодією онлайн з російськими військовими.

Фейкова інформація – неповна, спотворена чи неправдива інформація, створена з метою поширення паніки, дезорієнтації, зниження здатності критично оцінювати ситуацію, формування певних думок та рішень, вигідних маніпулятору. В умовах воєнного стану така інформація слугує ефективною зброєю на інформаційному фронті. Прикладами фейкової інформації можуть бути оголошення про швидкий заробіток чи отримання допомоги, прохання про допомогу військовим чи потерпілим, попередження про обстріли, новини про ситуацію в країні тощо.

Аби не стати жертвою фейку, варто завжди критично сприймати будь-яку інформацію, створену й поширену в текстовому, графічному, аудіо- чи відеоформатах, а також перевіряти інформацію за допомогою різноманітних інструментів фактчекінгу (Google Image Search, Youtube DataViewer тощо) чи фактчек-боту «Перевірка» (@perevir_bot в Телеграм).

Небезпечний контент – змістове наповнення вебсторінок, що може становити загрозу психічному, фізичному, соціальному чи матеріальному благополуччю інтернет-користувача. Прикладами такого контенту в умовах воєнного стану є: інструкції з виготовлення саморобної вибухівки, лайфхаки щодо виготовлення саморобних обігрівачів, сцени насилля/каліцтва/вбивства, зображення руйнувань тощо.

Шляхи захисту неповнолітніх від небезпечного контенту:

✓ Встановити «батьківський контроль» на облікових записах та пристроях неповнолітнього Інтернет-користувача:

- Google Family Link для пристроїв Android та Iphone,
- «Параметри»/«Екранний час»/«Контент і приватність» для пристроїв IPhone та IPad,
- «Сімейний доступ» для MacBook, IPhone та IPad,
- Microsoft Family Safety для комп’ютерів з ОС Windows 10,
- «Керування профілями» для Netflix,
- «Батьківський контроль» для Megogo,
- «Сімейний та батьківський контроль» (Family and Parental) для PlayStation,
- «Конфіденційність і безпека в інтернеті» (Privacy & online safety) для Xbox,
- «Сімейний зв'язок» в налаштуваннях профіля неповнолітнього в TikTok,

- налаштування з обмеженням контенту для WiFi-мережі тощо;

✓ Використовувати різні облікові записи на Smart TV для кожного члена родини.

✓ Використовувати безпечні пошуковики (YouTube Kids, Safe Search Kids тощо).

✓ Встановити блокувальники реклами (наприклад, AdBlock) в браузері.

✓ Налаштувати стрічку новин/відео соціальних мереж та відеохостингу YouTube в профілі неповнолітнього.

✓ Використовувати застосунки, групи, спільноти, канали, соц.мережі, відповідні віку.

✓ Не відкривати файли із позначками 18+/«можуть містити сцени насильства»/«неприйнятний контент».

✓ Розвивати й активізувати критичне мислення неповнолітнього, його вміння аналізувати інформацію, передбачати наслідки дій (участь в челенджах, використання лайфхаків і відеоінструкцій), цінувати життя й здоров'я.

Небезпечна взаємодія онлайн з російськими військовими може відбуватись у форматі відеозустрічі, обміну текстовими чи аудіоповідомленнями в соціальних мережах чи меседжерах. Це можуть бути як приватні повідомлення, так і чати груп, спільнот, каналів. Змістом такої взаємодії може бути виманювання конфіденційної інформації про близьких військових неповнолітнього, інформації військового значення (ситуація в населеному пункті, геолокація об'єктів стратегічного значення, переміщення й розміщення позицій українських військових тощо), залучення неповнолітнього до виконання спеціальних (таємних) завдань чи доручень, рис. 1.

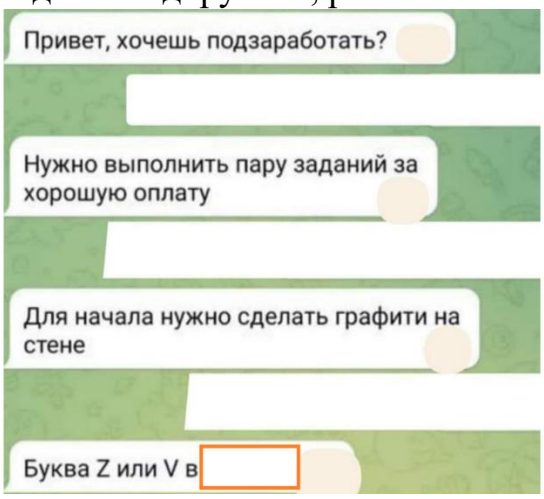

Рис. 1. Приклад взаємодії неповнолітніх онлайн з російськими військовими [2]

Приватні повідомлення неповнолітнім можуть надсилати з фейкового облікового запису від імені підлітка, який нібито нещодавно переїхав до населеного пункту і хотів би знайти в ньому нових друзів чи просто довідатись про ситуацію в цьому населеному пункті (наприклад, чи є поряд з новим місцем його проживання стратегічні об'єкти). У приватній переписці інформацію військового значення можуть виманювати зі зламаного акаунта знайомого, родича-військового тощо. Шляхом примусу, залякування, шантажування чи «легкого» заробітку неповнолітньому можуть пропонувати виконати спеціальне

доручення. Також хлопчиків чи дівчаток можуть додавати до чатів месенджерів, де надсилаються спеціальні пропозиції (за умови, якщо в обліковому записі неповнолітнього відсутні налаштування приватності і його номер телефону, аватарку може бачити будь-хто й додавати його до спільнот може будь-хто).

З різних причин неповнолітні вступають у небезпечну взаємодію онлайн з російськими військовими й долучаються до виконання спеціальних доручень: страх, бажання отримати легкий заробіток, гра («А що буде, якщо я саме так відповім?»), зацікавленість у виконанні таких завдань внаслідок відсутності патріотичних почуттів та впевненість в уникненні покарання. Наслідком такої взаємодії може бути скоєння злочину, за який неповнолітній нестиме покарання. Так, відповідно до Кримінального кодексу України [1], кримінальними правопорушеннями, відповідальність за які наступає з 14-річного віку, є: диверсія (ст. 113 КК), терористичний акт (ст. 258 КК), хуліганство (ст. 296 КК). Кримінальні правопорушення, відповідальність за які наступає з 16-річного віку: колабораційна діяльність (ст. 111^1 КК), пособництво державі-агресору (ст.111^2 КК); несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення ЗСУ чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану (ст. 114^2 КК). До того ж за ст. 114^2 КК передбачено кримінальну відповідальність за розповсюдження інформації про переміщення, розташування та рух ЗСУ, якщо ця інформація не була опублікована у відкритому доступі. Це може бути стрім, селфі, сторіс, відео, які містять таку інформацію. Таким чином, неповнолітній інтернет-користувач може допомогти російським військовим, навіть, ненароком (наприклад, знявши для TikTok відео про переміщення української військової техніки) і понести за це кримінальну відповідальність.

Як неповнолітньому захистити себе від небезпечної взаємодії онлайн з російськими військовими:

- встановити двофакторну аутентифікацію в обліковому записі Google, Facebook, Instagram, TikTok, Telegram, Viber, щоб захистити свій профіль від зламу;
- налаштувати приватності профіля в соцмережі/месенджері, щоб лише контакти могли додавати в чати й надсилати повідомлення;
- вимкнути геолокацію (функцію «поділитися розташуванням») у соцмережах/месенджерах, налаштуваннях застосунків та ігор;
- за жодних умов не повідомляти і не поширювати приватну інформацію (особистий номер телефону чи номер батьків, місце навчання й проживання, місце роботи батьків тощо), інформацію про ситуацію в населеному пункті, про родичів-військових, про військові об’єкти чи розміщення військової техніки, навіть якщо це онлайн-друг, якого неповнолітній знає в реальному житті (слід пам’ятати, що наразі особисті профілі зламують для отримання інформації або створюють фейкові профілі);
- у випадку надходження пропозиції виконати спеціальне таємне доручення чи надати інформацію військового значення, заблокувати користувача-адресанта або вийти з таємного чату, до якого було долучено

неповнолітнього інтернет-користувача, заблокувати чат та, зробивши скриншот переписки, звернутись разом з дорослим до кіберполіції (https://ticket.cyberpolice.gov.ua/, 0 800 50 51 70);

- не реагувати на заклики про допомогу від незнайомих акаунтів;
- не переходити за посиланнями від незнайомців та не сканувати QR-коди на дошках оголошень;
- не розміщувати у своїх акаунтах анонс чи пряму трансляцію події, в якій предбачено скупчення великої кількості людей (зокрема, захід в закладі освіти);
- не розповсюджувати відео з напрямками польотів ракет;
- не публікувати фото/відео, де можуть бути дорожні знаки, вказівники, таблички з назвами вулиць, музеїв, парків, шкіл, приватних підприємств, станціями метро, автобусними, тролейбусними та трамвайними зупинками, вивіски магазинів, супермаркетів, номерами приватних садиб та автомобілів;
- не поширювати фото/відео з українськими військовими, особливо зі знаками їх відмінності: шевронами, пагонами, пов'язками на руці, знаками на техніці чи будь-якими іншими засобами ідентифікації (зокрема, власні селфі/фото/відео, в кадр яких потрапляють військові ЗСУ чи об'єкти стратегічного значення);
- не вказувати точні координати та геолокацію місць, де відбуваються бойові дії та не демонструвати роботу українських військових (ППО, артилерії, авіації);
- не стрімити в місцях прильоту ракет, ворожих обстрілів, поблизу військових баз та об'єктів стратегічного значення та не уточнювати інформацію щодо цих місць у коментарях/чатах/обговореннях соціальних мережах чи месенджерів;
- не публікувати матеріали аудіо/відео формату з пересуванням військової техніки Збройних Сил України з місцями їх дислокації, ночівлі та укриттями;
- уникати репостів та згадок про публічних персон (блогерів, громадських діячів, політиків, військових) на гарячих точках чи військових пунктах;
- не поширювати інформацію, яка не опублікована та не підтверджена офіційними джерелами (Президент, представники уряду, СБУ, ГУР, ДБР, ЗСУ, ДСНС та інші).

Отже, безпеку неповнолітніх інтернет-користувачів в умовах воєнного стану слід розглядати з двох позицій. З одного боку, неповнолітній інтернет-користувач може потрапити в пастку тієї чи іншої інтернет-загрози, а з іншого боку – може сам становити загрозу для інших своїми необачними чи навмисними діями у Всемережжі. Критичне мислення й дотримання правил безпечного використання інтернет-мережі в умовах воєнного стану сприятиме зведенню нанівець потенційних негативних наслідків.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кримінальний кодекс України : Закон України № 2341-III від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 10.01.2024 р.).

2. Одеситам почали пропонувати «підзаробіток»: малювати графіті у вигляді символів армії РФ. НОВИНИ N: вебсайт. https://novosti-n.org/news/Odessytam-nachaly-predlagat-podrabotku-rysovat-graffyty-v-vyde-symvolov-armyy-RF-237618 (дата звернення 23.01.2023 р.)

3. Онлайн-злочини за участю дітей під час війни : посібник. 2022 р. 12 с. URL : https://stop-sexting.in.ua/wp-content/uploads/2022/05/broshura-nasylstvo-v-interneti.pdf.

4. Посібник для батьків: батьківські контролі для захисту дитини від онлайн ризиків. 2023 р. 49 с. URL : https://stop-sexting.in.ua/adult/wp-content/uploads/2023/11/Posibnyk-dlia-batkiv-kontroli.pdf.

5. Російські окупанти використовують неповнолітніх українських дітей для розвідок військових позицій. Служба безпеки України : youtube-канал. URL : https://youtu.be/lO6Siwgco-o?si=1TabGn7MnUt0i78W.

6. Філоненко В., Касілова А., Дьякова А. Онлайн-загрози в час війни: як захистити себе? Урок для 9-11 класів щодо безпечної поведінки у час війни. 2023р. 23 с. URL : https://stop-sexting.in.ua/.

СУЧАСНІ МЕТОДИ ВИЯВЛЕННЯ ФЕЙКІВ У СОЦІАЛЬНИХ МЕРЕЖАХ

Марина КУЧЕРЕНКО

В умовах воєнного стану поняття інформаційної безпеки як ніколи актуальне, а особливе значення це має для дітей, які не завжди можуть на достатньому рівні володіти ситуацією, що склалася в мережі та відреагувати на неї належним чином. Завдання батьків та школи – попередити можливі ризики, які можуть виникнути в таких ситуаціях.

Фейк – це подання фактів у спотвореному вигляді або подання свідомо неправдивої інформації. До того ж фейк – це спосіб маніпуляції свідомістю шляхом надання неповної інформації, спотворення контексту, частини інформації з метою підштовхнути аудиторію до дій чи думок, які потрібні маніпулятору [3]. В умовах воєнного стану сторона-агресор часто поширює неправдиву інформацію, маніпулює ситуаціями перекручуючи їх у зручний для себе формат [5]. Діти схильні сприймати усю інформацію, що є в Інтернеті, особливо в соціальних мережах, де вони проводять більшу частину свого часу, сліпо довіряючи та не аналізуючи отриману інформацію, що може привести до інколи фатальних наслідків. То як же розпізнати фейк та, перш за все, навчити дитину визначати недостовірну інформацію?

Визначимо основні ознаки, які можуть вказувати на фейк:

- джерело інформації відсутнє або хибне;
- посилання на анонімне, невідоме джерело інформації;
- інформацію взято з акаунта, який є підозрілим, щойно створеним, з відсутньою інформацією про власника;
- думка чи оцінка подається як факт;

- заголовок не відповідає наданій інформаціє або ж є занадто емоційним;
- в матеріалі переважають емоції;
- наявні поширені стереотипи в тексті;
- однобоке подання фактів;
- викривлене подання новин, коли реальна інформація вправно переплітається з вигаданою;
- недостовірні фото та відео;
- анонімні або підозрілі «експерти» [4].

Список можна продовжувати, адже варто врахувати дуже багато факторів, які впливають на достовірність інформації. Як же полегшити виявлення фейкової інформації? Для цього існує низка методів:

1. Перевірка на наявність слів та фраз, які виражають лише припущення автора.
2. Ознайомлення з профілем. Відсутність повних особистих даних, мало друзів або їх відсутність, доступ до сторінки обмежений, мало вподобайок та коментарів, акаунт створено нещодавно – перед появою підозрілої інформації.
3. Перевірка зображень за допомогою Google Image Search (рисунок 1), TinEye тощо. Ці інструменти дозволяють порівняти знайдені зображення, вказують дату їх появи в Інтернеті [2].

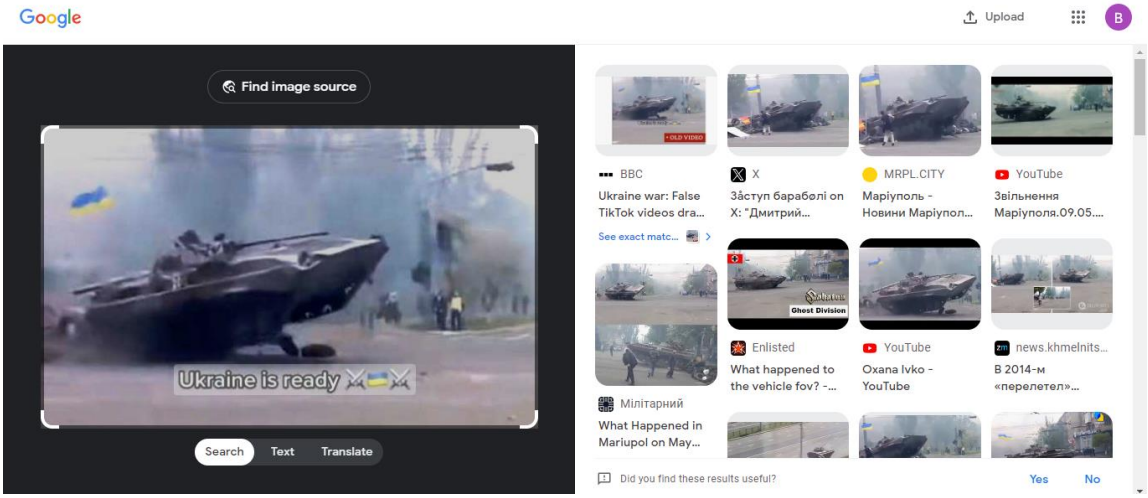

Рис. 1. Перевірка фейкового фото у Google Image Search

4. Перевірка інформації через фактчек-бот "Перевірка", який допомагає швидко розпізнати фейкові новини. Зокрема за допомогою нового фактчек-боту можна розрізнити фейкові новини в соцмережах, у політиці, визначити фейкові новини російських засобів масової інформації, спрямовані на боротьбу з Україною. Щоб розпізнати фейк, необхідно надіслати боту інформацію, яку потрібно перевірити на справжність. Крім того, за допомогою чат-боту можна проходити тести та навчатися виявляти фейки самостійно (рисунок 2).

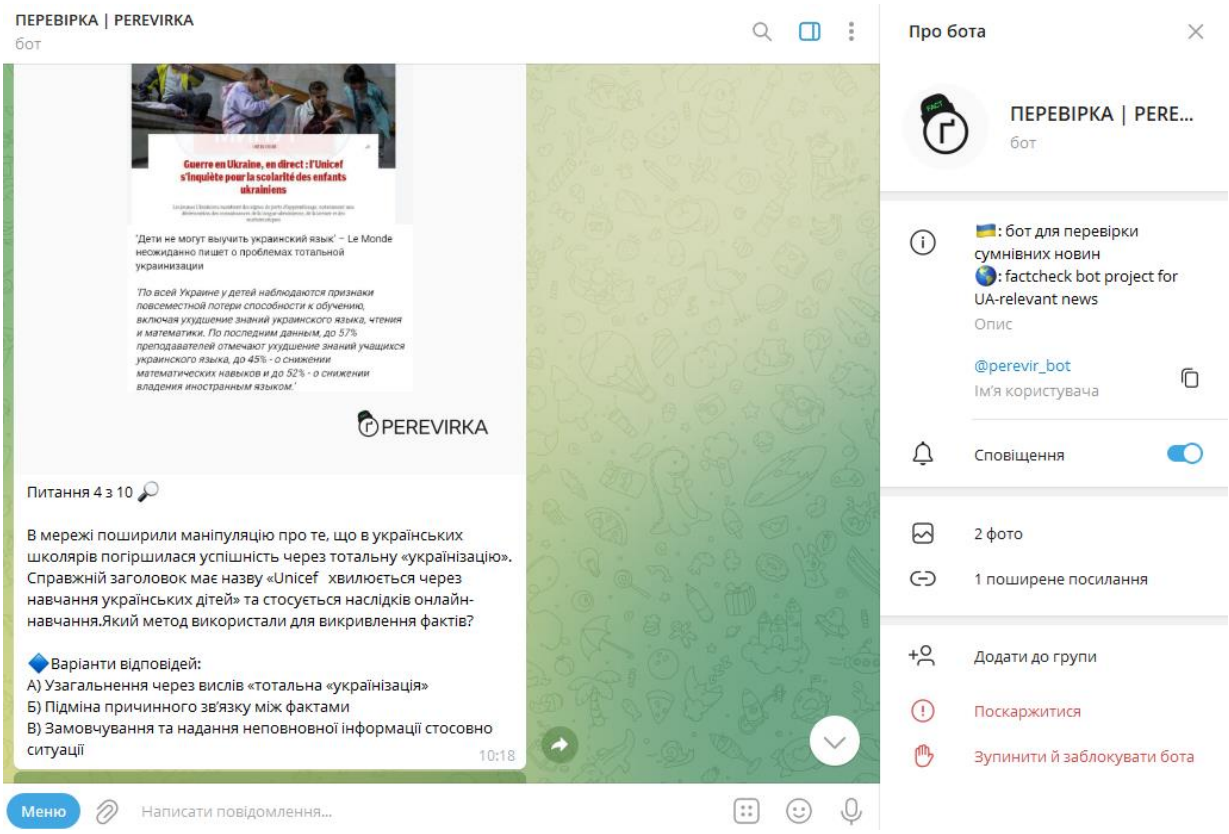

Рис. 2. Тестування у фактчек-боті «Перевірка»

5. Робота з сайтами за допомогою інструментів: Archive.is (створення посилання на архів вебсторінки в разі її видалення), SimilarWeb (аналіз трафіку), WaybackMachine (пошук архівних версій сторінок).

6. Пошук у соцмережах: Yomapic (пошук фото за заданою геолокацією у соціальних мережах), аналіз цифрового коду фото, який генерує Facebook для зображення та використання розширеного пошуку Facebook.

7. Перевірка відео через інструмент Youtube DataViewer, який показує точну дату й час завантаження відео (рисунок 3) [1].

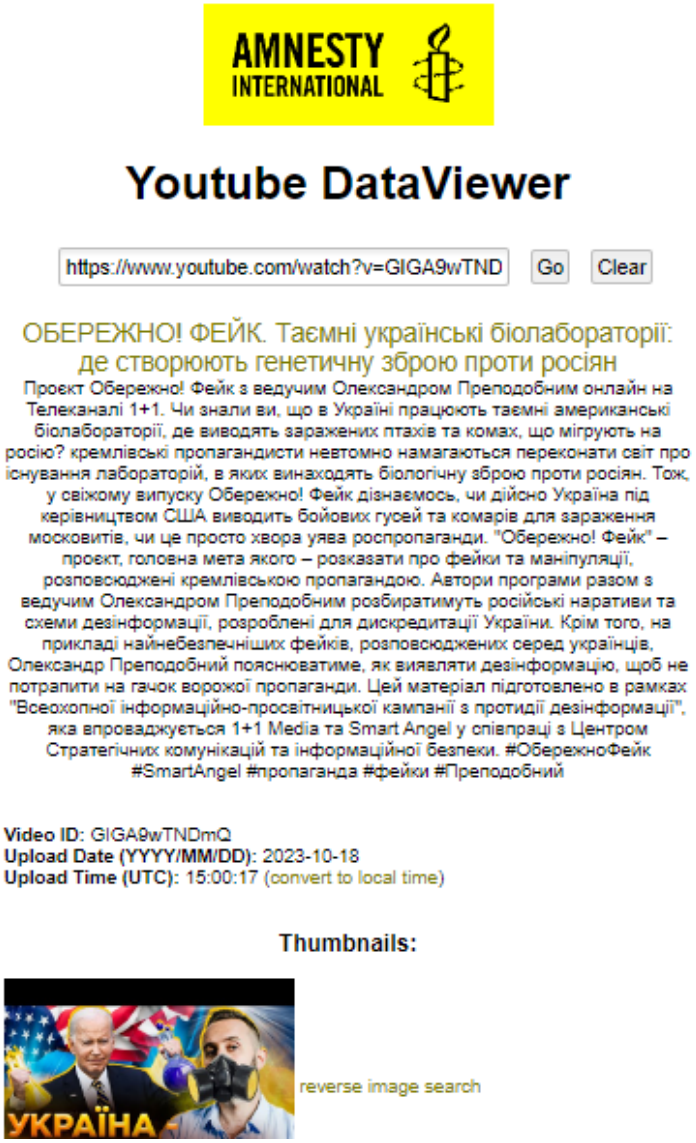

Рис. 3. Перевірка посилання на відео у Youtube DataViewer

Ці та інші інструменти дають змогу якнайточніше перевірити природу інформаційного ресурсу та виявити, чи дійсно інформація є фейковою.

Висновки. Інформаційна безпека дітей – це те, що має постійно контролюватися як батьками, суспільством, так і з боку школи. Щоб попередити ризики, які можуть виникнути в результаті впливу фейкової інформації, фейкових сторінок та акаунтів на дитину варто об’єднати вплив освіти, соціуму та батьків на дитину. На мою думку, варто дотримуватись наступних правил:

1. Проводити бесіди з учнями про фейки, фейкову інформацію, про шкоду, яку завдає недостовірна інформація.
2. Ознайомлювати та навчати учнів працювати з різними інструментами для виявлення та розпізнавання фейків.
3. Постійно ознайомлювати учнів з найпопулярнішими фейками та ґрунтовно спростовувати їх.
4. Синхронізувати роботу психолога, батьків та класного керівника.

5. Проводити опитування серед здобувачів освіти щодо їх емоційного стану та тривог, які вони мають, спілкуючись у соціальних мережах.

Лише комплексна робота може стати запорукою збереження емоційного та психологічного здоров'я дитини в умовах воєнного стану, а інколи це навіть може врятувати життя і не одне.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 12 інструментів, які допоможуть викрити фейк. ГО «Детектор медіа» : вебсайт. URL: https://ms.detector.media/how-to/post/16830/2016-06-21-12-instrumentiv-yaki-dopomozhut-vykryty-feyk/ (дата звернення 03.01.2024).

2. Дем'яненко Л. Особливості протидії недостовірній (фейковій) інформації в соціальних мережах. *Наукові праці Національної бібліотеки України імені В. І. Вернадського.* 2020. Вип. 58. С. 277-289. URL: http://nbuv.gov.ua/UJRN/npnbuimviv_2020_58_23.

3. Фейк. Кіровоградська обласна бібліотека для дітей ім. Т.Г.Шевченка: вебсайт. URL: http://librarychl.kr.ua/kn_in/informatoria/inf-f.php (дата звернення: 03.01.2024).

4. Фейки: Інструкція з перевірки фейків. Медіадрайвер : вебсайт. URL: http://mediadriver.online/fejki/instruktsiya-z-perevirki-fejkiv/ (дата звернення: 03.01.2024).

5. Як визначити та зловити фейк? Інститут масової інформації : вебсайт. URL: https://imi.org.ua/advices/yak-vyznachyty-ta-zlovyty-fejk-i2388 (дата звернення 03.01.2024)

ВПЛИВ МЕДІА ТА ІНТЕРНЕТУ НА ФОРМУВАННЯ Й ПОШИРЕННЯ СУЧАСНИХ МОЛОДІЖНИХ АГРЕСИВНИХ СУБКУЛЬТУР

ОЛЬГА ЛУНГОЛ, БОГДАН ПОЗІГУН

Вплив медіа та Інтернету на формування й поширення молодіжних агресивних субкультур є складним та актуальним явищем в сучасних умовах, в яких перебуває наша країна. Молодь, активно використовуючи медіа та Інтернет, є схильною до впливу відповідної інформації. Засоби масової інформації часто пропагують агресивні образи, що впливає на естетичні уподобання та уявлення молодого покоління. Молодь, в пошуках спільнот та вираження ідентичності у віртуальних просторах, може потрапляти на агресивні субкультури, які пропагують насильство як засіб вираження. Відомо, що деякі відеоігри також пропагують насильство, формуючи агресивне сприйняття світу та вчинків. Вплив медіа та Інтернету може відігравати роль у формуванні психологічних стереотипів та сприяти прийняттю агресивного способу вираження емоцій.

Серед робіт сучасних науковців, у яких розглядається питання розвитку та особливостей сучасних молодіжних агресивних субкультур, ми виділяємо дослідження Сокуренко В. [1], Гірняк А. [2], Гірняк Г. [2], Сіткар І. [3], Сіткар С. [3], Макаренко Н. [4] та ін. Через актуальність та складність питання формування

й поширення сучасних молодіжних агресивних субкультур й задля забезпечення безпеки дітей в умовах воєнного стану, фахівці Міністерства освіти і науки України проводять відповідні наради на всеукраїнському рівні. У нараді 08.03.2023 взяли участь понад 800 спеціалістів департаментів з питань позашкільної освіти та виховної роботи, фахівців інститутів післядипломної педагогічної освіти, керівників закладів позашкільної освіти та представники громадськості з усіх регіонів України. Учасники акцентували увагу на важливості посилення національно-патріотичного виховання, культурі взаємостосунків здобувачів освіти, доведення методів ненасильницького спілкування тощо.

Для формування та поширення агресивних субкультур активно використовуються різні техніки та методики соціальної інженерії. Соціальна інженерія являє собою метод впливу на людей з метою викликати певні реакції чи дії, використовуючи психологічні, соціальні та технічні засоби. Цей термін вживається для опису широкого спектру технік та прийомів, що можуть включати маніпуляцію емоціями, обман, використання соціального інформаційного інженерінгу або технічних засобів для отримання персональної інформації. У плані формування та поширення агресивних субкультур можуть бути використані наступні методики соціальної інженерії:

1. Маніпуляція медіа, що включає спрямовану роботу над виробленням агресивного сенсу життя та цінностей через масові медіа, платформи Інтернет та соціальні мережі.
2. Соціальна ізоляція через застосування технік, спрямованих на відокремлення молоді від позитивних соціальних взаємодій та стимулювання їх участі в агресивних групах.
3. Експлуатація соціальних конфліктів через залучення молоді до груп, що підтримують агресивний світогляд, через активне використання соціальних конфліктів та непорозумінь.
4. Використання психологічного тиску через застосування методів, що викликають психологічний тиск та стрес, щоб змусити молодь вступати в агресивні субкультури.
5. Рекрутинг через Інтернет за допомогою онлайн-ресурсів для залучення молоді до агресивних груп та субкультур.

Важливо відзначити, що такі практики є негативними і призводять до серйозних соціальних проблем, включаючи насильство, конфлікти та психологічні проблеми. У розвитку сучасної молоді повинен бути акцент на позитивних цінностях, толерантності та сприянню гармонійному розвитку особистості.

Отже, важливо розуміти, що віртуальний світ та медіа мають значний вплив на формування молодіжних агресивних субкультур. Суспільство та освітні інституції повинні працювати над розвитком медіаграмотності та підтримувати конструктивні форми вияву енергії та самовираження молодого покоління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Сокуренко В. В. «Редан» як новий агресивний напрям молодіжної субкультури. *Психологічні та педагогічні проблеми професійної освіти та*

патріотичного виховання персоналу системи МВС України: матеріали Всеукр. наук.-практ. конф. (м. Вінниця, 24 берез. 2023 р.). Вінниця: ХНУВС, 2023. С. 182-184.

2. Гірняк А., Гірняк Г. Формовияви девіантної поведінки у сучасних молодіжних субкультурах та їх соціально-психологічний аналіз. *Психологія і суспільство.* 2023, (1). С. 199-204.

3. Сіткар В. І., Сіткар С. В. «Редан»-спланована інформаційно-психологічна спецоперація проти України чи ідентичність молоді з культурним аніме світу? 2023 : Репозитарій Тернопільського національного педагогічного університету імені Володимира Гнатюка. URL: http://dspace.tnpu.edu.ua/bitstream/123456789/30150/1/117_Sitkar_Sitkar.pdf.

4. Макаренко Н. (2023). Кримінальна субкультура як об'єкт кримінологічного дослідження. *Вісник Кримінологічної асоціації України*, 28 (1). С. 99–107.

СОЦМЕРЕЖІ ТА ВІЙНА: ЯК УБЕРЕГТИ ДІТЕЙ ВІД НЕБЕЗПЕКИ

Любов СЕВЕРИНА

Повномасштабна війна в Україні, розв'язана російськими окупантами, кардинально змінила життя українських дітей. Безтурботне дитинство обірвалося для мільйонів наших найменших співгромадян. Вимушене переселення, евакуація, постійні сирени повітряної тривоги та укриття в бомбосховищах – усе це страшні реалії сьогодення. Єдиним вікном у звичайний мирний світ для багатьох дітей стали соціальні мережі та інтернет.

Інтернет-технології давно стали невід'ємною частиною життя сучасного суспільства. Діти, особливо підлітки, проводять багато часу в соціальних мережах та інтернеті. Для них це основний спосіб спілкування з друзями, пошуку розваги та інформації. Під час пандемії COVID-19 соцмережі стали ще більш важливими для дітей, оскільки школи були закриті, а спілкування обмежене. Це був один із важливих способів підтримки соціальних зв'язків. В умовах воєнного стану час, який проводять діти в соціальних мережах, лише збільшився. Проте соціальні мережі приховують чимало небезпек, про які мають пам'ятати як самі діти, так і їхні батьки. Поточні виклики вимагають від усіх великої уваги до того, яку інформацію публікуємо, що читаємо та які дані надаємо в інтернеті.

Соціальні мережі – один із найбільш відвідуваних ресурсів у глобальній мережі Інтернет. За результатами дослідження, проведеного громадянською мережею «Опора», найпопулярнішим джерелом інформації для українців у 2023 році залишаються соціальні мережі – їх для отримання новин обирають 77,9% опитаних (2022 року цей показник був співмірним – 76,6%, а до повномасштабного вторгнення – на рівні 63%). Найбільше соцмережами для отримання новин очікувано користується молодь (95,8%). Соцмережі стали не тільки каналом для отримання новин з різних джерел, але й простором для

активного обговорення та поширення інформації, роблячи своїх користувачів учасниками складного інформаційного процесу [1, с.51].

Доволі велика популярність соціальних мереж породжує важливе завдання – захист дітей від загроз, пов'язаних із неусвідомленими інформаційними впливами, формуванням штучної психічної залежності; маніпулюванням свідомістю з використанням спеціальних засобів впливу, що виконують чужу волю. За оцінками фахівців з інформаційних технологій, ефективність від використання соціальних мереж для впливу на підсвідомість суспільства в десятки разів вища, ніж від стандартних засобів психологічного впливу. Важливо розуміти, що під час війни ризики для дітей в інтернеті значно зростають і саме в соціальних мережах приховується чимало загроз [2, с.51].

Однією з головних небезпек для користувачів соціальних мереж є інтернет-шахраї, які намагаються заволодіти, зокрема, їхніми персональними даними. В умовах війни зросла кількість фейкових повідомлень від імені волонтерів чи благодійних організацій. Довірливі діти можуть надати доступ до своїх сторінок або клацнути на фейкове повідомлення, в результаті чого постраждають їхні акаунти та персональні дані.

В умовах воєнного стану в соцмережах збільшується кількість шкідливого для дітей контенту, пов'язаного з війною – жорстокі зображення, сцени насильства, емоційно травмуючі історії людей, які постраждали від війни, відео бойових дій. Це може шокувати дитину, травмувати її психіку та спотворювати уявлення про реальність.

Небезпечним є і вплив пропаганди та фейків про війну, які легко поширюються соцмережами. У соцмережах відбувається активізація ботів та тролів, які маніпулюють інформацією та свідомістю користувачів. Діти особливо вразливі до впливу пропаганди.

Соціальні мережі є привабливим інструментом для поширення дезінформації, пропаганди та маніпуляції громадською (у тому числі дитячою) свідомістю завдяки таким факторам:

− широке охоплення аудиторії (соціальні мережі використовують мільярди людей по всьому світу, що дозволяє швидко та ефективно поширювати інформацію);

− анонімність (у соціальних мережах користувачі часто можуть залишатися анонімними, що ускладнює відстеження джерела дезінформації або пропаганди);

− емоційний вплив (соціальні мережі використовують емоції для залучення користувачів, що може зробити їх більш сприйнятливими до дезінформації або пропаганди).

Ще одна серйозна загроза, про яку не варто забувати, це кібербулінг – цькування дітей в інтернеті з боку однолітків. В умовах воєнного конфлікту кібербулінг може бути ще більш небезпечним, оскільки може посилити стрес та тривогу дитини.

Також є ризик небезпечного спілкування дітей в соцмережах з незнайомцями. Інтернет надає можливість приховати свою ідентичність та вести велику кількість вигаданих облікових записів. Тому деякі особи можуть піддавати дітей негативному впливу, роблячи їх вразливими перед ризиком

втрати конфіденційної інформації, фізичної безпеки чи стикання з небажаними ситуаціями.

Згідно з проведеними дослідженнями, 51% дітей віком від 10 до 17 років, які користуються інтернетом, не знають про потенційні небезпеки в мережі; 52% дітей використовують інтернет переважно для взаємодії у соціальних мережах, де надають свої телефонні номери (46%), домашні адреси (36%) та особисті фотографії (51%); Також відзначено, що 44% дітей можуть опинитися в потенційно небезпечних ситуаціях, розміщуючи особисту інформацію, а 24,3% вже стикалися з ризиковими ситуаціями (в групі від 15 до 17 років цей показник становить 60,3%) [3].

Ураховуючи те, що Україна перебуває в активній фазі інформаційної війни, перед українським суспільством постають важливі виклики. Кожен з нас повинен дотримуватися визначених правил поведінки в інтернеті та вчити дітей основам інформаційної безпеки під час дії воєнного стану. В умовах війни важливо навчити дітей дотримуватися діючого законодавства України та утримуватися від розміщення інформації, яка може негативно впливати на безпеку країни та її громадян. Важливим правилом взаємодії в соціальних мережах під час війни повинно бути збереження режиму тиші для уникнення потенційних загроз та надання допомоги ворогу. Актуальні правила поведінки в інформаційному просторі у воєнний час розробила команда #stop_sextинг (громадська організація для підлітків, батьків та вчителів про захист дітей в інтернеті) [4].

Отже, в умовах війни соціальні мережі приховують чимало загроз для безпеки дітей. Але ці ризики можна мінімізувати, якщо дотримуватися простих правил.

Соціальні мережі дають дітям можливість творчого самовираження, спілкування з друзями та родичами, отримання освіти, оновлення новин та багато іншого. Проте важливо пам’ятати та нагадувати дітям, що соцмережі не є надійними новинними джерелами, оскільки їм часто бракує контексту та перевірки фактів. Така інформація може призвести до непорозумінь та сприяти поширенню недостовірних даних. Потрібно навчити дітей аналізувати інформацію, перевіряти джерела, розпізнавати фейки та пропаганду, давати критичну оцінку повідомленням. Крім того, важливо звертати увагу на те, що контент, пов’язаний з війною, може містити матеріали, що можуть негативно впливати на психічне здоров’я дітей. Також важливо бути обережними щодо можливої дезінформації, яка також може поширюватися через соціальні мережі.

Батьки повинні уважно стежити за активністю дітей в інтернеті та встановити правила й обмеження. Варто обмежити час, який дитина проводить в соцмережах, контролювати її акаунти та коло спілкування. Регулярно перевіряти, які групи відвідує дитина, з ким спілкується, про що говорить.

З дітьми потрібно розмовляти про безпечну поведінку в інтернеті; пояснювати, чому не можна спілкуватися з незнайомцями, відкривати підозрілі посилання та ділилися особистою інформацією; слідкувати, щоб дитина не потрапляла на маніпулятивний контент; заохочувати звертатися з питаннями і проблемами.

Дотримання вище наведених правил і рекомендацій забезпечить більш безпечний онлайн-простір для наших дітей, навіть у складний воєнний час. Дбайливе ставлення та відкрите спілкування – запорука захисту дитини від загроз інтернету.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ольга Снопок. Нокаут телебаченню: як соціальні мережі утримують першість в постачанні новин українцям. Українська правда : вебсайт. URL: https://www.pravda.com.ua/columns/2023/08/16/7415807/ (дата звернення 12.01.2024).
2. Деркаченко Я.А. Соціальні мережі, як середовище для технологій маніпулятивного впливу. *Сучасний захист інформації*. 2016. № 1. С. 51-59. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/531/493 (дата звернення 11.01.2024).
3. Більше половини дітей, які користуються Інтернетом, нічого не знають про ризики в мережі. Онляндія – безпечна веб-країна : вебсайт. URL: https://kubg.edu.ua/images/stories/Departaments/Anonces/safe_internet_day/about_onlandia.pdf (дата звернення 11.01.2024).
4. Освітній портал #stop_sextинг URL: https://stop-sexting.in.ua/adult/.

ІНФОРМАЦІЙНА ГРАМОТНІСТЬ ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ ЗАХИСТУ ДІТЕЙ ВІД ІНФОРМАЦІЙНИХ ЗАГРОЗ У ВОЄННИЙ ПЕРІОД

Дар’я ТКАЧЕНКО, Ольга ГАБОРЕЦЬ

На тлі сучасних воєнних конфліктів та глобальних загроз, інформаційна грамотність стає ключовим елементом захисту дітей. Воєнний період, як особливий час надзвичайних викликів та перетворень, привертає особливу увагу до ролі, яку відіграє інформація в житті дітей. У цих умовах, критичне розуміння, аналіз та ефективне використання інформаційних ресурсів стають надзвичайно важливими навичками для забезпечення безпеки та добробуту молодших громадян.

Воєнний контекст створює специфічні виклики для інформаційної грамотності дітей. Вони стикаються з підвищеним ризиком впливу пропаганди, дезінформації та психологічної маніпуляції. Недостатня інформаційна грамотність може робити їх уразливими перед впливом негативних інформаційних змістів, що потенційно можуть шкодити їх фізичному та психічному здоров'ю, а також сприяти реальним загрозам безпеки.

У воєнний період діти стають особливо вразливими перед інформаційними загрозами. Систематична дезінформація та маніпуляції з боку конфліктуючих сторін можуть викликати паніку, страх та недовіру серед них. Будучи під впливом таких інформаційних атак, діти можуть приймати неконтрольовані рішення, які можуть негативно вплинути на їх безпеку та добробут.

У зв'язку з цим, розвиток інформаційної грамотності у дітей відіграє критично важливу роль у захисті їхніх прав та безпеки. Навички критичного мислення та аналізу допомагають дітям розрізняти об'єктивну інформацію від пропаганди та маніпуляцій. Крім того, уміння ефективно користуватися різноманітними джерелами інформації дозволяє їм визначати достовірність та об'єктивність інформаційних джерел.

Таким чином, інформаційна грамотність стає не лише інструментом захисту, але й ключовим фактором у забезпеченні безпеки та добробуту дітей під час воєнного конфлікту. Розуміння важливості цих навичок та їх активне впровадження у виховання та освіту дітей може сприяти побудові стійкого та безпечного соціального середовища для молодших поколінь навіть у найскладніших умовах воєнного періоду.

ОСНОВНІ ІНФОРМАЦІЙНІ ЗАГРОЗИ ДЛЯ ДІТЕЙ В УМОВАХ ВОЄННОГО СТАНУ

Марина ТКАЧЕНКО

Інформаційна безпека є одним з найважливіших аспектів життєдіяльності людини, особливо в умовах воєнного стану. У цей період діти особливо вразливі до інформаційних загроз, які можуть завдати їм шкоди фізично, психологічно та морально.

До основних інформаційних загроз для дітей в умовах воєнного стану відносяться:

- **Пропаганда та дезінформація**.

Пропаганда та дезінформація є одними з найпоширеніших інформаційних загроз для дітей в умовах воєнного стану. Ворог активно використовує пропаганду та дезінформацію для дестабілізації ситуації в Україні та підриву довіри до української влади. Діти, які не мають критичного мислення, можуть легко піддатися впливу пропаганди та дезінформації, що може призвести до негативних наслідків для їхнього емоційного та психічного стану.

Приклади пропаганди та дезінформації, які можуть бути шкідливими для дітей:

- Інформація, яка може викликати у дітей страх, тривогу або паніку.
- Інформація, яка може підірвати довіру дітей до батьків, вчителів або інших авторитетних осіб.
- Інформація, яка може спонукати дітей до небезпечних дій, наприклад, до приєднання до незаконних формувань.

- **Кіберзлочинність.**

У воєнний час кіберзлочинність стає більш поширеною. Діти можуть стати жертвами кіберзлочинців, які можуть заволодіти їхніми особистими даними, вимагати гроші або навіть викрасти їх.

Приклади кіберзлочинів, які можуть бути шкідливими для дітей:

- Фішинг – це вид шахрайства, коли кіберзлочинці виманюють у людей їхні особисті дані, наприклад, номери кредитних карток або паролі.
- Сексуальне насильство над дітьми в Інтернеті – це серйозна проблема, яка може завдати шкоди фізично та психологічно.
- Розбещення неповнолітніх – це злочин, за який передбачена кримінальна відповідальність.

- **Психологічний вплив**.

Війна може викликати у дітей стрес, тривогу та інші психологічні проблеми. Діти можуть бути піддані негативному впливу інформації про війну, яка може посилити їхні психологічні проблеми.

Приклади негативного психологічного впливу інформації про війну на дітей:

- Стрес – це нормальна реакція на стресову ситуацію. Однак, якщо стрес продовжується тривалий час, він може призвести до проблем зі здоров'ям, таких як безсоння, головний біль та проблеми зі шлунково-кишковим трактом.
- Тривога – це почуття занепокоєння або страху, яке може виникати внаслідок воєнних дій. Тривога може бути дуже виснажливою та ускладнювати повсякденне життя.
- Депресія – це психічний розлад, який може призвести до почуття смутку, безнадії та безцільності. Депресія може серйозно ускладнити життя дітей та перешкодити їм нормально вчитися та розвиватися.

Інформаційний простір дозволяє бути на зв’язку з рідними, дізнаватись останні новини з фронту, хоч якось контролювати те, що відбувається навколо. Для дітей та підлітків інтернет залишається світом розваг та спілкування з друзями. Але важливо пам’ятати, що за позначкою геолокації на пості чи фотографії, веселим відео в соціальній мережі чи одним повідомленням може ховатися справжня небезпека. Особливо під час війни, коли інфопростір використовують окупанти для військових нападів на українські міста.

Як захистити себе та дітей в інформаційному просторі під час війни? Інформаційна безпека під час війни: покрокова інструкція для дітей [1]**.** Більше інформації можна знайти за посиланням (https://osvitoria.media/opinions/informatsijna-bezpeka-pid-chas-vijny-pokrokova-instruktsiya-dlya-ditej/)

Заходи щодо забезпечення інформаційної безпеки дітей

Для забезпечення інформаційної безпеки дітей в умовах воєнного стану необхідно:

- Виховувати у дітей критичне мислення. Діти повинні навчитися аналізувати інформацію, яка надходить до них, і не довіряти усьому, що вони бачать або чують.

Діти та підлітки отримують багато інформації саме в соціальних мережах. Часто — від лідерів думок, блогерів чи користувачів в інтернеті, які висвітлюють власну думку. У воєнний час ми спостерігаємо також за тим, як відбувається інформаційна війна та психологічний тиск у соціальних мережах. Як навчити дитину критично аналізувати інформацію під час війни? Проєкт #stop_sextинг пропонує покрокову інструкцію для дітей [3]:

1. *Чи є посилання на офіційні джерела? Чи це думка конкретної людини?*

До офіційних джерел інформації під час війни ми відносимо такі: Офіс Президента України, Генеральний штаб Збройних Сил України, Кабінет Міністрів України, Міністерство оборони України, Міністерство внутрішніх справ, Національна поліція України, ДСНС, Сухопутні війська ЗСУ, Військово-морські сили ЗСУ, Територіальна оборона ЗСУ, Центр стратегічних комунікацій та інформаційної безпеки.

Але не забуваємо і про те, що часом навіть ці канали можуть бути під кібератакою і там може з'явитися неправдива інформація. Якщо це так, то згодом на ресурсі буде інформація про це.

Думка конкретної людини часто виражається словами «На мою думку», «Мені здається», «Я впевнений/впевнена», «Я знаю, що…», «Я думаю, що…», «Всі думають…». Також оціночними є судження типу «ніхто», «ніколи», «всі», «завжди».

2. *Чи повідомлення емоційно забарвлене? Чи в ньому є лише факти?*

Факти — це конкретні цифри, назви певних міст, вулиць, посилання на автора слів чи перевірене джерело. І вони вказують на те, що інформація імовірно правдива.

Сильне емоційне забарвлення інформації, яку подають ресурси, найчастіше вказує на дезінформацію. І такий метод використовується для того, щоб викликати і підсилити певні переживання в людей — співчуття, злість, роздратованість, смуток, паніку, страх.

3. *Чи ця інформація на користь нам?*

Висвітлення подій у країні в цілому та в кожному окремому місті — те, що дозволяє розуміти повну картинку та певним чином контролювати перебіг подій, наприклад, для вибору більш безпечного місця перебування.

4. *Як це впливає на мене?*

Негативно емоційно забарвлена інформація часто викликає занепокоєння, підсилює тривогу та відчай. Доволі часто цей шлях обирають дезінформатори для того, щоб посіяти відчуття зневіри та паніки в читачів.

І пам'ятайте та наголосіть на цьому дітям, що повідомлення зі словами «Дуже терміново!», «Це правдива інформація, передайте далі», «Мені повідомили рідні/знайомі/люди» — найчастіше є неправдивими.

Тож перевіряємо інформацію та ділимося лише офіційними й перевіреними фактами!

Поради для батьків та педагогів щодо забезпечення інформаційної безпеки дітей в умовах воєнного стану:

- Розмовляйте з дітьми про війну. Не намагайтеся захистити дітей від інформації про війну, але поясніть їм, що відбувається, у доступній формі.
- Вчіть дітей не ділитися особистою інформацією з незнайомими людьми. Це стосується не тільки їхніх імен, адрес та номерів телефонів, а й будь-якої іншої інформації, яка може бути використана для їхньої ідентифікації.

- Навчіться розпізнавати ознаки кіберзлочинності. Розкажіть дітям про те, як кіберзлочинці можуть намагатися заволодіти їхніми особистими даними або вимагати гроші.
- Слідкуйте за тим, що діти дивляться в Інтернеті та по телевізору. Блокуйте доступ до сайтів та каналів, які можуть містити пропаганду або дезінформацію. Обмежуйте доступ дітей до інформації, яка може бути для них шкідливою.
- Створіть для дітей безпечне середовище. Забезпечте дітям достатньо часу для відпочинку та розваг, щоб вони могли впоратися зі стресом, викликаним війною.
- Вчіть дітей користуватися Інтернетом безпечно. Поясніть їм, як захистити свої особисті дані, як розпізнавати шкідливе програмне забезпечення та як не потрапити в пастку кіберзлочинців.
- Надавайте дітям психологічну підтримку. Діти, які відчувають стрес або тривогу, повинні мати можливість отримати психологічну допомогу.
- Підтримуйте зв'язок з дітьми. Дізнайтеся, що вони бачать і чують в Інтернеті та по телевізору. Обговорюйте з ними інформацію, яку вони отримують, і допомагайте їм розвинути критичне мислення.
- Будьте прикладом. Діти навчаються на прикладі дорослих. Якщо ви будете критично ставитися до інформації, яку отримуєте, діти також будуть це робити.

Більше корисних матеріалів можна переглянути за посиланням [4] https://stop-sexting.in.ua/adult/korysni-materialy/

Забезпечення інформаційної безпеки дітей в умовах воєнного стану є важливим завданням для всіх. Виконуючи ці поради, ми можемо допомогти захистити наших дітей від шкідливого впливу інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Інформаційна безпека під час війни: покрокова інструкція для дітей. Освіторія : вебсайт. URL: https://osvitoria.media/opinions/informatsijna-bezpeka-pid-chas-vijny-pokrokova-instruktsiya-dlya-ditej/
2. Stop-sexting : вебсайт. URL: https://stop-sexting.in.ua/adult/
3. Як навчити дитину критично аналізувати інформацію під час війни? Освіторія : вебсайт. URL: https://osvitoria.media/experience/yak-navchyty-dytynu-krytychno-analizuvaty-informatsiyu-pid-chas-vijny/
4. Корисні матеріали. Stop-sexting: вебсайт. URL: https://stop-sexting.in.ua/adult/korysni-materialy/

ФОРМУВАННЯ БЕЗПЕЧНОЇ ПОВЕДІНКИ ДІТЕЙ В ІНТЕРНЕТ-МЕРЕЖІ

Тетяна ЯКИМ

Діти значно швидше у порівнянні з дорослими адаптуються до стрімких змін інформаційних технологій, легко опановують їх. Більшість дітей не володіють достатньою інформацією про те, як безпечно користуватись Інтернетом, не мають відповідних навичок онлайн-культури, й частіше ризикують стати жертвою технологій. Безконтрольне та безвідповідальне використання інформаційно-комунікаційних технологій загрожує безпеці дітей та призводить до порушення їхніх прав. Сьогодні є вкрай необхідними своєчасне інформування підростаючого покоління, батьків, вчителів щодо загроз мережі Інтернет та навчання їх елементарним правилам її безпечного використання. Метою написання статті є висвітлення основних онлайн-небезпек та методів формування в дітей компетенцій безпечної поведінки в мережі Інтернет.

Інтернет є чудовим інструментом для задоволення таких потреб дітей як допитливість. Діти опиняються в неконтрольованому просторі з величезною кількістю інформації, у тому числі і шкідливою, що, безперечно, має негативний вплив на розвиток їх внутрішнього світу та сприйняття навколишнього середовища. У зв'язку з цим можемо чітко підкреслити 4 основних загрози безпеці дітей в інтернет-мережі: ***залежність від Інтернету, доступ до небажаного контенту, комунікаційні загрози та електронні (кібер) загрози***.

1. Залежність від Інтернету. Головною причиною виникнення комп'ютерної залежності у дітей психологи вважають недостатнє спілкування і взаєморозуміння з батьками, однолітками і значущими людьми. Інтернет-залежною визнається людина, яка не здатна контролювати свій час в Інтернеті; розумово або фізично виснажена; має порушення сну і концентрації уваги. Проявляється дратівливість, депресія, знервованість, труднощі у спілкуванні з людьми в реальному житті [2, с. 14].

2. Доступ до небажаного контенту. Під небажаним контентом розуміємо нелегальні та шкідливі матеріали, що не відповідають віковим особливостям дітей і негативно впливають на стан їх фізичного та психічного здоров'я. Контентні загрози в Інтернеті – це матеріали, які містять насильство, агресію, еротику і порнографію, нецензурну лексику, інформацію, що розпалює расову ненависть, пропаганду анорексії і булімії, суїциду, азартних ігор, наркотичних речовин і ін. [6, с. 172].

3. Комунікаційні загрози пов'язані з міжособистісними відносинами інтернет-користувачів і містять в собі небезпеку зіткнутися з психологічними нападами, які здійснюються через електронну пошту, сервіси миттєвих повідомлень (ICQ, Google talk, Skype), чати, форуми, блоги, соціальні мережі, сайти знайомств, вебсайти, а також за допомогою мобільного зв'язку.

Основними комунікаційними загрозами є: розкриття дитиною конфіденційної інформації про себе і сім'ю, кібербулінг і кібергрумінг [2, с. 18].

Розкриття дитиною конфіденційної інформації про себе і свою сім'ю зазвичай відбувається при використанні соціальних мереж. Інформація, яка розміщена на сайтах соцмереж, доволі часто нагадує досьє на користувача і тому, природно, викликає інтерес у сторонніх людей. Існує навіть таке поняття, як «викрадення особистості» [6, с. 172].

Кібербулінг (англ. cyberbullying від bully – хуліган, забіяка, грубіян) – переслідування, залякування і знущання з дитини за допомогою цифрових технологій, передачі повідомлень агресивного змісту, розміщення відеороликів, що містять знущання, розкриття анонімності акаунта на форумах і ін. Такі атаки зазвичай є регулярними з одночасним використанням декількох засобів і анонімними, що призводить до того, що залякування наносять серйозну психологічну травму дитині.

Кібергрумінг (анг, cybergrooming / child grooming) – це спілкування та встановлення довірливих відносин з дитиною з метою подальшої особистої зустрічі для вступу в статеві стосунки, фізичного нападу, шантажу, сексуальної експлуатації і насилля. Такі знайомства відбуваються у чатах, на форумах, в соціальних мережах. Злочинець видає себе за однолітка і намагається дізнатися особисту інформацію (адреса, телефон) і домовитися про зустріч [1, с. 70].

4. Електронні (кібер) загрози – це шкідливі програми (віруси, черв'яки, спам-атаки, шпигунські програми, боти), які можуть нашкодити комп'ютеру та порушити конфіденційність особистої інформації. Основними різновидами електронних загроз є віруси, спам-повідомлення, фішинг, фармінг. Всі ці загрози визначаються як кібершахрайство.

Користувачі Інтернету мають велику ймовірність заразити комп'ютер *вірусами*. Зазвичай діти навіть не здогадуються, що скачуючи музику, фільми, текстові документи та ін. і можна заразити комп'ютер шкідливим програмним забезпеченням [4, с. 11–12].

Фішинг **(**англ. fishing – рибальство) – підміна офіційного сайту схожим, шахрайським з метою виманювання у довірливих або неуважних користувачів мережі персональних даних. Шахраї використовують всілякі прийоми, які найчастіше змушують користувачів особисто повідомляти конфіденційні дані.

Існує так званий *фармінг* (англ. pharming) – це процедура прихованого перенаправлення жертви на помилкову IP-адресу. Шахраї створюють точну копію відомого сайту і після того, як користувач відвідає його, віруси і шпигунські програми проникають на комп'ютер. Таким чином шахраї дізнаються про всі переміщування дитини в Інтернеті і отримують доступ до особистої інформації [2, с. 21–22].

Ще одним різновидом електронної загрози є *спам* (англ. spam) – це масова розсилка шкідливих небажаних повідомлень. Вони засмічують електронну скриньку і можуть бути небезпечними для комп'ютера. Вони стають відмінним інструментом для шахрайства, реклами нелегальних, підроблених та контрафактних товарів, розповсюдження порнографії та інших злочинів [4, с. 17].

У зв'язку з використанням дітьми мобільних телефонів із безперешкодним доступом до інтернету у сучасних умовах батькам і вчителям важко контролювати, які сайти і соціальні мережі вони відвідують. У зв'язку з цим

можна запропонувати батькам десять правил, які сприятимуть формуванню в дітей умінь і навичок безпечного використання.

1) Заздалегідь погодьте тривалість перебування дитини в Інтернеті, аби не чинити шкоду стану її здоров'я та не сприяти комп'ютерній залежності, яка стала великою проблемою у всьому світі [3, с. 17].

2) Навчіть дитину не розголошувати свою конфіденційну інформацію, а особливо без вашого дозволу [7, с. 55].

3) Використовуйте технічні засоби захисту: функції батьківського контролю в операційній системі, антивірус та спам-фільтр [4, с. 57].

4) Поясніть дитині, що завантаження деяких файлів може бути незаконним чи небезпечним, тобто може заразити комп'ютер вірусами. Розкажіть, чому небезпечно відкривати підозрілі повідомлення електронної пошти, файли або вебсторінки від незнайомих людей.

5) Створіть сімейні правила онлайн-безпеки для дітей. Якщо ви зацікавлені у тому, аби ваша дитина навчалася не на своїх власних помилках, якомога частіше обговорюйте теми, пов'язані з Інтернетом [2, с. 29].

6) Поясніть дитині, чим небезпечні зустрічі з віртуальними знайомими в реальному житті. Якщо в дитини є бажання зустрітися з кимось із віртуальних знайомих, їй потрібно обов'язково домовлятися про зустріч у громадському місці і повідомити про це вас [7, с. 55].

7) Проводьте більше часу з дитиною, заохочуйте її до обговорення тем, пов'язаних з Інтернетом. Щоб не сталося, ваша дитина повинна знати, що вона завжди може розраховувати на ваше розуміння та підтримку. Хороший рецепт побудови довірливих відносин – щоденне спілкування та спільне проведення вільного часу [3, с. 17].

8) Навчайте дітей критично ставитися до інформації в Інтернеті. Розкажіть дитині, що практично кожен може створити свій сайт, і при цьому ніхто не може проконтролювати достовірність інформації, розміщеної на такому сайті. Діти повинні навчитися відрізняти надійні джерела інформації від ненадійних і перевіряти інформацію, яку вони знаходять в Інтернеті [7, с. 55].

9) Поясніть дитині, що Інтернет може коштувати реальних грошей. Діти можуть здійснювати покупки через Інтернет або оплатити певну послугу. Саме тому важливо проговорити з дитиною, що вона обов'язково повинна радитись із вами перш ніж робити щось подібне.

10) Навчіть дитину дотримуватись тих же правил поведінки, що і в реальному житті, дитина завжди повинна пам'ятати про ввічливість і толерантність при спілкуванні з іншими онлайн-користувачами.

Висновки. Таким чином, варто підкреслити, що саме в сім'ї закладаються основи поведінки дитини в реальному світі, віртуальний простір не має бути винятком. Батькам слід приділяти серйозну увагу вихованню дітей і підвищенню їхньої обізнаності щодо загроз інформаційного середовища. Необхідно пам'ятати, що комп'ютер для дітей повинен бути інструментом для навчання і розвитку, а не лише розваг та ігор. Попри широкі можливості віртуального спілкування, воно не може виключати чи замінювати реальних стосунків між людьми. Водночас для забезпечення єдиних вимог і умов онлайн-безпеки дітей, як у закладі освіти, так і

вдома, необхідною є співпраця батьків і педагогів. Педагоги повинні інформувати батьків стосовно питань інтернет-безпеки, розробляти спільні методи і засоби для ефективного навчання дітей основним правилам безпечної поведінки в інтернет-просторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Данильчук Л. О. Ризики та небезпеки мережі Інтернет: до проблеми інформаційної захищеності дітей. *Педагогічний дискурс*. 2012. Вип. 13. С. 68 – 71.
2. Діти в Інтернеті: як навчити безпеці у віртуальному світі : посібник для батьків / Литовченко І. В. та ін. К.: ТОВ «Видавничий Будинок Аванпост-Прим», 2010. 48 с.
3. Литвиненко О. В. Дитяча безпека в Інтернеті: технології та рекомендації на допомогу батькам. *Безпека дітей в Інтернеті: попередження, освіта, взаємодія* : Матеріали обласної науково-методичної Інтернет-конференції (м. Кіровоград, 11 лютого 2014 р.). Кіровоград, 2014. С. 15 – 18. URL: http://konf.koippo.kr.ua/blogs/index.php/blog2/
4. Кочарян А. Б., Гущина Н. І. Виховання культури користувача Інтернету. Безпека у всесвітній мережі : навчально-методичний посібник. Київ, 2011. 100 с.
5. Кузнєцова І. В. Дитина і комп'ютер: виховання особистості в інформаційному суспільстві. *Обдарована дитина*. 2010. № 6. С. 41– 46.
6. Кухарська Н. П., Кухарський В. М. Загрози безпеці дітей у соціальних мережах. *Безпека інформації*. 2014. Т. 20, № 2. С. 169 –175.
7. Паукова А. С. Ідея інформаційного захисту дітей на сторінках педагогічної преси США. *Вісник ЛНУ імені Тараса Шевченка*. 2013. № 13 (272), Ч. 3. С. 50 –58.

ОРГАНІЗАЦІЙНО-ПЕДАГОГІЧНІ УМОВИ ФОРМУВАННЯ БЕЗПЕЧНОЇ ПОВЕДІНКИ ЗДОБУВАЧІВ ОСВІТИ В ІНТЕРНЕТІ

ФОРМУВАННЯ БАЗОВИХ КОМПЕТЕНЦІЙ БЕЗПЕЧНОЇ ПОВЕДІНКИ ПІДЛІТКІВ В ІНТЕРНЕТІ

Олена БАБКОВА
Кіра СТАДНИЧЕНКО

У зв'язку з цифровою трансформацією суспільства інтернет-простір став невід'ємною частиною усіх сфер людської діяльності. Саме він спроможний задовольнити інформаційні, комунікативні, самопрезентаційні потреби дорослих і дітей. Останні, зокрема, активно долучаються до онлайн-спілкування в соціальних мережах та творчої самореалізації: знаходять цікаву навчальну інформацію; переглядають відеоролики, прослуховують подкасти, беруть участь в онлайн-іграх, за допомогою цифрових ресурсів створюють проєкти.

Поряд із численними перевагами, мережа Інтернет несе значний ризик для підлітків, які активно взаємодіють у віртуальному середовищі. Ця група користувачів вважається однією з вразливих, оскільки у підлітковому віці ще не повністю розвинені навички вибору, аналізу та критичного оцінювання інформації. Слід додати, вітчизняні і зарубіжні експерти зазначають, що ідеально «чиста», тобто позбавлена загроз, мережа Інтернет у принципі неможлива [1]. Саме через це актуальним є своєчасне інформування дітей, їхніх батьків, вчителів щодо загроз Всемережжя, а також навчання їх правилам безпеки використання Інтернет.

Проблемі формування безпечної поведінки дітей в мережі Інтернет протягом тривалого часу приділяється значна увага з боку українських науковців. Так, К. Варивода акцентував на актуальності формування безпечної поведінки дітей в інтернеті, яке має носити комплексний та міжінституційний характер і передбачає виховання інформаційної культури особистості [1]. А. Кочарян, Н. Гущина в рамках програми «Онляндія – безпечна Web-країна» розробили методичні рекомендації щодо формування у дітей компетенцій грамотного та безпечного використання Інтернет-ресурсів [3]. І. Сокол систематизувала понад 50 термінів, пов’язаних з інтернет-безпекою, до відповідного глосарію та навела їхні тлумачення [5]. С. Єфіменко визначила шляхи формування навичок безпечної поведінки в Інтернеті здобувачів закладу загальної середньої освіти. Здійснено характеристику цифрових інструментів та наведено приклади навчально-методичних розробок для роботи зі школярами з проблеми дослідження [2].

М. Снітко надала тлумачення поняттю «безпечна поведінка підлітків в Інтернет-мережі» як *засобу самореалізації та сукупності дій підлітків в Інтернет-мережі,* що характеризуються знаннями підлітків про ризики та правила поведінки в Інтернет-мережі, вміннями оптимально реагувати у ризикових ситуаціях, контролювати емоції, відповідально ставитися до власної діяльності в Інтернет-мережі [4]. О. Черних розглядає це поняття *як сукупність дій особистості під час користування Інтернетом*, що сприяють задоволенню потреб і водночас запобігають можливості завдання збитків, заподіяних фізичному, психічному, соціальному благополуччю та (або) майну самої людини та інших людей [6]. Узагальнюючи сказане вище, можна пов'язати дії підлітків в Інтернеті з їхніми знаннями щодо безпечності цих дій. Тобто у дітей має бути сформована *компетентність безпечної поведінки в Інтернеті*, а саме: втілена в практичну діяльність сукупність знань, умінь і цінностей, що під час користування Інтернетом сприяють задоволенню потреб особистості й водночас запобігають можливості завдання збитків, заподіяних фізичному, психічному, соціальному благополуччю та (або) майну самої людини та інших людей [6].

Тож метою нашого дослідження є визначення рівня сформованих базових компетенцій безпечної поведінки підлітків в Інтернеті та прогнозування заходів реагування на виявлену ситуацію.

Базовими компетенціями безпечної поведінки підлітків в Інтернеті відповідно до класифікації О. Черних є:

1. Розуміння застосування прав людини в Інтернеті – знання про права людини онлайн, дотримання прав людини онлайн, ставлення до Інтернету як до інструменту можливостей.

2. Електронна участь – знання про можливості участі, досвід участі онлайн, ціннісне ставлення до можливостей електронної участі.

3. Збереження здоров'я під час роботи з цифровими пристроями – знання про загрози в Інтернеті та їх вплив на здоров'я; здійснення заходів щодо збереження здоров'я під час користування Інтернетом, ціннісне ставлення до власного здоров'я.

4. Звернення по допомогу та захист – знання про механізми захисту прав, що порушені в Інтернеті; досвід звернень по допомогу у випадку наражання на загрози в Інтернеті; повага до прав людини в Інтернеті та розуміння механізму захисту [6].

Нами проведено експрес-опитування за інструментарієм О. Черних [6], у якому взяли участь 44 респонденти – учні 9-х класів запорізьких шкіл. Результати опитування продемонстрували переважно середній рівень сформованості в учнів усіх зазначених автором інструментарію базових компетенцій (рис. 1). При цьому найбільш чітко виявлено середній рівень, з незначними включеннями нижчих та вищих значень, виражений щодо розуміння застосування прав людини в Інтернеті. Перевага показників середнього рівня щодо електронної участі та збереження здоров'я під час роботи з цифровими пристроями є менш значною, але, на жаль, не на користь високого рівня сформованості відповідних компетенцій. За напрямом звернення за допомогою та захистом показників високого рівня не зафіксовано загалом, що свідчить про недостатність в учнів систематизованих знань щодо правових та процесуальних механізмів захисту прав людини та відсутність досвіду дій у випадку, якщо став жертвою або спостерігачем чиїхось зловмисних вчинків в інтернеті.

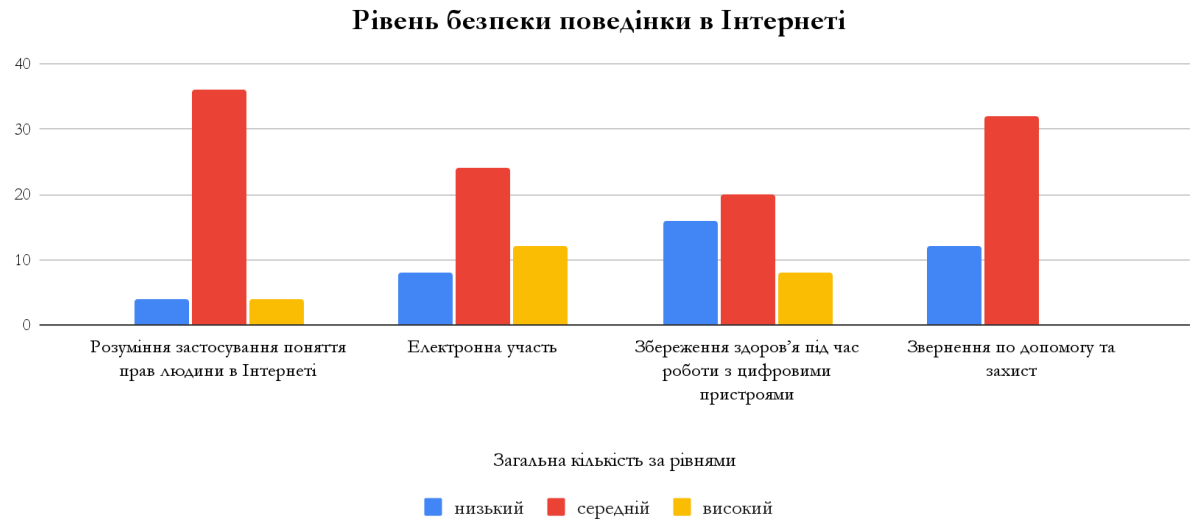

Рис. 1. Розподіл показників сформованості базових компетенцій безпечної поведінки підлітків в інтернеті за рівнями низький / середній / високий

За іншого варіанту візуалізації тих самих даних, можна помітити (рис. 2), що найбільший показник низького рівня зафіксовано за напрямом збереження здоров'я під час роботи з цифровими пристроями, тобто спостерігаються відсутність систематизованих знань про негативний вплив на здоров’я й умови збереження здоров’я під час тривалого користування інтернетом або нехтування такими знаннями; систематичне невиконання умов для збереження власного здоров’я під час користування інтернетом; нерозуміння власного здоров’я як цінності й необхідності створення умов для збереження психічного, фізичного й соціального видів здоров’я під час тривалого користування інтернетом. Також впадає в око цілковита відсутність показників високого рівня компетенції, що стосується напряму звернення за допомогою та захистом, навіть у респондентів, що демонструють високі показники за іншими напрямами. Таким чином, опитування дає змогу визначити загальний рівень сформованості базових компетенцій безпечної поведінки підлітків в Інтернеті як середній, що безумовно потребує ретельної подальшої роботи для поліпшення цього стану.

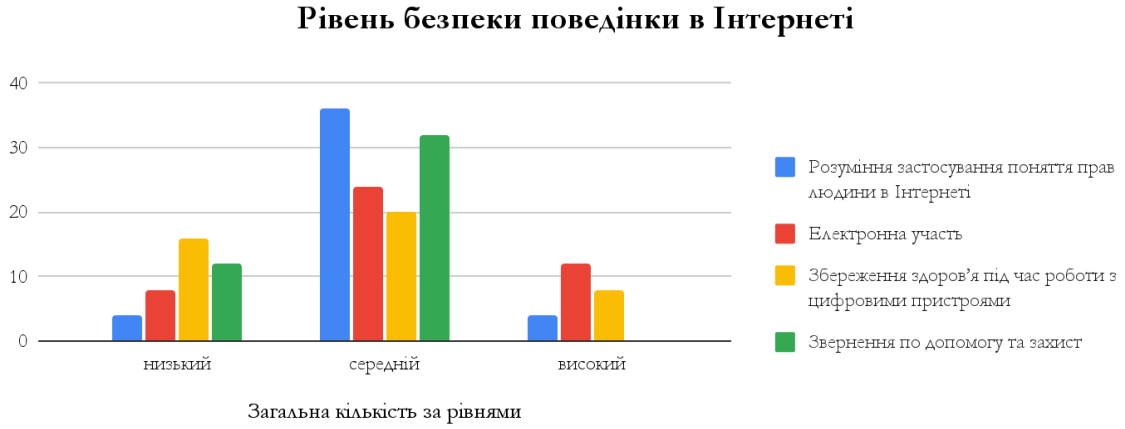

Рис. 2. Рівні сформованості базових компетенцій безпечної поведінки підлітків в інтернеті за окремими компетенціями

Отже, можна рекомендувати цей інструментарій для визначення рівня сформованості базових компетенцій безпечної поведінки підлітків в інтернеті вчителям-предметникам, класним керівникам задля планування виховних заходів, бесід для дітей та їхніх батьків. Варто проєктувати такі заняття на принципах і підходах освіти з прав людини, зосереджувати увагу дітей на розширенні ролей, які людина може грати завдяки інтернету; долучати учнів до відкритого діалогу щодо позитивного й негативного впливу на здоров’я користування цифровими пристроями та інтернетом й аналізування власних знань, навичок, ставлень до можливості звернення по допомогу під час користування інтернетом. Доречним є використання навчально-методичних посібників, які містять інформаційні та дидактичні матеріали, тренінгові вправи, симуляції, інтеракції, кейси [2, 6].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Варивода К.С. Формування в дітей компетенцій безпечного використання Інтернет-мережі. *Журнал Науковий огляд*. 2015. № 10 (20). URL: https://core.ac.uk/download/pdf/145611319.pdf.
2. Єфіменко С.М. Організаційно-педагогічні умови формування навичок безпечної поведінки школярів в Інтернеті : навчально-методичний посібник. Кропивницький : КЗ «КОІППО імені Василя Сухомлинського», 2023. 46 с. URL: https://drive.google.com/file/d/1LpVm8ZF04jg-hsrUUte2Xfa3QZHG_4TX/view.
3. Кочарян А.Б., Гущина Н.І. Виховання культури користувача Інтернету. Безпека у всесвітній мережі : навчально-методичний посібник. Київ. 2011. 100 с. URL: https://elibrary.kubg.edu.ua/id/eprint/1547/1/Internet.pdf.
4. Снітко М.А. Соціально-педагогічні умови формування у підлітків безпечної поведінки в Інтернет-мережі : автореф. дис. на здобуття наук. ступеня канд.пед. наук : 13.00.05. Київ, 2014. 22 с. URL: https://elibrary.kubg.edu.ua/id/eprint/4796/1/M_Snitko_Avtoref_IL.pdf.
5. Черних О. Онлайк : навчально-методичний посібник. Київ : BAITE, 2020. 108 с. URL: https://www.osce.org/files/f/documents/0/f/483533.pdf.
6. Safer Internet: глосарій / укл. І.М. Сокол. 2ге вид.: випр. та доп. Запоріжжя : СТАТУС, 2020. 32 с. (Педагогічне сьогодення).

ВИСОКИЙ РІВЕНЬ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ КОМПЕТЕНТНОСТІ ПЕДАГОГА ЯК НЕОБХІДНА УМОВА РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ КОМПЕТЕНТНОСТІ ЗДОБУВАЧІВ ОСВІТИ

Оксана БАРЛІТ

У сучасному соціумі, в умовах стрімкого розвитку сфери інформаційних і комунікаційних технологій, цифрової трансформації процесів і послуг, постає проблема підвищення ступеня цифрової компетентності фахівців будь-якої галузі, і, в першу чергу, педагогічних працівників.

В Концепції Нової української школи зазначено, що наскрізне застосування інформаційно-комунікаційних технологій в освітньому процесі та управлінні закладами освіти й системою освіти має стати інструментом забезпечення успіху Нової української школи.

Запровадження ІКТ в освітній галузі має перейти від одноразових проєктів у системний процес, який охоплює всі види діяльності. ІКТ суттєво розширять можливості педагога, оптимізують управлінські процеси, таким чином формуючи в учня важливі для нашого сторіччя технологічні компетентності [1].

Сучасний педагог має володіти високим рівнем інформаційно-комунікативної компетентності, яка є складовою професійної компетентності, є динамічною, і потребує постійного вдосконалення.

У Європейській рамці цифрової компетентності для освітян (DigCompEdu) зазначено 22 компетентності, які систематизовані в шести сферах цифрової компетентності педагогів:

1. Професійне залучення – використовувати цифрові технології для спілкування, співпраці та професійного розвитку.
2. Цифрові ресурси – шукати, створювати та обмінюватися цифровими ресурсами.
3. Викладання й навчання – управляти та організовувати робочий і навчальний процес за допомогою цифрових технологій.
4. Оцінювання – використовувати цифрові технології та стратегії для оцінювання учнів.
5. Розширення можливостей учнів – використовувати цифрові технології для підвищення інклюзивності та активного залучення учнів до навчання.
6. Сприяння цифровій компетентності учнів – дати їм можливості використовувати цифрові технології для спілкування, створення контенту, розвитку та розв'язання проблем [2].

Звертаємо увагу, що в межах даної роботи терміни «інформаційно-комунікаційна компетентність» та «інформаційно-цифрова компетентність» мають подібний зміст і вживаються як синоніми.

У законі України «Про освіту» компетентність визначено як динамічну комбінацію знань, умінь, навичок, способів мислення, поглядів, цінностей, інших особистих якостей, що визначає здатність особи успішно соціалізуватися, провадити професійну та/або подальшу навчальну діяльність.

Стаття 12 цього ж законодавчого акта зазначає, що досягнення мети повної загальної середньої освіти забезпечується шляхом формування ключових компетентностей, необхідних кожній сучасній людині для успішної життєдіяльності: вільне володіння державною мовою; здатність спілкуватися рідною (у разі відмінності від державної) та іноземними мовами; математична компетентність; компетентності у галузі природничих наук, техніки і технологій; інноваційність; екологічна компетентність; інформаційно-комунікаційна компетентність; навчання впродовж життя; громадянські та соціальні компетентності; культурна компетентність; підприємливість та фінансова грамотність; інші компетентності, передбачені стандартом освіти [3].

Ті ж 11 ключових компетентностей зазначені у Державному стандарті базової середньої освіти. Зауважмо, що усі компетентності однаково важливі й взаємопов'язані. Кожну з них здобувачі освіти набувають під час вивчення різних предметів на всіх етапах освіти. У документі визначено інформаційно-комунікаційну компетентність такою, що передбачає впевнене, критичне і відповідальне використання цифрових технологій для власного розвитку і спілкування; здатність безпечно застосовувати інформаційно-комунікаційні засоби в навчанні та інших життєвих ситуаціях, дотримуючись принципів академічної доброчесності [4].

Майже аналогічне визначення в Концепції НУШ надано інформаційно-цифровій компетентності: «інформаційно-цифрова компетентність передбачає

впевнене, а водночас критичне застосування інформаційно-комунікаційних технологій (ІКТ) для створення, пошуку, обробки, обміну інформацією на роботі, в публічному просторі та приватному спілкуванні. Інформаційна й медіаграмотність, основи програмування, алгоритмічне мислення, робота з базами даних, навички безпеки в інтернеті та кібербезпеці. Розуміння етики роботи з інформацією (авторське право, інтелектуальна власність тощо)» [1].

Оскільки перед системою освіти стоїть завдання – сформувати інформаційно-компетентну особистість здобувача освіти, сучасний педагог має орієнтуватися в інформаційному просторі, здійснювати пошук і критично оцінювати інформацію, ефективно використовувати наявні та створювати нові цифрові освітні ресурси, використовувати цифрові технології в освітньому процесі, розуміти елементи штучного інтелекту тощо.

Сучасний педагог має створювати умови, які сприяють розвитку інформаційно-комунікативної компетентності здобувачів освіти, а для цього педагог має володіти власним високим рівнем інформаційно-комунікативної компетентності, і це є одним з основних умов розвитку інформаційно-комунікаційної компетентності здобувачів освіти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Нова українська школа : Концепція реалізації державної політики у сфері реформування загальної середньої освіти на період до 2029 року. URL: https://osvita.ua/legislation/Ser_osv/54258/.
2. Як учителям підвищити цифрові компетентності. НУШ : вебсайт. URL: https://nus.org.ua/view/yak-uchytelyam-pidvyshhyty-tsyfrovi-kompetentnosti/.
3. Про освіту : Закон України від 05.09.2017 р. № 2145-VIII URL: http://zakon.rada.gov.ua/laws/show/2145-19#n740.
4. Про деякі питання державних стандартів повної загальної середньої освіти : Постанова Кабінету Міністрів України від 30 вересня 2020 р. № 898 URL: https://zakon.rada.gov.ua/laws/show/898-2020-%D0%BF#n16.

НАСТУПНІСТЬ У ФОРМУВАННІ КОМПЕТЕНТНОСТЕЙ УЧНІВ З ПИТАНЬ БЕЗПЕКИ В ІНТЕРНЕТІ: ПРОБЛЕМИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Ольга БАРНА

Навчання безпечній поведінці учнів в інтернеті є завданням усіх видів освіти: формальної, неформальної та інформальної. Тільки за умов злагодженої роботи усієї освітньої системи та включення усіх учасників освітнього процесу до вирішення проблем безпеки можна отримати стійкі результати в етичній поведінці, безпечному спілкуванні, правильному використанні мережевих сервісів, сформувати в учнів внутрішні мотиви діяти обачно в мережі упродовж тривалого часу.

Формальна освіта має вплив на формування компетентностей безпечної поведінки учнів як через результати навчання інформатики, де однією із змістовних ліній є лінія «Цифрове громадянство», так і через вивчення інших навчальних дисциплін, де ці питання можуть розглядатись в змісті текстів у мовно-літературній освітній галузі, в обчислювальних завданнях за результатами недотримання правил безпеки, в розгляді ситуацій щодо впливу на здоров'я та емоційний стан неетичної поведінки користувачів та користувачок інтернету, залежності від гаджетів чи булінгу в предметах природничого циклу тощо. Прикладами неформальної освіти є заходи, які проводяться в рамках Дня безпечного інтернету, тижнів коду, безпеки, онлайн-комерції та інші, можуть бути реалізовані як центрами дитячого розвитку чи творчості, так і різними громадськими організаціями, заходами, організованими громадянським суспільством. До інформальної освіти відносять самоорганізоване здобуття компетентностей з питань безпеки через спілкування з експертними колами, участь у тренінгах, використання чат-ботів, спеціальних ігор, в тому числі і комп'ютерних.

Різні аспекти проблеми формування уміння запобігати інтернет-загрозам досліджувалися як закордонними, так і вітчизняними науковцями. Зокрема охарактеризовано типологію електронних ресурсів у галузі медіаосвіти, визначено типи електронних ресурсів, які можуть бути успішними для розвитку інфомедійної грамотності [3], проаналізовано проблеми безпечної роботи учнів початкових класів у мережі інтернет [2], розглянуто окремі компоненти методичної системи навчання основам інформаційної безпеки [1] та інші.

Метою даного дослідження є розгляд організаційних умов формування здатностей учнів розрізняти ризики, діяти обачно та приймати адекватні рішення щодо мінімізації ризиків, які пов'язані із діяльністю в інтернеті.

Як показують дані опитування, яким було охоплено 140 респондентів з різних регіонів України, однією із перешкод, яка впливає на рівень засвоєння учнями правил безпечної поведінки в інтернеті та зниження інтересу до вивчення питань безпеки, є несистемність заходів. Для усунення цієї перешкоди, на нашу думку, варто більше уваги приділити реалізації принципу наступності. Адже наступність є однією з обов'язкових умов здійснення неперервності здобуття освіти, яка певною мірою має забезпечити єдність, взаємозв'язок та узгодженість мети, змісту, методів, форм навчання й виховання з урахуванням вікових особливостей дітей на суміжних ланках освіти.

Згідно з чинними Державними стандартами освіти початкової та базової/ старшої школи, інформатична освітня галузь передбачає послідовне здобуття очікуваних результатів навчання у розрізі питань безпеки: по 4 результати в 1-4 та 5-6 класах, 8 результатів у 7-9 класах та 10 результатів у старшій школі. Наприклад, наступність у вивченні питання мідіаграмотності на уроках інформатики, проілюстровано у таблиці 1. Аналогічно можна побудувати групи очікуваних результатів з питань безпеки інформаційного простору, цифрової комунікації, правового використання даних в інтернеті, зокрема дотримання авторського права.

Таблиця 1

1-4	5-6	7-9	10-11
Розрізняє правдиві та неправдиві твердження, здобуті з різних джерел [2 ІФО 1.4]	Висловлює припущення про достовірність інформації, отриманої з цифрових джерел, розрізняє факти і судження [4 ІФО 1.4]	Пояснює вплив джерел інформації на формування власних поглядів та інших точок зору [6 ІФО 1.4.1] Будує власні судження про медіатексти, визначаючи достовірність інформації та надійність джерел [6 ІФО 1.4.2]	Аргументує та обстоює власну позицію, використовуючи різноманітні ресурси, порівнює альтернативні погляди з кількох інформаційних джерел [9 ІФО 1.4.1]. Аргументовано доводить/спростовує автентичність медіа (зображень, відео, аудіо тощо) [9 ІФО 1.4.2]. Оцінює роль і розпізнає техніку маніпуляцій і пропаганди в медіатекстах [9 ІФО 1.4.3]. Обґрунтовує негативний вплив інформаційного сміття, дезінформації та емоційного перевантаження на власний добробут [9 ІФО 4.1.1]

Навчально-методичне забезпечення курсу інформатики, яке подане у чинних підручниках, по-різному забезпечує реалізацію очікуваних результатів навчання учнів питань безпеки, зокрема за обсягом, глибиною подання та систематичністю. Через особливість подання навчального контенту в друкованих засобах навчання, є потреба в додаткових інтерактивних засобах, відеоконтенті, анімаціях, навчальних іграх, ситуаційних симуляторах, які б відповідали віковим особливостям учнів. Цю проблему можна вирішити за допомогою навчальних матеріалів, які розроблені на платформі https://it-osvita.diia.gov.ua/ (рис. 1). Слід зазначити, що в розрізі загальної кількості тем, які запропоновані на платформі, розділ «Цифрове громадянство», у якому розглядаються питання, які пов'язані із безпечним використанням інтернету, становить 10%.

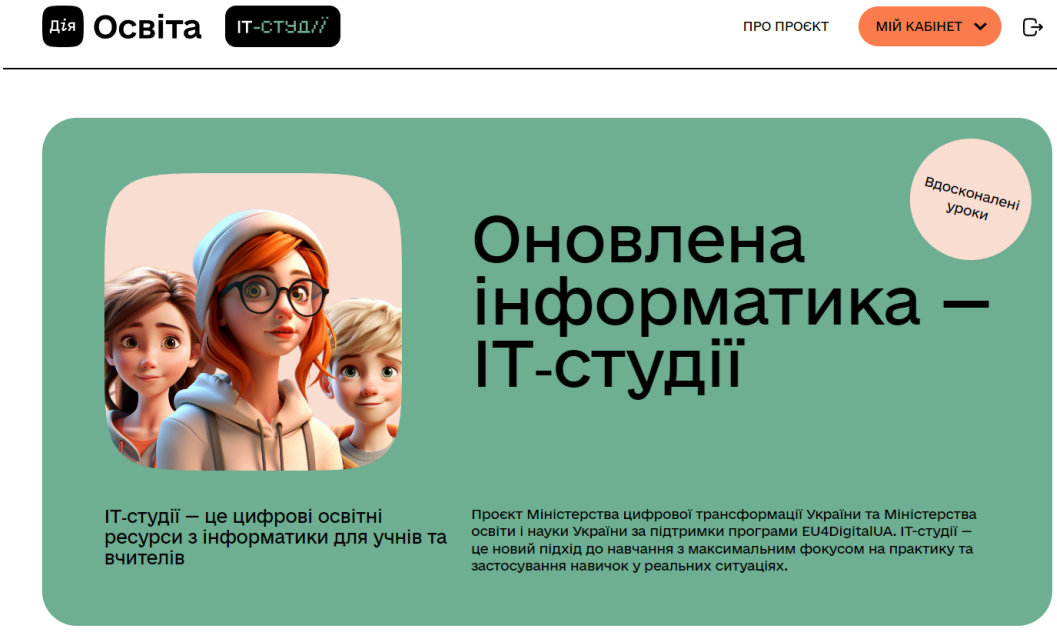

Рис. 1. Екранна копія стартової сторінки платформи ІТ-студії

Навчальний контент на платформі *IT-студій* згруповано за темами та класами (табл. 2).

Таблиця 2

1-2	3-4	5-6	7-9	10-11
1. Я в безпечному цифровому світі	1. Інтернет і його сервіси. 2. Інтернет і його безпечне та відповідальне використання	1. Спілкування та співпраця. 2. Безпека в інтернеті	1. Цифровий портрет. 2. Цифрова гігієна. 3. Цифрова освіта	1. Цифрова ідентичність. 2. Кібербезпека

Наприклад, урок «Безпечна поведінка в інтернеті» із теми 1-2 класу складається із 7 кроків та містить текстові та відеоматеріали, ігри та анімації, тести та завдання (рис. 2).

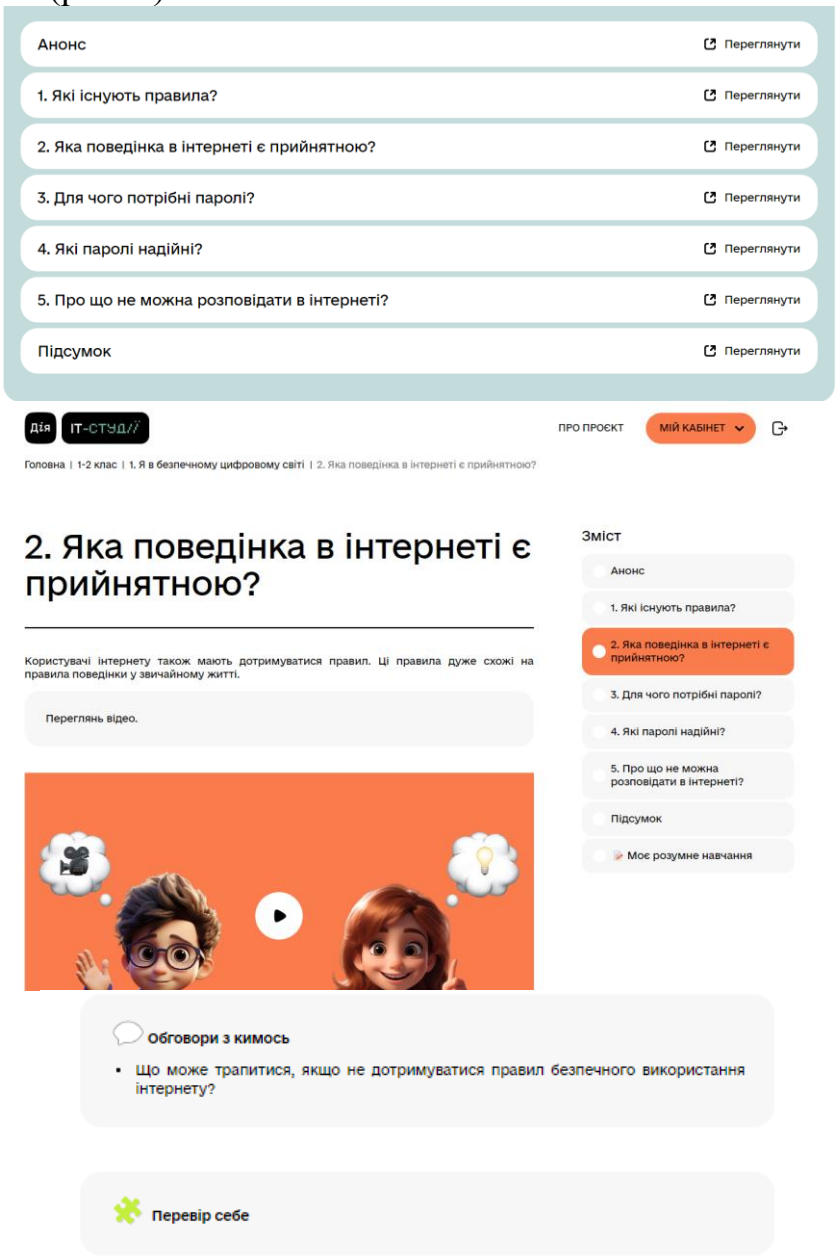

Рис. 2. Екранні копії сторінок платформи IT-студії

Щодо методів навчання основам безпеки в інтернеті, то тут важливо опиратись на основний вид діяльності певної вікової категорії: від гри (предметної, дидактичної, рольової), виконання інтерактивних вправ та самостійного здобування очікуваних результатів до розв'язування ситуацій та завдань на прийняття рішень до навчання за методом проєктів та дослідницько-пізнавальним методом. За типами програм, у яких розглядаються питання інтернет-безпеки [1], послідовність використання на уроках інформатики може бути наступною:

1) Комплексні програми, які охоплюють багато аспектів. Наприклад, https://spoofy.ee.uk – для учнів 1-4 класів, Інтерленд (https://beinternetawesome.withgoogle.com/en_us/interland) послідовно базова школа, https://www.netsmartzkids.org/ - старша школа.

2) Тематичні ігрові застосунки, які розкривають обмежене коло проблем безпеки. Наприклад, Кіберпес https://t.me/kiberpes_bot - 5-6 класи, https://mediasmarts.ca/sites/mediasmarts/files/games/reality-check/index.html#/sites/mediasmarts/files/games/reality-check/ - 7-9 класи.

3) Ігри, які дотичні до теми інтернет безпеки, як правило містять ширші поняття. Наприклад, Медіазнайко (https://www.aup.com.ua/Game/) – 4-5 класи, Пригоди Літературса https://media.am/literatus/?fbclid=IwAR25g5CeZyhCBgP4tqhuHl3WoIPaDy2drJE6YbqKPhC54hjOGIoN-O526ik#uk - 6-7 класи.

Звісно, що пропонований список можна продовжувати та розглядати й інші методи, які є доцільними при навчання питань безпеки.

Як показує практичний досвід, наступність грає важливу роль у формуванні навичок безпечної поведінки в інтернеті, оскільки вона дозволяє учням систематично здобувати знання та формувати навички, необхідні для безпечного та відповідального використання цифрового середовища. Систематичний та послідовний підхід не тільки не переобтяжує учнів надмірною кількістю інформації, а сприяє підвищенню внутрішньої мотивації учнів до навчання та забезпечує формування стійких та усвідомлених алгоритмів дій у різних ситуаціях, які пов'язані із використання інтернету.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Барна О.В., Ворончак В.І. Ігрові додатки для навчання основ інтернет-безпеки. *Сучасні цифрові технології та інноваційні методики навчання: досвід, тенденції, перспективи :* Матеріали XI Міжнародної науково-практичної інтернет-конференції (м. Тернопіль, 6 квітня, 2023), с. 21-25.

2. Петренко С.І. Аналіз проблеми безпечної роботи учнів початкових класів у мережі інтернет. *Вісник університету імені Альфреда Нобеля.* Серія «Педагогіка і психологія». Педагогічні науки. 2020. № 1 (19). С 85-92.

3. Друшяк М. Г. та інші. Типологія інтернет-ресурсів для розвитку інфомедійної грамотності молоді. *Інформаційні технології та засоби навчання*. 2022. Том 88, №2. С. 1–22.

РЕКУРСИВНЕ МИСЛЕННЯ ЗДОБУВАЧІВ ОСВІТИ В УСТАНОВАХ ВИКОНАННЯ ПОКАРАНЬ – УМОВА ФОРМУВАННЯ БЕЗПЕЧНОЇ ПОВЕДІНКИ В МЕРЕЖЕВОМУ ПРОСТОРІ

Вікторія ВОРОЖБІТ-ГОРБАТЮК

Право на освіту є одним із визначальних конституційних прав людини, громадянина України. У контексті розроблення фундаментальної теми «Дотримання прав людини при виконанні покарань і поводженні із засудженими в Україні», РК УкрІНТЕІ № 0121U114397 відділом дослідження проблем кримінально-виконавчого права Науково-дослідного інституту імені академіка В.В. Сташиса Національної академії правових наук України вбачаємо актуальним висвітлення аспекту використання практик рекурсивного мислення здобувачів освіти в установах виконання покарань як ключової умови формування безпечної поведінки у мережевому просторі. У цьому ми бачимо солідний потенціал ресоціалізуючого значення навчальних взаємодій і навчально-пізнавальних комунікацій, які визначаються Порядком організації здобуття повної загальної середньої освіти засудженими до позбавлення волі на певний строк або довічного позбавлення волі, а також неповнолітніми особами, взятими під варту [5].

Заявлена у темі публікації проблема певною мірою висвітлена в сучасних матеріалах, розміщених у відкритому мережевому просторі. Зокрема категорію рекурсії, рекурсивного мислення ми визначили з урахуванням пропозицій і висновків, перезентованих у публікації О. Вознюк [1]. Аспект безпечної поведінки у мережі Інтернет досить системно представлено у навчальному посібнику «Онлайн-безпека учасників освітнього процесу в умовах дистанційного і змішаного навчання» [3], публікації авторства І. Жадан [2]. Правові засади і практичні аспекти реалізації засуджених права на освіту представлено у монографії «Право засуджених на освіту в установах виконання покарань: виклики, рішення, перспективи» [4]. Разом з тим, до цього часу потребує уваги наукової спільноти, участі освітян-практиків до розроблення ключових питань формування критичного, дивергентного, інших типів мислення, що забезпечить сталий розвиток компетентностей інформаційної грамотності і інформаційної безпеки здобувача освіти. Рекурсивне мислення як феномен лише останнім часом набуває популярності, що посилює актуальність цієї публікації.

Рекурсивність як філософський, соціокультурний феномен системно презентовано у книзі «Рекурсивність і контингентність», автор Юк Хуей [6]. Рекурсивне мислення є одним з типів мислення, що допомагає сприймати інформацію критично, розуміти алгоритми подачі інформації чи даних засобом комп’ютерних технологій і цифрових застосунків, передбачає здатність людини будувати виразні, стрункі алгоритми і логічні ланцюжки інформації через різні варіації повторення чогось самоподібним способом. Цікаво, що з точки зору автора О. Вознюк, «у мисленні людини рекурсія реалізується в дипластії – притаманному тільки людській свідомості феномену ототожнення двох елементів, які одночасно виключають один одного, що проявляється в таких психологічних феноменах, як енантіосемія (подвійність, парадоксальність

смислів), «операційна інтеграція», бісоціація – остання, на відміну від асоціативності, є здатністю людини до створення абсолютно нових, нетривіальних зв'язків; це з'єднання того, що ніколи ще не було з'єднане через інтеграцію декількох елементів і формування з них нової цілісності» [1].

На наш погляд, рекурсивне мислення дає змогу здобувачеві освіти, що опановує освітню програму в установі виконання покарань, набути корисного досвіду долати залежності, так звані інформаційні зацикленості, долати негативний вплив таких нових явищ, як інформаційний каскад чи інформаційна кулька. Зокрема, зазначимо тут, що інформаційний каскад відбувається тоді, коли здобувач спостерігає за діями інших, і згодом, попри осмислене розуміння можливих суперечностей чи попередньо сформованого усвідомлення на кшталт «так не можна робити», вчиняє так само не розумно, небезпечно для себе та інших. Фактично інформаційний каскад утворюється, коли здобувач нехтує конструктивним досвідом і висновками на основі поведінки в інформаційному мережевому просторі інших людей. Інформаційна кулька по суті є штучним зовнішнім стандартизатором пошукових систем у мережевому просторі за ключовими словами чи повторюваними комбінаціями клавіш ПК, з яким працює здобувач освіти під час навчання. Інформаційна кулька спрямовує пошук інформації в стандартизовані потоки, тим самим обмежує доступ до відкритої інформації. Це може призвести до однобічного розгляду проблеми чи теми, яку вивчає здобувач освіти, що зазвичай призводить до стереотипного мислення і обмеженого зовнішніми патернами (інколи – нав’язаними чи навіяними кимось) світогляду. Низка інших небезпек в мережевому просторі, з якими стикається здобувач під час онлайн-навчання чи змішаного формату навчальних взаємодій, досить системно представлено у навчальному посібнику «Онлайн-безпека учасників освітнього процесу в умовах дистанційного і змішаного навчання» [3].

Рекурсивне мислення дозволяє здобувачеві освіти навчитися вирішувати проблему за попередньо розробленим алгоритмом, покроковою інструкцією чи повторюваними правилами, розробленими на основі попередніх дій з інформацією чи досвідом перебування в подібній ситуації. Умова успіху рекурсивного мислення: суворе дотримання послідовності, алгоритму, правила тощо, бо без точного виконання дій (операцій) не можна досягти позитивного результату. У цьому бачимо аналогію з комп’ютерною програмою. Процесуально формування рекурсивного мислення у здобувачів освіти в установах виконання покарань передбачає такі спільні дії педагогічного працівника і здобувачів: 1) поділ реальної проблеми інформаційної безпеки здобувача освіти на дрібні проблемні ситуації, операції, конкретні дії, які можна вирішити одним кроком чи одним правилом; 2) анотування, або фокусування уваги здобувача освіти на найважливішій частині інформації, яка може допомогти вирішити проблему інформаційної безпеки (конкретну, реальну, уявну, прогнозовану тощо), ігнорування дрібних аспектів, деталей тощо; 3) розпізнавання зразка, шаблону, що передбачає пошук подібності розглянутої проблеми інформаційної безпеки з іншими, такими, що вирішені успішно, що дозволить вичленити корисне правило, алгоритм дій і перенести уже відпрацьовані такі дії чи правила на реальну ситуацію чи проблему інформаційної безпеки, з якою зіткнувся чи може

зіткнутися здобувач освіти в установі виконання покарань; 4) формування алгоритму, що передбачає розроблення чіткої послідовності дій, покрокової інструкції з безпечної поведінки чи діяльності в інформаційному просторі для того, щоб не потрапити в проаналізовану небезпечну ситуацію, чи успішно її вирішити у разі повторення.

Рекурсивне мислення, регулярні вправи з використання прийомів такого мислення для вирішення проблемних ситуацій у контексті інформаційного мережевого простору сприятиме позитивній ресоціалізації і подальшій адаптації осіб, засуджених до обмеження чи позбавлення волі, у суспільстві.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вознюк О. Рекурсія як фундаментальна характеристика літературного процесу. *Текст і дискурс: когнітивно-комунікативні перспективи*: збірник матеріалів IV Всеукраїнської наукової інтернет-конференції (18–19 березня 2021 р.). Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2021. 118 с. С. 22-24. URL : http://eprints.zu.edu.ua/

2. Жадан І. Інформаційна безпека середовища як чинник розвитку громадянської компетентності молоді. *Проблеми політичної психології*, № *24*(1), 2021. С. 248-257. URL : https://doi.org/10.33120/popp-Vol24-Year2021-77

3. Онлайн-безпека учасників освітнього процесу в умовах дистанційного і змішаного навчання : навч.-метод. посіб. / С. О. Доценко, В. В. Ворожбіт-Горбатюк, Т. М. Собченко. Харків : Вид-во «Ранок», 2021. 192 с.

4. Право засуджених на освіту в установах виконання покарань: виклики, рішення, перспективи : монографія : електрон. наук. вид. / наук. ред. В.В. Пивоваров; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України, Від. дослідж. проблем кримін.-виконав. права. Харків : Право, 2023. 110 с.

5. Про затвердження Порядку організації здобуття повної загальної середньої освіти засудженими до позбавлення волі на певний строк або довічного позбавлення волі, а також неповнолітніми особами, взятими під варту. Постанова Кабінету Міністрів України № 526 від 25 червня 2020 р. URL : https://zakon.rada.gov.ua/laws/show/526-2020-%D0%BF#Text

6. Yuk Hui. Recursivity and Contingency. *Media Philosophy***.** London, 2019. 337 с.

ВПЛИВ МЕДІЙНОЇ ГРАМОТНОСТІ НА ЗАПОБІГАННЯ ОНЛАЙН-ЗАГРОЗ СЕРЕД ДІТЕЙ

Ольга ГАБОРЕЦЬ, Анастасія БАЛАНЕНКО

У сучасному цифровому світі вплив медійної грамотності на запобігання онлайн-загроз серед дітей є актуальною проблемою, що привертає увагу як вчених, так і громадськості. Швидкий та безперервний розвиток інформаційних технологій та Інтернету призвів до значного збільшення доступу дітей до онлайн-ресурсів та цифрового контенту. З одного боку, це відкриває нові можливості для навчання, розвитку та розваг, але з іншого – створює серйозні загрози для фізичного, психічного та соціального благополуччя дітей.

Онлайн-загрози, такі як кібербулінг, контент невідповідного віку, онлайн-домагання та інші форми цифрової агресії, можуть мати серйозні наслідки для психічного здоров'я, самооцінки та соціальної адаптації дітей. Зростаюча кількість випадків онлайн-експлуатації та зловживання цифровими технологіями свідчить про необхідність вивчення та впровадження стратегій медійної грамотності як засобу запобігання цим загрозам.

Медійна грамотність визнається як ключовий компонент сучасної освіти, спрямований на розвиток критичного мислення та аналізу інформації, розуміння медійних засобів та їх впливу на суспільство. Ефективна медійна грамотність дозволяє дітям розрізняти правдиву інформацію від маніпуляційного контенту, усвідомлювати власну цифрову слідку та ризики онлайн-взаємодії, а також адекватно реагувати на потенційно небезпечні ситуації в інтернеті.

Дослідження впливу медійної грамотності на запобігання онлайн-загроз серед дітей є актуальним не лише з практичної, а й з наукової точки зору. Розуміння механізмів, якими користуються діти при сприйнятті та взаємодії з цифровим контентом, а також визначення ефективних методів та програм медійної грамотності, може значно покращити захист дітей в онлайн-просторі та зменшити ризик зіткнення з негативними наслідками цифрової взаємодії. Освітні програми та курси медійної грамотності можуть бути інтегровані в шкільні навчальні плани, організації додаткової освіти, а також в програми підтримки батьків та опікунів, спрямовані на підвищення обізнаності про онлайн-безпеку.

Важливим аспектом упровадження медійної грамотності є розробка віково-адаптованих програм, які враховують психологічні, когнітивні та соціальні особливості дітей різного віку. Це дозволить не тільки навчити дітей безпечному користуванню інтернетом, але й розвинути в них навички критичного мислення, які будуть корисні у всіх сферах життя.

У підсумку, інтеграція медійної грамотності в освітній процес є ключовим елементом у формуванні безпечного та відповідального онлайн-простору для дітей. Вона не тільки сприяє захисту дітей від онлайн-загроз, але й підготовлює їх до життя в сучасному інформаційному суспільстві, де здатність критично мислити та безпечно користуватися інформаційними ресурсами є невід'ємними компонентами успіху.

НАВИЧКИ МЕДІАГРАМОТНОСТІ У ВЗАЄМОДІЇ З УЧАСНИКАМИ ОСВІТНЬОГО ПРОЦЕСУ В ЗАКЛАДІ ДОШКІЛЬНОЇ ОСВІТИ

Людмила ТКАЧЕНКО

На сучасному етапі розвитку суспільства в житті дитини почали все рішуче входити різноманітні гаджети, які загалом збагачують життя [1].

Саме тому перед мною гостро постало питання розвитку медіаосвіти, адже медіа потужно й суперечливо впливають на освіту дошкільників, часто перетворюючись на провідний чинник його соціалізації, стихійного соціального навчання. Завдання педагогів полягає в запобіганні вразливості дитини до медіаманіпуляцій, втечі від реальності в лабіринти віртуального світу, поширенню медіазалежності.

Розглянемо концепцію медіаграмотності та її визначення. Медіаграмотність визначається як рівень культури спільного користування медіа, досягнений через медіаосвіту. Цей рівень включає вміння використовувати інформаційно-комунікативні техніки, виражати себе та взаємодіяти з іншими за допомогою медіазасобів. Факторами медіаграмотності є знання, навички і уміння, які дозволяють аналізувати, критично оцінювати і створювати повідомлення різних жанрів та форматів для різних медіаплатформ. Терміни «медіаграмотність» та «медіаосвіта» часто використовуються взаємозамінно. У США термін «медіаграмотність» частіше застосовується замість «медіаосвіти». Однак у наукових колах медіаграмотність переважно розглядається як результат медіаосвіти.

За думкою американського вченого Роберта К'юбі, медіаграмотність визначається як здатність використовувати, аналізувати, оцінювати та передавати повідомлення в різних формах.

Медіаграмотність – рівень медіакультури, тобто вміння грамотно розуміти реальність, зроблену медіаджерелами, осмислювати владні стосунки, міфи і типи контролю, які вони культивують [8].

Медіакомпетентність – рівень медіакультури, що засвідчує її здатність бути носієм і передавачем медіакультурних смаків і стандартів, ефективно взаємодіяти з медіапростором, створювати нові елементи медіакультури сучасного суспільства [7].

Навчання дітей критичному мисленню в умовах війни є ключовим аспектом медіаграмотності і це питання не втрачає своєї актуальності з 2010 року, коли воно вперше було включено до програми Академії української преси. Як відзначив журналіст Андрій Юричко, у мирний період довіра до неперевіреної інформації може коштувати нервів, грошей і часу, але в умовах війни — це стає питанням людського життя. Тому сьогодні набуває особливого значення розвивати у людей навички оцінки та інтерпретації медійної інформації та вміння розпізнавати маніпулятивний та пропагандистський контент. Медіаосвітні теорії, які вивчаються у сучасних дослідженнях, включають філософську концепцію «діалогу культур» (представлену М. Бахтіном, В. Біблером, Ю. Лотманом та

іншими), аналіз теорій, тенденцій і проблем медіаосвіти за кордоном і в Україні (зокрема, дослідження Д. Бааке, О. Волошенюка, Н. Габор), а також аспекти теорії становлення інформаційного суспільства (представлені Д. Беллом, М. Кастельсом, К. Коліном). У свою чергу, професійна та масова медіаосвіта досліджується в роботах І. Жілавської, Н. Змановської, а також низки інших медіапедагогів, таких як Л. Баженова, О. Баранов, О. Бондаренко, І. Вайсфельд, Л. Зазнобіна, І. Львовшина, Ю. Лотман, С. Пензін, Г. Онкович, Б. Котятинін та інші. Крім того, у розгляді беруться концепції громадянського суспільства та виховання (представлені О. Бєляєвим, Т. Власовою) та теорії розвитку особистості в діяльності та спілкуванні (зокрема, Л. Виготським, В. Давидовим, А. Ельконіним та іншими) [3].

На це спрямовують і державні нормативні акти, Державний стандарт дошкільної освіти — Базовий компонент дошкільної освіти в Україні (далі – БКДО). Так, у Законі України «Про дошкільну освіту» зазначена необхідність модернізації першої освітньої ланки, вдосконалення її змісту, осучаснення освітніх технологій, приведення їх у відповідність до вимог сучасного життя. Базовий компонент дошкільної освіти в новій редакції скеровує педагогів на цілісний підхід до формування дитячої особистості, підготовку її до органічного, безболісного входження до соціуму, природного і предметного довкілля через освоєння основних видів життєдіяльності, а також у напрямку забезпечення реальної наступності та безперервності між дошкільною та початковою ланками, інтеграції родинного і суспільного виховання. Сучасний освітній процес, вимагає від педагогів нового підходу до своєї діяльності, впровадження новітніх форм, методів і технологій виховання, розвитку та навчання дітей.

Однією з актуальних проблем сучасної теорії та практики дошкільної освіти є використання медіаосвіти в освітній процес закладу дошкільної освіти для повноцінного розвитку і формування освітніх компетенцій дошкільника-випускника.

Слід відзначити, що медіаосвіта являє собою частину освітнього процесу, яка має на меті створення в суспільстві високого рівня медіакультури та готовності особистості до безпечної та ефективної взаємодії з сучасною системою мас-медіа. Ця взаємодія включає як традиційні медіа (друковані видання, радіо, кіно, телебачення), так і новітні медіа (комп’ютерне спілкування, Інтернет, мобільна телефонія), з особливим акцентом на врахуванні постійного розвитку інформаційно-комунікаційних технологій (ІКТ). Вона є своєрідним «інтелектуальним знаряддям», що дає людині змогу вийти на новий інформаційний рівень. Можна розглядати і як сучасний засіб діяльності старшого дошкільника. Дитина, яка опанувала елементарну цифрову компетентність, здатна краще розмірковувати, розв’язувати завдання не тільки з опорою на наочність, але й у внутрішньому (мисленнєвому) плані, почуватися впевненою у власних силах [1].

Результатом медіаосвіти має бути підвищення рівня медіакомпетенції, або її ще називають медіаграмотність. Це здатність експериментувати, інтерпретувати, аналізувати, оцінювати та створювати медіатексти та ін.

Необхідність розвитку медіаосвіти та медіаграмотності саме в дошкільному віці зумовлена декількома факторами.

По-перше, дошкільний вік є надважливим періодом для інтелектуального, фізичного та психоемоційного розвитку дитини.

Подруге, сучасна дитина до моменту вступу до школи активно спілкується з телевізійною, комп'ютерною технікою, володіє навичками спілкування з мобільною телефонією тощо.

По-третє, діти, що стикаються з постійним потоком інформації, відчувають значні труднощі — не можуть самостійно критично оцінити отриману інформацію.

Робота з використанням медіаосвіти в освітньому процесі закладу орієнтується на три основні напрями:

1) співпраця педагогів закладу;

2) освітня робота зі здобувачами освіти;

3) взаємодія з батьками вихованців.

Отримана медіакультура серед педагогів та батьків сприятиме ефективному вирішенню завдань, пов'язаних із готовністю дітей взаємодіяти із засобами масової комунікації під час соціалізації. Це дозволить забезпечити захист від потенційно шкідливих впливів медіа та виховати компетентного споживача медіа, який здатний ефективно користуватися різноманітними медіазасобами.

Важливо відзначити виклики, що виникають при впровадженні медіаосвіти в дошкільному закладі, на які варто звертати увагу. Серед них – недостатнє матеріально-технічне забезпечення, відсутність програмного забезпечення, обмежена доступність та низька швидкість інтернет-підключення. Також на долю викликів припадає неприйняття батьків щодо використання цифрових технологій у дошкільних закладах, а також обмежена інформаційно-технічна компетентність деяких педагогів, а часом і їхня небажання чи низька мотивація.

У контексті воєнного стану в Україні особливу увагу слід приділяти медіаосвіті в дошкільних закладах, оскільки саме вони виступають ключовими фігурантами у освітньому процесі та взаємодіють з учасниками освітньої діяльності. Результати спільної роботи значною мірою залежать від їхньої ефективності. Під час професійного розвитку педагогів дошкільних закладів слід звернути увагу на передовому ознайомленні з інноваціями в галузі медіаосвіти.

Саме тому в нашому закладі творчою групою організовано просвітницьку роботу з педагогічними працівниками закладу, зокрема: консультації, семінари, практикуми, майстер-класи, обмін досвідом, створення єдиної платформи для вихователів. Творча група дошкільного закладу постійно проводить серію практичних занять для педагогічних працівників закладу, на яких ми ознайомилися з Google та його додатками, віртуальною дошкою Padlet, обмінювалися досвідом використання в роботі онлайн-сервісів та платформ. Для надання педагогічної та консультативної допомоги створила Google blog «Педагогічна вітальня вихователя» [10].

Варто зазначити, що я налагодила партнерські відносини з батьками вихованців, тому їх активно залучаю до освітнього процесу. Освітня програма для дітей від 2 до 7 років «Дитина» рекомендує забезпечити заочний

(онлайновий) характер спілкування з батьками вихованців (сайт, блог, сторінки в Інтернет-мережі, viber-групи, Telegram-канали, чати, відеоконференції Meet) [4]. Виконуючи вимоги БКДО та Освітньої програми, спілкування з батьками організовую з використанням різних інструментів, проводжу анкетування за допомогою Google Форм, відеоконференції Google Meet, ZOOM, використовую віртуальну дошку Jamboard Google для проведення батьківських зборів. На основі отриманих відео чи аудіоматеріалів створюю відеосюжети, які надсилаю батькам у Viber-групу та Viber-канал, батьки активно відгукуються на такий підхід, беруть участь у заходах, які їм пропоную. У цілому творча група СДНЗ №65 сформувала в закладі медіаосвіту педагогів, дошкільників та їх батьків, яка є важливою умовою формування медіакомпетентності усіх учасників освітнього процесу. Роботу з даного питання продовжуємо, шукаємо шляхи поліпшення, нові підходи.

Висновок. Отже, можна зазначити, що використання медіазасобів в дошкільних навчальних закладах є ефективним і корисним, сприяючи гармонійному розвитку особистості дитини. Ці засоби відкривають нові можливості для досягнення визначених цілей у вихованні та розвитку дошкільників.

Основною метою використання медіа в дошкільних установах є формування у вихованців медіакультури та готовності ефективно взаємодіяти з сучасним інформаційним середовищем. Педагогам важливо забезпечувати підготовку дітей до використання медіа, навчаючи їх правильно користуватися інформацією та захищати себе від медіаманіпуляцій. Крім того, важливо уникати вразливості дітей до впливу віртуального світу і запобігати розвитку медіазалежності.

Медіаосвіта вважається не лише елементом освітнього процесу, але й основним правом кожного громадянина на свободу висловлювання та доступу до інформації. Завдання вихователів у цьому контексті полягає в ефективному навчанні дітей використовувати цю інформацію та захищати себе від негативного впливу медіа.

.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Базовий компонент дошкільної освіти та Методичні рекомендації до Базового компонента дошкільної освіти (Державного стандарту дошкільної освіти. К., 2021.

2. Концепція впровадження медіаосвіти в Україні (нова редакція). Detector.media : вебсайт. URL: https://ms.detector.media/mediaosvita/post/16501/2016-04-27-kontseptsiya-vprovadzhennya-mediaosvity-v-ukraini-nova-redaktsiya.

4. Дитина : Освітня програма для дітей від двох до семи років/наук. кер. Проєкту В.О. Огнев'юк; авт. Г.В. Бєлєнька та ін.; наук.ред. Г.В. Бєлєнька; Київ. ун-т Б.Грінченка, 2020. 440 с.

5. Роєва Т.Г. Дидактичний мультимедійний контент для дошкільної освіти «КМ MEDIA ED Profi». Чернігів: ККМЕДІА, 2021.

6. Дегтярьова Г.А. Особливості організації занять з аналізу й декодування аудіовізуальної продукції : презентація. URL: https://www.aup.com.ua/uploads/Metodyka_mediaosvitnix.pdf.

7. Крутій К.Л. Медіадидактичні особливості використання мультфільмів як засобу навчання мови і розвитку зв‘язного мовлення дошкільників. Медіаосвіта в Україні: наукова рефлексія викликів, практик, перспектив : зб.статей методолог. семінару / Нац. акад. пед. наук Укр. Інст. соц. та політ. психол. (Київ, 3 квітня 2013 р.) К. 2013. С.385.

8. Вікіпедія : вільна енциклопедія. URL: https://cutt.ly/N1dM6uP

9. Detector.media : вебсайт. URL: https://ms.detector.media/print/20202/

10. Сайт вихователя ЗДО : вебсайт. URL: http://surl.li/lknbq

СОЦІАЛЬНО-ПЕДАГОГІЧНИЙ ВИМІР ПОНЯТЬ «ЦИФРОВІ СЛІДИ», «ЦИФРОВІ ТІНІ»

СОЦІАЛЬНО – ПЕДАГОГІЧНИЙ ВИМІР ПОНЯТЬ «ЦИФРОВІ СЛІДИ», «ЦИФРОВІ ТІНІ»

Ірина ОРЕЛ

Щоденно інтернет-користувачі генерують ексабайти даних: пошукові запити та поштові сервіси, мобільні банкінги, відео та фотохостинги, чати в соціальних мережах. В результаті кожен залишає цифровий слід та цифрову тінь. Про те, які наслідки це принесе для користувачів, поговоримо в нашій статті [4].

Цифровий слід – це сукупність інформації про те, що користувач перебував у мережі. Розрізняють два види цифрових слідів: пасивні та активні. ***Пасивний цифровий слід –*** це дані, зібрані автоматично без відома власника. ***Активний цифровий слід*** з'являється, коли користувач навмисно публікує свої персональні дані на сайтах і в соцмережах [2].

Активні цифрові сліди часто можна знайти за реальним іменем людини. Їхнє поширення залежить не тільки від автора допису чи коментаря, а й від людей, які реагують на нього, роблячи вподобання, репости тощо.

Бажано регулярно слідкувати за своїм цифровим слідом, наприклад, шукаючи інформацію про себе в пошукових системах за іменем і прізвищем. Головний спосіб запобігти негативним наслідкам цифрового сліду – це обмежити його зміст налаштуваннями конфіденційності своїх облікових записів у соцмережах, сервісах, інтернет-магазинах та інших сайтах, де може публікуватися особиста інформація. Наприклад, заборонити бачити свої дописи всім, крім друзів; лишати мінімум конфіденційної інформації в реєстраційних формах; захищати свої дані надійними паролями та пін-кодами; користуватися анонімним режимом програм-вебоглядачів; видаляти історію відвідувань вебсайтів після користування чужим пристроєм.

Для різних активностей у мережі доцільно користуватися різними електронними адресами. Рекомендується слідкувати за згадками про себе від інших людей. Іноді варто попросити їх видалити дописи, коментарі з такими згадками, щоб не поширювати надмірні деталі.

Слід заздалегідь мати план дій на випадок втрати свого пристрою, що містить конфіденційні дані, мати резервні копії важливої інформації та можливість дистанційно її знищити. Свої неактивні облікові записи варто видаляти.

Інформація про користувача, що створюється без його участі, отримала назву «**цифрової тіні**», яка виникає і накопичується щоразу, коли хтось шукає користувача через пошукові системи, коли відбувається електронна поштова розсилка за списками, в яких він фігурує і в багатьох інших випадках. Індексація роботами пошукових машин сторінок з інформацією користувача і їх подальше кешування – це теж створення «цифрової тіні», доступної кожному. Крім «цифрових тіней відкритого доступу», створюються і накопичуються «цифрові тіні обмеженого доступу» – записи камер спостереження, банківські транзакції, сервіси продажу квитків, телефонних дзвінків тощо [1].

Цифрова тінь - явище доволі небезпечне. З поліпшенням якості фото- та відеотехніки, зростанням обсягу пам'яті та швидкості Інтернету, вона буде ставати все більш осяжною і небезпечною. Найголовніша небезпека цифрової тіні полягає в тому, що люди не в змозі її контролювати. З часом вона буде структурована, між тінню і цифровим слідом вже не залишиться різниці, і саме тоді настане кінець конфіденційності. А поки слід не здійснювати вчинків, за які доведеться виправдовуватися або відповідати за законом, адже ваша цифрова тінь вже сьогодні формує вашу «цифрову честь» та порядне ім'я. Варто використовувати «мережеву гігієну» та аналізувати свої дії, особливо в публічних мережах – це дозволить мінімізувати ризики [3].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ланде Д.В. Керування репутацією в інформаційних мережах. *Правова інформатика.* Науковий фаховий журнал з питань інформатики, інформатизації, інформаційного права та інформаційної безпеки. К.: Науково-дослідний інститут інформатики і права Національної академії правових наук України, 2013. № 3(39). С.3-10.

2. Цифровий слід. Вікіпедія : вільна енциклопедія. URL: https://uk.wikipedia.org/wiki (дата звернення: 21.0.2024).

3. Цифровий слід і безпека. Лекція. CCC'2019 : вебсайт. URL: https://www.victoria.lviv.ua/library/students/sss2017/theme10.html (дата звернення: 21.01.2024).

4. Які загрози несуть за собою збирання користувацьких даних? Безпека : блог. URL: https://www.imena.ua/blog/data-collection/ (дата звернення: 21.01.2024).

СТВОРЕННЯ ЯКІСНОГО БЕЗПЕЧНОГО УКРАЇНОМОВНОГО КОНТЕНТУ В МЕРЕЖІ ІНТЕРНЕТ: ТРЕНДИ, РОЛІ, МОЖЛИВОСТІ

РОЗВИТОК УКРАЇНОМОВНОГО КОНТЕНТУ В МЕРЕЖІ ІНТЕРНЕТ

Денис ВАСИЛЬЄВ

За останні роки спостерігається значний розвиток та популяризація контенту, створеного мовою, яка відображає національну самобутність України. Цей розвиток не лише сприяє збереженню та відтворенню культурної спадщини країни, але й відкриває нові можливості для спілкування, розвитку освіти, й розширення медійного простору.

Україномовний контент у мережі Інтернет не лише відображає розвиток мови, але й стає важливим інструментом для висловлення та сприйняття ідентичності. Це середовище активно дозволяє не лише споживати контент, але й активно спілкуватися, обмінюватися ідеями та власним досвідом [1].

Зростаюча популярність україномовного контенту свідчить про зростання зацікавленості аудиторії українською культурою, мовою та ідентичністю. Важливо відзначити інноваційність цього процесу, оскільки розвиток технологій дозволяє зростати якісному, доступному та різноманітному контенту українською мовою.

Цей розвиток стимулює не лише самовираження, але й сприяє підвищенню освіченості, розвитку креативності та національної самосвідомості. Наприклад, збільшення україномовних освітніх платформ сприяє доступності знань та розвитку освіти в країні.

Розглядаючи цей розвиток, можемо бачити важливість україномовного контенту як каталізатора для впровадження позитивних змін у суспільстві та розвитку національної культури.

На YouTube україномовний контент набуває популярності та розмаїття в різних категоріях, від розважального до освітнього та інформаційного:

– ***Блоги та ігрові канали:*** україномовні блогери діляться своїм життям, подорожами, досвідом та різноманітними ігровими контентами. Наприклад, канали, які присвячені геймінгу чи розвагам, а також подкасти про ігрову індустрію.

– ***Освітні канали:*** пропонують українською мовою освітні відео на різні теми: від наукових досліджень до підготовки до вступних іспитів чи навчання мовам.

– ***Кулінарні канали:*** демонструють рецепти, готують страви та діляться кулінарними хитрощами та секретами.

– ***Творчі проєкти:*** присвячені мистецтву, музиці, літературі, які демонструють творчий процес, навчають різним мистецьким навичкам чи виконують музичні кавери.

Це лише декілька прикладів, які показують різноманіття україномовного контенту на YouTube. Ці канали не лише розважають та навчають глядачів, але й

сприяють збільшенню культурного обміну та розвитку української спільноти в онлайн-середовищі.

Платформа TikTok стала місцем, де українська мова набуває нового життя. У морі коротких відеороликів, що майстерно танцюють під улюблені мелодії, жартують або діляться корисними порадами, звучить вільний та емоційний український голос.

Тут танцюють під різноманітні музичні біти, створюють власні челенджі та хореографію під улюблені треки, вирізняючи унікальність та креативність україномовної спільноти. Комедійні скетчі з сатиричним гумором ширять усмішки та заряджають позитивом.

Це не лише розважальний простір. Тут з'являються короткі відеоролики зі знаннями, де користувачі вчать новому, діляться корисними порадами або цікавими фактами. Така форма підвищує доступність знань та робить їх більш зрозумілими та захоплюючими.

Артисти та творчі особистості використовують TikTok для демонстрації свого мистецтва – малюнки, музичні кавери, роботи рукоділля – усе це знаходить своє місце в цьому калейдоскопі відео.

Платформа стала своєрідним вікном у світ життя, подорожей та вражень користувачів. Відео про щоденні моменти, подорожі, рецепти, поради – все це звучить українською мовою, віддзеркалюючи багатство та різноманіття української культури.

TikTok став місцем, де українці можуть вільно та творчо виражати себе, ділитися своїми ідеями, враженнями та культурним спадщиною, зближуючи спільноту та створюючи особливий простір для відчуття та розвитку української спільноти [2].

Україномовна музика в Україні за останні два роки пережила захопливий розвиток, відображаючи не лише музичні тенденції, а й суспільні зміни та почуття українського народу. Період 2022-2023 років відзначився різноманіттям жанрів, якістю виконання та актуальністю текстів, що зробило україномовну музику досить популярною та запитуваною.

У цей період виразний розвиток пройшли різні жанри від популярної та електронної музики до року, репу та фольку. Артисти активно експериментували зі звучанням, впроваджуючи сучасні музичні тенденції та техніки в українську музику.

Також було помітно підвищення уваги до текстів пісень. Багато виконавців звертали увагу на соціально-політичні питання, відображаючи реальність та почуття українського суспільства. Тексти стали більш проникливими та містичними, що стимулює слухачів роздумувати та відчувати емоції.

Крім того, успіх україномовної музики був підтверджений не лише внутрішньою популярністю, але й поза межами країни. Україномовні виконавці привертали увагу міжнародної аудиторії, показуючи високий рівень музичної культури та таланту.

Україномовна музика за останні два роки стала не лише засобом вираження емоцій, а й важливим культурним феноменом, який сприяє об'єднанню нації, відображає реальність та почуття, інспірує та дарує позитивні емоції.

Розвиток україномовного контенту в мережі Інтернет став ключовим фактором у висвітленні української культури, мови та ідентичності. Популярність та розмаїття україномовного контенту на різних платформах свідчить про активну участь громадськості та зацікавленість аудиторії у власній культурі та спільноті.

Цей розвиток не лише сприяє збереженню культурної спадщини, але й розширює можливості спілкування, взаєморозуміння та обміну ідеями. Україномовний контент відображає різноманіття життя, талантів та переконань, спонукаючи до рефлексії та об'єднуючи спільноту.

Цей розвиток також показує важливість мови як інструменту самовираження та збереження національної ідентичності в умовах сучасного цифрового світу. Україномовний контент в мережі Інтернет збагачує культурний ландшафт країни, сприяючи розвитку спільноти та підвищенню інтересу до української культури та мови як ніколи раніше.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Як гуглити україномовний контент. *Словопис: вебсайт.* URL: https://slovopys.kubg.edu.ua/iak-guglyty-ukrainomovnyi-kontent/ (дата звернення: 24.12.2023).

2. На кого підписатися у TikTok: гайд українськими трендами, блогерами та жанрами. *Suspilbe: вебсайт.* URL: https://suspilne.media/culture/512059-na-kogo-pidpisatisa-u-tiktok-gajd-ukrainskimi-trendami-blogerami-ta-zanrami/ (дата звернення: 25.12.2023).

3. UA YouTube: чим живе україномовний ютуб? *Informer: вебсайт.* URL: https://news.informer.od.ua/ua-youtube-chim-give-ukrainomovnii-youtube (дата звернення: 25.12.2023).

ШТУЧНИЙ ІНТЕЛЕКТ У ОСВІТНЬОМУ ПРОЦЕСІ: СУЧАСНІ ТЕНДЕНЦІЇ

Олена КРАВЧЕНКО

Україна знаходиться на шляху до інтенсивної реформи освіти, орієнтованої на створення інноваційного освітнього середовища. Головна мета полягає в тому, щоб забезпечити учнів та студентів ключовими компетентностями, необхідними для їхнього успіху в сучасному світі. Одночасно ця реформа надає науковцям можливості та ресурси для проведення досліджень, спрямованих на соціально-економічний та інноваційний розвиток країни.

Ключовим інструментом цієї освітньої трансформації стає цифрова трансформація, що передбачає впровадження сучасних технологій у освітній процес. Це включає в себе використання інформаційних систем, мобільних пристроїв та інших технологічних гаджетів.

У сучасних умовах штучний інтелект (ШІ) стає не лише важливим, але й невід'ємним елементом освітнього простору сучасності, надаючи нові можливості та змінюючи підходи до викладання та навчання. «Швидкий прогрес у сфері штучного інтелекту (ШІ) за останні десятиліття відкриває нові горизонти для наукових досліджень у всьому світі, зокрема в Україні. ШІ, суть якого полягає в здатності комп'ютерних систем розуміти, вивчати та ухвалювати рішення на підставі обробки великого обсягу даних, стає невід'ємною частиною сучасного життя» [1]. Актуальність вивчення можливостей ШІ в освіті зумовлена потребою в адаптації навчального процесу до вимог сучасного суспільства.

Штучний інтелект, відповідно до Концепції розвитку штучного інтелекту в Україні – це «організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань» [3].

Інструменти штучного інтелекту базуються на концепції машинного навчання, що передбачає необхідність великих обсягів даних для ефективного навчання. Під час взаємодії з моделями штучного інтелекту важливо враховувати, що їхнє навчання ґрунтується на великих наборах даних, створених раніше.

Також важливо пам'ятати, що генеративні змагальні мережі, які є основою штучного інтелекту, функціонують на засаді «усереднення» наявної інформації. Результати роботи цих мереж значно залежать від характеру даних, на яких вони були навчені, і можуть бути очікувані відповідно до цієї особливості. Важливо враховувати, що технологія лише пропонує користувачеві інформацію та рекомендації на основі доступного банку даних.

Сучасний штучний інтелект відкриває широкі перспективи для трансформації та покращення процесів навчання, роблячи їх більш ефективними та захопливими. Низка технологічних рішень, які використовуються у сфері штучного інтелекту, можуть допомагати навчальним установам, вчителям та учням на кожному етапі освітнього процесу.

Використання ШІ у навчанні приводить до наступних ключових трансформацій. Можливість персоналізованого навчання стає реальністю завдяки алгоритмам ШІ, що аналізують академічний прогрес, стиль навчання та інші індивідуальні параметри. Це дозволяє створювати індивідуальні програми навчання для оптимального розвитку кожного учня. Використання адаптивних та інтерактивних методів стає реальністю через можливості ШІ. Електронні платформи можуть адаптуватися до рівня знань та інтересів учнів та студентів, що забезпечує більший контроль та активну участь у власному процесі навчання.

Застосування гейміфікації в освіті стає доступним завдяки ШІ. Системи генерації ігрових сценаріїв та гейміфікації стимулюють інтерес та активність студентів за допомогою графіки, інтерактивних завдань та систем винагород. Додатково, ШІ забезпечує аналіз великих обсягів даних для вдосконалення

навчального процесу та виявлення трендів у розвитку студентів. Такий підхід дозволяє вчасно реагувати на труднощі учнів та оптимізувати навчальні плани.

Крім того, ШІ сприяє розвитку систем, що забезпечують доступ до освітніх ресурсів в регіонах з обмеженим доступом або для осіб з обмеженими можливостями. Це робить навчання більш доступним та інклюзивним. Усі ці аспекти допомагають зробити освітній процес більш динамічним та сприяють підвищенню якості навчання.

Штучний інтелект не замінить викладача, проте він надасть нових можливостей і викладачеві і здобувачеві освіти за умов, якщо:

– знати й розуміти всі можливості ШІ;

– уміти ефективно використовувати ШІ;

– критично оцінювати згенерований матеріал.

Штучний інтелект варто сприймати як партнера, що може вибудовувати діалог зі співрозмовником, відхиляти недоречні запитання, відповідати на складні запитання; як віртуального інтелектуального помічника; як мовленнєвий тренажер; як асистента викладача в організації персоналізованого навчання.

Завдання педагога – допомогти здобувачеві освіти коректно й ефективно використовувати ШІ в навчальній діяльності. Для цього потрібно навчитися працювати з великими мовними моделями безпечно й контрольовано як із віртуальним помічником (асистентом).

Застосування штучного інтелекту в освітньому середовищі не є безпроблемним і викликає певні виклики та проблеми. Однією з ключових етичних проблем є використання ШІ учнями як інструменту, замість розвитку власної творчості та критичного мислення. Учні, користуючись готовими алгоритмами та моделями ШІ, стикаються із ризиком зменшення активності у власному навчальному процесі. Це може призвести до втрати стимулу для творчого мислення та самостійного вирішення завдань.

Питання етики використання ШІ також пов'язане із можливістю порушення академічної доброчесності. У разі використання штучного інтелекту для написання робіт чи виконання завдань існує ризик втрати автентичності та оригінальності робіт, що може підірвати основи академічної доброчесності.

Крім того, питання безпеки та конфіденційності викликає занепокоєння, оскільки ШІ працює з особистою інформацією учнів для адаптації навчання. Недостатня захищеність цих даних може призвести до непередбачуваних наслідків, таких як недостатній рівень приватності або можливість зловживання інформацією.

Нарешті, використання ШІ породжує питання про підготовку педагогічного персоналу та їхню здатність адаптуватися до нових технологій. Забезпечення вчителів необхідними компетенціями для ефективної співпраці з системами ШІ є ключовим аспектом успішної інтеграції цих технологій в освітній процес.

Отже, важливо забезпечувати баланс між застосуванням технологій штучного інтелекту та збереженням важливих навичок та цінностей, які стимулюють розвиток критичного мислення. Попередні дослідження вказують на потенційну користь використання штучного інтелекту в освіті, проте важливо

уважно аналізувати його вплив на процес навчання та ретельно враховувати можливі ризики та виклики.

Потенціал використання штучного інтелекту в освіті є значущим і може сприяти вирішенню низки проблем, що існують у сучасних системах освіти. Однак існують виклики та обмеження, пов'язані з розробкою та впровадженням надійних та етичних алгоритмів, які забезпечують безпеку користувачів.

Продовження досліджень в сфері застосування штучного інтелекту в освіті є необхідним для виявлення нових можливостей для оптимізації освітнього процесу та підвищення ефективності навчання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бердо Р., Расюн В., Величко В. Штучний інтелект та його вплив на етичні аспекти наукових досліджень в українських закладах освіти. *Академічні візії.* 2023. Вип. 22. URL : https://zenodo.org/records/8174388 (дата звернення: 02.02.2024).

2. Візнюк І. Використання штучного інтелекту в освіті. *Сучасні інформаційні технології та інноваційні методики навчання в підготовці фахівців: методологія, теорія, досвід, проблеми.* 2021. № 59. С. 14–22.

3. Концепція розвитку штучного інтелекту в Україні: схвалено розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 02.02.2024).

4. ChatGPT Complete Guide: Learn Midjourney, ChatGPT 4 & More. URL : https://ua.udemy.com/course/complete-ai-guide/ (дата звернення: 02.02.2024).

5. ChatGPT: Complete ChatGPT Course For Work 2023 (Ethically). URL : https://ua.udemy.com/course/chatgpt-complete-chatgpt-course-for-work-2023-ethically-chat-gpt/ (дата звернення: 02.02.2024).

ЕВОЛЮЦІЯ CHATGPT: ВІД МОВНОЇ МОДЕЛІ ДО ІНТЕЛЕКТУАЛЬНОГО ПОМІЧНИКА

Ольга ЛИТВИНЕНКО

Освіта 4.0 – це концепція освіти, яка передбачає використання новітніх технологій для покращення процесу навчання та підготовки здобувачів освіти до життя в цифровому суспільстві і базується на принципах гнучкості, індивідуалізації, колаборації та розширеного навчання.

Метою освіти 4.0 є не тільки підготовка здобувачів освіти до цифрової економіки та роботизації праці, але й формування громадян, які можуть діяти в сучасному світі, критично і творчо мислити, розвивати навички життєвого та професійного самовдосконалення.

Для реалізації концепції освіти 4.0 необхідно забезпечити доступ здобувачів освіти до сучасних технологій, відповідної інфраструктури та належного педагогічного супроводу. До основних технологій, які використовуються в освіті

4.0, належать штучний інтелект, віртуальна реальність, інтернет речей, машинне навчання та інші.

Штучний інтелект – один із найзатребуваніших і найперспективніших напрямів в умовах загальної цифровізації. Що ж таке штучний інтелект? Це галузь інформатики, яка займається створенням комп'ютерних систем, здатних здійснювати розумові процеси, які зазвичай пов'язують зі здатністю людини мислити та розв'язувати проблеми.

Основні властивості штучного інтелекту включають:

- Навчання: ШІ може вдосконалювати свої здібності, збираючи та аналізуючи дані, здійснюючи прогнози та підбираючи найбільш оптимальні рішення.
- Розуміння мови: ШІ може розуміти людську мову та взаємодіяти з людьми, включаючи голосові та текстові команди.
- Сенсорна сприйнятливість: ШІ може збирати та аналізувати інформацію з різних джерел, включаючи зображення, звук та сенсорні дані. − Можливість прийняття рішень: ШІ може приймати рішення на основі зібраної інформації та розуміння контексту.
- Креативність: ШІ може генерувати нові ідеї та рішення, які раніше не були знайдені. Швидкість та точність: Штучний інтелект (ШІ) працює на основі алгоритмів, які дозволяють йому виконувати певні завдання. Одним з підходів є генеративні моделі, які використовують глибокі нейронні мережі, щоб згенерувати нові зображення, що відповідають певному запиту (промту).

ChatGpt – це чат-бот зі штучним інтелектом, прототип якого випустили в листопаді 2022 року. Він може працювати з текстом, програмним кодом, формулами та числами – генерувати все, що йому зададуть.

Завдяки можливостям ChatGpt педагоги можуть створювати якісний україномовний контент для викладання навчальних предметів.

Приклад 1. Опануйте підхід явного навчання. Разом з ChatGPT розробляйте плани уроків згідно з програмою і враховуйте потреби ваших здодувачів освіти. Наприклад, використайте промпт: «Створи план уроку про [тему, що викладається], який охоплює різні завдання та методи оцінювання, а також містить абзац, де я надам короткий опис навичок і знань моїх здобувачів освіти».

Приклад 2. Поясніюйте, моделюйте, направляйте. Використовуйте ChatGPT, щоб створювати візуальні матеріали, наприклад, слайди або робочі аркуші, згідно з навчальними цілями та критеріями успішності уроку. Введіть такий запит: «Розроби план уроку з навчальними цілями, творчими завданнями та критеріями успішності уроку з [теми, що викладається]».

Приклад 3. Контролюйте прогрес здобувачів освіти і перевіряйте, як вони розуміють матеріал. Використовуйте ChatGPT, щоб створити запитання для оцінювання, перевірити, як здобувачі освіти розуміють тему, та визначити прогалини. Наприклад, використайте такий запит: «Створи 5 запитань із декількома варіантами відповіді, які оцінюють, як здобувачі освіти розуміють [тему, що викладається]».

Приклад 4. Поясніть здобувачам освіти терміни з програми навчальної дисципліни. Використовуйте ChatGPT, щоб створити словник термінів і визначень, які стосуються програми або навчального блоку. Введіть такий запит у ChatGPT: «Створи глосарій термінів і визначень для розділу про [тему, яка викладається]».

Приклад 5. Створення сторітеллінгу. Попросіть ChatGPT занурити вас у пригодницьку історію. Введіть промпт: «Я намагаюся краще зрозуміти причини війни Червоної та Білої троянд. Створи цікаву пригодницьку історію з різними варіантами розвитку подій і постійно пропонуй мені вибрати варіант, перш ніж перейти до наступної частини оповіді». Це занурить вас в історію, якою ви керуєте самостійно. Організуйте заняття для закріплення матеріалу, де учні можуть поділитися своїми історіями, рішеннями та результатами з певної теми.

Пам’ятаємо, що використання CHATGPT передбачає, що педагог навчиться правильно чітко формулювати запити (промти) та **ПРИДІЛЯТИМЕ ЧАС ПЕРЕВІРЦІ БОТА!**

Презентація - ChatGPT – інноваційний помічник вчителя

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про схвалення Концепції розвитку штучного інтелекту в Україні. Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 20.01.2024).

2. Програма великої трансформації «Освіта 4.0: український світанок». URL: https://mon.gov.ua/ua/news/ministr-osviti-i-nauki-ukrayini-prezentuvav-programu-velikoyi-transformaciyi-osvita-40-ukrayinskij-svitanok (дата звернення: 20.01.2024).

3. ISO/IEC TR 24028:2020(en) Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence URL: https://www.iso.org/standard/77608.html (дата звернення: 20.01.2024).

4. Штучний інтелект. Як він вплине на освіту. URL: https://nus.org.ua/articles/shtuchnyj-intelekt-yak-vin-vplyne-na-osvitu/ (дата звернення: 20.01.2024).

5. Ґайд із промптами для вчителів ChatGPT - Студія онлайн-освіти EdEra — українська EdTech-компанія, що створює онлайн продукти: курси, інтерактивні підручники, освітні блоги та спецпроєкти. URL: https://educationpakhomova.blogspot.com/2023/05/chatgpt_27.html (дата звернення: 20.01.2024).

ІНСТРУМЕНТИ ВЧИТЕЛЯ-СЛОВЕСНИКА І РЕАЛІЇ СЬОГОДЕННЯ

Тетяна СІКОРСЬКА

На сьогоднішній день, я, як вчитель, не уявляю свій урок без використання цифрових технологій. І це не дивно, адже сучасні діти не будуть сприймати звичайний урок. А разом з тим учні вчаться сприймати, шукати та обробляти інформацію правильно.

Реалії сьогодення такі, що онлайн-навчання, завдання не у зошиті, а на певному порталі, підручники не завжди паперові, а електронні. І я маю навчити дітей правильно цим користуватися, відсіювати непотрібну інформацію.

Використання цифрових технологій в освітньому процесі – одна із найголовніших тенденцій до розвитку сучасного освітнього процесу. Вони неймовірно допомагають вчителеві провести урок, учням – у підготовці до уроку, але варто завжди пам’ятати: допомагають, а не повністю замінюють урок. Я помітила, що за допомогою різноманітних цифрових технологій на уроці можна опрацювати набагато більше інформації.

Мені, як вчителю-словеснику, у цьому дуже допомагає ***Canva***, віртуальна дошка ***Padlet*** та інші.

Візьмемо дошку ***Padlet.*** Вчить учнів не тільки розміщувати свої варіанти відповідей, працювати у групі, але і ознайомитись із цим цифровим засобом. Дуже зручно дистанційно перевіряти групові проєкти, завдання, а головне – швидко.

Додаток Canva я використовую лише як вчитель. Тобто мені зручно створювати роздатковий матеріал: *сторінки героїв, «перевірка 3, 2, 1», «Давайте разом»* та інші. Ще цей додаток зручний для створення різноманітних відео.

У залежності від мети та завдань уроку у своїй роботі також використовую різноманітні сервіси для створення тестів. Це не тільки економно, але і швидко: дитина відразу бачить свій результат. Доволі зручним для мене є створення тестів на освітніх порталах ***«Всеосвіта»*** та ***«На урок».*** Пробувала також ***Google-форми***, але коли спробувала ці освітні портали – вже не повернулася до Google – форм.

Для уроків літератури дуже зручно використовувати ***Tagul***. Можна створювати неймовірні хмари слів – чудове доповнення до уроку.

5-6 класи обожнюють домашні завдання в ***Learningapps***. З української мови подобається рубрика *«Поділ на групи»*, а з літератури: *«Знайди пару», «Кросворд», «Вікторина».*

Цифрові технології внесли у наше життя істотні зміни і навчання вони теж не оминули. І ці цифрові засоби, які сьогодні актуальні та цікаві, через два три роки зміняться новими. Проте, пам’ятаймо, живе спілкування не замінять ніякі програм.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. З досвіду роботи «Використання хмарних технологій та сервісів в освітньому процесі». НаУрок : вебсайт. URL: https://naurok.com.ua/z-dosvidu-roboti-vikoristannya-hmarnih-tehnologiy-taservisiv-v-osvitnomu-procesi-6840.html.
2. Концепція нової української школи. Інститут модернізації змісту освіти : вебсайт. URL: https://imzo.gov.ua/osvita/nush/.

НЕБЕЗПЕЧНЕ СПІЛКУВАННЯ ОНЛАЙН: РИЗИКИ, ПРАВИЛА, МЕХАНІЗМИ ЗВЕРНЕННЯ ПРО ДОПОМОГУ Й ЗАХИСТ

ІДЕНТИФІКАЦІЯ НЕБЕЗПЕК ТА РОЗВИТОК СТРАТЕГІЙ ЗАХИСТУ У ВІРТУАЛЬНОМУ СВІТІ

Ольга ЛУНГОЛ, Павло ТОРГАЛО

Онлайн-спілкування молоді займає центральне місце в їхньому повсякденному житті, визначаючи нові форми взаємодії та спілкування. З розвитком технологій та поширення Інтернету, молодь активно використовує онлайн-платформи для обміну інформацією, вираження своїх поглядів, взаємодії з оточуючими та розвитку власної ідентичності.

Соціальні мережі, чати, месенджери та інші онлайн-середовища стали не лише засобом спілкування, але і платформою для вираження творчості, розваг та освітнього розвитку. Молодь використовує ці інструменти для обговорення актуальних тем, створення власного контенту, знаходження подібно мислячих людей та розвитку власної соціальної мережі.

Онлайн-спілкування впливає на формування соціальних навичок та розвиток міжособистісних стосунків. Взаємодія в Інтернеті дозволяє молодому поколінню ефективно виражати свої емоції, розвивати комунікативні навички та будувати стосунки в цифровому просторі. Збільшенню часу перебування молоді у віртуальному світі спонукали спочатку карантинні обмеження внаслідок активного розповсюдження гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2, а зараз – повномасштабного вторгнення росії в Україну.

Онлайн-спілкування молоді, хоча й має численні позитивні аспекти, також пов’язане із певними ризиками та небезпеками. Проаналізувавши матеріали з сайту Кіберполіції України [1], інформацію Computer Emergency Response Team of Ukraine та дослідження вітчизняних науковців Агішевої А.В. [3], Кошової-Куклішини Л.С. [4], Денисюк О.М. [4], Іванюк Г.І. [5], Бовсунівської Д.В. [5] та ін., ми виокремили основні небезпеки онлайн-спілкування молоді:

- Кібербулінг – молодь може стати жертвою кібербулінгу, коли вони піддаються онлайн-засудженню, погрозам, образам або іншим формам психологічного впливу. Кібербулінг може призвести до розвитку стресу, психологічних проблем та соціальної ізоляції.

- Порушення онлайн-приватності. Недостатня поінформованість щодо захисту особистої інформації може призвести до її неправомірного використання або витоку. Зловмисники можуть використовувати цю інформацію для шахрайства, стеження чи інших проявів злочинної діяльності.
- Перегляд неприпустимого контенту. Молодь може ненавмисно потрапляти на онлайн-сайти або матеріали, які містять агресивний, неприязний чи шкідливий контент, що може впливати на їхнє емоційне та психічне здоров'я.
- Онлайн-залученість. Зайвий час перебування в Інтернеті може призвести до залученості та зневаження реального світу, що може негативно впливати на академічну, соціальну та фізичну діяльність молодого покоління.
- Онлайн-залежність. Занадто інтенсивне користування Інтернетом та соціальними мережами може викликати залежність, що впливатиме на психічне здоров'я та взаємовідносини в реальному житті.
- Шахрайства та обман. Молодь може стати жертвою інтернет-шахрайств, фішингу або обману, що може призвести до втрати особистої інформації чи фінансових втрат.

Захист від небезпек онлайн-спілкування для молоді важливий для їхньої цифрової безпеки та психологічного благополуччя. Серед стратегій захисту від небезпек онлайн-спілкування молоді ми в першу чергу виділяємо важливість інформування молоді про потенційні загрози онлайн, формування вмінь розпізнавати шахраїв, уникати фішингу та управляти власною приватністю в Інтернеті. Слід навчати молодь обережно ставитися до розголошення особистих даних, таких як адреса, номер телефону чи шкільна інформація. Батькам необхідно встановлювати розумні обмеження по часу, який неповнолітні проводять в Інтернеті, щоб уникнути перевантаження та залежності. Контролювати, що молодь використовує безпечні та довірені онлайн-платформи та додатки, які пропонують належні заходи безпеки. Освітянам та батькам слід вчити підростаюче покоління розпізнавати та повідомляти випадки кібербулінгу, навчати бути ввічливими та поважати інших онлайн. За можливості, батьки мають встановлювати фільтри та контроль за контентом, щоб обмежити доступ до неприйнятного або небезпечного матеріалу. Підкреслювати важливість уникання особистого спілкування чи обміну інформацією з незнайомцями в Інтернеті.

Загалом, онлайн-спілкування молоді визначає новий спосіб взаємодії та створює цифровий аспект їхнього соціального життя, що відображається в різноманітних сферах, від освіти та розваг до соціально-політичної активності. Проте, ідентифікація потенційних небезпек у віртуальному світі є першочерговою задачею для забезпечення безпеки користувачів. Розуміння ризиків, пов'язаних із кібербезпекою, кіберзлочинністю та іншими аспектами віртуального середовища є ключовим етапом. Основою для захисту від небезпек у віртуальному просторі є розробка та впровадження ефективних стратегій захисту. Це включає в себе використання технологічних засобів, розвиток цифрової грамотності, освіту та психологічну підтримку користувачів. Для успішного впровадження стратегій захисту важлива співпраця між громадськістю, бізнесом, урядом та освітніми установами. Освіта та

інформаційна кампанія щодо кібербезпеки мають займати важливу роль у підвищенні обізнаності та усвідомленості молоді.

З урахуванням постійної еволюції технологій та зміни характеру кіберзагроз, стратегії захисту повинні піддаватися постійному вдосконаленню. При розробці та використанні стратегій захисту важливо дотримуватися етичних стандартів та забезпечувати конфіденційність даних.

Узагальнюючи, можна зазначити, що ефективна ідентифікація небезпек та розробка стратегій захисту вимагає комплексного підходу, включаючи технічні, освітні та психологічні аспекти. Взаємодія всіх зацікавлених сторін та постійне вдосконалення заходів забезпечать стійку безпеку в віртуальному світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кіберполіція України : офіційний сайт. URL: https://cyberpolice.gov.ua.
2. Computer Emergency Response Team of Ukraine. Урядова команда реагування на комп'ютерні надзвичайні події України : вебсайт. URL: https://cert.gov.ua.
3. Лунгол О.М., Агішева А.В. Технології створення та застосування систем захисту інформаційно-комунікаційних систем. *The 2 nd International scientific and practical conference «Topical aspects of modern scientific research»* (October 26-28, 2023) CPN Publishing Group, Tokyo, Japan. 2023. p. 255.
4. Кошова-Куклішина Л.С., Денисюк О.М. Формування у старшокласників навичок спілкування у соціальних мережах. *Соціальна підтримка сім'ї та дитини у соціокультурному просторі громади:* матеріали IV Всеукраїнської науково-практичної конференції. 2022. С. 141-143.
5. Іванюк Г.І., Бовсунівська Д.В. Безпека дитини в інформаційному просторі: проблеми та шляхи вирішення. *The 14 th International scientific and practical conference «Actual problems of science and practice»* (27-28 April, 2020). Stockholm, Sweden 2020. P. 191.

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ВПЛИВИ У ФОРМІ ЦИФРОВОГО ГАЗЛАЙТИНГУ У СОЦІАЛЬНИХ МЕРЕЖАХ ТА СПОСОБИ ЗАХИСТУ

Єлизавета МЕЛЕШКО

Газлайтинг є методом інформаційно-психологічного впливу, спрямованого на примушення об'єкту впливу сумніватися у своїй здатності адекватно сприймати реальність та на виникнення бажання віддати контроль над собою суб'єкту впливу, що досягається застосуванням брехні, заплутування, залякування, звинувачень, знецінення та різних комбінацій цих стратегій [1-3]. Газлайтер змушує свою жертву сумніватися у власній пам'яті, емоційній стабільності та адекватності, знецінює її почуття і думки, навіює їй уявну нікчемність, звинувачує у речах, які вона не робила, заперечує свої попередні слова і дії тощо. Виділимо такі різновиди газлайтингу: *побутовий*, *соціальний*,

політичний та *інституційна зрада*. За формою реалізації у сучасному світі газлайтинг буває звичайний та *цифровий.*

Газлайтинг особливо небезпечний для дітей та молоді, адже вони часто ще не мають достатньо розвинених навичок критичного мислення та емоційної стійкості для виявлення та протистояння такій маніпуляції. Молодь може стикатися з газлайтингом як в офлайн так і в онлайн середовищі. Це може призвести до серйозних психологічних наслідків, зокрема, низької самооцінки, тривоги, депресії, потрапляння під психологічний валив газлайтера. Тому дуже важливо навчати дітей та молодь розпізнавати газлайтинг та зміцнювати їхні навички критичного мислення й емоційної резильєнтності.

Побутовий газлайтинг відбувається у стосунках між членами однієї родини та використовується для знецінення потреб і почуттів близьких людей, для нерівноцінного обміну ресурсами на користь газлайтера [3]. Типові фрази побутових газлайтерів: «Ти дуже гостро реагуєш», «Я просто пожартував(-ла)!», «Якби ти мене любив(-ла), ти дозволив(-ла) би мені робити те, що я хочу», «Це твоя вина» тощо. Побутовий газлайтинг може бути як несвідомим, так і свідомим. При несвідомому – газлайтер знецінює думки, почуття та бажання жертви, тому що не хоче робити зусилля для їх розуміння чи задоволення. При свідомому газлайтингу суб'єкт впливу прагне заплутати і обдурити жертву для реалізації своїх корисливих цілей. Свідоме використання газлайтингу не обмежується знеціненням почуттів, думок та бажань жертви, а полягає також у вчиненні різних дій для її заплутування. Такі дії можуть полягати у переставлянні предметів у домі, підкиданні чи приховуванні речей, стеженні за жертвою з подальшим використанням зібраної інформації, відправленням листів від чужого імені, запереченням сказаних раніше слів та здійснених дій тощо. Усі ці вчинки направлені на виникнення у жертви сумнівів у власній пам'яті та здоровому глузді, у формуванні у неї враження, що суб'єкт впливу адекватніший та краще розуміє, що відбувається довкола. *Соціальний газлайтиг* схожий на побутовий, відбувається з боку друзів, знайомих тощо. Може здійснюватися однією людиною або бути груповим.

Політичний газлайтинг здійснюється владними установами або політичними діячами, наприклад, для заплутування виборців, боротьби з конкурентами тощо [4-6]. Прикладом є переслідування дисидентів у Східній Німеччині у 1970-х та 80-х рр. [4, 5], деякі з прийомів – приховане проникнення у помешкання дисидентів і переставляння там меблів, підробка їх листів тощо.

Інституційна зрада є різновидом газлайтингу, коли у ролі газлайтеру виступають інституції – організації, які повинні допомагати людям [7]. Приклад – *медичний газлайтинг*, коли медики кажуть пацієнту, що його симптоми та скарги вигадані і відмовляють у допомозі при дійсній наявності симптомів [8].

Цифровий газлайтинг відрізняється від звичайного тим, що переважно здійснюється за допомогою комп'ютерної техніки та інформаційних технологій [9]. Наприклад, приховане спостереження з використанням комп'ютерних технологій за жертвою та використання отриманих даних для її заплутування; створення фейкових акаунтів і спілкування від імені інших людей з жертвою або від імені жертви з іншими людьми; потайки здійснене видалення важливих для

жертви даних у її акаунтах для заперечення наявних фактів; злом акаунтів жертви для публікації у них деякої інформації від її імені тощо. Мета цих дій така ж, як і в звичайному газлайтингу. Цифровий газлайтинг може використовуватися будь-яким типом газлайтерів. У роботі [9] відзначається зростання домашнього насильства з застосуванням цифрового газлайтингу, пов'язаного із системами домашнього моніторингу, такими як Google Nest.

Газлайтинг призводить до зниження самооцінки та впевненості у жертви. Може викликати тривогу і депресію [10]. В ряді випадків призводить до посттравматичного стресового розладу [10-12]. Жертви можуть мати такі симптоми, як флешбеки, кошмари, надмірну настороженість, емоційну відстороненість та поведінку уникнення. Наслідки інституційної зради включають психологічний стрес, тривогу, дисоціацію і спроби самогубства [7].

Газлайтинг має такий згубний вплив на психіку, тому що об'єкт впливу часто почувається нікчемним і вважає, що не заслуговує на краще ставлення і не шукає допомоги [1, 3]. Ефективність газлайтингу викликана тим, що його застосовують люди, які попередньо сформували довіру до себе у жертви.

Для захисту від цифрового газлайтингу можна запропонувати наступне:

– Ставитися з довірою до власних почуттів, думок та спогадів, навіть якщо хтось намагається заперечити, знецінити чи перекрутити їх.

– Зберігати докази – переписки, електронні листи, фіксувати дати та події, усе, що може слугувати підтвердженням вашої версії подій.

– Обмеження взаємодії з газлайтером – в онлайн-середовищі це може означати блокування користувача або вихід зі спільних чатів.

– Одержання підтримки від друзів та сім'ї – слід поділитися своїми переживаннями з друзями або членами сім'ї, яким можна довіряти, вони можуть надати підтримку та об'єктивний погляд на ситуацію.

– Консультація з професіоналами – розглянути можливість консультації з психологом, якщо є відчуття тривоги, стресу або інші негативні емоційні наслідки; консультації з юристом для юридичного захисту від газлайтера; консультації із спеціалістами у галузі інформаційних технологій та кібербезпеки для забезпечення своєї інформаційної безпеки тощо.

– Розвиток критичного мислення та медіаграмотності для того, щоб краще аналізувати інформацію та відрізняти правду від маніпуляцій.

– Використання цифрових інструментів для налаштування конфіденційності і безпеки у соціальних мережах та інших вебсайтах.

Стратегії боротьби з цифровим газлайтингом повинні бути комплексними. Вони можуть містити наступні заходи, засновані на різних сферах впливу:

– Освітні та профілактичні заходи – поширення інформації про газлайтинг, його шкоду та методи розпізнавання.

– Технологічні заходи – забезпечення захисту приватної інформації користувачів соціальних мереж і вебсайтів, забезпечення модерації та системи подачі скарг і вирішення проблем користувачів в соціальних мережах тощо.

– Юридичні заходи – законодавчі ініціативи, направлені на встановлення відповідальності за підтверджені факти цифрового газлайтингу.

Отже, знання, що таке газлайтинг, дозволяють вчасно помітити його та

захиститися. Основний спосіб боротьби з газлайтингом – розірвання токсичної взаємодії. Якщо це неможливо, після виявлення суб'єкту впливу, треба ретельно перевіряти інформацію від нього, не довіряти йому, зберігати довіру до своїх думок та почуттів, шукати юридичний захист та підтримку від інших.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Rietdijk N. Post-truth Politics and Collective Gaslighting / Cambridge University Press. 2021. P. 1-17. DOI: https://doi.org/10.1017/epi.2021.24.
2. Gaslight / Cambridge English Dictionary. URL: https://dictionary.cambridge.org/dictionary/english/gaslight (дата звернення: 15.12.2023).
3. Dickson P., Ireland J. L., Birch P. Gaslighting and its application to interpersonal violence / Journal of Criminological Research, Policy and Practice. 2023. Vol. 9(1). P. 31-46. DOI: https://doi.org/10.1108/JCRPP-07-2022-0029.
4. Naraharisetty R. How 'Political Gaslighting' Undermines the Truth / The Swaddle. 2021. URL: https://theswaddle.com/how-political-gaslighting-undermines-the-truth/.
5. Williams L. 10 Terrifying Facts about the East German Secret Police / Foundation for Economic Education. 2019. URL: https://fee.org/articles/10-terrifying-facts-about-the-east-german-secret-police/.
6. Caldwell A. How Russia Successfully Gaslighted the West /./ Huffington Post. 2016. URL: https://www.huffingtonpost.ca/adam-caldwell/the-gaslighting-of-the-west_b_13657466.html.
7. Ahern K. Institutional betrayal and gaslighting /./ Journal of Perinatal & Neonatal Nursing. 2018. Vol. 32(1). P. 59-65. URL: https://doi.org/10.1097/jpn.0000000000000317.
8. Fraser S. The toxic power dynamics of gaslighting in medicine // Canadian Family Physician. 2021. Vol. 67(5) P. 367-368. DOI: https://doi.org/10.46747/cfp.6705367.
9. Marcotte A. Tech Trends /./ American Libraries. 2019. URL: https://americanlibrariesmagazine.org/2019/03/01/tech-trends-libraries/.
10. Gaslighting at Work: Tips for Coping and Thriving / Bay Area CBT Center, Cognitive Behavioral Therapy. URL: https://bayareacbtcenter.com/gaslighting-at-work-tips-for-coping/.
11. Adams N. A., Delaney M., Goldsberry T., Bell, R. L. Gaslighting Female Leadership: All Gas, No Brakes! / Journal of Business Diversity. 2023. Vol. 23(3). URL: https://doi.org/10.33423/jbd.v23i3.6418.
12. Arabi S. PTSD Symptoms: Romantic Relationships with Individuals Who Have Narcissistic and Psychopathic Traits / Doctoral dissertation, Harvard University. 2022. 95 p.

ПРЕВЕНЦІЯ СЕКСТИНГУ СЕРЕД ШКОЛЯРІВ У НЕБЕЗПЕЧНОМУ ВІРТУАЛЬНОМУ СВІТІ

Іванна МИХАЙЛЮК

Для сучасних школярів Інтернет став невід'ємною частиною життя.

Спочатку змалечку батьки дають своїм дітям гаджети, щоб чимось відволікти дитину і зайнятися своїми справами. Згодом це переростає в ситуації, коли батьки взагалі не контролюють, що їхня дитина дивиться у віртуальних мережах. Тим паче, що відібрати у дитини шкільного віку мобільний телефон, коли поширилось дистанційне навчання, практично неможливо.

Інтернет містить багато інформації небезпечного та вразливого змісту, оскільки несе особливу небезпеку, яка потім може негативно впливати на психіку особистості.

За час пандемії діти стали проводити на 80% більше часу онлайн. Паралельно з цим збільшилась кількість скарг щодо булінгу з використанням цифрових технологій, а сексуальна експлуатація дітей у віртуальному просторі збільшилась вдвічі [1].

Секстинг – це обмінювання інтимними фото/відео/текстами, які можуть надсилатися як за власним бажанням, так і під впливом шантажу або насильства.

Наука почала цікавитися секстингом ще на початку 2000-х. Варто знати, що секстинг – це небезпечний штамп спілкування, яке може не лише нашкодити дитині, але й зробити її жертвою сексуального насильства.

Секстинг в основному відбувається за допомогою додатків для смартфонів, таких як Телеграм (Telegram), Вайбер (Viber), тоді як електронна пошта (e-mail) чи Фейсбук (Facebook) є менш популярними серед секстерів [2]. Це тому, що додатки для смартфонів/айфонів більш зручні для обміну фото/відеоконтентом, а телефон знаходиться завжди під рукою і в полі зору секстера, а отже менше шансів, що батьки зможуть помітити відверті фото (на відміну від комп'ютера, який може бути в спільному користуванні).

Відсоток тих, хто практикує секстинг, зростає з віком: у 12–13 років інтерес до оголених фото однолітків значно нижчий, ніж у 16–17 років.

Немає єдиного твердження щодо гендерного аспекту: іноді відсоток хлопців і дівчат, що секстують, однаковий, іноді одна стать переважає іншу.

Варто зауважити, що все ж таки дівчата частіше отримують прохання від протилежної статі надіслати оголені фото.

Цікавим є те, що ставлення суспільства до хлопців і дівчат, котрі надсилають приватні оголені фотографії, різне: якщо хлопці отримують «бали за мужність», то на дівчат за такі дії навішуються ярлики «дешевої повії» або дівчини з низькою самооцінкою [3].

Основними причинами секстингу серед школярів підліткового віку є особливості переживання даного вікового етапу, недостатня увага батьків (опікунів), можливість самоствердитись серед однолітків (кола свого

спілкування). Підлітки хочуть продемонструвати свою зовнішність, думаючи, що на фотографіях вони виглядають більш дорослими.

Школярі шукають уваги серед віртуального світу і не знають про наслідки своїх дій.

Наслідки секстингу для дітей є дуже небезпечними [4]. Навіть якщо фотографії не публікуються для загального доступу і залишаються таємницею, дитина зазвичай перебуває в пригніченому стані. Вона боїться, що її приватні фото побачать і опублікують незнайомі люди, або вона стане об'єктом знущань з боку однокласників.

Щоб захистити дітей шкільного віку від негативних наслідків секстингу, необхідно:

1. Забезпечити «безпечну секстингову» освіту, яка включає в себе інформування школярів про можливі наслідки участі в секстингу, ризики такої поведінки, та дозволить мінімізувати можливу шкоду, яка може бути спричинена секстингом.

Важливу роль у процесі секст-освіти відіграють батьки.

Секстингу можна запобігти завдяки відповідній освіті та готовності тат і мам говорити про «це» відверто, не завуальовуючи, не караючи, а будуючи рівний діалог зі своїми дітьми. Потрібно забезпечити інформативну профілактичну освіту, а не реагувати панікою на такі дії.

Однак, доволі незначна кількість тінейджерів розповідає батькам про секстинг. Це викликає занепокоєння, оскільки спілкування та підтримка батьків є ваговими у зменшенні негативного впливу використання Інтернету.

2. Забезпечити батьківський психологічний контроль, спілкування та моніторинг. Це впливає на розвиток безпечної сексуальної поведінки підлітків [3].

Поясніть дитині, що секстинг може загрожувати її конфіденційності й безпеці; що її тіло недоторканне і жодна людина на світі не має на нього права [5]. Секстинг підлітків не є явищем глобальної загрози, більше причин для хвилювання дає ймовірний витік інтимної інформації.

Слід зауважити, що наслідком надмірної опіки може стати те, що дитина сприйматиме найближчих людей як диктатора/диктаторку.

Належне спілкування та довіра між батьками і дітьми може призвести до зменшення випадків секстингу серед підлітків. Батьки повинні захистити свою дитину, якщо вона стала жертвою секстингу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Константінова Н. Діти і сексуальне насильство в інтернеті. Що таке «секстинг» і «грумінг»? *Радіо Свобода* : вебсайт. URL: https://www.radiosvoboda.org/a/sexing-grooming-sexualne-nasylstvo-v-interneti/31116184.html (дата звернення: 19.01.2024).

2. Van Ouytsel J., Van Gool E., Walrave M., Ponnet K., Peeters E. Sexting: adolescents' perceptions of the applications used for, motives for, and consequences of sexting. Journal of Youth Studies. 2017. Vol. 20. P. 446–470. URL: https://doi.org 10.1080/13676261.2016.1241865 (дата звернення: 19.01.2024).

3. Dolev Cohen M., Ricon T. Demystifying sexting: Adolescent sexting and its associations with parenting styles and sense of parental social control in Israel. Cyberpsychology: Journal of Psychosocial Research on Cyberspace. 2020. № 14 (1). Article 6. URL: https://doi.org/10.5817/ CP2020 (дата звернення: 19.01.2024).
4. Шайнюк О. В. Секстинг: причини та наслідки – Все в твоїх руках. *Все в твоїх руках – Шукайте причину, щоб попередити наслідки!* URL: https://psychologist.net.ua/sekstyng-prychyny-ta-naslidky/ (дата звернення: 19.01.2024).
5. Мізіна Д. (Не)дитячі листування: що таке секстинг і чим він загрожує підліткам. *Український фонд «Благополуччя дітей»*. URL: https://rescentre.org.ua/bezpeka-ditei-v-interneti/nedytiachi-lystuvannia-shcho-take-sekstynh-i-chym-vin-zahrozhuie-pidlitkam (дата звернення: 19.01.2024).

ОБЕРЕЖНО! ШАХРАЙСТВО! ЯК НЕ ПОТРАПИТИ НА ГАЧОК ШАХРАЯ? ДОПОМОЖЕ STOPFRAUD/MRIYA

Денис ПАВЛЮК

У відеоматеріалі наведено приклад шахрайської схеми та механізми захисту від інтернет-шахрайства.

Відеоматеріал буде актуальним як дітям так і дорослим користувачам Інтернет-мережі.

Ключові слова: шахраї, жертва шахрайства, злам сторінки, кіберполіція, STOPFRAUD/MRIYA.

ПРОБЛЕМА ІНТЕРНЕТ-ЗАЛЕЖНОСТІ ДІТЕЙ ТА ПІДЛІТКІВ

Сергій ПОДМАЗІН

Сьогоднішній світ – це технологічний світ, де майже всі люди пов'язані із використанням Інтернету в той чи інший спосіб. Але, в основному саме підлітки користуються більшою частиною інтернет-послуг. Кожне нововведення призводить як до багатьох нових можливостей так і нових ризиків. Одним із головних ризиків, пов'язаних із використанням Інтернету, є інтернет-залежність.

За всю історію людства не було ще такого часу, коли люди б не страждали від яких-небудь залежностей. У цілому *залежність можна визначити як поведінку, що руйнує життя людини, життя фізичне, психічне, соціальне, особисте.*

Діти і підлітки, які майже весь вільний час проводять в Інтернеті – реальність сьогоднішнього дня. Віддалені наслідки для молодого організму регулярного багатогодинного сидіння у віртуальному світі, перенасиченому випромінюваннями від комп'ютерів, планшетів, смартфонів, виявляються пізніше. А ще втрата зору, дратівливість, підвищена збудливість і стомлюваність, порушення сну або, навпаки, сонливість та інше. Ця проблема останнім часом хвилює представників багатьох професій. Дослідники Інтернету, вчені і засоби масової інформації стверджують, що інтернет-залежність – це негативне явище, яке виникло при проникненні Мережі в повсякденне життя. Інтернет-залежність – це психологічний феномен, який полягає у тому, що у людини виникає нав'язливе бажання постійно перебувати у всесвітній мережі. Науковець А. Голдберг поряд з поняттям інтернет-залежності використовує термін «патологічне використання комп'ютера». Це поняття розглядається дещо ширше у контексті, а інтернет-адикція – як один з його видів, специфіка якого полягає у використанні комп'ютера для встановлення соціальної взаємодії [1, С. 149-154].

В Україні однією з перших дослідницьких праць була робота Л. Юр'єва та Т. Больбот. Ними була проведена скринінг-діагностика даного виду залежності за допомогою спеціально розробленої методики скринінгової діагностики комп'ютерної залежності [2, С. 171-176].

Автори виділяють 3 групи підлітків:

1-а група – без ризику розвитку комп'ютерної залежності – 189 чол. (40,82 %);

2-а група – стадія захоплення – 209 чол. (45,14 %);

3-я група – стадія ризику розвитку комп'ютерної залежності (початковий етап формування комп'ютерної залежності) – 65 чол. (14,04 %).

Р.В Моцик вказує, що інтернет-залежність має системний негативний вплив на всі сфери життя дітей та підлітків, зокрема на процес навчання та розвитку дітей [3, С. 292-297].

Особливою, майже не вивченою, проблемою інтернет-залежності є кіберсекс. Результати закордонних досліджень [4] показали, що більшість підлітків відвідують порносайти, а 67% хлопців та 49% дівчат підліткового віку вважають сайти порнографічного змісту цілком прийнятними для свого віку. Як вважає американський психіатр Кімберлі Янг, сексуально дезорієнтовані інтернет-залежні – це взагалі новий тип людини, гідний окремого опису. За статистикою, кожен п'ятий користувач так чи інакше залучений в сексуальну онлайнову діяльність. Драматизм даного виду залежності для підлітків полягає в тому, що він наздоганяє їх в перехідному віці, в момент статевого дозрівання, і тоді у підлітка формується асоціальне уявлення про секс. Для розуміння, що робить кіберсекс залежністю, К. Янг виділяє доступність та контроль своєї сексуальної активності, які є базовими причинами цієї залежності [5-6]. Проблема полягає в тому, що важко дослідити феномен кіберсексуальності в умовах соціального табу щодо сексуального самозадоволення, яке найбільш сильне саме у підлітковому середовищі. Саме тому в нашому дослідженні ми не включили питання щодо

кіберсексу до опитування. По-перше, це могло поставити учнів у непевне становище, а по-друге, ми б не отримали достовірних результатів.

Кімберлі Янг виділила п'ять головних підтипів основного діагнозу «інтернет-залежність», які визначають характер залежності:

1. Кіберсексуальна залежність – непереборний потяг до відвідування порносайтів і заняття кіберсексом.

2. Пристрасть до віртуальних знайомств – надмірність знайомих і друзів в Мережі.

3. Нав'язлива потреба в Мережі – гра в онлайнові азартні ігри, постійні покупки або участі в аукціонах.

4. Інформаційне перевантаження (нав'язливий web-серфінг) – нескінченні подорожі по Мережі, пошук інформації по базах даних і пошукових сайтах.

5. Ігрова залежність – нав'язлива гра в комп'ютерні ігри.

К. Янг визначає, що чільним фактором, завдяки якому всі ці явища набули широкого поширення, є анонімність особистості в Мережі.

Нами було проведено емпіричне дослідження інтернет-залежності дітей та підлітків. Перший етап дослідження проводився у 2019 році на базі гімназії №11 м. Запоріжжя серед учнів 12-17 років. Обсяг вибірки – 250 чол. Другий етап дослідження проводився у 2023 році. Методами дослідження було тестування та анкетування. Використано тест інтернет-залежності Кімберлі Янг. Питання анкет стосувалося різних форм діяльності в інтернеті відповідно до основних форм залежності: ігри, інтернет-серфінг та перебування в соціальних мережах. Питання, які стосувались б кіберсексу, не ставились. Також не ставилися питання щодо використання підлітками ресурсів Інтернету для навчання.

У результаті дослідження були отримані наступні результати:

1. У хлопців інтернет-залежність формується до 12 років, досягає максимуму у 14 років (15%), а потім різко зменшується. У хлопчиків 16-17 років присутній тільки низький рівень залежності.

2. Середній відсоток інтернет-залежності серед дівчат 12-17 річного віку складає 12 відсотків. Інтернет-залежність формується до 12 років, досягає максимуму у 15 років (29%), а потім різко зменшується. У дівчат 17 років присутній тільки низький рівень залежності.

У дослідженні 2023 року було виявлено, що рівень часу, який учні проводять в інтернеті не для навчання, дещо знизився. Це вони пояснюють тим, що з початку реалізації дистанційного навчання більшу частину «комп’ютерного часу» вони почали витрачати на процес навчання.

Таким чином можна дійти до висновків:

1. Інтернет-залежність у хлопчиків формується до 12 років, досягає максимуму у 14 -15 років (15%), а потім різко зменшується. У хлопчиків 16-17 років присутній тільки низький рівень залежності. Високий та критичний рівень залежності спостерігається у хлопчиків у віці 13-15 років (8,4 %).

2. Середній відсоток інтернет-залежності у дівчат 12-17 річного віку складає 12 відсотків. Інтернет-залежність формується до 12 років, досягає

максимуму у 15 років (29%), а потім різко зменшується. У дівчат 17 років присутній тільки низький рівень залежності, Критичного рівня залежності не виявлено на всіх вікових етапах.

3. Порівняння динаміки інтернет-залежності хлопців і дівчат 12-17 віку вказує на спільність у віковому вимірі – інтернет-залежність формується до 12 років, досягає піку у 13-15 років, а у віці 16-17 років істотно зменшується. У той же час, існують суттєві міжстатеві відмінності – хлопчики більше часу проводять у пошуку різноманітної інформації та іграх, а дівчата спілкуються у соціальних мережах.

4. Профілактичну роботу щодо інтернет-залежності у підлітків потрібно починати, щонайменше з 10-11 років.

5. Дослідження 2023 року показало, що з упровадженням дистанційного навчання обсяг часу, який учні проводять в Інтернеті задля розваг, значно зменшився.

Враховуючі сьогоднішні умови життя, доцільно змінити розуміння адикції та норми у використанні Інтернету. Так в умовах дистанційного навчання та вимушеного спілкування через Інтернет час, проведений за комп'ютером, набуває більш продуктивного характеру. Навіть ігрова активність в Інтернеті стала ґрунтовною основою для ведення бойових дій на фронті, наприклад для операторів дронів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Церковний А. Аспекти формування Інтернет-залежності. *Соціальна психологія*. К., 2004. № 5 (7). С. 149-154.

2. Юрьева Л. Н., Больбот Т. Ю. Комп'ютерна залежність: формування, діагностика, корекція і профілактика. Дніпропетровськ: Пороги, 2006. 196 с. URL: http://phtiziatr.ru/library/knigi/?lib=1559.

3. Моцик Р. В. Інтернет-залежність та її вплив на виховання сучасної людини. *Педагогічна освіта: теорія і практика*. 2015. Вип. 18. С. 292-297. URL: http://nbuv.gov.ua/UJRN/znppo_2015_18_54.

4. The Impact of Pornographyon Children. URL: https://www.acpeds.org/the-college-speaks/position-statements/the-impact-of-pornography-on-children (дата звернення: 13.01.2024).

5. Young K.S. What makes the Internet Addictive: potential explanations for pathological Internet use. CyberPsychology and Behavior. 1999. №1. P. 57-60.

6. Young K.S. Caught in the Net. How to Recognize the signs of Internet Addiction And a Winning strategy for Recovery. New York: John Wiley and Sons, Inc., 1998. – 55 p.

БЕЗПЕЧНЕ СПІЛКУВАННЯ В ІНТЕРНЕТІ: ЦІКАВІ КАЗКИ, ІГРИ ТА ВПРАВИ ДЛЯ ДІТЕЙ РІЗНОГО ВІКУ

Ольга СУРЖКО

Інтернет – дуже потужний ресурс, який значно полегшує життя людини та відкриває майже необмежені можливості для самореалізації та саморозвитку юної особистості через спілкування, навчання, дозвілля. Однак разом з тим, в інтернеті приховано досить багато небезпек як для дітей, так і для дорослих.

Знання цих небезпек дозволить їх уникнути [1].

Комп'ютери, смартфони, інтернет – усе це сьогоднішня реальність, яку складно ігнорувати [2]. Проте потрібно навчити учнів, що мережа «Інтернет» може бути як корисною, так і небезпечною, варто ознайомити дітей з правилами поводження в інтернеті. Тому була розроблена авторська казка «Безпечна дружба з диво-звіром» [3], створена з метою ознайомлення дітей 1-6 класів з правилами спілкування в інтернеті та гра «Безпечний інтернет» [4].

Мета гри – поглиблення та закріплення розуміння учнями небезпек, що чекають на кожного, хто мандрує мережею «Інтернет». Ці розробки будуть актуальними для практичних психологів, соціальних педагогів, педагогічних працівників під час проведення тренінгових занять, виховних годин тощо.

Ключові слова: Інтернет, комп'ютери, безпека в Інтернеті, казка, гра.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кочарян А. Б., Гущина Н. І. Виховання культури користувача Інтернету. Безпека у всесвітній мережі : навчально-методичний посібник. Київ, 2011. С. 12

2. Життя молоді у цифровому світі: користь і небезпека. Олександрійський професійний ліцей : вебсайт. URL: http://surl.li/qtbar.

3. Казка «Безпечна дружба з диво-звіром». Ольга Суржко : youtube-канал. URL: https://www.youtube.com/watch?v=5w_-M3HiNmc.

4. Гра «Безпечний інтернет» : Google документ. URL: https://docs.google.com/document/d/1-Ebdert4VXmDEqpn76C0OP-XZ-FvtBbM/edit?usp=sharing&ouid=106457217349447917775&rtpof=true&sd=true.

РІЗНОВИДИ ЗАГРОЗ В ОСВІТНІЙ ОНЛАЙН-КОМУНІКАЦІЇ

Лариса ФАМІЛЯРСЬКА

Онлайн-комунікація стала невід'ємною складовою сучасного суспільства, яка впливає на більшість аспектів життя людини, включаючи освітній процес, бізнес, соціальні відносини тощо.

Визначаємо онлайн-комунікацію як міжособистісну взаємодію, обмін інформацією, спілкування за допомогою мережевих технологій та цифрових засобів.

Використання можливостей мережі Інтернет значуще для взаємодії в професійних спільнотах, з друзями, родиною, колегами. У контексті освіти, онлайн-комунікація використовується для навчання та співпраці, обміну ідеями між учасниками освітньої комунікації за допомогою різноманітних інтернет-інструментів.

Онлайн-комунікація значима для сучасної освіти з низки причин:

1. Глобальний доступ до інформації, що надає можливість отримувати інформацію будь-де та будь-коли, роблячи освітній контент доступним повсюдно.
2. Дистанційна освіта, що дозволяє здійснювати навчання незалежно від місця знаходження. Це особливо важливо в умовах обмежень, таких як дія правового режиму воєнного стану, пандемія тощо.
3. Розширення можливостей навчання з використанням інтерактивних та інноваційних форм навчання, відеоуроків, інтерактивних завдань, віртуальних лабораторій та інших технологічних засобів.
4. Сприяння співпраці та обміну ідеями, що стимулює активний обмін ідеями та співпрацю між учасниками освітнього процесу, розширюючи можливості для колективного навчання та обговорень.
5. Спілкування в онлайн-середовищі, що зумовлює адаптування до швидкозмінних технологічних трендів та важливе для підготовки здобувача освіти до професійного майбутнього.

Однак, разом з перевагами онлайн-комунікації, існують і певні ризики та загрози, які потрібно знати та уникати.

Державна політика в сфері кібербезпеки є однією із важливих складових системи національної безпеки України, особливо в умовах дії правового режиму воєнного стану [3].

«Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [1].

Кібербулінг – один із аспектів небезпеки в онлайні, це агресивна усвідомлена дія, що здійснюється особистісно або групою людей з використанням електронних форм комунікації. Ця дія повторювана та тривала у

часі по відношенню до жертви, якій важко захистити себе. Кібербулінг охоплює різні види негативної поведінки в інтернеті, зокрема, флеймінг, фішинг, цькування тощо. Найпоширенішими видами загроз в онлайн-комунікації сучасних дітей є флеймінг та цькування.

Флеймінг (перепалки) – це коли людина в запалі обмінюється з іншими якимись гнівними постами чи повідомленнями. Як правило, це короткі повідомлення, які розраховані на емоційне сприйняття іншими. Флеймінг (перепалки) є мовою ненависті, ворожнечі. Починається все з короткого повідомлення, яке підбурює, ніби емоційно «інфікує» та створює відчуття та потребу відреагувати у відповідь. Емоційна реакція миттєво відбувається, коли не сформована особистісна саморегуляція. Але можна уникнути такої ситуації, запобігти. Для формування саморегуляції потрібно навчити дитину:

- припиняти спілкування, якщо вона почувається некомфортно;
- якщо щось не сподобалося, засмутило – вимкнути екран (не комп'ютер) або відкласти телефон, але не виходити із цієї програми. Тобто припинити комунікацію та зберегти «сліди» для подальшої розмови дорослого з дитиною. Це важливо, бо дитина може не пояснити, що саме її засмутило чи налякало, вразило.

Цькування – це постійні атаки, знущання, які виснажують. Наприклад, це особливо стосується дитини, коли їй постійно говорять, що вона якась не така (товста або, навпаки, худа). Цькування є конкретне діставання та спрямоване на особистість, щоб спровокувати. Практикою запобігання негативних наслідків є розмова з дитиною. Алгоритм може бути такий:

- похваліть за те, що вона розповіла вам про ситуацію, та запевніть, що разом ви впораєтеся;
- поясніть, що явище кібербулінгу говорить більше про кривдників, ніж про постраждалих;
- не обмежуйте доступ до інтернету та не забирайте гаджети у дитини – це може викликати ще більше занепокоєння та погіршити ситуацію.

Роль педагога та дії у процесі створення безпечного середовища міжособистісної та онлайн-комунікації:

- навчання дітей основам онлайн-безпеки;
- підтримка у разі виникнення проблем;
- застосування відповідних стратегій та технологій безпеки задля мінімізації ризиків та наслідків кібербулінгу;
- розвиток критичного мислення здобувачів освіти;
- навчання навичкам цифрової безпеки.

Міністерство цифрової трансформації спільно з ЮНІСЕФ в Україні, Міністерством освіти і науки України, Координаційним центром з правової допомоги та Міністерством юстиції України створили середовище інформаційної підтримки. Інтерактивний бот у Telegram і Viber «Кіберпес» надає послідовний механізм дій для дітей, батьків, вчителів у випадку кібербулінгу. Кожен користувач може швидко та просто з'ясувати спосіб самостійного вилучення неприємного контенту з соціальних мереж, а також де шукати допомогу у цьому питанні.

Інформаційну підтримку щодо безпечного користування цифровими засобами можна знайти на сайті «Nadiyno». Як зазначають автори проєкту ,«… на нашій платформі ви знайдете відповіді на свої запитання, пов'язані із захистом персональних даних, акаунтів і пристроїв» [2].

Забезпечення безпеки в онлайн-просторі важливо для збереження ефективності освіти та запобігання негативним наслідкам для здобувачів освіти, вчителів та освітніх закладів. З практиками запобігання детальніше можна ознайомитися в освітньому серіалі, створеному з ініціативи Мінцифри для платформи «Дія. Освіта» за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України». Зміст містить тлумачення психології та прийомів, які використовують онлайн-шахраї, природу фейків, вірусів і способи ефективної протидії.

Онлайн-комунікація актуалізує ще одну проблему в контексті поточних викликів та загроз повномасштабної російсько-української війни – перекручення та фальсифікації історичних подій. Запобігання ІПСО (інформаційно-психологічна спеціальна операція) країни агресора на території України надзвичайно важливе для збереження суверенітету держави, ефективної діяльності державних структур і гармонійного існування українського суспільства [4]. Відтак створення педагогом умов для розвитку критичного мислення сучасних здобувачів освіти зумовлює вміння аналізувати, співставляти та оцінювати факти та історичні події важливі для країни.

Онлайн-комунікація може бути корисною та позитивною, якщо знати, як уникнути потенційних загроз та захистити свою приватність та безпеку.

Отже, розвиток цифрової грамотності здобувачів освіти сприятиме безпечній онлайн-комунікації, що важливо в сучасному інформаційному суспільстві. Адаптація до технологічних трендів відіграє ключову роль у модернізації освіти, забезпечуючи більше можливостей для навчання, співпраці та інновацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 02.02.2024).
2. Проєкт Nadiyno : вебсайт. URL: https://nadiyno.org/about-us/.
3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України; Стратегія від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення 02.02.2024 р.).
4. Фамілярський В.О. Російсько-українська повномасштабна війна: проблема перекручень та фальсифікацій історичних подій. Development of Education, Science and Business: Results 2023: Proceedings of the International Scientific and Practical Internet Conference, December 21-22, 2023. FOP Marenichenko V.V., Dnipro, Ukraine, 261 p., P. 218-220.

ТЕХНОЛОГІЧНІ ІНСТРУМЕНТИ ТА РІШЕННЯ ФОРМУВАННЯ БЕЗПЕЧНОГО ІНТЕРНЕТ-ПРОСТОРУ ДИТИНИ

СУЧАСНІ ТЕХНОЛОГІЇ ЯК ІНСТРУМЕНТ СОЦІАЛЬНОЇ ПРОФІЛАКТИКИ КІБЕРПРАВОПОРУШЕНЬ СЕРЕД ДІТЕЙ

Анна АМАНГЕЛДІЄВА

Науковий керівник: Габорець Ольга Андріївна – доцентка кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету № 3 Донецького державного університету внутрішніх справ, доктор філософії, доцент.

У сучасному світі кіберправопорушення є серйозною загрозою для суспільства та визначається як одна із загроз національній безпеці України в інформаційній сфері.

Відповідно до Закону України «Про основи забезпечення кібербезпеки України» кіберзлочин (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [1].

Також одним з головних нормативно правових актів є Конвенція про кіберзлочинність. Вона відіграє важливу роль в системі заходів протидії кіберзлочинності на міжнародному рівні [2].

Сучасні технології мають великий потенціал для соціальної профілактики кіберправопорушень серед дітей. Вони можуть використовуватися для підвищення обізнаності про кібербезпеку, навчання дітей цифровим навичкам і надання їм підтримки в разі кібербулінгу або інших форм кіберзлочинності.

Основними напрямками у використані технологій для соціальної профілактики кіберправопорушень серед дітей мають бути:

– розробка і поширення освітніх матеріалів про кібербезпеку. Ці матеріали можуть бути представлені у вигляді відео, навчальних ігор, вебсайтів або інших форматів. Вони повинні бути доступними для дітей у різних вікових групах;

– створення онлайн-платформ для спілкування і підтримки дітей. Ці платформи можуть використовуватися для обміну інформацією про кібербезпеку, надання підтримки дітям, які стали жертвами кіберзлочинності, і навчання дітей цифровим навичкам;

– розробка і впровадження нових технологій для виявлення і запобігання кіберправопорушень. Ці технології можуть використовуватися для моніторингу онлайн-активності, виявлення потенційних кіберзлочинців і запобігання кіберзлочинності.

Використання сучасних технологій для соціальної профілактики кіберправопорушень серед дітей має низку переваг:

1) технології можуть бути використані як для певних вікових груп, так і для усіх дітей в цілому (великої аудиторії);

2) технології можуть використовуватися для надання інформації і підтримки в режимі реального часу;

3) технології можуть застосовуватися для персоналізації навчання і подальшої підтримки.

Важливо зазначити, що використання сучасних технологій для соціальної профілактики кіберправопорушень серед дітей також має ряд обмежень. Ці технології можуть бути використані для поширення шкідливої інформації та можуть бути використані для маніпуляції та порушення приватності дітей.

Для того, щоб мінімізувати ці обмеження, важливо використовувати сучасні технології в поєднанні з іншими формами соціальної профілактики кіберправопорушень, такими як освіта в родині і школі, а також співпраця з правоохоронними органами тощо.

В Україні існують ініціативи, спрямовані на використання сучасних технологій для соціальної профілактики кіберправопорушень серед дітей.

Міністерство освіти і науки України спільно з Міністерством внутрішніх справ України розробили програму «Безпечний Інтернет», яка передбачає проведення освітніх заходів про кібербезпеку в школах і інших навчальних закладах [3]. Крім того, в Україні діє ряд громадських організацій, які займаються освітою дітей про кібербезпеку.

Стратегія кібербезпеки України затверджена Указом Президента України від 14 травня 2021 року № 287 та визначає основні напрями та завдання забезпечення кібербезпеки України і включає у себе напрямок «Підвищення обізнаності про кібербезпеку», що є важливим аспектом для профілактики кіберправопорушень серед дітей.

Стратегія кібербезпеки України є прогресивним документом, який враховує сучасні виклики і загрози у кіберпросторі. Вона спрямована на створення ефективної системи кібербезпеки, яка буде здатна захистити інтереси України у цифровому світі [4].

Запровадження сучасних технологій для соціальної профілактики кіберправопорушень серед дітей є ефективним способом захисту їхньої кібербезпеки. Однак, важливо використовувати ці технології в поєднанні з іншими формами соціальної профілактики, щоб мінімізувати можливі обмеження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основи забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 19.01.2024).

2. Конвенція про кіберзлочинність від 23.11.2001 № 994_575. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 19.01.2024).

3. Безпечний Інтернет. Міністерство освіти і науки України : вебсайт. URL: https://mon.gov.ua/ua/osvita/pozashkilna-osvita/vihovna-robota-ta-zahist-prav-ditini/bezpeka-ditej-v-interneti (дата звернення: 19.01.2024).

4. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України; Стратегія від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення 02.02.2024 р.).

ІНСТРУМЕНТИ ЗАБЕЗПЕЧЕННЯ ФОРМУВАННЯ БЕЗПЕЧНОГО ІНТЕРНЕТ-ПРОСТОРУ ДИТИНИ

Анна БАБІЧ

У сучасному цифровому світі доступ до Інтернету став необхідністю, але разом з цим існує загроза безпеці, особливо для дітей. Вони є активними користувачами мережі як під час навчання, так і вдома, під час відпочинку. За допомогою технологій батьки можуть активно працювати над тим, щоб гарантувати безпечний інтернет-простір для власних дітей. Розглянемо деякі технологічні інструменти та рішення, які допомагають у цьому.

1. Батьківський контроль у роутерах і програмах

Багато роутерів мають вбудовані функції батьківського контролю, які дозволяють обмежувати доступ до певних вебсайтів або встановлювати графік використання Інтернету. Мікропрограми для маршрутизаторів TP-Link (HomeCare) та ASUS забезпечує моніторинг мережі в режимі реального часу для виявлення зловмисного програмного забезпечення, вірусів і вторгнень до того, як вони досягнуть персонального комп'ютера або пристрою. Батьківський контроль дозволяє планувати час, коли підключений пристрій має доступ до Інтернету. Також є можливість обмежити доступ до небажаних вебсайтів та програм [1].

Перепоною використання подібних програмних засобів є їхня вартість. Альтернативою є батьківський контроль Google.

Google, один із провідних інтернет-гігантів, пропонує потужний інструмент для батьківського контролю, який дозволяє батькам ефективно керувати тим, як їхні діти використовують онлайн-ресурси. Google Family Link - це додаток, який дозволяє батькам встановлювати обмеження та контролювати використання пристроїв своїми дітьми.

Основні функції Google Family Link:

- Блокування непридатного вмісту

Батьківський контроль Google дозволяє обмежити доступ до вмісту, який може бути небезпечний для дітей. Це включає фільтрацію вебсайтів та блокування додатків із сумнівним вмістом.

- Установлення годин використання

Батьки можуть встановлювати обмеження для використання пристроїв та окремих додатків. Це допомагає уникнути надмірного часу, витраченого на екранах.

- Відстеження місцезнаходження

Функція GPS дозволяє батькам бачити, де знаходиться їхня дитина. Це особливо корисно для гарантування безпеки дітей та контролю їхніх переміщень.

- Керування контактами

Батьки можуть встановлювати, з ким можуть спілкуватися їхні діти через телефон або повідомлення.

Для використання Google Family Link необхідно завантажити додаток на свої пристрої, створити обліковий запис для дитини та підключити його до свого облікового запису Google та встановити необхідні обмеження [2].

2. Контент-фільтри

Використання фільтрів контенту може забезпечити захист від небажаного матеріалу в Інтернеті. Такі програми допомагають блокувати доступ до вебсайтів з обмеженим вмістом і контролюють використання Інтернету.

Перевіреним сервісом, який досить надійно блокує небажаний контент, є сервіс *1.1.1.1 For Families* від компанії *CloudFlare*, яка надає послуги CDN (Content Delivery Network) і захисту від DDoS-атак.

Застосовувати DNS-фільтр з метою захисту дітей можна як удома, так і в закладі освіти. Використовуючи рівні захисту, можна захистити особистий комп'ютер або мобільні пристрої від сайтів, що розповсюджують шкідливе програмне забезпечення та використовуються в шахрайських схемах [3].

3. Освіта та усвідомленість

Освіта є ключовим елементом в формуванні безпечного інтернет-простору для дітей.

В умовах війни заклади освіти, повністю або частково, переходять на дистанційне навчання. Безпека персональних даних, спілкування та навчання, дітей в онлайн-середовищі виходить на перший план.

Google Workspace for Education є потужним інструментарієм, який пропонує різноманітні можливості для створення безпечного навчального середовища для учнів.

- Захист Приватності та Даних

Google Workspace відповідає законам про приватність, таким як Закон про права на освітні записи та конфіденційність в США (FERPA). Це забезпечує конфіденційність даних учнів та їхню безпеку, адже інформація обробляється безпечно та не використовується для спрямованої реклами.

- Безпечний пошук

Використання технології безпечного пошуку допомагає уникнути доступу учнів до шкідливих вебсайтів та захищає їх від фішингових атак.

- Фільтрація контенту

Адміністратори можуть налаштовувати фільтри контенту, обмежуючи доступ до неприйнятного чи неосвітнього контенту, що сприяє створенню безпечного онлайн-середовища для учнів.

- Моніторинг електронної пошти

Google Workspace надає можливість адміністраторам моніторити та контролювати електронну пошту, що допомагає у запобіганні кібербулінгу, домагань чи обміну нецензурним контентом.

- Контроль Google Classroom

Вчителі та адміністратори мають повний контроль над Google Classroom, що дозволяє їм моніторити та модерувати обговорення, завдання та інші колективні дії для створення позитивного та безпечного середовища для навчання.

- Керування пристроями

Google Workspace надає можливості управління мобільними пристроями, що дозволяє адміністраторам контролювати та забезпечувати безпеку пристроїв, які використовують учні, забезпечуючи дотримання правил школи.

- Аутентифікація та авторизація користувачів

Механізми сильної аутентифікації та авторизації забезпечують, що доступ до чутливої інформації мають лише авторизовані особи.

- Оновлення безпеки

Google регулярно оновлює свої сервіси для вирішення вразливостей безпеки, гарантуючи захист від потенційних загроз.

- Тренінг та ресурси

Google надає навчальні матеріали та ресурси для освітян, адміністраторів та батьків, щоб вони могли розуміти функції безпеки та кращі практики використання Google Workspace for Education [4].

Під час освітнього процесу доцільно використовувати додатки та ігри, які вчать правилам використання Інтернету та онлайн-безпеці. *"Be Internet Awesome"* [5] від Google, допоможе сприяти усвідомленості серед дітей важливості питання Інтернет-безпеки. Сервіс з пошуку системи облич Face Search Engine [6] показує учням на практиці значення поняття «цифровий слід», та дає можливість знайти в Інтернеті обличчя та захистити власну конфіденційність.

4. Моніторинг соціальних мереж

Соціальні мережі можуть бути плацдармом для небезпечних взаємодій. Зазначені програмні засоби батьківського контролю від Google та можливості Google Workspace дають можливість батькам та педагогам виявляти потенційні загрози шляхом контролю додатків, які буде використовувати дитина на своєму пристрої.

Але, незважаючи на зручність використання програмних засобів з віддаленим доступом, найбільш ефективний спосіб контролю - це відкрите спілкування. Батьки повинні створювати відкрите середовище для обговорення онлайн-активностей, навчаючи дітей про потенційні ризики та навички безпеки.

Технології можуть бути справжнім союзником для батьків та педагогів у гарантуванні безпечного інтернет-простору для своїх дітей. Застосування батьківського контролю, фільтрів контенту, освітніх програм та моніторингу соціальних мереж дозволяє створити ефективний бар'єр перед онлайн-загрозами. Однак важливо також регулярно спілкуватися з дітьми, навчаючи їх правилам безпечного користування Інтернетом і підтримуючи їхню усвідомленість.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бездротовий маршрутизатор. Як налаштувати батьківський контроль? Asus : вебсайт. URL: https://www.asus.com/ua-ua/support/faq/1008720/ (дата звернення: 31.01.2024).
2. Допоможіть дитині освоїтися у світі сучасних технологій. Google Family Link – Home : вебсайт. URL:https://families.google.com/familylink/ (дата звернення: 31.01.2024).

3. Безкоштовний інтернет фільтр для дітей вдома та в школі. Informatik : вебсайт. URL: https://informatik.pp.ua/tekhnichna-pidtrimka/komp-yuterna-merezha/bezkoshtovnyi-internet-filtr-dlia-ditei-v-shkoli-ta-vdoma/ (дата звернення: 31.01.2024).
4. Google Workspace for Education : довідковий центр URL: https://support.google.com/a?sjid=2257322419729973941-EU#topic=4388346 (дата звернення: 31.01.2024).
5. Інтерленд : вебсайт. URL: https://beinternetawesome.withgoogle.com/en_us/interland.
6. Сервіс з пошуку системи облич Face Search Engine. Pimeyes : офіційний сайт. URL: https://pimeyes.com/en.

ФОРМУВАННЯ БЕЗПЕЧНОГО ОНЛАЙН-ПРОСТОРУ ДЛЯ ДІТЕЙ З ОСОБЛИВИМИ ОСВІТНІМИ ПОТРЕБАМИ

Тетяна ВОЛОШИНА, Наталія МАРКО

Форми здобуття освіти організовуються відповідно до нормативно-правових актів, зокрема Закону України «Про освіту», де у ст. 9 йдеться про право особи здобувати освіту в різних формах або поєднуючи їх. Це - інституційна (очна, заочна, дистанційна, мережева), індивідуальна (екстернатна, сімейна, педагогічний патронаж, на робочому місці), дуальна. За визначенням Закону, дистанційна форма здобуття освіти є індивідуалізованим процесом з опосередкованою взаємодією (віддалено) у спеціалізованому середовищі на базі інформаційно-комунікаційних технологій (далі по тексту – ІКТ). Дистанційне навчання передбачає фізичну відсутність особи в закладі освіти, що надає можливість запобігання скупченості учасників освітнього процесу в одному місці, тому така форма організації надання освітніх послуг стала єдино можливою у період пандемії, що призвело до безпрецедентного прискорення цифровізації освіти у всьому світі. Завдяки такому досвіду на території нашої держави під час воєнних дій не довелося припиняти навчання дітей і навіть особам, які тимчасово опинилися за межами України, було створено умови щодо надання освітніх послуг.

На сьогодні сучасні технології та Інтернет відкрили для дитини багато можливостей для соціальної інтеграції, освіти, комунікації тощо і стали невід'ємною частиною її життя.

Діти з особливими освітніми потребами (далі по тексту – ООП) не є виключенням у цьому процесі. Вони так само активно використовують інтернет-технології для спілкування у соціальних мережах, навчання та розвитку, прослуховування музики, перегляду фільмів, онлайн-ігор. Це допомагає їм відчувати себе частиною суспільства, розширює можливості доступу до інформації та освітніх ресурсів, створює умови для комунікації. Слід зауважити, що при навчанні засоби ІКТ доцільно добирати з урахуванням особливостей психофізичного розвитку дитини, що надасть можливість повноцінно

включитися в онлайн-діяльність, створювати прийнятні для неї індивідуальні освітні стратегії [4, с.28] та підвищувати ефективність засвоєння навчальних матеріалів.

Дистанційна освіта має великі переваги, зокрема можливість засвоювати інформацію асинхронно; індивідуальний темп навчання; доступність незалежно від місця знаходження та стану психофізичного розвитку особи, але є й мінуси, які стосуються відсутності безпосереднього спілкування, браку практичних занять тощо [3, с. 25-28].

Разом з тим Інтернет містить загрози, які можуть мати негативні наслідки для благополуччя самої дитини та її родини [5]. Діти з ООП більш схильні до вразливості та через це частіше, ніж їхні однолітки, можуть стикатися з викликами та загрозами в онлайн-середовищі. Тому формування безпечного онлайн-простору для дітей з ООП має бути одним з ключових завдань сучасного інформаційного суспільства.

Тож з якими викликами в інтернет-просторі можуть зустрічатися діти з ООП та через які причини діти з порушеннями психофізичного розвитку частіше потрапляють у ризикові ситуації в Інтернеті? Наприклад:

діти з порушеннями інтелектуального розвитку можуть мати труднощі у розпізнаванні та сприйнятті сигналів небезпеки в інтернет-середовищі, що може впливати на їхню здатність уникати ризикованих ситуацій. Обмеження у функціонуванні деяких когнітивних процесів може вплинути на формування критичного мислення і цифрової грамотності, що не дозволяє розрізняти факти та фейки в мережі, розпізнавати дезінформацію та підроблений контент;

діти з функціональними труднощами, які полягають в обмеженні життєдіяльності різного ступеня прояву слухової, зорової, опорно-рухової, мовленнєвої функцій, можуть частіше зустрічатися з проблемами доступності до інформації. Оскільки не всі онлайн-ресурси та платформи можуть бути адаптовані до потреб дітей з різними порушеннями психофізичного розвитку, це може змушувати їх шукати альтернативні варіанти, менш безпечні;

діти, які мають соціоадаптаційні/соціокультурні труднощі через недостатній розвиток комунікаційних навичок, обмежене почуття небезпеки, невпевненість у собі, можуть бути більш вразливі до кібербулінгу. Крім того, деякі з них схильні до залежності від онлайн-розваг та онлайн-спілкування через відсутність соціальної активності офлайн. Надмірно витрачений час у віртуальному середовищі може викликати електронну залежність;

батьки дітей з особливими потребами можуть бути недостатньо зорієнтовані у проявах ризикованої поведінки в Інтернеті або відчувати труднощі у супроводі та контролі за їхніми онлайн-активностями у зв'язку з недостатньою цифровою обізнаністю. Це в свою чергу може призвести до витоку особистої конфіденційної інформації через неправильне конфігурування акаунтів, відсутності захисту інформації, небезпечні дії в Інтернеті.

Запобігання цим викликам вимагає комплексного підходу, який містить у собі розвиток нормативно-правової бази щодо безпеки дітей з ООП в Інтернеті, інвестування у фундаментальні інклюзивні та доступні цифрові інфраструктури для забезпечення доступу до Інтернету для всіх, у тому числі осіб з ООП,

підвищення цифрової та інформаційної грамотності у державному секторі та за його межами [2, с. 70], удосконалення технологічних інструментів і рішень щодо формування безпечного інтернет-простору та консолідацію зусиль між державою, закладами освіти та батьками дітей з ООП.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Безпека дітей в Інтернеті: попередження, освіта, взаємодія: збірник матеріалів ІІ Всеукраїнської науково-практичної конференції, м.Кропивницький, 06-10 лютого 2023 року / уклад. С.М. Єфіменко; за заг. ред. Г.В. Скрипки. Кропивницький: КЗ «КОІППО імені Василя Сухомлинського», 2023. 192 с.
2. Дорожня карта використання науки, технологій, інновацій для досягнення цілей сталого розвитку / Ухвалено колегією Міністерства освіти і науки України. Протокол від 22.12.2023 № 3. Київ - 2023. URL: http://surl.li/pjggz (дата звернення: 02.02.2024).
3. Лавриненко Л.М. Освіта в реальності сьогодення – дистанційне навчання: МЦНД. Луцьк, 2020. С. 25-28.
4. Сучасні засоби ІКТ підтримки інклюзивного навчання : навчальний посібник / А. В. Гета та ін.; за заг. ред. Ю. Г. Носенко. Полтава : ПУЕТ, 2018. 261 с. URL: http://surl.li/qblkz.
5. Черних О.О. Формування безпечної поведінки дітей в інтернеті як актуальний напрям соціально-педагогічного супроводу. Інновації педагогічної освіти в умовах викликів сьогодення : монографія / за наук. ред. С. Я. Харченка. К. : Талком, 2019. 343 с. URL: http://surl.li/qblwv.

БЕЗПЕКА В ІНТЕРНЕТІ ДЛЯ ДІТЕЙ: ЯК ХМАРНІ ТЕХНОЛОГІЇ ТА РОЗВИНЕНА ЦИФРОВА КОМПЕТЕНТНІСТЬ СТАЮТЬ КЛЮЧОВИМИ РІШЕННЯМИ

Роман ГРУШКО

У сучасному світі, де технології є обов’язковою частиною повсякденного життя, питання безпеки дітей в Інтернеті стає надзвичайно важливим. З кожним роком діти стають активнішими користувачами онлайн-ресурсів, використовуючи цифрові простори для навчання, розваг та соціалізації. У цьому контексті ключовою стає необхідність розробки та впровадження ефективних технологічних інструментів, спрямованих на формування безпечного інтернет-простору для наймолодших користувачів. Хмарні технології стали необхідною складовою сучасного цифрового суспільства від функцій зберігання та резервного копіювання даних до моніторингу та фільтрації контенту. Хмарні технології можуть надати ефективні інструменти для батьків та педагогів у вирішенні питань, пов'язаних із безпекою юних інтернет-користувачів.

Однією з основних переваг хмарних технологій у контексті забезпечення безпеки дітей в Інтернеті є їх здатність ефективно зберігати та керувати даними. Замість локального зберігання інформації на пристроях, де є ризик втрати, хмарні платформи надають можливість зберігати дані в безпечному та доступному з

будь-якого пристрою місці. Від сімейних фотографій до особистих налаштувань безпеки, хмарні технології стають ефективним засобом для забезпечення конфіденційності та інтегрованого керування цифровою інформацією дитини.

У світі, де потоки інформації безперервно зростають, важливо визначати та фільтрувати контент, до якого діти мають доступ. Хмарні платформи надають зручний інструментарій для батьків та педагогів для моніторингу та фільтрації контенту, що надходить до пристроїв дітей. За допомогою розумних алгоритмів та налаштувань безпеки, батьки можуть ефективно відстежувати та контролювати доступ до відповідного контенту, надаючи дітям безпечне та відповідальне Інтернет-середовище [2, с. 34].

Розвиток цифрової компетентності стає важливим елементом відповідального використання інтернет-ресурсів. Вивчення навичок інтернет-грамотності включає в себе уміння розрізняти достовірні та недостовірні джерела інформації, розуміння основних принципів цифрової безпеки та етичної поведінки в мережі. Розвинуті навички критичного мислення допомагають дітям аналізувати та оцінювати інформацію, з якою вони стикаються в Інтернеті, забезпечуючи їм усвідомлене та відповідальне використання онлайн-ресурсів. Цифрова компетентність включає в себе уміння ефективно користуватися цифровими ресурсами та інструментами. Діти повинні навчитися безпечно взаємодіяти з різноманітними онлайн-сервісами, розуміти принципи конфіденційності даних та вміти захищати свою особисту інформацію. Розвиваючи ці навички, діти можуть стати не лише компетентними користувачами Інтернету, а й власниками своєї цифрової безпеки. Цифрова компетентність є ключовим елементом у створенні безпечного інтернет-середовища для дітей.

Хмарні рішення для контролю з боку батьків стають ефективним засобом моніторингу онлайн-активності дітей. Вони надають змогу відстежувати відвідувані вебсайти, контролювати час, проведений в Інтернеті, та блокувати небезпечний чи неприйнятний контент.

Інноваційні методики в сфері цифрової безпеки допомагають вирішувати сучасні виклики та адаптувати підходи до змінного інтернет-середовища. Прикладом є використання штучного інтелекту для аналізу поведінкових зразків дітей в Інтернеті та розпізнавання можливих загроз. Це дозволяє вчасно виявляти та реагувати на небезпечні ситуації.

Іншим інноваційним підходом є створення ігрових платформ, які навчають дітей основам цифрової безпеки через інтерактивний та захопливий досвід. Це дозволяє дітям засвоювати важливі принципи безпеки, граючи в ігри та виконуючи завдання.

Цифрові інструменти в навчанні можуть допомагати формувати цифрову компетентність та забезпечувати безпеку дітей в Інтернеті. Наприклад, інтерактивні навчальні платформи можуть надавати матеріали з цифрової грамотності та інтернет-безпеки, використовуючи групові завдання та взаємодію в онлайн-середовищі.

Іншим прикладом є впровадження цифрових асистентів у навчальний процес, які надають підтримку та консультації з питань цифрової безпеки. Це

сприяє формуванню навичок безпеки в онлайн-середовищі та забезпечує педагогічну підтримку у впровадженні цифрових технологій в навчання.

Практичне використання цифрових інструментів у даних контекстах може значно покращити рівень безпеки дітей в Інтернеті та підготувати їх до відповідального використання цифрових технологій.

Проведені дослідження підтверджують, що комбінація цифрової компетентності та ефективного використання хмарних технологій може значно підвищити безпеку дітей в Інтернеті. Важливим є те, що формування навичок інтернет-грамотності та використання передових технологій може створити надійний щит для дітей, захищаючи їх від ризиків та негативного впливу онлайн-середовища.

З огляду на швидкий технологічний розвиток та зростання онлайн-активності серед дітей, тема безпеки в Інтернеті буде надзвичайно актуальною і в майбутньому. Прогнозується, що високий рівень взаємодії дітей з цифровими технологіями та збільшення їх онлайн-присутності створять нові виклики та потреби в сфері захисту юних користувачів від цифрових загроз.

Враховуючи швидкі темпи технологічного розвитку, важливо регулярно оновлювати інструкції та навчальні матеріали з цифрової безпеки. Використання актуальних прикладів та сценаріїв допоможе дітям краще розуміти та адаптуватися до нових викликів.

Вдосконалення методик може включати в себе використання новітніх технологій, таких як віртуальна реальність, інтерактивні платформи та штучний інтелект, для створення більш ефективного та захопливого навчального середовища [1, с. 72].

Співпраця з технологічними компаніями може сприяти впровадженню новітніх технологій та розробці інноваційних методик безпеки в Інтернеті. Розробка персоналізованих технологічних інструментів, які враховують індивідуальні особливості та потреби дітей, може значно підвищити ефективність засобів безпеки. Співпраця на глобальному рівні між урядовими структурами, освітніми установами та технологічними компаніями дозволить обмінюватися кращими практиками та створювати єдині стандарти безпеки в Інтернеті для дітей. Залучення до участі спільноти та формування культури цифрової безпеки в родинах та школах сприятиме створенню стійкого та безпечного інтернет-середовища.

Розглянемо деякі практики та інноваційні підходи, спрямовані на розвиток цифрової компетентності та формування у дітей навичок безпеки в онлайн-середовищі.

«Цифрова гігієна» у шкільній програмі. Ця методика включає в себе інтеграцію основ цифрової безпеки та цифрової грамотності у навчальні плани та програми. *Ефективність* – діти отримують систематичні знання щодо безпеки в Інтернеті, які застосовують у повсякденному житті.

Використання інтерактивних ігор для навчання безпеки. Розробка та впровадження інтерактивних ігор, що моделюють ситуації в Інтернеті та навчають правилам безпеки. *Ефективність* – граючись, діти отримують практичний досвід та розвивають навички безпечної поведінки в Інтернеті.

Організація відкритих лекцій для батьків. Проведення лекцій та семінарів для батьків щодо цифрової безпеки дітей, з врахуванням актуальних тем та тенденцій. *Ефективність* – батьки отримують інформацію та рекомендації щодо контролю та підтримки безпеки своїх дітей в Інтернеті.

Рекомендується включати методики з цифрової безпеки у шкільні програми як обов'язкову складову. Це створить систематичний підхід та забезпечить розвиток відповідних навичок протягом усього навчання.

Розробка мобільних додатків та онлайн-ресурсів, які надають інтерактивний спосіб навчання безпеки в Інтернеті, може стати ефективним засобом залучення дітей та підтримки їх навчання.

Важливо організувати спільні заходи для батьків та дітей, де будуть відзначені досягнення у цифровій безпеці. Це підтримає спільноту та сприятиме позитивній динаміці.

Використання власних технічних можливостей, таких як віртуальна реальність та інші інтерактивні технології, дозволить створити захопливі та ефективні уроки з безпеки в Інтернеті.

Впровадження цих рекомендацій допоможе забезпечити ефективне та систематичне навчання з питань цифрової безпеки, готуючи дітей до відповідального та безпечного використання інтернет-ресурсів.

Формування цифрової безпеки дітей – це завдання, яке вимагає комплексного підходу, співпраці всіх зацікавлених сторін – від батьків та вчителів до технологічних компаній та урядових структур. Захистити молоде покоління від цифрових загроз і забезпечити їхній розвиток у цифровому середовищі – це спільна відповідальність, яка має долучити всіх учасників суспільства [3, с. 27].

Забезпечення цифрової безпеки для дітей в Інтернеті – це завдання, що стає все більш актуальним і вимагає від нас системного та інноваційного підходу. Інтернет визначає наше сучасне життя і зростання дітей у цьому цифровому світі вимагає від нас ефективних стратегій, щоб забезпечити їх безпеку та розвиток.

Хмарні технології, цифрова компетентність та практичне використання цифрових інструментів у шкільному та сімейному середовищі виявляються ключовими компонентами успішної політики цифрової безпеки. Розглядаючи інноваційні методики, досліджуючи знахідки та інновації, а також аналізуючи думки користувачів, ми робимо важливий крок у напрямку створення безпечного та підтримуючого інтернет-середовища для дітей.

Безпека в Інтернеті – це виклик для нашого суспільства і від нашої спільної уваги та зусиль залежить майбутнє наших дітей в цифровому світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кочарян А.Б., Гущина Н.І. Виховання культури користувача Інтернету. Безпека у всесвітній мережі: навчально-методичний посібник. Київ, 2011. 100 с.

2. Безпечне користування сучасними інформаційно-комунікативними технологіями / О. Удалова та ін. К.: Україна, 2010. 72 с.

3. Діти в Інтернеті: як навчити безпеці у віртуальному світі : посібник для батьків / Литовченко І.В. та ін. К.: Видавництво: ТОВ «Видавничий Будинок Аванпост-Прим», 2010. с. 48.

ІНСТРУМЕНТИ ФОРМУВАННЯ НАВИЧОК БЕЗПЕЧНОГО ВИКОРИСТАННЯ СЕРВІСІВ МЕРЕЖІ ІНТЕРНЕТ

Сергій ПОЙДА

Не можна уявити сучасну дитину без гаджета з підключенням до Інтернету. Щодня діти користуються онлайн-сервісами, соціальними мережами, месенджерами. На жаль, саме вони займають у житті дитини чільне місце, відсуваючи в бік родину та друзів. Таку саму долю має і навчання, адже чільну роль у взаємодії дітей та гаджетів займають розваги. Водночас активна взаємодія з онлайн-сервісами збільшує ризик для дитини стати жертвою кібератаки. Часто діти не розуміють, що їх дії можуть стати причиною суттєвих втрат, аж доки ці втрати не стануть явними.

Перш за все, це стосується відсутності в дітей розуміння принципів безпечної роботи в мережі інтернет. Діти можуть ненавмисно розміщувати персональні дані чи компрометуючі матеріали в Інтернет. Це може статись внаслідок недостатньої їх обізнаності щодо захисту особистої інформації, або вони можуть піддатися тиску прийомів соціальної інженерії.

Ще одна проблема, яка може постати перед дітьми, це кібербулінг - небажана та агресивна поведінка в Інтернеті та соціальних медіа з боку інших дітей. Кібербулінг може приймати різні форми, такі як образи, загрози, поширення неправдивої інформації або навіть потенційно шкідливих матеріалів. Це серйозна проблема, яка може мати негативні наслідки для постраждалих - психологічні травми, самознецінювання та соціальна ізоляція.

Разом із тим, крім психологічної шкоди, неправильне поводження у мережі Інтернет може призвести і до суттєвих матеріальних втрат. Діти можуть стати жертвами кібершантажу, коли зловмисники отримують доступ до їх персональних даних, фотографій чи іншої конфіденційної інформації та вимагають викуп за її повернення або нерозголошення через мережу. Недбалість у захисті персональних даних, зокрема, паролів, номерів банківських карт, адреси проживання, номерів телефонів тощо, може призвести до вчинення щодо них злочинів та спричинити серйозні наслідки для дитини і її сім'ї. Діти можуть ненавмисно завдати шкоди безпеці сімейних комп'ютерів, смартфонів, планшетів та інших пристроїв, дозволивши встановлення шкідливого програмного забезпечення, або надавши дані кіберзлочинцям.

Водночас заборона користування онлайн-сервісами, скоріше за все, не дасть очікуваного позитивного результату – безпечного та відповідального використання сервісів Інтернет з боку дитини. Такі дії з боку батьків змусять дитину шукати шляхи та можливості обійти заборону, що може призвести до гірших наслідків. Саме тому варто зосередитись на двох підходах до організації безпечного використання дітьми сервісів мережі Інтернет, а саме, батьківському контролі та навчанні дітей кібербезпеці.

Батьківський контроль дозволяє батькам керувати доступом до небажаного контенту, встановлювати часові обмеження для використання пристрою, а також

контролювати та відстежувати активність своєї дитини в мережі. Це допомагає захистити дітей від небезпеки онлайн, недоречних звернень та шкідливого впливу. Реалізація таких функцій на дитячих пристроях стає необхідністю у світі, де технології є невід'ємною частиною нашого життя, а безпека дітей отримує найвищий пріоритет.

Для того, щоб зрозуміти, як реалізовано функції батьківського контролю, зокрема на пристроях, які працюють на операційній системі Android, можна скористатись порадами онлайн-ресурсу «Навчайте, де б Ви не були» від Google https://teachfromanywhere.google/intl/uk/#for-families. Ресурс містить цікаву та корисну інформацію для керівників закладів освіти, вчителів та батьків, повністю перекладену українською. Крім того, тут можна знайти посібники та ігри з кібербезпеки, зокрема, Be Internet Avesome (https://beinternetawesome.withgoogle.com/uk_ua/interland), яка також нещодавно отримала українську локалізацію.

Зрозуміло, що лише батьківський контроль не може вберегти дітей від небезпек мережі Інтернет. Найкращим інструментом для цього є розвинуте критичне мислення дітей та навички безпечної взаємодії з сервісами мережі Інтернет. Отримати необхідні знання та навички діти можуть як у закладах освіти, так і самостійно, скориставшись для навчання онлайн-курсами на платформах:

- https://osvita.diia.gov.ua/
- https://prometheus.org.ua/
- https://vumonline.ua/
- https://ed-era.com/
- https://cyberkidsukraine.org/mc/index.php/usr/login/login

Наведені ресурси є безоплатними та можуть використовуватись як учителями, так і дітьми для підвищення власного рівня навичок безпечного поводження у мережі Інтернет. Крім матеріалів з кібербезпеки на вказаних ресурсах можна знайти велику кількість навчальних курсів, які можуть стати у пригоді користувачам мережі Інтернет.

Таким чином, навчання дітей принципам кібербезпеки сприяє розвитку критичного мислення та формуванню відповідальної поведінки в мережі. Батьки та вчителі відіграють важливу роль у цьому процесі. Вони повинні розуміти принципи відповідального використання сервісів мережі Інтернет для того, щоб підтримувати дітей в цьому питанні, надавати їм необхідну допомогу та рекомендації. Водночас надзвичайно важливим також є приклад безпечної поведінки учителів та батьків в мережі. При цьому, хоча батьківський контроль і захищає дітей, значно важливішим для організації безпечного середовища є формування навичок безпечного та відповідального використання ресурсів Інтернет через навчальні курси та ігри. Навчальні курси з кібербезпеки для дітей можуть стати корисним доповненням шкільної програми та є важливим інструментом формування цифрової грамотності.

БЕЗПЕКА: АКСІОЛОГІЧНИЙ ПІДХІД

Ірина БОЙКО

Безпекова парадигма в українській освіті сьогодні є надто актуальною, зокрема, через війну рф-ії вУкраїні, Covid-19 та, загалом, у зв'язку з подіями, що відбуваються у світі (Ізраїль). Вона потребує більш детального та глибинного аналізу і це спонукає не лише науковців, а й педагогічних працівників зосередитися на проблемних питаннях реагування організму людини/дитини на небезпеку, на систему понять і уявлень про безпеку в цілому, на механізми та шляхи забезпечення безпеки людини, суспільства та держави в умовах сьогодення. У сфері освіти феномен безпеки тісно пов'язаний з уявленням про безпеку усіх її суб'єктів (науково-педагогічних, педагогічних працівників, здобувачів освіти та ін.). Актуальність питання зачіплює і самі сучасні підходи щодо дефініції поняття «безпека», його відповідності сучасним викликам, небезпекам і загрозам. За різних методологічних підходів дефініція «безпека» має, здебільшого, альтернативні тлумачення.

Вітчизняні дослідники (С. Пирожков, О. Бєлов, С. Селиванов, М. Косолапов, Г. Мурашин, Є. Кравець, С. Гордієнко, В. Картавцев та ін.) «безпеку» характеризують як певний стан системи та її структурних складових - як стан захищеності (соціального об'єкта та суб'єкта - особи, суспільства, держави) [4]. У тлумачному словнику Даля В.І. дефініція поняття «безпека» дається як відсутність небезпеки, збереження життя, надійність; стан захищеності [3]. У сучасній Вікіпедії зазначено: «безпека людини – такий стан людини, коли дія зовнішніх і внутрішніх факторів не призводить до смерті, погіршення функціонування та розвитку організму, свідомості, психіки та людини в цілому і не перешкоджає досягненню певних бажаних для людини цілей» [1]. У законодавчих актах України щодо безпеки вживаються такі поняття як розуміння «захищеність від загроз»: національна безпека, державна, інформаційна, екологічна, гуманітарна, інформаційна, кібербезпека, безпека життєдіяльності, конкретних видів діяльності тощо [2].

Поняття «безпека» у наукових джерелах (відносно суб'єкта життєдіяльності) у широкому та вузькому значеннях розуміється як: певні умови, у яких перебуває суб'єкт - «… коли дія зовнішніх факторів і внутрішніх чинників не призводить до процесів, що вважаються негативними по відношенню до даної складної системи у відповідності до наявних, на даному етапі, потреб, знань та уявлень»; як «безпека людини – такий стан людини, коли дія зовнішніх і внутрішніх факторів не призводить до смерті, погіршення функціонування та розвитку організму, свідомості, психіки та людини в цілому і не перешкоджає [2]. Філософське тлумачення природи безпеки витікає з об'єктивної цілісності природи та суб'єктивного сенсу людського життя [3]. Саме суб'єктивність сенсу життя, суб'єктивність психічних процесів щодо рефлексії та здатності людини до аналізу, прогнозування наслідків (як позитивних, так і негативних) зовнішнього

(внутрішнього) впливу, зумовлює феномен безпеки. Природна властивість людського організму на рівні безумовних реакцій (інстинктивних, або психологічних механізмів захисту) забезпечує ідентифікацію будь-якої ситуації як «безпечна – небезпечна» та забезпечує збереження життя як «homo sapiens», так і соціальній істоті – особистості. Без такої ідентифікації «безпека – небезпека» неможлива нормальна адаптація особи як у суспільстві, так і забезпечення збереження її психологічного здоров'я у нормі. Отже, здатність людини до передбачування будь-яких негативних наслідків у майбутньому, які пов'язані з реальними зовнішніми (внутрішніми) впливами, або визначення небезпечності об'єкта (предмета), спричинює феномен небезпеки. Саме цей феномен забезпечує процес виживання.

Як соціальне явище, безпека розглядається від глобального до локального аспектів: від якості системи та її цілісності (В.Могилевський), наявності силового ресурсу та конкретних зусиль усіх державно-суспільних структур у забезпеченні безпеки до безпеки окремої особистості. У соціальному просторі – під час процесу адаптації/дезадаптації особистість здатна до рефлексії, самоаналізу свого фізичного та психічного стану відносно будь-якого об'єкта щодо небезпеки. Феномени «безпека – небезпека» у соціальному просторі (людському) виступають як однополярні, тобто, має місце суб'єктивність відношення до ситуації: те, що є природнім для людини – є безпечним, а те , що проти природнього буття, як загроза його існуванню – є небезпечним. Відтак, феномен «безпека – небезпека» спричиняється та функціонує у суб'єктивній формі [5].

Безпека та проблема цінності психологічного здоров'я людини (психологічна безпека) особливо у гострій формі виникає у суспільстві, у якому знецінюється культурна традиція та ідеологічні установки. *Психологічна безпека*: розглядається науковцями як наслідок, як чинник психологічного благополуччя особистості. Сьогодні воно набуває особливого звучання, значення та потребує першочергової уваги, зокрема, у сфері освіти. Проблеми створення та збереження психологічного благополуччя особистості (ВООЗ: стан благополуччя – психічного/психологічного здоров'я) у сфері освіти є прологом до здоров'я конкретної особи, зокрема, та формування/функціонування здорового суспільства, загалом. Питання психологічного благополуччя знаходять своє відображення у роботах відомих американських психологів А.Маслоу, В. Франкла, К. Роджерса, К. Ріффа, Едварда Дісі &Річарда Раяна та інші. Цікавим фактом в історії вивчення проблем психологічного здоров'я є те, що Мартін Селігман першим, звернув увагу на те, що у вивченні питання психічного/психологічного здоров'я необхідно перенести акцент на вивченні його на фізично, соціально-психологічно здорових людях, а не клінічно хворих. Теорія самодетермінації Едварда Дісі & Річарда Раяна базується на припущенні (доведених гіпотезах) про те, що, за наявності певних фруструючих обставин, і соціальні, і культурні чинники стимулюють і посилюють, або придушують вольові і ініціативні якості особистості, що впливає, здебільшого, насамперед, на її суб'єктивне психологічне благополуччя і на якість діяльності загалом. Складові теорії: 1) теорія базових психологічних потреб (Basic Psychological Needs Theory, BPNT); 2) теорія організмічної інтеграції (Organismic Integration Theory, OIT);

3) теорія каузальних орієнтацій (Causality Orientations Theory, COT); 4) теорія когнітивної оцінки (Cognitive Evaluation Theory, CET); 5) теорія змісту цілей (Goal Contents Theory, GCT). Вона, теорія, перегукується з поглядами К. Ріфф, яка теж виокремлює наступні показники психологічного благополуччя:

1) «самоприйняття» - позитивна оцінка себе і свого минулого життя;

2) «особистісне зростання» - почуття подальшого зростання і розвитку;

3) «ціль у житті» - особистості переконання, що життя людини є цілеспрямованим і значущим;

4) «позитивні відносини з іншими» - успішні відносини з оточуючими людьми;

5) «управління середовищем» - здатність керувати ефективно своїм життям і навколишнім середовищем;

6) «почуття самовизначення» - здатність виносити власні судження.

Можна зробити висновок, що феномен психологічного благополуччя виступає тією людською цінністю, яка дозволяє людині відчути та усвідомити власну автономію переживання щастя і повноти самореалізації. Цей стан людини, без сумніву, виступає для неї у якості індикатора безпеки та синергічно пов’язаний із середовищем – з внутрішнім і зовнішнім. На думку науковців (В.Панов, К.Роджерс, В.Рубцов, Є.Клімов, В.Слободчиков, В.Ясвін та ін.), домінантну роль у цьому відіграє освітнє середовище, яке вони визначають як таке, що є підсистемою соціокультурного середовища як сукупність факторів, обставин, ситуацій, які склались історично як цілісність спеціально організованих умов розвитку особистості, суб’єктів освітнього простору. Є.Клімов виокремлює наступні складові освітнього простору: *соціально-контактну* (особливості внутрішньої та зовнішньої взаємодії, структура колективу(наявність угрупувань, неформальних лідерів (зірок), ізольованих (ізгоїв), референтних груп та ін.; рівень захищеності від різного роду домагань); *інформаційну* (прийняті норми і правила взаємодії учасників освітнього процесу, традиції, засоби наочного подання інформації); *предметну* (матеріальні та гігієнічні умови); *соматичну* (здоров’я, самопочуття). Векторами аналізу психологічної безпеки освітнього середовища виступають дефініції: 1) *свобода – залежність*: домінанта чиїх інтересів (пріоритет) в даному освітньому середовищі (особистості чи групи); ведений – ведучий: підлаштування у педагогічній взаємодії (хто кого веде?); індивід – група: яка форма виховання переважає в даному середовищі; 2) *активність – пасивність*: перевага використання «батіг – медовик» - чи практикується у даному освітньому середовищі покарання, чи стимулюється прояв ініціативи учасників освітнього процесу; 3) *сензитивність до…*– чи знаходять позитивний відгук у середовищі ті чи інші творчі прояви учасників освітнього процесу. А також, слід ефективність педагогічного впливу (аналіз впливу) розглядати через призму *основних ознак психологічного безпечного середовища* – людиноцентризм, гуманістичну спрямованість; взаємодію, вільну від проявів психологічного насильства; референтну значущість і причетність кожного до конструювання і підтримки психологічної комфортності освітнього середовища. Результатом, на який сподіваємося, має бути особистісне зростання кожного суб'єкта освітнього процесу.

Висновок. Отже, за певних умов, бажаний результат забезпечується наступними факторами створення психологічно безпечного освітнього середовища: 1) моніторинг психологічної безпеки освітнього середовища та учасників освітнього процесу; 2) психолого-управлінське консультування керівників закладів освіти щодо управління освітнім середовищем у контексті психологічної безпеки; 3) організація спеціального соціально-психологічного навчання учасників освітнього процесу; 4) підготовка практичних психологів системи освіти до психологічного супроводу взаємодії суб'єктів освітнього процесу та утворення ними безпечного освітнього середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Безпека. Вікіпедія : вільна енциклопедія: https://uk.wikipedia.org › wiki ›
2. Горлинський В.В. Феномен безпеки як об’єкт аксіологічної рефлексії. *Мультиверсум. Філософський альманах*. Київ: Центр духовної культури, 2014. № 40.
3. Гордієнко С.Г. Сутність та зміст поняття «державна безпека». *Стратегічна панорама*. Київ: науково-практичний журнал Національного інституту стратегічних досліджень. 2013. № 2. С. 114-120
4. Корж І.Ф. Адміністративно-правове регулювання відносин у сфері державної безпеки України: монографія. Вінниця : ТОВ «Нілан-ЛТД», 2013. 384 с.
5. Рибалка В.В. Аксіологічні основи психологічної культури особистості: навч.-метод. посіб. К.: АПН України, Ін-т пед. освіти і освіти дорослих; Ін-т обдарованої дитини; АПН і МОН України, Укр. наук.-метод. центр практ. психології і соц. роботи. Чернівці: «Технодрук», 2009. 228 с.

ЦИФРОВІЗАЦІЯ ОСВІТНЬОГО ПРОЦЕСУ ЗАКЛАДУ ДОШКІЛЬНОЇ ОСВІТИ ЯК ТРЕНД СУЧАСНОГО СУСПІЛЬСТВА

Наталія ВОЛЄГОВА

Цифровий простір – невід’ємна складова життя кожної сучасної людини, якому властива тенденція до швидких змін та постійної трансформації в нові форми, у тому числі і суспільні. Такі зміни стають прямою передумовою до формування нових підходів до розвитку системи освіти, тобто цифровізації.

Науковці розглядають цифровізацію як: трансформацію, що передбачає широкий спектр інтерактивних та мультимедійних ресурсів, які дозволяють вибудувати онлайн-діалог між усіма учасниками освітнього процесу; як перехід на цифровий спосіб комунікації, збереження та передачі інформації за допомогою цифрових пристроїв; як зміна парадигми того, як ми мислимо, як ми діємо, як ми спілкуємося із зовнішнім середовищем та один з одним [2].

Цифровізація освітньої сфери дошкільної освіти постає актуальним питанням в низці нормативно-правових документів, а саме: Законах України «Про освіту», «Про дошкільну освіту», Базовому компоненті дошкільної освіти (нова

редакція). Зокрема в Базовому компоненті дошкільної освіти (нова редакція) введено у варіативну складову освітній напрям «Дитина в сенсорно-пізнавальному просторі. Комп'ютерна грамота», що передбачає формування цифрової компетентності дошкільника, адже для сучасної дитини дошкільного віку, у якої провідною є ігрова та пізнавальна діяльність, цифровий простір став невід'ємною складовою та способом отримання нових знань та емоцій, формування інформаційно-комунікаційної компетентності.

Цифрові технології досить швидко та стрімко інтегруються в освітні процеси закладів освіти, у тому числі і закладів дошкільної освіти, що характеризує сучасний етап її розвитку, якісні зміни змісту, структури освітніх процесів, активне впровадження дистанційних технологій, особливо коли в цьому виникає нагальна потреба.

На мою думку, упровадження та використання цифрових технологій в освітньому процесі закладу дошкільної освіти передбачає:

- модернізацію технічного забезпечення закладу дошкільної освіти;
- створення безпечного цифрового освітнього середовища;
- розвитку інформаційно-комунікаційної компетентності педагогів;
- якісних змін у підходах до організації освітньої діяльності дітей дошкільного віку;
- стимулювання пізнавальної активності дошкільнят за допомогою використання інформаційно-комунікаційних технологій;
- виховання інтелектуальної, різнобічно розвиненої, креативної особистості та підготовку дошкільника до цифрових реалій сьогодення.

Виходячи з зазначених вище умов та вимог сучасного суспільства в умовах цифровізації щодо формування інформаційно-комунікаційної компетентності, у дітей дошкільного віку дещо змінюється і роль педагога, оскільки тепер «він є не лише носієм знань, якими ділиться з вихованцями, а й провідником до цифрового світу» [5]. Згідно з Професійним стандартом «Вихователь закладу дошкільної освіти», затвердженим наказом Міністерства економіки України від 19 жовтня 2021 року за №755-21, в описі трудових функцій, а саме професійного розвитку та самовдосконалення, виокремлено інформаційно-комунікаційну здатність як окрему опцію вихователя.

Інформаційно-комунікаційна здатність, у свою чергу, передбачає формування у вихователя дошкільного закладу таких професійних компетентностей, як здатність орієнтуватися в інформаційному просторі; здатність ефективно використовувати ІКТ та електронні освітні ресурси в професійній діяльності; здатність дотримуватися правил в цифровому середовищі. Кожна здатність в свою чергу формується лише за умови сформованих у вихователя сталих знань, умінь та навичок.

Покликаючись на Професійний стандарт, варто деталізувати:

- здатність орієнтуватися в інформаційному просторі передбачає сформовані знання педагога з основ медіаграмотності, способів та правил використання сучасного медіапростору, культури користування мережею Інтернет; розвинених умінь та навичок знаходити, опрацьовувати, критично оцінювати зміст та достовірність, надійність інформаційних джерел та

застосовувати їх у професійній діяльності;

- здатність ефективно використовувати ІКТ та електронні освітні ресурси в професійній діяльності передбачає вільне орієнтування педагога в нормативно-правовому забезпеченні та дотриманні правових вимог використання ІКТ та електронних освітніх ресурсів в професійній діяльності; а також дотримання санітарно-гігієнічних вимог ІКТ в професійній діяльності, їх особливостей;
- здатність дотримуватися правил в цифровому середовищі передбачає те, що педагог знає та орієнтується в правилах безпечної поведінки в цифровому середовищі, способах контролю контенту та реагування на ризики в цифровому середовищі, що передбачає дотримання вимог щодо безпечної поведінки та використання інструментів контролю контенту, захисту персональних даних, охорони прав інтелектуальної власності в цифровому середовищі [4].

Сформовані вищезгадані здатності на сучасному етапі становлення суспільства «стали потужним ресурсом професійного розвитку педагогів, забезпечуючи їм швидку адаптацію до сучасних умов існування в інформаційному суспільства, розширення комунікаційних можливостей, самореалізацію, збагачення професійного досвіду» [5].

На мою думку, в професійній діяльності педагога варто виокремити чотири основні напрями, в яких реалізовуються навички цифровізації та медіаграмотності вихователя дошкільного закладу:

- організація освітнього процесу та безпосередня педагогічна діяльність з дітьми дошкільного віку відповідно до запитів та потреб здобувачів освіти, у тому числі і забезпечення здобуття дошкільної освіти дітьми з особливими освітніми потребами;
- організація ефективної співпраці та безконфліктної комунікації з батьками;
- співпраця з колегами на принципах командної взаємодії;
- планування та реалізація індивідуального професійного розвитку та самоосвіти.

Розкриваючи зміст першого виокремленого напряму, доцільно зазначити, що сьогоднішні реалії цифровізації суспільних відносин дозволяють визначити дошкільний вік як початковий та сенситивний етап формування цифрової компетентності. Цифрову компетентність дитини дошкільного віку варто виокремити як нову форму грамотності, яка в сучасному соціумі постає необхідним компонентом будь-якого процесу життєдіяльності та співумовою набуття дитиною особистісного практичного досвіду [5]. Дитина дошкільного віку вже є активним користувачем цифрових пристроїв, вміло користується різного роду гаджетами, й поява та постійне оновлення технологій, орієнтованих на дошкільний вік, є не чим іншим, як формою задоволенням суспільного запиту. На дітей дошкільного віку орієнтовані: комп’ютерні ігри на розвиток математичних здібностей; ігри, які навчають навичкам планування та управління; ігри з розвитку основних психологічних процесів; програми, що сприяють мовному розвитку; ігри-подорожі; артстудії; віртуальні екскурсії тощо. Цифрові технології приходять на допомогу сучасному вихователю як потужний засіб

моделювання процесу, який складно візуалізувати в реальних умовах та робить освітній процес наочним, формує інформаційну культуру дитини дошкільного віку, сприяє розвитку розумово-аналітичних, дослідницьких здібностей. Цифровізація освітнього процесу, особливо в спеціальних закладах дошкільної освіти, інклюзивних закладах дошкільної освіти, за умов дозованого впровадження коректних технологій в педагогічну діяльність, відкриває дітям дошкільного віку з особливими освітніми потребами великий спектр нових можливостей пізнання світ та форм соціалізації, забезпечує індивідуалізацію освітнього процесу та набуття дитиною практичного досвіду.

Однак, не дивлячись на значну кількість переваг, інтенсивна цифровізація та вплив на ранній розвиток дитини широкого інформаційного простору має і низку негативних сторін, а саме: негативний вплив на фізичне здоров'я дитини (зір, постава); негативний вплив на соціальний розвиток дитини при безконтрольному використанню нею інформаційно-цифрового простору; негативний вплив на розвиток пізнавальних здібностей; витіснення інших видів діяльності, які характерні для дітей дошкільного віку та слугують підґрунтям для повноцінного розвитку дитячого організму; ризики негативного небезпечного контенту.

Окремою проблематикою цифровізації закладу дошкільної освіти, на мою думку, варто виокремити питання впливу ІКТ на дітей, що мають вади зору. При використанні моніторів, екранів потрібно враховувати такі чинники:

- відстань дитини від екрану;
- оснащення, наприклад, діти зі складним ураженням зорового апарату потребують спеціальних пристосувань, індивідуального режиму та постійного контролю окуліста; діти з розладами зору можуть працювати із засобами цифровізації після консультації окуліста за умови оптимальної оптичної корекції, нормального об'єму акомодації та індивідуального режиму, періодичного офтальмологічного контролю;
- якість цифрового зображення (розмір та чіткість);
- освітлення;
- періодичне виконання гімнастик для очей; відпочинок, адже перевтома, яку отримують очі та опорний апарат при тривалому використанні гаджетів знімається досить довго [1].

Шкідливий вплив на зоровий апарат відбувається поступово, негативний ефект теж накопичується поступово, тож важливим є контроль зі сторони дорослого за дотриманням тривалості використання цифрових засобів дитиною та безпечності цифрового контенту [1].

Організація ефективної співпраці та безконфліктної комунікації з батьками забезпечує синергію партнерства учасників освітнього процесу, ефективність та спрямованість виховання дітей дошкільного віку в єдності поглядів. Також цифровізація освітнього процесу впливає на форми роботи з батьками, а саме: забезпечує появу нових, відкритість системи взаємодії. Використання нових форм роботи дозволяє вихователю дошкільного віку йти в ногу з часом, здійснювати швидкий збір інформації та її узагальнення, поширення потрібного інформаційного контенту, спрямованого на педагогічний супровід батьківської

громадськості. Також висвітлення діяльності дітей в закладі протягом дня чи під час певного заходу дозволяє створювати позитивну атмосферу взаємодії, фасилітації батьківського колективу зі сторони педагога, пропедевтичну роботу з конфліктами тощо. Однак, відповідно до Методичних рекомендацій щодо організації освітнього процесу у 2023/2024 н. р., у закладах дошкільної освіти (додаток до листа МОН від 21.08.2023 №1/012490-23) йдеться про те, що: «Звітування батькам фото та відео про перебіг заходів не входить до посадових обов'язків педагогів, вони можуть це робити виключно за своїм бажанням» [3]. Також вихователю важливо враховувати нормативно-правовий аспект щодо розміщення фото- та відеопрезентування своєї педагогічної діяльності чи висвітлення заходів закладу за участі дітей в соціальних мережах, на сайтах, а саме наявність письмового дозволу батьків, або представників дитини.

Співпраця з колегами на принципах командної взаємодії теж асимілювала в себе методи та прийоми цифровізації. З досвіду роботи можу зазначити, що це: створення спільних документів, проєктів за умови дистанційної діяльності один з одним та в зручний для кожного з педагогів час; висвітлення власного педагогічного досвіду на електронних ресурсах та обмін досвідом з колегами через інтернет-платформи, дошки, програми тощо; методичний супровід педагогічного колективу чи окремо визначеного педагога. Також володіння цифровими засобами спілкування, обміну інформацією, створенням цифрового контенту дозволяє забезпечити безперервність освітнього процесу за умови здійснення дистанційної освітньої діяльності закладу дошкільної освіти.

Модель сучасного педагога передбачає готовність до застосування нових освітянських ідей, здатність постійно навчатися, бути у постійному творчому пошуку; здійснення планування та реалізації індивідуального професійного розвитку та самоосвіти. За словами Сухомлинського «...немає людей більш допитливих, невгамовних, більш одержимих думками про творчість, як учителі», гадаю, до цього числа сміливо можна віднести і модель вихователя дошкільного закладу. Для сучасного вихователя підвищення рівня своєї обізнаності в сучасних освітніх тенденціях передбачає добір та проходження різного роду курсів, семінарів-практикумів, тренінгів; участь в офлайн та онлайн зустрічах з різного роду методичних питань; поділ досвідом з колегами в межах та поза межами закладу тощо. У Професійному стандарті щодо здатності вихователя планувати та реалізовувати індивідуальний професійний розвиток та самоосвіту зазначено: «Планує професійний розвиток відповідно до визначених цілей. Критично обирає види форми, програми та суб'єктів підвищення кваліфікації відповідно до власних професійних потреб та вимог законодавста». Все це потребує володіння навичками цифровізації та вміння аналізувати та критично оцінювати наявний інтернет-контент. Особливо це вміння актуальне в сучасних реаліях українського суспільства, коли безпекова ситуація спонукає до використання онлайнових ресурсів та різного роду форм дистанційного комунікування, що неможливе без розвинених диджитал навичок.

Висновки. Виходячи з викладеного вище, можна зробити висновок, що цифровізація як тенденція розвитку сучасного суспільства вдало впроваджується в освітній процес та є невід'ємною його складовою. Вимагає від вихователя

сформаваних здатностей, умінь та навичок ефективно використовувати ІКТ та електронні ресурси в професійній діяльності: здійсненні роботи з дітьми та батьками, як учасниками освітнього процесу; в командній взаємодії з колегами; самовдосконаленні власних професійних знань та вмінь. Певним чином законодавчо регламентовані вимоги до формування інформаційно-комунікаційної компетентності у вихованців закладів дошкільної освіти передбачають виховання «дошкільника XXI сторіччя, дитини, яка є активним користувачем цифрових пристроїв» [5]. Завданням педагога ж у цьому зрізі є формування користувацької культури дошкільника з дотриманням санітарно-гігієнічних вимог користування ІКТ, безпечної поведінки та формування корисного, дидактичного спрямованого контенту. Отже, цифровізація як тренд сучасного суспільства передбачає ранню дитячу цифрову соціалізацію, в тому числі дітей з ООП; потребу у відповідно сформованих знаннях дорослого; синергію партнерства закладу дошкільної освіти та батьківської громадськості, завданням якої постає мінімізація впливу цифрових технологій на дошкільників.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Інклюзивне навчання дітей з порушенням зору: монографія / за ред. д-ра психол. н. проф. Синьової Є.П.., д-ра мед. н., проф. Рикова С.О. та авторів. К.: Кафедра, 2017. 320 с.

2. Колеснікова І. В. Цифровізація освітнього процесу в закладі післядипломної педагогічної освіти. Науковий часопис Нац. пед. ун-т імені М. П. Драгоманова. Серія 5. Педагогічні науки: реалії та перспективи, 2020. Вип. 78. С. 117-120.

3. Про окремі питання діяльності закладів дошкільної освіти у 2023/2024 навчальному році : лист МОН України від 21.08.2023 №1/012490-23. URL: https://mon.gov.ua/ua/npa/pro-okremi-pitannya-diyalnosti-zakladiv-doshkilnoyi-osviti-u-20232024-navchalnomu-roci (дата звернення 01.09.2023 р.).

4. Професійний стандарт «Вихователь закладу дошкільної освіти» : наказ Міністерства економіки України від 19 жовтня 2021 року за №755-21. URL: https://mon.gov.ua/ua/npa/pro-zatverdzhennya-profesijnogo-standartu-vihovatel-zakladu-doshkilnoyi-osviti (дата звернення 01.02.2024 р.).

5. Колеснікова І.В., Орлова О.А. Цифровізація освітнього процесу в закладі дошкільної освіти. *Інноваційна педагогіка*, Том 2, 2022. С. 188-191. URL: http://www.innovpedagogy.od.ua/archives/2022/50/part_2/37.pdf (дата звернення 01.02.2024 р.).

ПІДГОТОВКА МАЙБУТНІХ УЧИТЕЛІВ ДО РОЗВИТКУ ЦИФРОВОЇ БЕЗПЕКИ В УЧНІВ

Галина ГЕНСЕРУК, Сергій МАРТИНЮК

Швидкий темп розвитку мережі Інтернет, цифрового обладнання, використання цифрових технологій в закладах освіти є дуже важливими передумовами для багатьох повсякденних дій в сучасному суспільстві. Цифрова компетентність стала необхідною для багатьох професій. Концепція цифрової компетентності і цифрової грамотності зазнала тривалого розвитку. Серед найпоширеніших поглядів на цифрову грамотність на сьогоднішній день є те, що цифрову грамотність можна розуміти як взаємопов'язаний набір навичок або компетенцій, необхідних для успіху в епоху цифрових технологій. Компетенції щодо використання цифрових технологій вважаються необхідною умовою для розвитку цифрових навичок [1].

Важливість цифрової компетенції була визнана Європейським парламентом та Європейською радою в 2006 році. Цифрова компетентність була визначена як одна з восьми ключових компетенцій для навчання впродовж життя та передбачає впевнене та критичне використання цифрових технологій для роботи, дозвілля, навчання та спілкування. Комп'ютерна та інформаційна грамотність описується науковцями як «досягнення учнів у роботі з технологіями в різних контекстах», як «здатність використовувати комп'ютер для дослідження, створення та спілкування з метою ефективної участі вдома, у школі, на робочому місці та в суспільстві» [4].

Здатність розпізнавати проблеми, пов'язані з цифровими технологіями у контексті безпеки є однією з важливих компетенцій. У сучасних дослідженнях виокремлено такі компоненти цифрової безпеки: кібербулінг, безпека в Інтернеті та захист користувачів.

Безпека передбачає захист інформації та комунікації користувачів від проблем, спричинених використанням цифрових технологій. Це пов'язано з конфіденційністю, цілісністю та ефективністю інтернет-технологій та інформації. Безпека означає знання, здібності та ставлення вчителів до розробки навчального контенту, який сприяє, моделює та навчає учнів як цифрових громадян. Вчителі відіграють особливу роль у розвитку цифрової компетентності учнів, оскільки вчитель є зразком, який піклується, орієнтує та навчає інших відповідальному використанню цифрових технологій, безпечному спілкуванню та співпраці, а також обміну інформацією через Інтернет. Однак ця роль може викликати проблеми через помилкову концепцію, згідно з якою вчителі навчають про безпеку так, ніби учні розуміють і мають єдине поняття про Інтернет.

Рамки DigComp і DigCompEdu забезпечили основу для розвитку цифрової компетентності освітян. Вони включають компетенції щодо цифрової безпеки. У них наголошено на відповідальному використанні, повазі до принципів конфіденційності в Інтернеті, які стосуються особистості та інших, піклування про довкілля. У сфері безпеки компетентний користувач може переглядати

конфігурацію безпеки систем і програм, власного комп'ютерного обладнання, налаштовувати та змінювати параметри безпеки своїх електронних пристроїв, шифрувати електронні листи та архіви, а також застосовувати фільтри, щоб уникнути електронного спаму.

Рамки цифрової компетентності для громадян (DigComp) та вчителів (DigCompEdu) включають та описують усі 5 сфер цифрової компетентності. В нашому дослідженні ми детальніше зупинимось на сфері Безпека (Safety).

В рамці DigComp четвертою компетенцією є Безпека. Вона включає наступні виміри [2]:

- 4.1. Захист пристроїв.
- 4.2 Захист персональних даних і конфіденційність.
- 4.3 Захист здоров'я та благополуччя.
- 4.4 Захист навколишнього середовища.

Рівень компетентності майбутніх учителів у часи постправди та фейкових новин, зокрема пов'язаних із цифровою безпекою, є ключовими індикаторами освітньої підготовки.

В нормативних документах, дослідженнях та стратегічних планах окреслено заходи, які сприяють запобіганню проблем, пов'язаних з безпекою, особливо в уразливих групах, за допомогою таких дій, як включення контенту про безпеку та відповідальне використання Інтернету; розробка програм для підвищення обізнаності та покращення довіри та спілкування під час використання Інтернету; розвиток цифрової компетентності батьків і вчителів в контексті цифрової безпеки.

Системи освіти в різних країнах визнають важливість підготовки вчителів до володіння цифровими технологіями, особливо щодо питань безпеки [4]. У підготовці майбутніх учителів безпека має визначатися як питання високого пріоритету в освітній галузі. Цифровому вчителю потрібні знання (педагогічні та змістовні), здібності (соціальні та технічні), а також ставлення до цифрової безпеки та того, як цьому навчати. Вчителі мають взяти на себе відповідальність за навчання цифровій безпеці та ознайомленню своїх учнів з правилами поведінки в Інтернеті. Однак вчителям часто бракує достатньої підготовки, щоб зрозуміти усі ризики. Педагог може слугувати моделлю, щоб допомогти покращити поведінку учнів під час використання технологій, вести бесіди про ризики та шкоду і суттєво впливати на учнів своїми діями.

Нова цифрова культура вимагає вчителів, які є компетентними, практичними та орієнтованими на навчання критичних, відповідальних громадян. Різноманітні дослідження вказують на нагальну потребу в тому, щоб заклади вищої освіти взяли на себе цілісну спрямованість, яка гарантувала б підготовку з підвищення безпеки як питання високого пріоритету в освіті, особливо в програмах підготовки вчителів [3, 5].

Отже, сьогодні є важливою консолідація дій і освітніх заходів в закладах освіти, спільна відповідальність батьків і вчителів, а також необхідність у створенні освітніх програми, які допомагали б уникнути загроз і захиститися від небезпек цифрового світу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Генсерук Г. Р. Цифрова компетентність як одна із професійно значущих компетентностей майбутніх учителів. *Open educational e-environment of modern University*. Київ. 2019. № 6. С. 8–16.
2. DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC106281.
3. Engen B.K., Giæver T.H., & Mifsud L. Guidelines and regulations for teaching digital competence In schools and teacher education: a weak link? Nordic Journal of Digital Literacy. 2015. 10. P. 172-186.
4. Napal M., Peñalva-Vélez A., & Mendióroz A. Development of digital competence in secondary education teachers' training. Education Sciences. 2018. 8, P. 104-112.
5. Shin S. K. Teaching critical, ethical, and safe use of ICT to teachers. Language Learning & Technology. 2015. vol. 19. no. 1. pp. 181–197.

ЦИФРОВІ ІНСТРУМЕНТИ GOOGLE ДЛЯ ЗАХИСТУ КОРИСТУВАЧА В ІНТЕРНЕТІ ЯК СКЛАДОВА КІБЕРГРАМОТНОСТІ ПЕДАГОГА

Петро ГРАБОВСЬКИЙ

Сучасні трансформаційні процеси у сфері освіти, що відбуваються завдяки застосуванню цифрових засобів, передбачають серед іншого створення безпечного електронного освітнього середовища у відповідних закладах (ЗВО, ЗЗСО і тд.) та розвиток цифрової компетентності педагогічних працівників [1]. Разом з тим, відповідно до діючого професійного стандарту вчитель має бути здатним уникати небезпек у інформаційному середовищі, забезпечувати захист і збереження персональних даних (зокрема власних або учнів та їх батьків) [2]. Водночас, переважна більшість педагогічних працівників, учнів ЗЗСО для реалізації освітнього процесу в умовах воєнного стану [3] за дистанційною або змішаною формами навчання використовують відповідні цифрові застосунки Google (ClassRoom, Meet, Forms, Drive та інші), що доступні у особистому або корпоративному (Workspace for Education) облікових записах. Таким чином, обізнаність про пропоновані Google цифрові інструменти для захисту користувача в інтернеті, здатність їх використання у професійній діяльності є наразі важливою складовою кіберграмотності сучасного педагога та основою його кібербезпеки.

У відповідних нормативних документах [4] останній із зазначених вище термінів трактується як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз. Серед них можна виділити такі: програмно-технічні, що передбачають ураження програмно-апаратного забезпечення інформаційно-комунікаційних систем та мереж; економічні (зловмисне

використання систем інтернет-платежів, інтернет-банкінгу тощо); контентні (викрадення та зловмисне використання даних із соціальних мереж, хмарних сховищ, пропаганда наркотиків, розповсюдження фото- та відеоматеріалів щодо вчинення насильства, злочинів тощо) [5].

Необхідно зазначити, що переважна більшість програмно-технічних, економічних та значна частина контентних загроз для користувачів цифрових застосунків, хмарних сервісів від Google нейтралізуються автоматичними засобами захисту, що вбудовані в ці продукти та функціонують на основі штучного інтелекту і квантової криптографії (більш детально див. матеріали [6]). Водночас, саме протидія контентним загрозам передбачає активну участь користувача. Зокрема, педагог у налаштуваннях власного облікового запису Google або його корпоративного варіанту має можливість моніторити такі параметри безпеки:

– відслідковувати «підозрілі дії» – вхід у обліковий запис із пристроїв, що раніше не використовувалися, при цьому користувач має змогу заблокувати на майбутнє такі входи, якщо це здійснив не він;

– налаштовувати параметри входу у свій обліковий запис: активувати двоетапну перевірку, визначити ключі доступу (дають змогу виконувати безпарольний вхід в обліковий запис), змінити за необхідності поточний пароль, уточнити резервну електронну адресу і номер телефону для відновлення доступу до свого облікового запису або двоетапної перевірки;

– контролювати сеанси роботи у обліковому записі з використанням «своїх» пристроїв (часто використовуються для такої діяльності), за необхідності здійснювати дистанційний вихід на таких пристроях, що знаходяться поза межами фізичної досяжності для користувача у відповідний момент часу;

– контролювати зв’язки зі сторонніми додатками і сервісами, що для авторизації використовують функцію «Вхід через Google»;

– активувати безпечний перегляд (передбачає фільтрацію відвертого контенту) із розширеним захистом від небезпечних вебсайтів, розширень і завантажень;

– відстежувати можливе розповсюдження (зокрема купівлю/продаж) особистої інформації (електронної адреси, пароля, імені користувача, дата народження, номер телефону тощо) викрадену через порушення безпеки даних на інших ресурсах та ознайомлюватися із рекомендаціями від Google щодо уникнення таких випадків у майбутньому;

– здійснювати перевірку збережених паролів (засіб «Менеджер паролів») щодо можливого їх зламу через порушення безпеки даних третьої сторони або щодо повторного використання і надійності тощо.

Використання описаних вище можливостей сприятиме кібербезпеці педагогічного працівника закладу загальної середньої освіти у процесі реалізації ним дистанційної форми навчання за допомогою відповідних цифрових засобів освітньої взаємодії Google. Також доцільно зазначити, що ці матеріал можуть бути використані як зміст навчання у закладах післядипломної педагогічної освіти для організації процесу підвищення кваліфікації вчителя що забезпечить розвиток інформаційно-цифрової компоненти його професійних компетентностей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Програма великої трансформації Освіта 4.0: український світанок. МОН України : вебсайт. URL: https://mon.gov.ua/storage/app/media/news/2022/12/10/Osvita-4.0.ukrayinskyy.svitanok.pdf (дата звернення 02.02.2024 р.).

2. Про затвердження професійного стандарту за професіями «Вчитель початкових класів закладу загальної середньої освіти», «Вчитель закладу загальної середньої освіти», «Вчитель з початкової освіти (з дипломом молодшого спеціаліста)»: Наказ Міністерства розвитку економіки, торгівлі та сільського господарства України від 23.12.2020 р. № 2736-20. URL: https://zakon.rada.gov.ua/rada/show/v2736915-20#Text (дата звернення 02.02.2024 р.).

3. Про деякі питання організації здобуття загальної середньої освіти та освітнього процесу в умовах воєнного стану в Україні : Наказ Міністерства освіти і науки України від 28.03.2022 р. № 274 URL: https://mon.gov.ua/storage/app/uploads/public/624/200/1c5/6242001c570a8380605603.pdf (дата звернення 02.02.2024 р.).

4. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України; Стратегія від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення 02.02.2024 р.).

5. Грабовський П. П. Протидія кіберзагрозам під час використання цифрових засобів освітньої взаємодії. *Житомирщина педагогічна.* 2022. №2 (26). URL: https://imso.zippo.net.ua/wp-content/uploads/2022/07/6.-Грабовський-П.-П..pdf

6. Центр безпеки Google : вебсайт. URL:https://safety.google/intl/uk_ALL .

ПРАВИЛА КІБЕРБЕЗПЕКИ ОСВІТНЬОГО СЕРЕДОВИЩА

Олексій ЗДОРОВЕЦЬ, Любов СЕВЕРИНА

У сучасних умовах, коли заклади освіти працюють в умовах війни та воєнного стану, необхідно вжити конкретних заходів для забезпечення дистанційного навчання та асинхронної взаємодії між учнями та вчителями. Це передбачає не лише використання педагогічних практик, але й навички та застосування технологічних можливостей, а також мережевих та онлайн (офлайн) технологій з урахуванням забезпечення безпеки в інтернеті. Обізнаність та вміння застосовувати спеціальні технічні можливості, критичне мислення щодо великих масивів інформації здатне забезпечити початковий рівень кібербезпеки.

Використання технологій робить наше життя більш комфортним, але водночас породжує нові, раніше невідомі загрози [1]. Основна небезпека в інтернеті полягає в ризику втрати або розкритті особистих даних, а також у можливості стати вразливим і втратити конфіденційність. Похідна загроза

полягає в уявній складності теми кібербезпеки, що призводить до того, що більшість людей просто ігнорує ці загрози.

Комп'ютерна безпека є сукупністю заходів захисту у сфері телекомунікацій та інформатики, пов'язаних із оцінкою та контролем ризиків, що виникають при використанні комп'ютерів та комп'ютерних мереж. Її реалізація спрямована на забезпечення конфіденційності, цілісності та доступності інформації [2].

Закон України «Про основні засади забезпечення кібербезпеки України» дає таке визначення: «Кібербезпека — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі». Створення безпечних комп'ютерних систем і додатків є основною метою діяльності мережевих інженерів і програмістів, а також предметом теоретичних досліджень як у галузі телекомунікацій та інформатики, так і в економіці. Завдяки складності та трудомісткості більшості процесів і методів захисту цифрового обладнання, інформації та комп'ютерних систем від ненавмисного чи несанкціонованого доступу, вразливості комп'ютерних систем стають значущою проблемою для їхніх користувачів.

Кібербезпека – це забезпечення безпеки IT-систем (обладнання та програм). Вона має велике значення, оскільки урядові, військові, корпоративні, фінансові та медичні організації збирають, обробляють та зберігають надзвичайно великі обсяги даних на комп'ютерах та інших пристроях. Значна частина цих даних може бути конфіденційною інформацією, такою як інтелектуальна власність, фінансові дані, особиста інформація тощо, і несанкціонований доступ чи викриття можуть мати серйозні наслідки. Компанії та організації, особливо ті, які мають відповідальність за захист інформації, пов'язаної з національною безпекою, охороною здоров'я чи фінансовою документацією, повинні приймати заходи для захисту конфіденційної інформації про бізнес та персонал. Вже в березні 2013 року представники розвідки країни застерегли, що кібератаки та цифрове шпигунство є головною загрозою національній безпеці, перевершуючи навіть тероризм [2]. Щодо системи кібербезпеки України, то її формують [2]:

- Академічна кібербезпека (ВНЗ, дослідницькі інститути і т. д.);
- Державна кібербезпека (законодавча база, Держспецзв'язку(CERT-UA), кіберполіція, СБУ, Міністерство оборони, Розвідувальні органи, НБУ);
- Комерційна кібербезпека (вендори, програмні та апаратні рішення, методики та методи, досвід, технології і т. д.);
- Некомерційні волонтерські та громадські організації (ІнформНапалм, Український кіберальянс).

Навіть при всіх зусиллях рівень кіберзахищеності України залишається на незадовільному рівні. За думкою експертів, українські системи залишаються вразливими перед потенційними хакерськими атаками. Цьому сприяє низька кваліфікація фахівців, які працюють в державному секторі. Освітній сектор також виявляється вразливим через недостатню обізнаність та розуміння загрози. Україна на даний момент немає централізованого управління для реагування на

кіберзлочини, а ця сфера є найважливішою у наш час. Брак координації і реалізації цих заходів в Україні породжує серйозні проблеми.

Освіта в цьому контексті також відіграє ключову роль, оскільки відсутність навчання та обізнаності сприяє поширенню загроз. В Україні ця ситуація поглиблюється тим, що нова галузь кіберзахисту є ще малорозвиненою, і її викладання здійснюється лише в обраних вищих навчальних закладах [2].

Для набуття необхідних навичок та знань щодо захисту особистих даних у мережі Інтернет можна ознайомитися з кількома простими правилами інформаційної безпеки, наданими українським порталом DefenseUA [3].

Надійний пароль. Ні в якому разі не використовуйте прості паролі, їх дуже легко зламати. Паролі мають бути різні для кожного ресурсу. Якщо ви скрізь використовуєте однаковий пароль, то зламавши один сайт, злочинці отримують доступ до решти ваших акаунтів.

Двоетапна аутентифікація. Двоетапна аутентифікація - це процес підтвердження входу в банківський акаунт чи особистий кабінет за допомогою телефону. Якщо ця функція увімкнена, ніхто не матиме доступу до ваших особистих даних, якщо ви не підтвердите вхід за допомогою телефону. Наприклад, в Google аккаунтах також слід увімкнути двоетапну аутентифікацію. Якщо ви використовуєте телефон з операційною системою Android, то ваш Google аккаунт фактично представляє ваш телефон разом з усією інформацією, збереженою на ньому.

Безпека мобільних пристроїв. Смартфон відкриває перед нами вікно до світу банкінгу та стає електронним гаманцем. Це пристрій, де зберігаються наші особисті фотографії та приватна переписка, що відображає історію нашого життя у вигляді зображень з коментарями. З урахуванням цього смартфон вимагає не менше захисту, ніж наші офіційні документи. Особливу увагу слід приділяти захисту смартфона, особливо коли йдеться про його використання дітьми. На сьогоднішній день існує велика кількість фейкових додатків, які поширюються через рекламу в іграх та на сумнівних вебсайтах. Головною метою цих додатків є викрадення особистих даних користувачів.

Фішингові атаки. Фішингові атаки – це форма шахрайства, спрямована на викрадення конфіденційних даних, зараження пристрою або знищення інформації. Часто цей вид атак використовує електронну пошту як основний засіб. Щоб сплутати користувачів, хакери можуть створювати листи, які виглядають досить правдоподібно. Надзвичайно важливо не запускати програми, які вам відправили незнайомці, і утриматися від включення макросів в Excel, якщо хтось відправив вам таблицю з «важливими даними». Безпека особистої інформації потребує пильності та обачливості до електронних повідомлень.

Неправдиві повідомлення або фейки. Фейки представляють собою неправдиві або підроблені новини, які не витримують жодних перевірок на відповідність фактам, але при цьому можуть суттєво впливати на свідомість значної кількості людей. На сучасному етапі інформаційного розвитку наш інформаційний простір переповнений дезінформацією та фейками. Тому важливо споживати і довіряти лише офіційним та перевіреним джерелам інформації. Під час перегляду емоційних новин чи постів важливо не втрачати критичне

мислення. Фейкові матеріали майже завжди спрямовані на виклик емоцій та шоку.

Ненадійні посилання. Ці посилання всюди – месенджери, соціальні мережі, електронна пошта, смс тощо. Цю тему вже декілька разів обговорювали вище. Наразі посилання – це основна зброя хакера в інформаційному полі. Їх створюють задля крадіжки ваших паролів, доступу, викривлення інформації, знищення інформації та пристроїв.

Ненадійні сайти. Один з найпоширеніших видів шахрайства – це сайти-клони. Їх створюють для розповсюдження фейків або крадіжки даних. Це може бути сайт новин, урядових структур, відомих інтернет-магазинів тощо. Наприклад реальний сайт Служби безпеки України – https://ssu.gov.ua/, а сайт-клон може бути https://ssu.gov.ua.kiev.ua/. Якщо посилання на новину довге, можна і не помітити.

Соціальна інженерія. Соціальна інженерія – нетехнічні прийоми маніпуляцією користувачами. Основною метою соціальної інженерії є:

- дослідження причин тієї чи іншої поведінки людини;
- обставин та середовища, що впливають на формування системи цінностей індивіду, і як наслідок — їх поведінки.

На базі цих досліджень можна визначити, що саме спонукає людину на конкретну дію. Ці технології маніпуляцій свідомістю активно використовують інтернет-шахраї для досягнення своїх цілей у тому чи іншому виді злочину.

Безпека соціальних мереж. Даний розділ просто квінтесенція всього, що було до цього. Тут і розсилка посилань, і розповсюдження фейків, і псевдодрузі. Тому декілька разів обдумайте, перш ніж опублікувати допис.

Програмне забезпечення. Вкотре наголосимо, що потрібно користуватися ліцензійними програмами. Пріоритетно використовуйте антивіруси, програми, соцмережі, системи управління бізнесом чи процесами, які створені українськими розробниками, або ж світовими лідерами галузі.

Замість висновку. Дотримання основних правил та порад забезпечить більшу захищеність особистих даних та пристроїв від кіберзлочинців. Проте важливо розуміти, що кібербезпека - це постійний інтерактивний процес, оскільки кіберзлочинці постійно вдосконалюють свої методи та атаки. Додатково, рекомендації з кібербезпеки можуть залежати від конкретних обставин та технічних умов. Важливо регулярно оновлювати свої знання та заходи з кібербезпеки, слідкувати за новими загрозами та використовувати найновіші інструменти та методи захисту. Нарешті, свідоме та відповідальне використання технологій, а також навчання оточуючих принципам кібербезпеки, важливі чинники для створення безпечного цифрового освітнього середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Українська фундація правової допомоги: вебсайт. URL: https://ulaf.org.ua/covid19/cybersafety/ (дата звернення: 20.08.2023).

2. Комп'ютерна безпека. Wikipedia.org: вебсайт. URL: https://uk.wikipedia.org/wiki/Комп%27ютерна_безпека (дата звернення: 12.12.2023).

3. Інформаційний портал DefenseUa: вебсайт. URL: https://www.defenseua.com/cybersafe (дата звернення: 12.09.2022).

4. Урядова команда реагування на комп'ютерні надзвичайні події України, яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України. CERT-UA: вебсайт. URL: https://cert.gov.ua (дата звернення: 20.08.2023).

РОЗВИТОК ПРОГРАМ ІНФОРМАЦІЙНОЇ ГРАМОТНОСТІ В ЗАКЛАДАХ ОСВІТИ ЯК СКЛАДОВА СОЦІАЛЬНОЇ БЕЗПЕКИ ДІТЕЙ У КІБЕРПРОСТОРІ

Анна МАКАРИНСЬКА, Ольга ЛУНГОЛ

Розвиток програм інформаційної грамотності в закладах освіти є необхідною складовою стратегії забезпечення соціальної безпеки дітей у кіберпросторі. З урахуванням зростаючого впливу цифрового середовища на їхнє життя, важливо створювати навчальні програми, спрямовані на розвиток комплексу навичок, необхідних для безпечного та ефективного взаємодії з інтернет-середовищем.

Програми інформаційної грамотності в закладах освіти мають включати оволодіння важливими навичками, такими як розуміння цифрових технологій, критичне мислення, ефективний пошук та оцінка інформації в Інтернеті. У комплексній дії це формуватиме у дітей аналітичний підхід до використання онлайн-ресурсів та допомагатиме їм уникати потенційних кіберзагроз.

Як окремий елемент ми виділяємо розвиток критичного мислення, що в сучасному світі стає ключовою складовою соціальної безпеки дітей у кіберпросторі. Оскільки цифровий ландшафт стає неодмінною частиною повсякденного життя підростаючого покоління, важливо формувати у них навички, які дозволять аналізувати інформацію та приймати обґрунтовані рішення в онлайн-середовищі. Критичне мислення передбачає здатність розрізняти правдиву інформацію від маніпуляцій та фейків, аналізувати ризики та визначати потенційні небезпеки в кіберпросторі. Програми, спрямовані на розвиток критичного мислення в закладах освіти, мають ставити за мету створення свідомих та відповідальних користувачів Інтернету. Важливо навчити дітей критично ставитися до інформації, яку вони зустрічають в мережі. Це включає в себе перевірку джерел, перекладання та порівняння інформації, а також вміння розпізнавати підроблені або необ'єктивні матеріали. Спроможність аналізувати вірогідність інформації стає ефективним засобом захисту від дезінформації та маніпуляцій. Критичне мислення також сприяє формуванню в дітей власної позиції та самосвідомості в мережі. Здатність аналізувати та обговорювати онлайн-ситуації робить їх менш вразливими до негативних впливів та забезпечує їх психологічну стійкість. Розвиток критичного мислення дітей в кіберпросторі є необхідним елементом виховання грамотних, компетентних та

самостійних особистостей, які можуть ефективно навігувати в цифровому світі та зберігати власну соціальну безпеку.

Важливим аспектом є також впровадження системної співпраці між освітніми закладами, батьками та органами безпеки, що створюватиме інтегровану систему захисту, яка охоплюватиме як освітній процес, так і позанавчальні аспекти життя дітей в Інтернеті.

Як приклад подібних програм можна навести комплексну програму, спрямовану на розвиток та зміцнення навичок критичного мислення та інформаційної гігієни задля посилення стійкості до дезінформації, маніпуляцій та пропаганди – «Вивчай та розрізняй: інфомедійна грамотність» [1]. Програма виконується Радою міжнародних наукових досліджень та обмінів (IREX) за підтримки Посольства США в Україні та Міністерства закордонних справ і міжнародного розвитку Великої Британії у партнерстві з Міністерством освіти і науки України, Міністерством культури та інформаційної політики України та Академією української преси.

Отже, розвиток інформаційної грамотності в закладах освіти є стратегічною інвестицією в соціальну безпеку дітей у кіберпросторі, надаючи їм необхідні знання та навички для впевненого та безпечного існування в цифровому світі. По-перше, упровадження цих програм сприяє формуванню у дітей навичок безпечної навігації в цифровому оточенні, розпізнаванню кіберзагроз та ефективному використанню інформаційних ресурсів. По-друге, розвиток інформаційної грамотності сприяє створенню позитивного цифрового середовища, де діти можуть вільно та відповідально взаємодіяти, розвивати творчість та реалізовувати свій потенціал. По-третє, такі програми допомагають дітям розпізнавати та уникати ризикованих ситуацій в кіберпросторі, підвищуючи їхню здатність до критичного мислення та саморегуляції.

Загалом, розвиток інформаційної грамотності в закладах освіти є ключовим елементом підготовки молодого покоління до життя в цифровому суспільстві та сприяє забезпеченню їхньої соціальної безпеки в кіберпросторі. Такий підхід є важливою інвестицією у майбутнє та забезпечує сталість та стійкість суспільства в умовах постійно зростаючої цифрової залежності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Програма «Вивчай та розрізняй: інфомедійна грамотність». Міністерство освіти і науки України : вебсайт. URL: https://mon.gov.ua/ua/ministerstvo/diyalnist/mizhnarodna-dilnist/spivpracya-z-mizhnarodnimi-organizaciyami/rada-mizhnarodnih-naukovih-doslidzhen-ta-obminiv-irex/programa-vivchaj-ta-rozriznyaj-infomedijna-gramotnist (дата звернення 02.02.2024 р.).

БЕЗПЕКА ДИТИНИ В МЕРЕЖІ ІНТЕРНЕТ: ОСВІТНІ ПРОЄКТИ НА ДОПОМОГУ ПЕДАГОГАМ І БАТЬКАМ

Вікторія НАУМОВА

Сучасні цифрові технологій розвиваються надзвичайно інтенсивно. Переважній частині населення планети складно уявити своє життя без безперервного потоку інформації через всесвітню мережу Інтернет. Сьогодні у всьому світі спостерігається тенденція цифровізації багатьох сфер життєдіяльності людини, зокрема й освіти. Нагадаємо, що в Україні з 2020 р. запущені вебпортал і мобільний застосунок «Дія» (як сервіс із надання державних послуг онлайн), розроблені Міністерством цифрової трансформації України. Цифрова освіта на сучасному етапі реалізується в Україні різними засобами. Одним з найбільш інноваційних і масових проєктів є Національна онлайн-платформа «Дія. Освіта»[1], яка функціонує з 30 січня 2020 р. (розробник – Міністерство цифрової трансформації України). Відтак, кожен українець має безкоштовний доступ до цифрової освіти. На онлайн-платформі доступна ціла низка освітніх продуктів, зокрема для освітян, учнів і батьків, з питань безпечної поведінки в мережі Інтернет. Для навчання цифровій грамотності обраний інноваційний формат – освітні серіали. Наразі на онлайн-платформі доступні такі освітні серіали:

- базовий серіал з безпечного поводження в мережі Інтернет «Основи кібергігієни» (серіал допоможе навчитися елементарним правилам кібергігієни в інтернеті при користуванні поштою, соцмережами та мобільними пристроями);
- серіал «Персональна кібергігієна» (про базові правила інформаційної гігієни в інтернеті);
- серіал «Кіберняні» (як попередити кібератаку та захищати дані в інтернеті);
- серіал «Безпека дітей в інтернеті для батьків» (розкриває питання убезпечення дітей від шкідливого контенту, цькування, суїцидальних інтернет-спілок та сексуальної експлуатації в інтернеті);
- серіал «Про кібербулінг для підлітків» (роз'яснює, як виглядає кібербулінг, які причини та потенційні наслідки кібербулінгу, як припинити кібербулінг і що робити, якщо хтось із друзів став жертвою кібербулінгу);
- серіал «Обережно! Кібершахраї» (про захист від шахраїв в інтернеті та в ґаджетах);
- серіал «Персональні дані» (йдеться про політику приватності та керування персональними даними).

Окрім освітніх серіалів, на онлайн-платформі «Дія. Цифрова освіта» містяться інші матеріали з означеної теми, а саме: ґайд «Навіщо нам кібергігієна?» (йдеться про основні типи хакерства та способи протидії шахраям в інтернеті), симулятор «Персональна кібергігієна» (допоможе перевірити свої знання з основ кібергігієни), цифрограм «Кіберграм» (тест на розуміння кібергігієни та вміння захищати свої персональні дані).

Під час розроблення освітніх серіалів і матеріалів цієї платформи автори спирались на загальноєвропейські стандарти оцінки цифрової компетентності DigComp 2.1 [2].

Міністерство цифрової трансформації у співпраці з ЮНІСЕФ та за інформаційної підтримки Міністерства освіти і науки України, Координаційного центру з надання правової допомоги та Міністерства юстиції України запустило освітній проєкт проти кібербулінгу – чат-бот «Кіберпес» [3]. У чат-боті у Telegram і Viber можна дізнатись про те, як визначити кібербулінг, як діяти дітям, батькам і вчителям у разі кібербулінгу.

Освітній проєкт щодо захисту дітей в мережі Інтернет – проєкт #stop_sextинг [4] отримав премію Глобального договору ООН та навчив більше ніж пів мільйона дітей та батьків безпеці в інтернеті. У рамках освітньо-інформаційної кампанії проєкт #stop_sextинг та Урядовий контактний центр [5] створили консультаційну «гарячу лінію» з питань безпеки дітей в мережі Інтернет за номером телефону 1545 (далі обрати 3). Фахівці лінії надають кваліфіковані консультації щодо особливостей технічних налаштувань застосунків, якими діти користуються в цифровому середовищі, а також підвищують рівень обізнаності дітей, батьків, фахівців, які працюють у контакті з дітьми щодо попередження ризиків, на які діти можуть наражатися в мережі Інтернет, та реагування на них. Здійснювати дзвінки на лінію можна цілодобово, безкоштовно й анонімно.

Ще одним важливим інноваційним освітнім проєктом є «Школа онлайн-безпеки дітей» [6]. Школу запустила громадська організація «МІНЗМІН» за сприяння Міністерства цифрової трансформації України. «Школа онлайн-безпеки дітей» – це освітній проєкт для вчителів і батьків, які хочуть захистити своїх дітей від загроз в мережі Інтернет. Під час навчання учасники дізнаються, як забезпечити максимальну користь Інтернету для дітей, які загрози чекають на дітей в онлайн-середовищі та як від них убезпечити.

Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України запустив проєкт подкастів Qwerty [7]. Свою назву проєкт отримав від розташованих поряд на клавіатурі клавіш QWERTY, які є одним із самих популярних паролей у світі – його використовують близько 18 мільйонів людей. У випусках фахівці розповідають про кейси світових кібератак, кібергігієну, блокчейн та хакерів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дія. Освіта : вебсайт. URL: https://osvita.diia.gov.ua/ (дата звернення: 26.01.2024).
2. DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC106281 (дата звернення: 26.01.2024).
3. Безпека дітей в Інтернеті. *Міністерство освіти і науки України* : вебсайт. URL: https://mon.gov.ua/ua/osvita/pozashkilna-osvita/vihovna-robota-ta-zahist-prav-ditini/bezpeka-ditej-v-interneti (дата звернення: 26.01.2024).

4. Проєкт #stop_sextинг : вебсайт. URL: https://stop-sexting.in.ua/.
5. Безпека дітей у цифровому світі. *Урядовий контактний центр* : вебсайт. URL: https://ukc.gov.ua/bezpeka-ditej-u-tsyfrovomu-sviti/ (дата звернення: 26.01.2024).
6. Школа онлайн-безпеки дітей. *МІНЗМІН* : вебсайт. URL: https://minzmin.org.ua/projects/ (дата звернення: 30.01.2024).
7. Проєкт подкастів Qwerty : вебсайт. URL: https://podcasters.spotify.com/pod/show/qwerty05?fbclid=IwAR0t7umpfvafM61K0WZcv-AzdzPZeMsRdWoHiiT5hZjWHN6MOiRGIMKNYZ8.

КІБЕРГРАМОТНІСТЬ ПЕДАГОГА: УДОСКОНАЛЕННЯ ПРОФЕСІЙНОЇ КОМПЕТЕНТНОСТІ В ЕПОХУ ТЕХНОЛОГІЙ

Людмила СІМОКОП

Постановка проблеми. Зі стрімким розвитком технологій у світі, кіберграмотність є надзвичайно актуальною і важливою в сучасному освітньому контексті та стає ключовою складовою професійної компетентності педагогічних працівників. Щоб забезпечувати якісну освіту, педагог повинен ефективно використовувати інноваційні засоби навчання, вміти знаходити і критично оцінювати інформацію, а також безпечно використовувати цифрові ресурси.

Аналіз останніх досліджень і публікацій. Важливість кіберграмотності працівників освіти, для підвищення її якості, висвітлена в численних наукових працях українських (і не тільки) експертів, учених та дослідників. Наприклад: безпека освітніх закладів через кібербезпеку – Гончарова І.; розпізнавання фейків в соціальних мережах – Скрипка Г.; створення системи інформаційної безпеки – Амеліна А.; цифрові технології в професійному розвитку – Потапчук Т., Пукас І., Серман Т.; «Концептуально-референтна Рамка цифрової компетентності педагогічних й науково-педагогічних працівників», яку було використано для створення Стандарту вчителів та керівників ЗЗСО, Типової програми підвищення кваліфікації, та Цифрограму на платформі Дія.

Мета: Розгляд компонентів кіберграмотності педагога, визначення шляхів удосконалення професійної компетентності, а також ключових викликів та перспектив розвитку кіберграмотності в системі сучасної освіти.

Виклад основного матеріалу. Часовий проміжок 2020-2022 років став для України визначальним – спочатку превентивний карантин COVID-19, згодом повномасштабне вторгнення рф. Цей період вивів онлайн-спілкування на новий рівень, надавши йому нових можливостей і викликів. Застосування цифрових технологій підвищило зацікавленість учнів до навчання, однак, поставило завдання – створення якісного освітнього середовища та безпеки комунікації. Технічні навички, розуміння е-етикету і безпеки в мережі, використання інтернет-ресурсів в навчальному процесі та особистому професійному зростанні – це питання, які окреслює цифрова грамотність сучасного педагогічного працівника. При цьому, щоб уникнути загроз, пов'язаних із опрацюванням

цифрових даних, важливо враховувати сфери інформаційної безпеки. Сьогодні кожен із нас залишає цифровий слід в електронному просторі - це акаунти, підписи, особисті і робочі комунікації та інше. І головне завдання полягає у забезпеченні конфіденційності інформації, тобто у дотриманні принципів інформаційної безпеки. «Існує певна проблема, пов'язана з засвоєнням основ інформаційної безпеки. Ніщо так не вчить фінансової грамотності, як втрата грошей, і ніщо так не вчить кіберграмотності, як витік персональних даних, зламування акаунту і знову ж таки втрата грошей» [1, с. 60].

Такий підхід сприяє створенню безпечного та ефективного онлайн-середовища для навчання і спілкування. Саме на вчителя покладено задачу стати для учнів зразком у цифровому світі – розуміти та ефективно використовувати цифрові технології для досягнення освітніх (і не тільки) цілей. Без кіберграмотності тут не обійтись, адже саме вона визначає вміння захистити себе і свою безпеку в світі інтернету. Кіберграмотний педагог повинен знати правила захисту в онлайн-просторі, вміти розпізнавати та вживати заходів для запобігання інтернет-загрозам, наприклад, шахрайства, фішингу, вірусів та інших атак. Тому сьогодні кіберграмотність є важливою складовою професійної компетентності педагогічного працівника.

Розглянемо ключові аспекти кібернетичної грамотності педагога.

Перш за все, це навички пошуку, критичної оцінки та використання отриманої інформації. Застосовуючи інструменти пошуку, ми маємо справу з різними типами джерел, від офіційних законодавчих актів до відгуків та дописів у соцмережах. Ефективне використання цифрових ресурсів вимагає від педагога визначення оптимальних шляхів для знаходження та систематизації необхідної інформації з урахуванням конкретних запитів та цілей. Тут потрібні навики роботи з пошуковими системами, фільтрами, базами даних.

Отримана інформація потребує аналізу та оцінки – перевірки достовірності (авторитетності джерела, дати, контексту). Критична оцінка - це необхідний етап, який допомагає уникнути поширення неперевірених даних та неточностей. У час, коли інформаційний потік постійно зростає, надзвичайно важливим для вчителя стає не лише вміння відрізняти факти від міфів, визначати часову актуальність інформації, а й забезпечити розвиток цих навичок в учнів.

Однією з найважливіших засад є безпека в Інтернеті - захист особистої інформації, використання надійних засобів зв'язку та антивірусний захист. Від цих критеріїв залежить безпека всіх учасників освітнього процесу та якість освіти в цілому. Тут вчитель має бути обізнаним та свідомим користувачем мережі. Виховувати в учнів відповідальне ставлення до власної онлайн-безпеки - застосовувати надійні паролі, використовувати двоетапну аутентифікацію, регулярно переглядати налаштування конфіденційності, вміти розпізнавати підозрілі ситуації та загрози. «Функціональні критерії захисту інформації від певного виду загроз розділено на чотири групи. Загрози щодо несанкціонованого ознайомлення з інформацією становлять загрози конфіденційності; загрози щодо несанкціонованої модифікації інформації – загрози цілісності; загрози щодо порушення можливості використання комп’ютерних систем або оброблюваної інформації – загрози доступності» [2, с. 300]. Одним із ефективних методів

захисту особистих даних є обмеження доступу до них. Потрібно уважно вибирати параметри конфіденційності на онлайн-платформах, це дозволить обмежити доступ до особистих даних та уникнути їх неправомірного використання.

Міжнародний розробник антивірусного програмного забезпечення для корпоративних та домашніх користувачів «ESET» надає рекомендації щодо кібергігієни для інтернет-користувачів. Дотримання цих правил допоможе своєчасно виявити зловмисників та запобігти втраті особистої інформації:

- перевірка безпеки існуючих облікових записів електронної пошти та акаунтів в соцмережах;
- аналіз необхідних для роботи програм;
- своєчасне оновлення операційної системи та окремих додатків, передбачених для виправлення вразливостей програмного забезпечення;
- створення надійних унікальних паролів для кожного акаунта;
- використання двофакторної аутентифікації;
- регулярне резервне копіювання інформації;
- використання надійного захисту від різних загроз [3].

Важливим елемент кіберзахисту є використання безпечних засобів зв'язку. Педагог повинен використовувати тільки визнані та безпечні інструменти для зв'язку з учнями, батьками та колегами, забезпечуючи надійність і конфіденційність інформації. Це включає в себе унікальні прийоми використання електронної пошти, месенджерів та соціальних мереж, з урахуванням забезпечення приватності та безпеки даних.

Крім технічних, не менш вагомим аспектом свідомого використання онлайн-простору є дотримання принципів етичного поводження в мережі. Розвиваючи навички моральної поведінки в Інтернеті, вчитель допомагає учням стати відповідальними громадянами цифрового світу, формує в них позитивну інтернет-культуру.

Загалом, у навчанні та вихованні сучасного покоління вирішальне значення має професійна компетентність «цифрового» вчителя, використання ним інноваційних методів та прийомів в освітньому процесі – створення унікальних уроків, адаптованих до різних стилів та підлаштованих до індивідуальних потреб кожного учня. Ключову роль у цьому процесі відіграє знання та дотримання принципів цифрової безпеки, які зумовлюють впевнене застосування цифрових інструментів не лише на уроках, а й сприяють особистому і професійному росту вчителя.

Здатність педагога використовувати онлайн-простір для самоосвіти та професійного вдосконалення визначає його розвиток в галузі кіберграмотності. Цифрова епоха потребує системного підходу та безперервного вдосконалення. Тому вчителі, які постійно підтримують свої знання та навички відповідно до новітніх технологій, зможуть ефективно реагувати на зміни та впроваджувати їх у свою професійну практику.

Висновки. Розвиток кіберграмотності в сфері освіти є важливим кроком для адаптації молодого покоління у сучасному цифровому світі. Для забезпечення якісної підготовки учнів до життя в епоху технологій педагоги

повинні не лише покращити свої навички у сфері кіберграмотності, а й успішно інтегрувати їх у освітній процес.

На цьому шляху важливо враховувати конкретні напрями:

- навчання, зосереджене на безпечному використанні онлайн-ресурсів, сучасних методах пошуку інформації, критичному аналізі;
- активне впровадження інноваційних методик у професійну практику;
- самоосвіта та постійний професійний розвиток.

Відповідальне використання педагогом інтернет-простору є ключовим чинником для забезпечення високої ефективності та надійності онлайн-середовища в освітній сфері. Це впливає на якість освіти та створює сприятливі умови для подальшого прогресивного розвитку освітньої системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гончарова І. Кібербезпека в цифровому освітньому середовищі закладів професійної освіти / електронний навчальний курс. Біла Церква, 2022 URL: http://surl.li/mxthz.

2. Бондаренко В. Умови та засоби формування навичок інформаційної безпеки майбутніх учителів. *Інформаційні технології і засоби навчання*, 2019. Том 74, № 6. URL: http://surl.li/qebjf.

3. Правила кібергігієни: 7 кроків для покращення захисту даних. Eset : вебсайт. URL: http://surl.li/mdzrt

ВИКЛИКИ КІБЕРБЕЗПЕКИ В УМОВАХ ДИСТАНЦІЙНОГО НАВЧАННЯ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Ганна СКАСКІВ

Основні положення щодо організації питань безпеки у кіберпросторі викладено у Законі України «Про основні засади забезпечення кібербезпеки України». Закон регулює основні напрямки та принципи політики держави у сфері кібербезпеки, координує основні положення державних органів та установ щодо захисту інтересів громадян у міжнародному цифровому просторі [1].

Однак відкритими залишаються питання про виклики освітнього кіберпростору під час організації навчання в онлайн-форматі у закладах вищої освіти.

Мета статті: подати огляд найважливіших викликів кібербезпеки, які мають відношення до системи вищої освіти в умовах організації освітнього процесу в дистанційній або змішаній формі.

У діджиталізованому освітньому онлайн-просторі однією з найбільших загроз є соціальна інженерія, що охоплює і шахрайські атаки. Кіберзлочинці отримують користь від облікових даних для отримання доступу до шкільної або університетської мережі. Найпоширенішим способом отримання таких облікових даних є успішна спроба фішингу.

Організація безпечної дистанційної роботи у вищій школі є своєрідним викликом у мирних умовах, що значно ускладнюється в умовах воєнного стану, оскільки доступ до освітніх платформ здійснюється через Інтернет [2] великою кількістю користувачів через різні мережі, які характеризуються стандартною архітектурою.

Сучасні цифрові технології, що використовуються у закладах вищої освіти України, забезпечують для студентів нові можливості для формування базових знань, практичного досвіду та розвитку ключових компетентностей. Однак значна кількість систем електронного навчання, зокрема і Moodle, є великими за обсягом, містять багато інформації та передбачають різні способи взаємодії та обміну даними. І основною проблемою стає захист, підтримка конфіденційності користувачів, збереження цілісності контенту та авторського права з забезпеченням однакових можливостей і рівнів доступу до освітніх послуг усіх користувачів.

Проведений аналіз забезпечення якості надання освітніх послуг та визначення загроз інформаційної безпеки в умовах навчання онлайн у Центрі дистанційного навчання Тернопільського національного педагогічного університету імені Володимира Гнатюка (ТНПУ) дає можливість визначити наступні виклики з проблем кібербезпеки:

1. Атаки програм-зловмисників (вірусів, макросів);
2. Помилки ППЗ (збої у функціоналі програмного забезпечення);
3. Технічні збої (проблеми з кодуванням та декодуванням даних);
4. Несанкціонований доступ (шпигунські та хакерські атаки);
5. Несанкціоноване використання контенту (стороннє втручання сторонніх осіб, порушення авторського права);
6. Проблеми з електропостачанням (тривалі відключення електроенергії, проблеми з послугами WAN);
7. Зношеність техніки (використання застарілого обладнання, яке складно підтримувати та оновлювати в умовах війни) [3].

З огляду на визначення подібних загроз, для успішної реалізації дистанційного навчання в умовах війни заклади вищої освіти визначають чіткі лінії передачі даних, встановлюють брандмауери та оновлюють антивірусне програмне забезпечення, проводять постійну перепідготовку фахівців з організації безпеки та онлайн-комунікації, удосконалюють рівні доступу, авторизації та ідентифікації користувачів.

Безпека даних у закладах вищої освіти – це практика захисту даних від несанкціонованого доступу, від маніпулювання та несанкціонованого розповсюдження інформації. Тому рівні безпеки включають фізичні заходи, такі як замки та паролі для запобігання зловмисному доступу, а також цифрові засоби захисту, такі як шифрування та брандмауери для захисту від хакерів. Вона також охоплює політику та процедуру для належного поводження з конфіденційною інформацією.

Безпека даних набуває все більшого значення в освіті. Університети та школи повинні захищати не лише власну інформацію, але й інформацію про

студентів чи учнів, батьків, викладачів чи учителів, персоналу та інших зацікавлених сторін.

Зі збільшенням обсягу даних, що зберігаються в електронному вигляді в освітянських мережах, зростає і потреба в безпечній практиці їх передачі, яка ніколи не була такою важливою. Коли справа доходить до безпеки в Інтернеті, усі учасники освітнього процесу повинні бути особливо обережними. Сьогодні існує безліч сайтів, які зберігають персональні дані та використовують їх у зловмисних цілях – наприклад, для отримання коштів або навіть викрадення людей. Ось чому важливо інформувати молодь про небезпеку надання особистої інформації на підозрілих сайтах.

Умови успішного подолання викликів у сфері кібербезпеки, які впроваджуються у ТНПУ:

1. Захист конфіденційних даних.

У ТНПУ обробляють та зберігають велику кількість конфіденційної інформації, включаючи інформацію про студентів, фінансову звітність, результати досліджень тощо. Важливо, щоб ці дані зберігалися у безпеці, щоб захистити конфіденційність залучених осіб і забезпечити доступ до них лише уповноваженому персоналу.

2. Забезпечення нормативно-правової відповідності.

Дотримання вимог регуляторних органів, які висувають до закладів вищої освіти щодо керування безпекою даних. Невиконання цих вимог може призвести до великих штрафів або інших санкцій, які можуть зашкодити репутації закладу, а також його фінансовому стану.

3. Уникнення втрати даних.

Незахищені дані піддаються ризику крадіжки або випадкової втрати через людські помилки або технічні збої, що може мати серйозні наслідки. Тому з метою захисту регулярно проводиться резервного копіювання інформації на віддалених захищених серверах, щоб уникнути будь-яких потенційних втрат.

4. Захист інтелектуальної власності.

Кожен ЗВО часто володіє цінною інтелектуальною власністю, яку потрібно захистити від несанкціонованого використання або розголошення. Тому заходи безпеки даних можуть допомогти захистити цю інтелектуальну власність, щоб вона залишалася безпечною та конфіденційною.

5. Запобігання кібератакам.

Кіберзлочинці все частіше націлюються на вищі навчальні заклади через цінну інформацію, яку вони містять, що робить ефективні заходи безпеки даних необхідними для захисту від цих атак.

6. Мінімізація репутаційних втрат.

Витік даних може зашкодити репутації установи, а також її фінансовому стану, з довгостроковими наслідками для кількості студентів, відносин з донорами тощо. Впровадження надійних заходів безпеки може допомогти запобігти подібним інцидентам.

Навчальні заклади повинні демонструвати свою прихильність до безпеки своїх студентів, викладачів, співробітників та інших зацікавлених сторін,

впроваджуючи надійну політику та процедуру захисту даних. Це допоможе захистити всіх від будь-яких потенційних ризиків, пов'язаних з витоком даних.

Щоб забезпечити безпеку в освіті, слід дотримуватися деяких найкращих практик [3]. Встановлення чітких правил і процедур, пов'язаних з використанням технологій, онлайн-сховищ і цифрових комунікацій, може допомогти захистити конфіденційні дані навчального закладу. Ці правила повинні включати вказівки щодо прийнятного використання пристроїв і мереж; налаштування конфіденційності; протоколів управління паролями; процедур затвердження нових програмних додатків тощо.

Усі дані, що зберігаються, мають бути зашифровані, щоб запобігти несанкціонованому доступу. Шифрування робить інформацію нечитабельною для будь-кого, хто не має ключа для її розшифрування. Також важливо регулярно перевіряти, хто має доступ до конфіденційної інформації. Це допоможе виявити потенційні загрози та спроби несанкціонованого доступу.

Вживаючи необхідних заходів для захисту своїх даних, вищі навчальні заклади можуть краще захистити конфіденційну інформацію. Таким чином, вони можуть продемонструвати високий рівень безпеки та відповідність до вимог законодавства [1]. Безпека даних має важливе значення для захисту від будь-яких потенційних загроз. Завдяки налагодженій роботі у сфері кібербезпеки заклади вищої освіти, навіть в умовах воєнного стану, можуть продовжувати надавати якісні освітні послуги без перебоїв або втрати даних у форматі дистанційного чи змішаного навчання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 01.02.2024).
2. Про електронні комунікації Закон України від 30 вересня 2020 року. URL: https://dslua.org/publications/zakon-pro-elektronni-komunikatsii-universalnyy-dostup-subsydii-na-internet-zakhyst-personalnykh-danykh-ta-ryzyk-shatdauniv-v-zoni-ato/ (дата звернення: 01.02.2024).
3. Chen Y. and He W. Security and Protection in Online Learning: A Survey. The International Review of Research in Open and Distance Learning, 2013. URL: http://www.irrodl.org/index.php/irrodl/article/view/1632/2712.

КІБЕРГРАМОТНІСТЬ ДЛЯ ВЧИТЕЛІВ І НЕ ТІЛЬКИ

Марина ФЕДОРИШИНА

Останнім часом все більше сфер людського життя переходить у кіберпростір. Цьому передував Covid-19 та воєнний стан в Україні.

Якщо ще 20 років тому інтернет не був широко розповсюджений в Україні, то зараз не тільки державні і приватні компанії, а й кожна родина, кожна дитина має сайт, блог, сторінку в соціальній мережі. Великої популярності набули соціальні мережі, інтернет речей, «хмарні сховища».

Такі сервіси інтернету – це зручно, сучасно, необхідно, але для того, щоб безпечно користуватись благами цивілізації, потрібно бути обізнаним і захищеним.

З початком нового століття перспектива загального оцифровування інформації та зв'язку робить кіберпростір, ймовірно, головним каналом інформації.

Якщо кіберпростір розкриває широкі можливості для користувачів, то водночас він показує нам не відомі раніше виклики та небезпеки, ставить нові задачі до підготовки потенційних користувачів.

Кібербезпека – це технології захисту інформаційних систем, комп’ютерних мереж, баз даних, програмного забезпечення, аби вони безперебійно працювали, забезпечувалась цілісність даних і доступ до них відповідних осіб. Також це забезпечення конфіденційності та запобігання витокам інформації. Важливою складовою кібербезпеки є моніторинг і виявлення загроз, аналіз інцидентів, відновлення роботи інформаційних систем після атак.

Основним способом захисту від методів соціальної інженерії є навчання учасників освітнього процесу. Вони мають бути попереджені про небезпеку розкриття персональної конфіденційної інформації, а також про способи запобігання витоку даних.

Інформатику вивчають з 2 класу і тому діти змалечку знають про небезпеку в інтернеті, про те, яких правил потрібно дотримуватись при спілкуванні з незнайомцями, як розрізняти фейкову інформацію, що можна, а що заборонено робити в мережі. Вчителі інформатики проводять уроки і позакласні заходи з дітьми на тему «Безпечний інтернет». Але діти опановують ґаджети задовго до школи. Тому саме батьки змалку повинні прививати їм правила безпечної поведінки своїм прикладом. Батьки, вихователі, вчителі, викладачі повинні знайомити дітей з кіберграмотністю і прививати їм кіберкультуру, допомагати правильно і безпечно користуватись різноманітними інформаційно-цифровими ресурсами, зберігати, перетворювати і передавати інформацію за допомогою сучасних каналів зв’язку.

Міністерство цифрової трансформації розробило «Кіберграм» – онлайн-тест для перевірки рівня кіберграмотності. Кожна людина може перевірити власний рівень кіберграмотності і після проходження тестування отримати сертифікат.

Також для підвищення кіберграмотності, як вчителів так і усіх охочих, існує низка безкоштовних ресурсів:

- онлайн-курс із кібербезпеки від Google — передбачає 6 місяців навчання та можливість пройти сертифікацію. Ви навчитеся захищати мережі, пристрої, людей і дані від несанкціонованого доступу та кібератак за допомогою інструментів безпеки інформації та керування подіями. Також отримаєте практичний досвід роботи з Python, Linux і SQL.
- https://www.cybrary.it/ — базовий курс із кібербезпеки для початківців про те, як захистити мережі та себе в інтернеті.

Introduction to Cybersecurity — вступ до кібербезпеки.

Дізнайтеся про основи кібербезпеки та вдосконаліть свої навички, щоб краще захищати вашу цифрову інформацію від загроз безпеці.

- SANS Cyber Aces — на платформі понад 85 практичних курсів з кібербезпеки від найбільшого у світі постачальника онлайн-тренінгів з кібербезпеки SANS.
- Codecademy — курси про те, як захистити свої дані та інформацію від хакерських атак в цифровому просторі, для початківців і тих, хто вже має певні знання з кібербезпеки.

Також на платформі «Дія.Освіта» запустили модуль «Оновлена інформатика — IT студії» https://it-osvita.diia.gov.ua/, який містить сучасні інструменти для викладання та вивчення інформатики в школах. Міністерство цифрової трансформації допомагає Міністерству освіти і науки України сформулювати новий підхід до управління системою освіти.

Крім цього, за покликанням https://osvita.diia.gov.ua/courses/cyber-hygiene можна пройти навчання з кібергігієни під час війни.

Тобто дуже багато цікавого, корисного, сучасного і безпечного можна знайти для себе і своїх близьких. Учитися ніколи не пізно.

СОЦІАЛЬНА ПРОФІЛАКТИКА ПРАВОПОРУШЕНЬ ДІТЕЙ У КІБЕРПРОСТОРІ

СІМ'Я ЯК ПЕРШОЧЕРГОВИЙ ФАКТОР У СОЦІАЛЬНОМУ ЗАХИСТІ ДИТИНИ ВІД ПРАВОПОРУШЕНЬ В КІБЕРПРОСТОРІ

Олена Бєляєва

На сьогоднішній день відбувається швидкий розвиток інформаційних технологій, який займає все більший простір у нашому кожноденні в усіх сферах діяльності людини. Завдяки сучасним тенденціям і інноваціям прогрес розвитку технологій буде тільки збільшуватися.

У світовій історії людства проблема шахрайства була завжди. Тому одночасно з розвитком нових технологій, у нас виникла і нова проблема: злочинність у віртуальному просторі. Вона поєднала в собі одночасно всім нам

відомі крадіжки, шахрайства, вимагання грошей з різними напрямками у сфері високих технологій: поширення шкідливих програм і вірусів, злом паролів, крадіжку номерів кредитних карт, перехоплення та розповсюдження особистих даних, внесення протиправної інформації на сайти компаній і міністерств, незаконний доступ шляхом злому, обману та іншими засобами [1, с.33].

Віртуальний простір, що постійно розвивається, переймає від реального злочинність у її нових формах і проявах.

Поняття кіберпростору, введеного письменником Вільямом Гібсоном у п'єсі «Le Neuromancer», описує віртуальний простір як такий, в якому циркулюють електронні дані всіх комп'ютерів світу [2].

Наразі кіберзлочинність є, напевно, однією з найглобальніших загроз як для України, так і для всього світу. Жертвами зловмисників, які здійснюють свою діяльність у кіберпросторі, стають не тільки окремі громадяни, а й цілі держави [4, с.476]. Зараз, в умовах війни в Україні, ми це особливо відчуваємо. У кожному осередку, у кожній окремій сім`ї постає питання: як ми можемо вберегти своїх дітей від різних правопорушень у кіберпросторі, від затягування дітей у різні підозрілі програми та ігри, що несуть в собі приховане насильство та провокують на різні негативні дії.

Для забезпечення необхідної протидії правопорушенням дітей у кіберпросторі необхідно застосувати сукупність правових, організаційних, інформаційних, пояснювальних заходів дитині у тому форматі, який буде для неї доступним, свідомим та прийнятним [3, с.302].

Задачу розробити і впровадити міри, що будуть, спрямовані на попередження, обмеження, зупинення негативних дій та поведінки дитини, можуть реалізувати батьки, педагоги, соціальні працівники, правоохоронні органи та кіберполіція. Батьки повинні проконтролювати безпечне середовище навкруги дитини, встановити з дитиною довірливу форму спілкування, сприяти створенню безпечного середовища навкруги дитини, знати найближчий соціум своєї дитини.

Якщо у дитини висока ступінь свідомості, впевненість у собі, своїх діях, своїх знаннях в комп'ютері, якщо вона буде обізнаною про різні негативні дії та можливі правопорушення, ця дитина вже буде підготовленою до віртуального світу. Батьки повинні володіти інформацією про те, з ким спілкується дитина, з якими програмами працює, як швидко вона опановує нові програми та ґаджети, чи захоплюється крім комп'ютера ще чимось: спортивними секціями, гуртками, кіно, до яких саме телевізійних програм має більшу прихильність. Знаючи свою дитину, саме батьки можуть спрогнозувати, як може поводити себе дитина в тій чи іншій ситуації.

Актуальним буде роз'яснення щодо різних важливих питань, довірча розмова з дитиною, розповідь про види злочинів, застереження про існування злочинних програм, що приводять до нанесення собі фізичної шкоди і дитячих самогубств, які є в кіберпросторі, про різні сайти з дитячою порнографією. Враховуючи важливість цього, в сім`ї не повинно бути накладено «вето» на їх обговорення. Краще за всякчас попередити проблему, ніж потім вирішувати її негативні наслідки.

Якщо виникла необхідність убезпечити дитину від інформації, сайту, конкретного телеканалу тощо, необхідно застосувати ті методи, які дають результат в таких випадках: автентифікацію користувача, встановлення антивірусних програм на пристрої, використання інструментів конфіденційності та безпеки Google чи інших браузерів.

Щоб підготувати дитину до того, як необхідно діяти і вести себе в критичній ситуації, викладачі, батьки та правоохоронці повинні навчити дитину комунікації з обов'язковими «контактами» – до кого вона, за необхідності, може звернутися за допомогою, передзвонити, отримати роз'яснення, подати сигнал SOS. Поінформована та обізнана дитина, яку навчили певному алгоритму дій в критичних ситуаціях, вже буде підготовлена до викликів сучасного віртуального світу.

Якщо ж дитина має певний хист до комп'ютерних наук, вона є обдарованою дитиною, необхідно допомогти направити її потенціал в необхідному напрямку, щоб не втратити його: стати учасником олімпіад з інформатики, спробувати написати роботу для МАН, стати учасником STEM-гуртків у закладах позашкільної освіти. Для більш практичної роботи батьки для дитини можуть підібрати комп'ютерні курси і підвищити рівень її знань, зробивши такий потенційний внесок у розвиток і майбутнє своєї дитини.

При глобальній діджиталізації нашого суспільства [4, с.478], педагогічні працівники, правоохоронці, соціальні працівники, діячі громадських організацій, повинні розробляти, координувати та приймати міри по безпеці дітей в інтернеті. У першу чергу в запобіганню цій проблемі повинна виступати сім'я, як основний фактор захисту дитини від правопорушень та створення для неї безпечного середовища у кіберпросторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Пфо О.М. Основні поняття і класифікація кіберзлочинності. *Актуальні задачі та досягнення у галузі кібербезпеки:* матеріали Всеукр. наук.-практ. конф., м. Кропивницький. 23-25 листопада 2016 р. С. 33-34. URL: https://core.ac.uk/download/pdf/84825482.pdf.

2. Анастасія Голуб. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. *Портал ГУРТ.* 2016 р. URL: https://gurt.org.ua/articles/34602/.

3. Прокопенко Євгеній, Мул Дмитро, Равлюк Віталій. Загрози безпечного функціонування кіберпростору Державної прикордонної служби України. *Збірник наукових праць Національної академії державної прикордонної служби України.* №2(80) 2019. С. 300-309. URL: https://periodica.nadpsu.edu.ua/index.php/military_tech/article/view/205/207.

4. Думчиков М.О., Каріх І.В. Становлення та ґенеза кримінальної відповідальності за кримінальні правопорушення у кіберпросторі на тернах України. *Юридичний науковий електронний журнал:* №5/2022. С. 476-478. URL: http://lsej.org.ua/5_2022/113.pdf.

5. Причини правопорушень серед дітей та відповідальність за них. Сайт Городищенської громади : вебсайт. URL:https://gorodyshe.gr.org.ua/prychyny-pravoporushen-sered-ditej-ta-vidpovidalnist-za-yih-skoyennya/ (дата звернення: 16.01.2024).

ОСОБЛИВОСТІ ВИЯВЛЕННЯ, ФІКСАЦІЇ ТА РОЗКРИТТЯ ПРАВОПОРУШЕНЬ, ВЧИНЕНИХ ВІДНОСНО ДІТЕЙ З ВИКОРИСТАННЯМ МЕРЕЖІ ІНТЕРНЕТ

ПРОТИПРАВНА ПОВЕДІНКА В КІБЕРПРОСТОРІ: МЕЖІ ВІДПОВІДАЛЬНОСТІ ДІТЕЙ, БАТЬКІВ ТА ЗАКЛАДУ ОСВІТИ

Лариса ГРЕТЧЕНКО

Аналіз стану освітнього середовища свідчить про сталу тенденцію поширеності випадків кібербулінгу та осучаснення його проявів. На інформаційних ресурсах органів влади та громадських організацій нерідко оприлюднюються статистичні дані, однак чи відображають цифри реальний стан проблеми?

За даними медіаресурсу Опендатабот, щонайменше 614 справ про булінг було зафіксовано в країні протягом останніх 5 років і кількість таких справ в українських школах становить близько 100 на рік [1]. З інформації, оприлюдненої Освітнім омбудсменом Сергієм Горбачовим, до початку повномасштабної війни (за період із січня 2019 року по 2021 рік) суди першої інстанції розглянули 978 справ про цькування [2]. За повідомленням заступника начальника управління ювенальної превенції Нацполіції України Ярослава Шанька, за чотири місяці 2023 року в Україні було зафіксовано 99 фактів булінгу [3]. Як правило, наведена статистика включає кількість оформлених органами поліції протоколів про адміністративні правопорушення за статею 173-4 КУпАП «Булінг (цькування) учасника освітнього процесу», та відомості про рішення, ухвалені судами у справах за результатом розгляду відповідних матеріалів. Ураховуючи множинність суб'єктів реагування на випадки булінгу (цькування), ймовірно, що кожен з органів та посадових осіб провадять окремий облік повідомлень (заяв, скарг, звернень) про випадки булінгу чи підозру на його вчинення, що ситуативно враховується в статистичних даних, без їх уніфікованого узагальнення. На повноту й достовірність статистики, що відображає ситуацію з булінгу у закладах освіти, впливає також можливість застосування до особи, що вчинила цькування, не лише адміністративної, а й дисциплінарної та/або цивільно-правової відповідальності. Таким чином, нині залишається відкритим питання щодо фактичної кількості випадків булінгу, у тому числі із застосуванням засобів електронних комунікацій, що вчиняються стосовно малолітньої чи неповнолітньої особи або такою особою стосовно інших учасників освітнього процесу, та вжитих заходів реагування і впливу.

У системному аналізі положень статті 173-4 КУпАП [4], пункту 3-1 статті 1 Закону України «Про освіту» [5] та Порядку реагування на випадки булінгу (цькування) [6] можливо констатувати, що учасники освітнього процесу в ситуації кібербулінгу виступають у наступних правових статусах: керівник закладу освіти, суб'єкт реагування, член комісії з розгляду випадку булінгу

(цькування), мама чи батько здобувача освіти, кривдник (булер), жертва (потерпілий), спостерігач (свідок).

У ситуації онлайн-цькування, залежно від обраного заявником суб'єкта реагування та способу захисту порушених прав, адміністрацією закладу освіти до кривдника може бути застосовано заходи дисциплінарного стягнення (наприклад, відрахування учня зі школи, оголошення догани педагогу чи його звільнення за вчинення аморального проступку, несумісного з продовженням роботи). В порядку притягнення до адміністративної відповідальності суд накладає на особу, що вчинила правопорушення, штраф чи громадські роботи, інколи — в разі висновку про малозначність вчиненого діяння - оголошує усне зауваження. Ініціюючи притягнення кривдника до цивільної відповідальності, потерпіла особа може заявити в суді вимоги про відшкодування матеріальної та/або моральної шкоди. Непоодиноким є розгляд судом справ про захист честі, гідності, ділової репутації (спростування недостовірної інформації), пов'язаної з ситуацією цькування.

На практиці при розгляді справ про кібербулінг суди виходять з того, що булінг (цькування) тривожна тенденція, особливо для сучасного дитячого і молодіжного середовища вирішальна роль у протидії насильству і булінгу належить педагогам. Проте впоратися з цією проблемою вони можуть тільки завдяки системному підходу та підтримки керівництва школи, батьків, представників місцевих органів влади та громадських організацій, а також із залученням та участі дітей та молоді. Оскільки поняття «кібербулінгу» в законодавстві не визначено, то виходячи із загальних понять, кібербулінг є різновидом булінгу (цькування) із застосуванням цифрових технологій. Кібербулінг - це відносно нова форма агресії, що трапляється в інтернеті та може відбуватися в соціальних мережах, платформах обміну повідомленнями (месенджерах), ігрових платформах та мобільних телефонах. При цьому нападник використовує соціальні мережі, електронну пошту, месенджери та інші засоби спілкування, щоб дошкулити, нашкодити та принизити людину. Разом з тим, кібербулінг залишає цифровий слід - записи, які можуть слугувати доказами, що дозволять зупинити цькування [7].

Окреслюючи межі відповідальності дітей, батьків, вчителів в ситуації булінгу, варто підкреслити персональну відповідальність керівника закладу освіти за приховування випадку цькування. Постановою Іваничівського районного суду Волинської області від 13.03.2023 р. у справі № 156/51/23 директора школи визнано винною у вчиненні правопорушення, передбаченого ч. 5 ст. 173-4 КУпАП, і накладено на неї стягнення у виді штрафу в розмірі 850 грн. За обставинами справи, керівник закладу освіти, перебуваючи на своєму робочому місці, не повідомила уповноважені підрозділи органів національної поліції України про факт кібербулінгу відносно неповнолітнього учня даного навчального закладу, що проявилося у створенні фейкових акаунтів у мережі інтернет з висвітленням фото неповнолітнього з непристойними написами. В оцінці судом фактичних обставин справи відзначено, що суд під час розгляду протоколу не встановлює чи дійсно мав місце факт булінгу, це не є предметом розгляду діяння, що передбачене ч. 5 ст. 173-4 КУпАП. Для кваліфікації за цією

статтею достатньо встановити обґрунтованість підозри наявності булінгу і відповідно неповідомлення про це керівником закладу освіти. Суб`єкт зазначеного правопорушення зобов`язаний в разі надходження заяви про вчинення дій, які підпадають під ознаки булінгу, на протязі доби повідомити органи Національної поліції, а не самостійно, на свій розсуд, чи колегіальним органом, встановлювати наявність факту булінгу і в залежності від результатів здійснювати таке повідомлення [7].

Прикладом притягнення до адміністративної відповідальності батьків за кібербулінг, вчинений дитиною, слугує справа № 522/9953/23, що розглянута Приморським районним судом м. Одеси. Зі змісту постанови суду від 27.06.2023 р. вбачається, що неповнолітня учениця вчинила булінг (кібербулінг) до хлопця, а саме дії психологічного насильства із застосуванням засобів електронних комунікацій, що проявилось у висловленні нецензурною лайкою у мережі «Телеграм». З пояснень законного представника потерпілого, неповнолітня разом з іншими однокласниками вчинила булінг стосовно її неповнолітнього сина, а саме: неодноразово писала в публічній групі однокласників образливі та такі, що принижують гідність висловлювання на її адресу та адресу її сина, внаслідок чого була заподіяна шкода психічному здоров`ю останнього. Враховуючи пояснення учасників та дослідивши докази, суд дійшов до висновку про наявність у діях неповнолітньої учениці булінгу (ч. 3 ст.173-4 КУпАП) та наклав на її матір штраф у розмірі 1700 грн, а також присудив до стягнення в державний бюджет судовий збір 536,80 грн [8].

Випадок кібербулінгу, вчинений групою учнів, був розглянутий Славутицьким міським судом Київської області як правопорушення, передбачене ч. 4 ст. 173-4 КУпАП, з притягненням до відповідальності батьків дітей у виді накладення штрафу у розмірі 1700 грн та відповідного стягнення судового збору. Як вбачається з постанови суду від 02.03.2023 р. у справі № 377/129/23, учениця 8 класу спільно з групою однокласників вчинила булінг стосовно учениці 7 класу, який полягав у психологічному насильстві, а саме: словесних образах та висміюванні стосовно її зовнішнього вигляду, із застосуванням засобів електронних комунікацій, які були розміщені в телеграм-каналі «...», внаслідок чого могла бути заподіяна шкода психічному здоров`ю потерпілої. З пояснень учениці 8 класу, наданих в присутності практичного психолога, даний телеграм-канал був створений саме для образ, цькування, висміювання учениці 7 класу. Читаючи дописи в цьому телеграм-каналі, їй було цікаво дивитися як ображають, цькують та принижують дівчину. Свідок-учень, у суді пояснив, що він не підтримував цих дій, але з цікавості спостерігав. Визнає, що під час існування телеграм-каналу, спілкувався з іншими учнями та заохочував їх участь у цьому телеграм-каналі [9]. За тих самих обставин аналогічним чином до адміністративної відповідальності притягнено також батьків групи учнів - адміністраторів телеграм каналу, про що свідчать постанова Славутицького міського суду Київської області від 22.02.2023 р. у справі №377/104/23 [10], від 21.02.2023 р. у справі № №377/106/23 [11].

Роменський міськрайонний суд Сумської області розглянув ситуацію ігнорування як елемент булінгу зі сторони вчителя відносно учениці під час

дистанційного навчання у справі № 585/1343/23. За змістом протоколу про адміністративне правопорушення вчитель математики, фізики, систематично вчиняла діяння, які полягають у ігноруванні дитини з використанням засобів електронних комунікацій, що виразилось у непідключенні до онлайн-уроків, ненадання додаткових консультацій і роз`яснень по пройденому матеріалу або за результатами виконаних контрольних робіт дитини, внаслідок чого була заподіяна шкода психічному здоров`ю потерпілої. Постановою суду 1-ої інстанції від 15.05.2023 року вчителя визнано винною у вчиненні адміністративного правопорушення, передбаченого ч. 1 ст. 173-4 КУпАП, та накладено на неї адміністративне стягнення у виді штрафу в розмірі 850 гривень. На думку суду, пояснення вчителя про те, що вона не змогла підключити дитину 03.03.2023 року до онлайн-навчання через оголошену повітряну тривогу спростовуються скріншотами із сайту, де розміщено історію оголошення тривог за вказану дату, зокрема, яка тривала на території Сумської області з 09:10 год. до 10:55 год., тоді як урок фізики у 10 класі школи згідно з розкладом мав розпочатись об 11:10 год. Також суд визнав такими, що не знайшли підтвердження у ході судового розгляду доводи вчителя щодо виходу зі строю (поламки) хромбуку, що призначений для проведення онлайн-уроків, неможливості забезпечити на ньому інтернет-з`єднання саме 02.03.2023 р., так як про таку обставину керівництво навчального закладу вчитель у будь-якій формі не повідомляла [12]. Однак, 11 грудня 2023 року Сумський апеляційний суд розглянув справу за апеляційною скаргою особи, яка притягується до адміністративної відповідальності, і постановив скасувати постанову суду 1-ої інстанції від 15.05.2023 р. та закрити провадження у справі щодо педагога на підставі п.1 ч. 1 ст. 247 КУпАП, у зв`язку із відсутністю в її діях складу адміністративного правопорушення, передбаченого ч.1 ст. 173-4 КУпАП. З урахуванням доводів апеляційної скарги, фактичних обставин та зібраних у справі доказів, апеляційний суд вважає, що в діях вчителя відсутні як об`єктивна, так і суб`єктивна сторона правопорушення, зокрема відсутня систематичність як ознака булінгу, а також наслідки у вигляді заподіяння чи можливості заподіяння шкоди психічному або фізичному здоров`ю потерпілого та відповідно не встановлений причинний зв`язок між конкретними діяннями та наслідками. Також, апеляційним судом не встановлено доказів того, що педагог діяла умисно, з метою заподіяння психологічної чи психічної шкоди неповнолітній учениці, її приниження, підпорядкування своїм інтересам чи спричинення соціальної ізоляції останньої з мотивів особистої неприязні до неповнолітньої чи бажання самоутвердитися тощо [13].

Прикладом притягнення педагога до дисциплінарної відповідальності за порушення антибулінгової політики закладу освіти слугує справа № 347/558/22 за позовом вчителя про визнання незаконним наказу про накладення дисциплінарного стягнення. Постановою Косівського районного суду Івано-Франківської області від 24.08.2023 р. у задоволенні позову відмовлено, оскільки суд дійшов переконання про правомірність оголошення догани за вчинення булінгу. В оскаржуваному наказі зазначено вид дисциплінарного стягнення та підстави його застосування, а саме: скарга учнів 9 класу та протокол засідання комісії з розгляду питань булінгу. Крім того, позивач визнана судом винуватою у

вчиненні адміністративного правопорушення, передбаченого ч.1 ст. 173-4 КУпАП - булінг (цькування) учасника освітнього процесу [14].

Розглядаючи питання відповідальності учасників освітнього процесу за кібербулінг, не можна оминути увагою чинники, що перешкоджають належному розгляду справи судом та притягненню до відповідальності осіб, що вчинили правопорушення. Зокрема, проблема бездоказовості онлайн-цькування прослідковується за змістом постанови Києво-Святошинського районного суду Київської області від 11.12.2023 р. у справі №369/17814/23. Згідно з протоколом про адміністративне правопорушення, учениця 9-В класу вчинила кібербулінг по відношенню до своєї однокласниці, в результаті чого виклала її фотозображення з образливим написом в Телеграм-каналі. В ході розгляду матеріалів справи суд дійшов до висновку, що вина учениці не доведена достатніми та беззаперечними доказами, оскільки з наявних в матеріалах справи фотокопій не можливо ідентифікувати той факт, що саме вона вчинила кібербулінг по відношенню до своєї однокласниці [15].

Згідно з протоколом про адміністративне правопорушення в іншій справі, 24.01.2023 р. неповнолітня вчинила кібербулінг по відношенню до дівчини, яка разом навчається з нею в класі, що виразилося в образливих смс-повідомленнях у соціальній мережі «Інстаграм» та психологічний булінг, що виразилося в систематичних особистих словесних образах непристойного характеру. Постановою Бородянського районного суду Київської області від 14.03.2023 р. у справі № 939/582/23 матеріали повернуто судом до відділення поліції для належного оформлення. В протоколі про адміністративне правопорушення не зазначено час і місце його вчинення, що є обов`язковим. Крім того, до матеріалів справи також не додані докази, які підтверджують батьківство особи, відносно якої складено протокол щодо неповнолітньої [16].

Проблему строків притягнення до адміністративної відповідальності можливо прослідкувати на прикладі справи № 210/655/22, що розглянута Дзержинським районним судом м. Кривого Рогу Дніпропетровської області. За обставинами справи, вчитель гімназії вчинила кібербулінг у відношенні неповнолітнього учня, що виразилося у нападках (домаганні) багатьма СМС-повідомленнями, телефонних дзвінків, чим вчинила адміністративне правопорушення, передбачене ч.1 ст.173-4 КУпАП. До матеріалів справи долучено скрін-шоти переписки у месенджерах «Telegram», «Viber» між вчителем та абонентом певного номеру. Зміст конкретних фраз, лексики та характеру використання мовних засобів, які вчитель застосовує у переписці з неповнолітнім, дає підстави для висновку, що її дії слід кваліфікувати як кібербулінг у формі психологічного насильства, що небезпідставно викликає у неповнолітнього побоювання за свою безпеку і завдає шкоду психічному здоров`ю. Постановою суду від 10.02.2022 р. вчителя визнано винною у вчиненні адміністративного правопорушення, передбаченого ч.1 ст.173-4 КУпАП, провадження у справі закрито у зв`язку із закінченням строків накладення адміністративного стягнення [17].

Тривожним видається збільшення випадків групового кібербулінгу в освітньому середовищі. У зв'язку з цим чимало дискусій породжує практика

звільнення судом від відповідальності особи, яка вчинила правопорушення, з огляду на висновок про малозначність діяння. В одній із справ, що розглянута судом, учениця 6-А класу ліцею спільно зі своїми однокласниками із застосуванням засобів електронних комунікацій, а саме в чат-групі «Viber» та «Telegram» каналі, створили групу з метою систематичного приниження честі та гідності, вчинила булінг (цькування) відносно однокласниці, де під час спілкування і СМС- повідомлень усіляко висміювала зовнішні риси та поведінку потерпілої, а також застосовувала ненормативну лексику в її адресу. Постановою Первомайського міськрайонного суду Миколаївської області від 15.03.2023 р. у справі № 484/1054/23 особу визнано винуватою у вчиненні адміністративного правопорушення, передбаченого ч. 4 ст. 173-4 КУпАП та звільнено від адміністративної відповідальності за малозначністю правопорушень, обмежившись усним зауваженням. Судом враховано, що правопорушення вчинено вперше, не є суспільно небезпечним, не спричинило і не здатне було спричинити будь-яку значну шкоду суспільним або державним інтересам, а також правам та свободам громадян. При цьому суддя враховує ту обставину, що мама учениці щиро розкаялася, усвідомила протиправність своєї поведінки, провела бесіду із донькою і є підстави вважати, що у подальшому не буде скоювати правопорушень [18].

Вільнянський районний суд Запорізької області розглянув справу № 314/5492/23, за обставинами якої мама учня не у повному обсязі виконувала свої батьківські обов`язки відносно малолітнього сина, внаслідок чого останній вчинив кібербулінг. У судовому засіданні мама учня підтвердила обставини, викладені у протоколі про адміністративне правопорушення, вину визнала, розкаялася, повідомила суд, що з сином проведено виховну та превентивну бесіди, йому видалено усі акаунти, син переживає підлітковий період, тому не завжди може знайти до нього підхід, однак прикладає до цього максимум зусиль. Конфлікт між дітьми вичерпано. Надала суду характеристику з закладу освіти і довідку про отримання допомоги підрозділу соціального захисту населення. Проаналізувавши характер та обставини вчиненого правопорушення, враховуючи особу правопорушника, ступінь вини, приймаючи до уваги, що мама учня вину у вчиненому визнає, розкаялася, суд вважає, що її слід звільнити від адміністративної відповідальності у зв`язку з малозначністю вчиненого нею правопорушення та оголосити усне зауваження. Постановою суду від 05.12.2023 р. матір учня звільнено від адміністративної відповідальності за ч. 1 ст. 184 КУпАП, оголошено усне зауваження та закрито провадження у справі [19].

За змістом Національної стратегії розбудови безпечного і здорового освітнього середовища у Новій українській школі неодноразово вказується на безвідповідальне використання Інтернету учасниками освітнього процесу, уразливість дітей шкільного віку під час використання Інтернету, нестача навичок безпечної поведінки в інформаційному середовищі, неконтрольований доступ до Інтернету під час освітнього процесу, потреба просвітницької роботи з питань медіагігієни та цифрової грамотності, що сприятимуть безпечній комунікації [20].

Проаналізовані приклади з судової практики переконливо вказують на необхідність застосування заходів, спрямованих на запобігання та протидію булінгу (цькуванню) в закладі освіти, у складі яких - заходи щодо організації безпечного користування мережею Інтернет та контролю за використанням засобів електронних комунікацій малолітніми чи неповнолітніми здобувачами освіти під час освітнього процесу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Близько 100 справ щодо булінгу в українських школах на рік. Опендатабот : вебсайт. URL: https://opendatabot.ua/analytics/bullying-in-school-2023 (дата звернення: 23.01.2024 р.).

2. Антибулінгове законодавство потребує змін. Освітній омбудсмен Сергій Горбачов : facebook. URL: https://www.facebook.com/Education.Ombudsman.Sergii.Gorbachov/posts/428927625694238 (дата звернення: 28.01.2024 р.).

3. Булінг в Україні: експерти пояснюють, куди звертатись тим, хто зазнав цькування. Суспільне. Новини : вебсайт. URL: https://suspilne.media/466703-buling-v-ukraini-eksperti-poasnuut-kudi-zvertatis-tim-hto-zaznav-ckuvanna (дата звернення: 27.01.2024 р.).

4. Кодекс України про адміністративні правопорушення. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення: 23.01.2024 р.).

5. Про освіту : Закон України від 05.09.2017 р. № 2145-VIII URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text (дата звернення: 23.01.2024 р.).

6. Порядок реагування на випадки булінгу (цькування) : наказ Міністерства освіти і науки України 28.12.2019 р. № 1646 URL: https://zakon.rada.gov.ua/laws/show/z0111-20#Text (дата звернення: 20.01.2024 р.).

7. Постанова Іваничівського районного суду Волинської області від 13.03.2023 р. у справі №156/51/23 URL: https://reyestr.court.gov.ua/Review/109600059# (дата звернення: 27.01.2024 р.).

8. Постанова Приморського районного суду м. Одеси від 27.06.2023 р. у справі №522/9953/23 URL: https://reyestr.court.gov.ua/Review/111825396 (дата звернення: 19.01.2024 р.).

9. Постанова Славутицького міського суду Київської області від 02.03.2023 р. у справі №377/129/23 URL: https://reyestr.court.gov.ua/Review/109329444# (дата звернення: 20.01.2024 р.).

10. Постанова Славутицького міського суду Київської області від 22.02.2023 р. у справі №377/104/23 URL: https://reyestr.court.gov.ua/Review/109147798 (дата звернення: 20.01.2024 р.).

11. Постанова Славутицького міського суду Київської області від 21.02.2023 р. у справі №377/106/23 URL: https://reyestr.court.gov.ua/Review/109119217 (дата звернення: 13.01.2024 р.).

12. Постанова Роменського міськрайонного суду Сумської області від 15.05.2023 р. у справі № 585/1343/23 URL: https://reyestr.court.gov.ua/Review/110834358# (дата звернення: 02.02.2024 р.).

13. Постанова Сумського апеляційного суду від 11.12.2023 р. у справі у справі № 585/1343/23 URL: https://reyestr.court.gov.ua/Review/115885775 (дата звернення: 03.02.2024 р.).

14. Постанова Косівського районного суду Івано-Франківської області від 24.08.2023 р. у справі №347/558/22 URL: https://reyestr.court.gov.ua/Review/113212426 (дата звернення: 23.01.2024 р.).

15. Постанова Києво-Святошинського районного суду Київської області від 11.12.2023 р. у справі №369/17814/23 URL: https://reyestr.court.gov.ua/Review/115886741# (дата звернення: 23.01.2024 р.).

16. Постанова Бородянського районного суду Київської області від 14.03.2023 р. у справі №939/582/23 URL: https://reyestr.court.gov.ua/Review/109573281 (дата звернення: 20.01.2024 р.).

17. Постанова Дзержинського районного суду м. Кривого Рогу Дніпропетровської області від 10.02.2022 р. у справі № 210/655/22 URL: https://reyestr.court.gov.ua/Review/104244197# (дата звернення: 24.01.2024 р.).

18. Постанова Первомайського міськрайонного суду Миколаївської області від 15.03.2023 р. у справі № 484/1054/23 URL: https://reyestr.court.gov.ua/Review/109587181 (дата звернення: 24.01.2024 р.).

19. Постанова Вільнянського районного суду Запорізької області від 05.12.2023 р. справа №314/5492/23 URL: https://reyestr.court.gov.ua/Review/115428247 (дата звернення: 20.01.2024 р.).

20. Національна стратегія розбудови безпечного і здорового освітнього середовища у Новій українській школі : Указ Президента України від 25 травня 2020 року № 195/2020 URL: https://zakon.rada.gov.ua/laws/show/195/2020#Text (дата звернення: 02.02.2024 р.).

МЕТОДОЛОГІЧНІ ПІДХОДИ ДО АНАЛІЗУ ТА КЛАСИФІКАЦІЇ ПРАВОПОРУШЕНЬ, ЗДІЙСНЮВАНИХ ВІДНОСНО ДІТЕЙ В ІНТЕРНЕТ-ПРОСТОРІ

Артем КУШКОВИЙ

У сучасному інформаційному суспільстві розвиток технологій та доступ до Інтернету стали неодмінною складовою життя, включаючи дітей та підлітків. Проте, разом із зростанням можливостей, які надає цей інтерактивний простір, також зростає й кількість правопорушень, вчинених відносно дітей в Інтернеті. Забезпечення їхньої безпеки та захист прав стає надзвичайно важливою проблемою, яка потребує комплексного та системного підходу.

Дослідження методологічних підходів до аналізу та класифікації правопорушень, здійснюваних відносно дітей в інтернет-просторі, є актуальним завданням на сучасному етапі. Ця тема створює можливість глибше зрозуміти сутність та особливості правопорушень, що відбуваються в Інтернеті та мають вплив на дітей, а також розробити ефективні стратегії їхнього виявлення, класифікації та протидії.

У даному контексті важливо дослідити різноманітні методологічні підходи, які використовуються для аналізу і класифікації правопорушень в Інтернеті, враховуючи особливості цифрового середовища та вплив на дітей. Відповідна методологія дозволить ефективно виявляти та реагувати на ці правопорушення, а також розробляти запобіжні заходи для забезпечення безпеки та захисту прав дітей у цифровому просторі.

Методологічні підходи до аналізу та класифікації правопорушень базуються на різних теоретичних концепціях та методиках, які дозволяють систематизувати та розуміти різноманітні правопорушення в їхніх різних аспектах. Серед цих підходів можна виділити наступні:

Кримінологічний підхід. Цей підхід базується на вивченні злочинності як соціального явища, включаючи аналіз причин, умов та наслідків правопорушень. Він використовує кримінологічні теорії для пояснення та класифікації різних видів злочинів.

Правознавчий підхід. Цей підхід спрямований на дослідження правових аспектів правопорушень, таких як їхнє визначення в законодавстві, процедури виявлення та реагування на них з точки зору права.

Соціологічний підхід. Цей підхід вивчає правопорушення з соціологічної перспективи, зосереджуючись на соціальних факторах, які сприяють виникненню та поширенню злочинності, а також на їхніх соціальних наслідках.

Психологічний підхід. Цей підхід аналізує правопорушення з точки зору психологічних аспектів, таких як мотивація, особистісні риси винуватців та їхній вплив на жертв, а також психологічні наслідки для обох сторін.

Криміналістичний підхід. Цей підхід спеціалізується на використанні наукових методів та технік для збору, аналізу та інтерпретації фізичних слідів та доказів, пов'язаних з правопорушеннями.

Отже, дослідження методологічних підходів базується на різних теоретичних концепціях та методиках, які спрямовані на систематизацію та розуміння різноманітних правопорушень у їх різних аспектах. Розробка та використання цих підходів є важливим кроком для ефективної боротьби з правопорушеннями в Інтернеті та забезпечення безпеки дітей у цифровому середовищі.

ЗАЛУЧЕННЯ НЕПОВНОЛІТНІХ ДО ПРОТИПРАВНИХ ДІЙ ЩОДО НАРКОТИЧНИХ РЕЧОВИН ЗА ДОПОМОГОЮ ЦИФРОВОГО СЕРЕДОВИЩА

Олена ЮШКЕВИЧ

Цифрове середовище розуміється як таке, що охоплює інформаційно-комунікаційні технології (ІКТ), включаючи Інтернет, мобільні та пов’язані з ними технології та пристрої, а також цифрові мережі, бази даних, контент та послуги. Водночас воно є складним і швидко розвивається, і багато в чому змінює життя дітей, що призводить як до можливостей, так і до небезпеки їхньому

благополуччю та втіленню прав людини. ІКТ є важливим інструментом у житті дітей для освіти, соціалізації, вираження та залучення, водночас їх використання може створювати певні ризики [1].

Одним із ризиків використання дітьми ІКТ можна назвати залучення неповнолітніх до протиправних дій щодо наркотичних речовин, зокрема незаконне виробництво, виготовлення, придбання, зберігання, перевезення чи пересилання з метою збуту, а також незаконний збут наркотичних засобів, психотропних речовин або їх аналогів (ч. 2 ст. 307 Кримінального кодексу України [2]). Молодим людям та підліткам – користувачам Інтернет нав'язується думка про те, що не всі наркотичні засоби є шкідливими для здоров'я, про існування недорогих і безпечних речовин і сумішей, які допомагають «розслабитися» і не викликають звикання та залежності [3].

При цьому діти реалізують наступні свої права: право вільно висловлювати свої думки, що включає свободу шукати, одержувати і передавати інформацію та ідеї будь-якого роду незалежно від кордонів в усній, письмовій чи друкованій формі, у формі творів мистецтва чи за допомогою інших засобів на вибір дитини (ст. 13 Конвенції про права дитини [4, 1]); право на таємницю кореспонденції (ст. 16 Конвенції про права дитини); право на освіту (ст. 28 Конвенції про права дитини); право на участь у грі і право на зібрання та об'єднання, право на конфіденційність та захист даних [1]).

Відповідно до ст. 33 Конвенції про права дитини [4] держави-учасниці мають вживати всіх необхідних законодавчих, адміністративних та соціальних заходів, а також заходів в галузі освіти, з тим, щоб захистити дітей від незаконного зловживання наркотичними засобами та психотропними речовинами, як вони визначені у відповідних міжнародних договорах, та не допускати залучення дітей до протизаконного виробництва таких речовин і торгівлі ними.

Проте, як показує практика, зазначені заходи малоефективні. Наприклад, правоохоронці затримали двох 18-річних хлопців, які почали свою злочинну діяльність ще будучи неповнолітніми. Фігуранти виконували інтернет-замовлення у Кременчуцькому районі. Під час обшуків у юнаків вилучили речові докази - розфасовані наркотики в особливо великих розмірах, чорнові записи, ваги та інше. Зокрема, поліція вилучила понад 2 кг солей α-PVP, які призначалися для «закладок». Також четверо неповнолітніх «закладчиків», віком 16-17 років, троє хлопців та одна дівчина, робили «закладки», використовуючи Telegram [5]. У Кам'янці-Подільському Хмельницької області перед судом постане 17-річна «закладчиця» синтетичних наркотиків. У підозрюваної правоохоронці вилучили понад 150 згортків з амфетаміном, метамфетаміном та PVP (солями), в якої вилучили 62 «закладки» (як у згортках, так і у пластикових флаконах) [6].

Способи втягнення неповнолітнього у протиправну діяльність як умовляння, залякування, підкуп, обман, розпалювання почуття помсти, заздрощів або інших низьких спонукань, розповідей про легкість і доступність певних дій, навчання способам та прийомам їх виконання тощо [7].

Найбільш поширеною формою втягнення неповнолітніх у вказану діяльність є збут неповнолітніми наркотиків за допомогою мережі Інтернет (89 %

випадків). Варто звернути увагу, що такий вид вчинення кримінального правопорушення за допомогою мережі Інтернет вчиняється через: замовлення (в режимі онлайн за допомогою програми типу ICQ, Skype, через інтернет-переписки в режимі онлайн у форумах (чатах) чи з використанням електронної пошти тощо); передоплати, оплати за замовлений наркотик (способів переказу грошей - термінали самообслуговування, система віддаленого банкінгу, поповнення електронного гаманця «електронними грошима», поповнення мобільного номеру телефону); пакування наркотиків залежно від виду речовини, пересилання та місця організації закладок (повідомлення про місцезнаходження наркотика та спосіб його отримання також можуть бути різними: розмова по телефону, відправка текстової інформації чи фотографії про місце приховування наркотику через Інтернет чи SMS-повідомлення) [8].

До процесу збуту наркотиків через мережу Інтернет залучаються у більшості випадків підлітки, які добре орієнтуються у сучасних технологіях та комп'ютерній техніці, а тому, розуміючи можливість бути викритими, вдаються до різних хитрощів приховуючи місце свого перебування змінюючи IP - адреси різними методами. Так, зокрема використовується TOR-браузер - система проксі-серверів, що дозволяє встановлювати анонімне мережеве з'єднання, захищене від прослідковування, тобто анонімна мережа віртуальних тунелів, що дозволяє передачу даних в зашифрованому вигляді. Також злочинці використовують VPN підключення - тобто технологію, яка забезпечує створення в Інтернеті зашифрованої додаткової «чорної» сітки для передачі даних. У випадках, коли для контакту використовуються номери мобільних операторів, збувачі систематично змінюють свої контакти тим самим уникаючи можливості своєї ідентифікації [9].

Пам'ятаючи про швидкість, з якою розвивається цифрове середовище та ІКТ, держава та громадянське суспільство повинні вживати запобіжних заходів, в тому числі регулярно оцінюючи будь-які ризики і шкоду, які вони можуть становити для здоров'я дітей, незважаючи на відсутність на даний час визначеності стосовно науково-технічного знання про існування або обсяг таких ризиків; повині вимагати застосування ефективних систем вікової перевірки для забезпечення захисту дітей від продуктів, послуг та контенту в цифровому середовищі, які юридично обмежуються з урахуванням конкретних вікових категорій, використовуючи методи, які узгоджуються з принципами мінімізації даних; співпрацювати з засобами масової інформації з належною повагою до свободи засобів масової інформації, з навчальними закладами та іншими відповідними зацікавленими сторонами для розробки програм підвищення обізнаності, спрямованих на захист дітей від шкідливого контенту, а також запобігання їх участі в незаконній онлайн-діяльності [1].

Підсумовуючи, слід зазначити, що інформаційно-комунікаційні технології є сьогодні одним з найважливіших факторів, що впливають на формування особистості та загального розвитку дитини. Але, на жаль, окрім користі (наприклад, допомога ефективному навчанню) завдає шкоду дитині. Одним із негативних наслідків використання інформаційно-комунікаційних технологій є залучення неповнолітніх до протиправних дій щодо наркотичних речовин у

цифровому середовищі. Якщо раніше наркозалежні особи знали, за якою адресою можна придбати дозу наркотику, то сьогодні прямий контакт покупця з продавцем повністю відсутній.

Інтернет повинен бути безпечним, надійним, відкритим та сприятливим середовищем для всіх, включаючи дітей, але нагальною потребою сучасного розвитку цифрового середовища є розробка послідовної державної політики за участю дітей, яка враховує взаємозалежність можливостей та ризиків у цифровому середовищі та необхідність забезпечення відповідних заходів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Рекомендації CM/Rec (2018) 7 Комітету Міністрів Ради Європи державам-членам про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі). URL: https://mvs.gov.ua/upload/file/rekomendac_ya_schodo_zahistu_d_tey_u_cifrovomu_seredovisch_2018.pdf (дата звернення: 09.01.2024).

2. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#n25 (дата звернення: 09.01.2024).

3. Лапта С. П. Використання Інтернету як інструмента незаконного продажу наркотичних засобів і сильнодіючих речовин. *Сучасні тенденції розвитку криміналістики та кримінального процесу :* тези доп. міжнар. наук.-практ. конф. до 100-річчя від дня народження проф. М. В. Салтевського (м. Харків, 8 листоп. 2017 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків: ХНУВС, 2017. С. 114-116. URL: https://dspace.univd.edu.ua/items/4d2ab601-a292-497e-bf9f-af0a1bdee566/.

4. Конвенція про права дитини від 20.11.1989 р. № 995_021. URL: https://zakon.rada.gov.ua/laws/show/995_021#Text (дата звернення: 09.01.2024).

5. За 5 місяців поліція вилучила у полтавців близько 10 кілограмів наркотиків. Полтавщина : інтернет-видання. URL: https://poltava.to/news/71639/ (дата звернення: 09.01.2024).

6. Кримінальна відповідальність за торгівлю наркотиками з 16 років: на Хмельниччині неповнолітня відповідатиме за свої дії. День за днем : інтернет-видання. URL: https://denzadnem.com.ua/nadzvychajno/157444 (дата звернення: 09.01.2024).

7. Савченко А.В., Вартилецька І.А., Семенюк О.О., Луцак О.О. Кримінально-правова характеристика злочинів у сфері обігу наркотичних засобів та психотропних речовин, вчинених із залученням неповнолітніх та щодо неповнолітніх : монографія. Київ : НАВС, 2016. 267 с.

8. Кукос М. В. Способи втягнення неповнолітніх у незаконне виробництво, виготовлення, придбання, зберігання, перевезення, пересилання чи збут наркотичних засобів, психотропних речовин або їх аналогів. *Науковий вісник Ужгородського Національного Університету*. Серія ПРАВО. 2023. Випуск 78: частина 2. С. 275-281. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/08/45.pdf.

9. Використання Інтернету як інструмента незаконного продажу наркотичних засобів і сильнодіючих речовин. Черкаська селищна рада : вебсайт. URL: https://cutt.ly/owJDogmQ (дата звернення: 09.01.2024).

ВІДОМОСТІ ПРО АВТОРІВ

Амангелдієва Анна Анатоліївна – курсантка 2 курсу факультету №3 Донецького державного університету внутрішніх справ.

Бабіч Анна Вікторівна – учитель інформатики гімназії «Семицвіт» Знам'янської міської ради Кіровоградської області.

Бабкова Олена Олексіївна – кандидат педагогічних наук, доцент, завідувач науково-дослідної лабораторії «Науково-методичні засади створення безпечного і здорового освітнього середовища у Новій українській школі» комунального закладу «Запорізький обласний інститут післядипломної педагогічної освіти» Запорізької обласної ради.

Баланенко Анастасія Дмитрівна – курсантка 2 курсу факультету №1 Донецького державного університету внутрішніх справ.

Барліт Оксана Олександрівна – кандидат педагогічних наук, доцент, головний науковий співробітник науково-дослідної лабораторії «Науково-методичні засади створення безпечного і здорового освітнього середовища у новій українській школі» комунального заклду «Запорізький обласний інститут післядипломної педагогічної освіти» Запорізької обласної ради.

Барна Ольга Василівна – Заслужений працівник освіти України, кандидат педагогічних наук, доцент, доцент кафедри інформатики та методики її навчання Тернопільського національного педагогічного університету імені Володимира Гнатюка.

Бєляєва Олена Іванівна – методист обласного науково-методичного центру інформатизації освіти комунального закладу «Запорізький обласний інститут післядипломної педагогічної освіти» Запорізької обласної ради.

Бойко Ірина Іванівна – кандидат психологічних наук, завідувач кафедри психології комунального закладу «Житомирський обласний інститут післядипломної педагогічної освіти» Житомирської обласної ради.

Васильєв Денис Олегович - викладач інформатики та математики Регіонального центру професійно-технічної освіти №1 м.Кременчука.

Відіборенко Інна Володимирівна – методист науково-методичної лабораторії суспільно-гуманітарних та естетичних дисциплін комунального закладу «Кіровоградський обласний інститут післядипломної педагогічної освіти імені Василя Сухомлинського».

Волошина Тетяна Анатоліївна - завідувач обласного ресурсного центру підтримки інклюзивної освіти комунального закладу «Запорізький обласний інститут післядипломної педагогічної освіти» Запорізької обласної ради.

Ворожбіт-Горбатюк Вікторія Вікторівна – доктор педагогічних наук, професор, головний науковий співробітник відділу дослідження проблем кримінально-виконавчого права науково-дослідного інституту вивчення проблем злочинності імені академіка В.В. Сташиса НАПрН України.

Волєгова Наталія Олександрівна - вихователь-методист спеціального дошкільного навчального закладу (ясла-садок) №46 «Краплинка».

Габорець Ольга Андріївна – доцентка кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету № 3 Донецького державного університету внутрішніх справ, доктор філософії, доцент.

Генсерук Галина Романівна – кандидат педагогічних наук, доцент, завідувач кафедри інформатики та методики її навчання Тернопільського національного педагогічного університету імені Володимира Гнатюка.

Грабовський Петро Петрович – кандидат педагогічних наук, старший викладач кафедри методики викладання навчальних предметів комунального закладу «Житомирський обласний інститут післядипломної педагогічної освіти» Житомирської обласної ради.

Гретченко Лариса Леонідівна – адвокатка, медіаторка, Голова Комітету НААУ з питань сімейного права, керівниця Центру «Адвокат дитини» Вищої школи адвокатури НААУ.

Грушко Роман Сергійович – аспірант спеціальність 011 Освітні педагогічні науки Кафедра інформатики та методики її навчання Тернопільського національного педагогічного університету ім. В. Гнатюка.

Дуняшенко Наталія Василівна – вчитель вищої кваліфікаційної категорії, старший вчитель, вчитель української мови та літератури і зарубіжної літератури комунального закладу «Ліцей «Мрія» Кропивницької міської ради»

Єфіменко Світлана Миколаївна – кандидат педагогічних наук, старший викладач кафедри інформаційно-комунікаційних технологій та безпечного освітнього середовища комунального закладу «Кіровоградський обласний інститут післядипломної педагогічної освіти імені Василя Сухомлинського».

Здоровець Олексій Федорович – завідувач обласного науково-методичного центру інформатизації освіти комунального закладу «Запорізький обласний інститут післядипломної педагогічної освіти» Запорізької обласної ради.

Кравченко Олена Вікторівна – кандидат філологічних наук, начальник відділу наукової та виховної роботи Центральноукраїнського інституту розвитку людини.

Кучеренко Марина Олександрівна – вчитель фізики та інформатики Івангородської філії комунального закладу «Олександрівський ліцей №2» Олександрівської селищної ради Кропивницького району Кіровоградської області, консультант комунального унітарного підприємства «Олександрівський центр професійного розвитку педагогічних працівників» Олександрівської селищної ради Кропивницького району Кіровоградської області.

Кушковий Артем Олександрович – курсант 1 курсу факультету №3 Донецького державного університету внутрішніх справ.

Литвиненко Ольга Валентинівна – завідувач навчально-методичного центру дистанційного навчання комунального закладу «Кіровоградський обласний інститут післядипломної педагогічної освіти імені Василя Сухомлинського».

Лунгол Ольга Миколаївна – кандидатка педагогічних наук, доцентка кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету підготовки фахівців для підрозділів кримінальної поліції Донецького державного університету внутрішніх справ, доцент.

Макаринська Анна Вадимівна – рядова поліції, курсантка факультету підготовки фахівців для підрозділів кримінальної поліції Донецького державного університету внутрішніх справ.

Марко Наталія Вікторівна - методист обласного ресурсного центру підтримки інклюзивної освіти комунального закладу «Запорізький обласний інститут післядипломної педагогічної освіти» Запорізької обласної ради.

Мартинюк Сергій Володимирович – кандидат фізико-математичних наук, доцент кафедри інформатики та методики її навчання Тернопільського національного педагогічного університету імені Володимира Гнатюка.

Мелешко Єлизавета Владиславівна – доктор технічних наук, професор, до-центка кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету, магістрантка факультету педагогіки, психології та мистецтв Центральноукраїнського державного університету імені В. Винниченка.

Михайлюк Іванна Олександрівна - курсантка 2 курсу, 203 навчальної групи, навчального-наукового інституту 3 Національної академії внутрішніх справ.

Наумова Вікторія Юріївна – старший викладач кафедри природничо-математичної освіти і технологій Інституту післядипломної освіти Київського столичного університету імені Бориса Грінченка.

Орел Ірина Станіславівна – викладач інформатики, комп'ютерної та обчислювальної техніки Гайворонського політехнічного коледжу.

Павлюк Денис Андрійович – студент 4-го курсу спеціальності «Професійна освіта. Цифрові технології» факультету математики, природничих наук та технологій Центральноукраїнського державного університету, волонтер Відділу Протидії Кіберзлочинам в Кіровоградській області департаменту кіберполіції нацполіції України.

Подмазін Сергій Іванович – доктор філософських наук, кандидат психологічних наук, доцент, методист комунального закладу «Запорізький обласний інститут післядипломної педагогічної освіти» Запорізької обласної ради.

Позігун Богдан Васильович – рядовий поліції, курсант факультету підготовки фахівців для підрозділів кримінальної поліції Донецького державного університету внутрішніх справ.

Пойда Сергій Андрійович – кандидат педагогічних наук, доцент, старший викладач кафедри управління та адміністрування КЗВО «Вінницька академія безперервної освіти».

Северина Любов Миколаївна – методист науково-методичного центру інформатизації освіти комунального закладу «Запорізький обласний інститут післядипломної педагогічної освіти» Запорізької обласної ради.

Сікорська Тетяна Сергіївна – вчитель зарубіжної літератури Червоненської філії КЗ «Хащуватський ліцей» Гайворонської міської ради Кіровоградської області.

Сімокоп Людмила Іванівна – консультант комунальної установи «Міський центр професійного розвитку педагогічних працівників Кропивницької міської ради».

Скасків Ганна Михайлівна – асистент кафедри інформатики та методики її навчання, аспірант Тернопільського національного педагогічного університету імені Володимира Гнатюка.

Стадниченко Кіра Валентинівна – старший викладач кафедри інформатичної та технологічної освіти комунального закладу «Запорізький обласний інститут післядипломної педагогічної освіти» Запорізької обласної ради.

Суржко Ольга Миколаївна – практичний психолог комунального закладу «Торговицький ліцей імені Є. Ф. Маланюка» Новоархангельської селищної ради Голованівського району Кіровоградської області.

Ткаченко Дар'я Андріївна – курсантка 2 курсу факультету №3 Донецького державного університету внутрішніх справ.

Ткаченко Людмила Іванівна — вихователь санаторного дошкільного навчального закладу (ясла-садок) № 65 «Лукомор'я» м. Кропивницький; здобувач вищої освіти освітнього ступеня Бакалавр спеціальності 013 Початкова освіта Миколаївського національного університету імені В. О. Сухомлинського, м.Миколаїв.

Ткаченко Марина Василівна – вчитель інформатики «Комунальний заклад «Ліцей «Перспектива» Світловодської міської ради»».

Торгало Павло Романович – рядовий поліції, курсант факультету підготовки фахівців для підрозділів кримінальної поліції Донецького державного університету внутрішніх справ.

Фамілярська Лариса Леонідівна – кандидат педагогічних наук, старший викладач кафедри педагогіки й андрагогіки комунального закладу «Житомирський обласний інститут післядипломної педагогічної освіти» Житомирської обласної ради.

Федоришина Марина Станіславівна – викладач Гайворонського політехнічного фахового коледжу та вчитель інформатики комунального закладу «Гайворонський ліцей №2».

Шаєц Єлизавета Олександрівна – курсантка 2 курсу факультету №3 Донецького державного університету внутрішніх справ.

Юшкевич Олена Геннадіївна – кандидат юридичних наук, доцент кафедри теорії та історії держави і права факультету № 1 Харківського національного університету внутрішніх справ.

Яким Тетяна Олександрівна – вихователь Калинівського закладу дошкільної освіти «Сонечко» Миколаївського району Воскресенської громади Миколаївської області; здобувач вищої освіти освітнього ступеня Бакалавр спеціальності 013 Початкова освіта Миколаївського національного університету імені В. О. Сухомлинського, м.Миколаїв.

Матеріали III Всеукраїнської науково-практичної конференції «БЕЗПЕКА ДІТЕЙ В ІНТЕРНЕТІ: ПОПЕРЕДЖЕННЯ, ОСВІТА, ВЗАЄМОДІЯ»

(м. Кропивницький, 05-09 лютого 2024 року)

Відповідальний редактор: Скрипка Г.В.
Укладач: Єфіменко С. М.

Підписано до друку 11.03.2024 р.
Формат 60х84 1/16. Папір офсетний. Гарнітура «Times New Roman».
Друк – принтер. Тираж 100 прим.
Зам. № 434

КЗ «КОІППО імені Василя Сухомлинського», вул. Велика Перспективна, 39/63, м. Кропивницький, 25006.