

КОМУНАЛЬНИЙ ЗАКЛАД
«КІРОВОГРАДСЬКИЙ ОБЛАСНИЙ ІНСТИТУТ ПІСЛЯДИПЛОМНОЇ
ПЕДАГОГІЧНОЇ ОСВІТИ ІМЕНІ ВАСИЛЯ СУХОМЛИНСЬКОГО»

Світлана Єфіменко

Організаційно-педагогічні умови формування навичок безпечної поведінки школярів в Інтернеті

Навчально-методичний посібник

*Друкується за рішенням вченої ради
комунального закладу «Кіровоградський обласний інститут післядипломної
педагогічної освіти імені Василя Сухомлинського»
(від 17 жовтня 2023 року, протокол №5)*

Кропивницький
2023

Єфіменко С.М. Організаційно-педагогічні умови формування навичок безпечної поведінки школярів в Інтернеті : навчально-методичний посібник. Кропивницький : КЗ «КОППО імені Василя Сухомлинського», 2023. 46 с.

У посібнику розглядається проблема безпечної поведінки в Інтернеті неповнолітніх користувачів. Здійснено аналіз наукових праць та нормативно-правових актів з проблематики посібника. На основі узагальнення результатів дослідження визначено сутність таких інтернет-загроз як «кібергрумінг», «сексторшен», «секстинг», «кібербулінг», «інтернет-шахрайство», «фейкова інформація», «небезпечний контент», «небезпечна онлайн-взаємодія», «інтернет-залежність». Виокремлено наслідки впливу інтернет-загроз на здоров'я та матеріальне благополуччя людини. Окреслено вимоги, критерії та індикатори безпечного і здорового освітнього середовища. Визначено 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.

Для керівників закладів загальної середньої освіти і їх заступників, педагогів різних фахів, психологів, бібліотекарів, усіх зацікавлених осіб.

Рецензенти:

Садовий М.І – професор кафедри математики та цифрових технологій Центральноукраїнського державного університету імені Володимира Винниченка, доктор педагогічних наук, професор;

Скрипка Г.В. – завідувач кафедри інформаційно-комунікаційних технологій та безпечного освітнього середовища комунального закладу «Кіровоградський обласний інститут післядипломної педагогічної освіти імені Василя Сухомлинського», кандидат педагогічних наук.

Відповідальний за випуск – Віталій ДМИТРУК

ЗМІСТ

Вступ.....	4
Інтернет як потенційне поле можливостей та загроз	6
Розбудова безпечного цифрового освітнього середовища.....	8
Шляхи формування навичок безпечної поведінки в Інтернеті здобувачів закладу загальної середньої освіти.....	12
Список використаних джерел.....	43

ВСТУП

В умовах цифровізації суспільства інтернет-простір став невід'ємною складовою усіх сфер діяльності людини. Всесвітня мережа містить безмежне потенційне поле можливостей для задоволення різноманітних потреб як дорослих так і дітей. Вона слугує простором розкриття творчого потенціалу своїх користувачів, сучасним засобом комунікації (інколи єдиним), інструментом взаємодії з державою, майданчиком розвитку й розваг, праці й відпочинку тощо. Діти й молодь переважно використовують онлайн-простір для спілкування й творчої самореалізації в соціальних мережах, пошуку цікавої інформації для навчання й розвитку, створення творчого продукту, перегляду відеороликів, прослуховування подкастів, участі в онлайн-іграх. Цифрове середовище збагачує світогляд своїх користувачів у різноманітних сферах життя та надає можливість реалізувати права: на доступ до Інтернету, на участь у житті суспільства, зокрема, на мирні зібрання та об'єднання з іншими особами в Інтернеті, на освіту, на свободу від дискримінації, на свободу вираження поглядів та інформації, на повагу до приватного життя і захист даних, на захист інтелектуальної власності, у тому числі авторського права та інші.

Формування знань та навичок безпечної поведінки громадян в інформаційному просторі Всемережжя є однією зі складових соціальної політики України, про що свідчать законодавчі акти, які її регламентують: Конституція України, Сімейний Кодекс України, Цивільний кодекс України, Кримінальний кодекс України, Конвенція про кіберзлочинність, Конвенція про права дитини, Концепція розвитку цифрових компетентностей, Концепція безпеки закладів освіти, Національна стратегія розбудови безпечного і здорового освітнього середовища у Новій українській школі, Модельний закон про захист дітей від інформації, яка шкодить їхнім здоров'ю та розвитку, Закон України «Про Національну програму інформатизації», Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про охорону дитинства», Закон України «Про безоплатну правову допомогу», Закон України «Про інформацію», Закон України «Про Освіту», Закон України «Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню)», Порядок реагування на випадки булінгу (цькування), Положення про дистанційну форму здобуття повної загальної середньої освіти, Порядок проведення інституційного аудиту закладів загальної середньої освіти, Рекомендація СМ/Рес (2018)7 Комітету Міністрів державам-членам про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі та інші.

В означених законодавчих актах окреслено правове регулювання процесу інформатизації суспільства, створення цифрового освітнього середовища, використання й поширення інформації, захисту персональних даних, захисту суспільства від кіберзлочинності, формування у громадян цифрових навичок й, зокрема, навичок безпечної поведінки в мережі Інтернет.

Водночас Всесвітня павутина є інструментом порушення прав людини та може містити загрози її *фізичному, психічному, соціальному й матеріальному благополуччю*. Проте, безпечна поведінка в Інтернеті сприяє задоволенню потреб

користувачів і водночас запобігає можливості стати як потенційною жертвою, так і потенційним джерелом (ненароком чи навмисне) інтернет-загроз.

Через відсутність достатнього рівня розвитку критичного мислення й життєвого досвіду саме неповнолітні є найбільш вразливими до інтернет-небезпек. Вони потерпають від кібербулінгу, від сексуального насильства онлайн й залучення до виготовлення дитячої порнографії, від смертельних челенджів, від інтернет-шахрайства, від шокуючого контенту, від фейкової інформації й інших інструментів інфотерору, а також від небезпечної взаємодії онлайн з російськими військовими через онлайн-ігри, закриті телеграм-канали чи приватне спілкування у соцмережах та месенджерах.

Заборонити дітям користуватись Інтернетом неможливо й не доцільно, оскільки онлайн-середовище має безліч переваг та можливостей для розвитку. Важливо технічно забезпечити умови безпечного інтернет-простору та навчити дітей користуватись Інтернетом безпечно.

Створення безпечного цифрового середовища й формування в дітей навичок безпечної поведінки в Інтернеті є спільним завданням батьків, освітян, громадських організацій, правоохоронних органів й суспільства в цілому.

Наведені у посібнику ідеї й методичні розробки спрямовані на допомогу освітянам ефективно організувати продуктивну, змістовну, цікаву, інтерактивну взаємодію учасників освітнього процесу щодо формування в школярів навичок безпечної поведінки в Інтернеті під час очного, дистанційного та змішаного навчання.

ІНТЕРНЕТ ЯК ПОТЕНЦІЙНЕ ПОЛЕ МОЖЛИВОСТЕЙ ТА ЗАГРОЗ

На сьогоднішній день інтернет-мережа, окрім безмежних можливостей для взаємодії з державою в цифровому полі, спілкування, самовираження, саморозвитку, самоосвіти й дозвілля, переповнена найрізноманітнішими інтернет-загрозами, спрямованими, у першу чергу, на неповнолітнього інтернет-користувача.

Загроза в Інтернеті – це імовірність завдання збитків, заподіяних *здоров'ю* людини та (або) її *майну* внаслідок користування Інтернетом [22, с.7]. У свою чергу, *здоров'я* – це стан повного *фізичного, психічного та соціального благополуччя*, а не лише відсутність хвороб або фізичних дефектів [23].

Наведемо приклади найбільш актуальних інтернет-загроз, спрямованих на неповнолітнього інтернет-користувача або ж неповнолітньою особою на інших інтернет-користувачів:

кібергрумінг – налагодження дорослим/групою дорослих осіб довірливих стосунків із неповнолітнім користувачем Інтернету з метою сексуального насильства над ним у реальному житті чи онлайн (сексуальне насильство онлайн відбувається шляхом примусу неповнолітнього виконати певні відверті дії на камеру під час відеозустрічі);

сексторшен – налагодження довірливих стосунків із неповнолітнім користувачем Інтернету з метою отримання інтимних фото/відео матеріалів, подальшого шантажування та вимагання додаткових/відвертіших інтимних матеріалів чи грошей в обмін на нерозповсюдження матеріалів, отриманих раніше;

секстинг – надсилання адресату у приватні повідомлення чи розміщення у відкритому доступі на вебсторінках власних інтимних фото/відео/аудіо/текстових матеріалів, що в подальшому може призвести до булінгу чи псуванню цифрово/ділової репутації;

кібербулінг – булінг (систематичне цькування) неповнолітнього здобувача освіти іншими учасниками освітнього процесу чи булінг неповнолітнім здобувачем освіти іншого учасника освітнього процесу у різних формах і проявах із застосуванням інформаційно-комунікаційних технологій;

інтернет-шахрайство – нанесення збитків матеріальному благополуччю інтернет-користувача шляхом незаконних операцій, заволодіння конфіденційної інформації, обману чи зловживання довірою з використанням інформаційно-комунікаційних технологій;

фейкова інформація – неповна, спотворена чи неправдива інформація, подана за допомогою інформаційно-комунікаційних технологій із метою поширення паніки, дезорієнтації, зниження здатності критично оцінювати ситуацію, формування певних думок та рішень з подальшим зловживанням ними для досягнення злочинних цілей маніпулятора;

небезпечний контент – змістове наповнення вебсторінок, що може містити інструкції з виготовлення саморобної вибухівки, опалювальних/електричних приладів, сцени насилля, суїциду, вбивства/каліцтва, порнографію, пропаганду дискримінації, екстриму, вживання

алкоголю, наркотичних речовин тощо;

небезпечна онлайн-взаємодія – взаємодія у форматі відеозустрічі, обміну текстовими чи аудіоповідомленнями з онлайн-друзем, який може виявитись російським військовим, інтернет-шахраєм чи іншим злочинцем, мета спілкування якого з неповнолітнім: виманювання конфіденційної інформації, приватних матеріалів, інформації військового значення, залучення неповнолітнього до виконання спеціальних завдань чи доручень (диверсія, терористичний акт, хуліганство, колабораційна діяльність, пособництво державі-агресору, 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) тощо;

інтернет-залежність – психічний розлад, що характеризується нав'язливим бажанням скористатись інтернет-мережею, нездатністю вчасно переключити свою увагу з віртуального світу на реальний, підвищенням пріоритету використання інтернет-мережі над іншими інтересами й справами та може проявлятися у вигляді систематичного онлайн-серфінгу (тривалого блукання вебсторінками в пошуку інформації), відеоігрової залежності (геймінговий розлад), залежності від соціальних мереж тощо.

Детальна характеристика означених інтернет-загроз та механізми захисту від них містяться на сайті освітнього проєкту #stop_sexтинг (<https://stop-sexting.in.ua/adult/ryzyk/>).

Загрози в Інтернеті можуть негативно впливати як на окремі сфери благополуччя неповнолітнього інтернет-користувача, так і на всі сфери одразу:

- **наслідки впливу інтернет-загроз на фізичне благополуччя:** астенопатія, хвороба сухого ока, біль у спині/ший, сколіоз, остеохондроз, артроз, зап'ястковий тунельний синдром, тендиніт, стенокардія, аритмія, тахікардія, тромбоз, варикоз, гіпертонія, геморої, енурез, хронічний головний біль, фізична втомленість, запаморочення, нехтування харчуванням, наявність шкідливих звичок у зв'язку з їх онлайн-пропагандою, потерпання від фізичного чи сексуального насильства, заподіяння собі фізичної шкоди випадково через неухважність (наприклад, потрапляння в дорожньо-транспортну пригоду у зв'язку з зосередженням уваги на цифровому пристрої під час руху), необачність (наприклад, під час експериментів в домашніх умовах) або навмисні травмуючі й, навіть, суїцидальні дії внаслідок маніпуляційного впливу онлайн-переслідування, залякування й шантажування, смертельних челенджів («Випий 40 таблеток і подивись, що буде», «Перебігти автомагістраль», «Їстивне-неїстивне», «2 таблетки парацетамолу і алкоголь» тощо), лайфхаків (наприклад, «Знаєш, як швидко потрапити в лікарню на 2-3 місяці?»), напрямів (наприклад, суїцидальний Deer TikTok), спільнот (руфинги (ті, хто здираються на дахи), дігери (ті, хто подорожують підземеллями), зацепинги (ті, хто чіпляються до вагонів – трамваїв, поїздів)) та смертельних ігор (Тихий ліс, Новий шлях, Синій кит, Червона сова тощо) в соціальних мережах/месенджерах;

- **наслідки впливу інтернет-загроз на психічне благополуччя:** зниження концентрації уваги, синдром дефіциту уваги й гіперактивність, погіршення пам'яті, підвищена дратівливість/збудженість/агресивність/тривожність, порушення сну, нестійкість психіки, депресивні стани, психологічне травмування внаслідок цькування онлайн чи участі у виготовленні дитячої порнографії, приниження власного почуття гідності внаслідок використання й поширення іншими у різних злочинних цілях конфіденційної/приватної інформації, вживання психоактивних речовин і наркотиків внаслідок їх пропаганди в Інтернеті, втрата здатності мозку до критичного мислення внаслідок інформаційного перевантаження фейковою інформацією тощо;

- **наслідки впливу інтернет-загроз на соціальне благополуччя:** адміністративна/кримінальна відповідальність за правопорушення, спричинені за допомогою інтернет-мережі (наприклад, булінг, взаємодія з російськими військовими тощо), псування цифрово/ділової репутації, втрата навичок реального спілкування внаслідок онлайн-комунікативної залежності, втрата життєвих інтересів, соціальних зв'язків, нераціональна витрата часу, відсутність змістовного дозвілля й зниження працездатності внаслідок надання пріоритету інтернет-мережі тощо;

- **наслідки впливу інтернет-загроз на матеріальне благополуччя:** збитки матеріальному благополуччю внаслідок незаконних операцій, заволодіння конфіденційною інформацією, обману чи зловживання довірою з боку інтернет-шахраїв, нераціональна витрата коштів внаслідок неконтрольованих покупок в інтернет-магазинах без необхідності їх придбання та урахування власних фінансових можливостей тощо.

РОЗБУДОВА БЕЗПЕЧНОГО ЦИФРОВОГО ОСВІТНЬОГО СЕРЕДОВИЩА

Аби уникнути інтернет-небезпек та не стати їх джерелом, керівник закладу загальної середньої освіти має врахувати всі вимоги, критерії та їх індикатори у розбудові безпечного і здорового освітнього середовища, зокрема цифрового освітнього середовища, керуючись відповідною нормативно-правовою базою.

Освітнє середовище закладу освіти - сукупність умов, що створюється в закладі освіти для навчання, виховання і розвитку здобувачів освіти і праці педагогічних працівників [15].

Безпечне освітнє середовище – сукупність умов у закладі освіти, що унеможливають заподіяння учасникам освітнього процесу фізичної, майнової та/або моральної шкоди, зокрема внаслідок недотримання вимог санітарних, протипожежних та/або будівельних норм і правил, законодавства щодо кібербезпеки, захисту персональних даних, безпечності та якості харчових продуктів та/або надання неякісних послуг з харчування, шляхом фізичного та/або психологічного насильства, експлуатації, дискримінації за будь-якою ознакою, приниження честі, гідності, ділової репутації (зокрема шляхом булінгу (цькування), поширення неправдивих відомостей тощо), пропаганди та/або

агітації, у тому числі з використанням кіберпростору, а також унеможлиблюють вживання на території та в приміщеннях закладу освіти алкогольних напоїв, тютюнових виробів, наркотичних засобів, психотропних речовин [17].

Всі учасники освітнього процесу мають бути залучені до процесу розбудови безпечного освітнього середовища та, відповідно, до створення організаційно-педагогічних умов формування безпечної поведінки школярів в Інтернеті.

Так, відповідно до закону України «Про освіту» [17], формування поваги до прав і свобод людини, нетерпимості до приниження її честі та гідності, фізичного або психологічного насильства, а також до дискримінації за будь-якими ознаками, є одним з важливих принципів освітньої діяльності (стаття 6). Також згідно з законом, одним із обов'язків освітян є захист здобувачів освіти під час освітнього процесу від будь-яких форм фізичного та психологічного насильства, приниження честі та гідності, дискримінації за будь-якою ознакою, пропаганди та агітації, що завдають шкоди здоров'ю здобувача освіти, запобігати вживанню ними та іншими особами на території закладів освіти алкогольних напоїв, наркотичних засобів, іншим шкідливим звичкам (стаття 54).

У свою чергу, Національна стратегія розбудови безпечного і здорового освітнього середовища у Новій українській школі [11] визначає безпечне й здорове освітнє середовище як сукупність умов у закладі освіти, що унеможлиблюють заподіяння учасникам освітнього процесу фізичної, майнової та/або моральної шкоди, зокрема, «внаслідок недотримання законодавства щодо: кібербезпеки, захисту персональних даних ...», та «шляхом фізичного та/або психологічного насильства: приниження честі, гідності, ділової репутації (булінг (цькування), поширення неправдивих відомостей тощо), експлуатації, дискримінації за будь-якою ознакою, пропаганди та/або агітації, у тому числі з використанням кіберпростору».

Відповідно до Порядку проведення інституційного аудиту закладів загальної середньої освіти [17] директорів закладу освіти слід дотримуватись **трьох вимог до розбудови безпечного і здорового освітнього середовища:**

- 1) *забезпечення комфортних і безпечних умов навчання та праці;*
- 2) *створення освітнього середовища, вільного від будь-яких форм насильства та дискримінації;*
- 3) *формування інклюзивного, розвивального та мотивуючого до навчання освітнього простору.*

Зокрема, з метою попередження випадків булінгу у різних формах і проявах, у тому числі із застосуванням засобів електронних комунікацій, керівнику закладу освіти варто враховувати критерії й індикатори *другої вимоги: «Створення освітнього середовища, вільного від будь-яких форм насильства та дискримінації»*. А саме: планувати та реалізувати діяльність щодо запобігання будь-яким проявам дискримінації, булінгу в закладі; співпрацювати з представниками правоохоронних органів, іншими фахівцями з питань запобігання та протидії булінгу; оприлюднювати й сприяти дотриманню в закладі учасниками освітнього процесу правил поведінки, етичних норм, поваги до гідності, прав і свобод людини; психологічній службі закладу освіти

(практичному психологу, соціальному педагогу) здійснювати системну роботу з виявлення, реагування та запобігання булінгу, іншому насильству (діагностування, індивідуальна робота, психолого-соціальна підтримка, тренінгові заняття тощо); керівнику та заступникам керівника закладу освіти, педагогічним працівникам протидіяти булінгу, іншому насильству, дотримуючись чинного законодавства (Закон України «Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню)», Порядок реагування на випадки булінгу (цькування)).

Також у Порядку проведення інституційного аудиту закладів загальної середньої освіти [17] *шостим критерієм першої вимоги («Забезпечення комфортних і безпечних умов навчання та праці»)* є забезпечення у закладі умов для безпечного використання мережі Інтернет та формування в учасників освітнього процесу навичок безпечної поведінки в Інтернеті.

У рекомендаціях до побудови внутрішньої системи забезпечення якості освіти у закладі загальної середньої освіти [1, с. 19-22] *забезпечення у закладі умов для безпечного використання мережі Інтернет* передбачає: наявність контент-фільтрів (на пристроях, якими користуються діти та на Wi-Fi роутерах) для обмеження доступу до сайтів з небажаним змістом; наявність антивірусних програм та їх вчасне оновлення; користування інтернет-ресурсами під час навчальних занять під наглядом педагогів; моніторинг шкільних ресурсів (вебсайт, сторінки у соціальних мережах) на предмет розміщення на них несанкціонованої інформації. Важливо також застосовувати в закладі освіти ліцензійне програмне забезпечення, безпечні пошуковики (Kiddle, YouTube Kids тощо), застосунки, що відповідають віковій категорії неповнолітнього користувача, налаштування брандмауера й параметрів конфіденційності у браузері, спеціальні розширення браузера (наприклад, «Ad-Blocker», «Adblock для YouTube», «AdGaurd Антибанер» для блокування банерної реклами), які допоможуть захистити учасників освітнього процесу в мережі Інтернет від небажаного контенту.

З метою збереження персональних даних учасників освітнього процесу не допускається в закладі освіти збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини (частина 2 статті 32 Конституції України). Таким чином, перед зйомкою та оприлюдненням на вебсайті закладу освіти або персональному вебсайті/блогі педагога чи сторінці в соціальній мережі фото-, відеоматеріалів, потрібно отримати дозвіл на це від батьків чи інших законних представників дитини. Однак, такий дозвіл не потрібен, якщо відзняті матеріали не дають можливості ідентифікувати особу дитини; у разі проведення заходів публічного характеру в закладі та відсутності прямої заборони батьків чи інших законних представників дитини на зйомку та розміщення матеріалів (частина 1 та 3 статті 307 Цивільного кодексу України); здійснення зйомки та розміщення матеріалів у інтересах національної безпеки, економічного добробуту та прав людини (частина 2 статті 32 Конституції України). У законодавстві України також закріплені відповідні положення щодо прав дитини з питань інформації, яка її

стосується. Так, згідно зі ст. 171 Сімейного кодексу України «Дитина має право на те, щоб бути вислуханою батьками, іншими членами сім'ї, посадовими особами з питань, що стосуються її особисто, а також питань сім'ї». Тому персональна інформація про дитину (фото-, відео-, інші матеріали) може оприлюднюватись не лише з дозволу батьків чи інших законних представників дитини, а й з дозволу самої дитини.

Наразі, враховуючи Указ Президента України №64/2022 «Про введення воєнного стану в Україні» [14], згідно з яким право на розповсюдження інформації може тимчасово обмежуватися, керівники й педагогічні працівники мають уникати розміщення в інтернет-мережі інформації, яка може нашкодити учасникам освітнього процесу, освітньому закладу, населеному пункту, збройним силам України, Україні в цілому. У першу чергу, це стосується прямих трансляцій, стрімів та анонсів масових заходів, організованих на базі закладу освіти, особливо, якщо в їх рамках відбувається збір коштів для збройних сил України та залучення військовослужбовців, волонтерів; інформації про проведення заходів з відміткою військовослужбовця чи волонтера на світлинці в соціальній мережі; інформації щодо військовослужбовців – членів сімей здобувачів освіти; фото- й відеоматеріалів території закладу освіти, поряд з якою знаходяться стратегічні об'єкти тощо. Більше інформації щодо висвітлення інформації про заклад освіти в умовах воєнного стану від Служби освітнього омбудсмена та Асоціації Digital Ukraine розміщено за покликанням: <https://cutt.ly/TVTrYNt>.

Корисними у забезпеченні в закладі освіти умов для безпечного використання мережі Інтернет, зокрема унеможливлення витоку персональних даних учасників освітнього процесу, є відеоматеріали «[Про права людини, Інтернет та заклад освіти](#)», «[Права людини та Інтернет. Інтерв'ю з Оленою Черних](#)», підготовлені студією онлайн-освіти EdEra, а також у [Методичних рекомендаціях щодо організації роботи сайту закладу освіти](#). Роз'яснення від освітнього омбудсмена у співпраці з Українською Гельсінською спілкою з прав людини про те, які дані є персональними, які правові підстави обробки персональних даних закладом освіти, чи є заява про зарахування до закладу освіти підставою для обробки персональних даних, яка ціль обробки персональних даних у закладі освіти у межах встановленої мети, чи потрібно закладу освіти брати згоду на обробку персональних даних у батьків, як діяти закладу освіти, коли батьки відкликають або не надають згоду на обробку персональних даних у закладі освіти, розміщено за покликанням: <http://surl.li/kztet>. Також на сайті Служби освітнього омбудсмена розміщено Роз'яснення щодо «[Обробки персональних даних в електронних журналах та щоденниках](#)» та «[Обробка персональних даних в інформаційних системах та електронних реєстрах. Права учасників освітнього процесу та дії закладу освіти](#)». На сайті Міністерства освіти і науки України (далі МОН) розміщено «[Рекомендації уповноваженого Верховної Ради України з прав людини щодо захисту персональних даних під час дистанційного надання освітніх послуг](#)». Також на сторінці МОН України у Facebook можна ознайомитись із записом трансляції зустрічі з фахівцями Департаменту кіберполіції Національної поліції

України, які надали інформацію про безпечне використання онлайн-платформ Zoom, Google Classroom, Google Meet або Microsoft Teams в освітньому процесі (https://fb.watch/mVD5r9pL_4/).

Аби звести нанівець можливість потрапити до пастки тієї чи іншої інтернет-загрози, не лише в закладі освіти, а й вдома мають бути забезпечені технічні умови безпечного користування мережі Інтернет дитиною. Як і в закладі освіти, в домівках родини дитини (не лише в сім'ї, де мешкає неповнолітній користувач інтернет-мережі, а й у домівках її бабусі й дідуся) мають використовуватись контент-фільтри (наприклад, Google Family Link), антивірусні програми, ліцензійне програмне забезпечення, застосунки, що відповідають віковій категорії неповнолітнього користувача, безпечні пошуковики, налаштування брандмауера й параметрів конфіденційності у браузері, спеціальні розширення браузера для блокування банерної реклами на всіх девайсах, якими користується дитина. Якщо родина користується спільним комп'ютером чи Smart TV, варто створювати окремі облікові записи для кожного члена родини. Також як і у закладі освіти, так і в родині слід дотримуватись чинного законодавства щодо дотримання прав дитини, зокрема щодо недоторканності приватного життя дитини (у першу чергу, це питання стосується розміщення інформації різного формату в соціальних мережах/месенджерах про життя дитини її рідними).

ШЛЯХИ ФОРМУВАННЯ НАВИЧОК БЕЗПЕЧНОЇ ПОВЕДІНКИ В ІНТЕРНЕТІ ЗДОБУВАЧІВ ЗАКЛАДУ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ

Окрім забезпечення у закладі освіти та в родині технічних умов для безпечного використання мережі Інтернет, необхідно сприяти формуванню в неповнолітніх здобувачів освіти навичок безпечної поведінки в Інтернеті.

Безпечна поведінка в Інтернеті – 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 [23, с. 7].

Така поведінка є **результатом** сформованості:

- *знань*

про права людини в цілому, та, зокрема, права, які потенційно забезпечуються чи порушуються в Інтернеті;

щодо можливостей активної, свідомої й відповідальної електронної участі в «житті» закладу освіти, населеного пункту, громади, країни, світу засобами цифрових сервісів;

про позитивний та негативний вплив Інтернету й цифрових пристроїв на благополуччя людини й шляхи його попередження;

з необхідних дій у випадку, якщо став жертвою або спостерігачем чиїхось дій в Інтернеті, які загрожують здоров'ю та/або матеріальному благополуччю людини;

- *вмінь*

реалізовувати й дотримуватись прав людини в Інтернеті;

брати активну, свідому й відповідальну електронну участь в «житті» закладу освіти, населеного пункту, громади, країни, світу засобами цифрових сервісів;

виконувати умови/дотримуватись правил збереження власного благополуччя і благополуччя інших під час користування Інтернетом й цифровими пристроями;

звертатись за допомогою й захистом в разі наражання на загрози в Інтернеті;

- *ціннісного ставлення до*

прав людини в інтернет-просторі;

інтернет-можливостей активної, свідомої й відповідальної електронної участі в «житті» закладу освіти, населеного пункту, громади, країни, світу;

власного благополуччя й благополуччя інших;

механізмів захисту прав людини, що порушені в Інтернеті (визнання їх дієвості, сприйняття звернення про допомогу й захист як умови безпечного користування Інтернетом).

Навчання з безпечного використання мережі Інтернет має бути обов'язковою складовою процесу підвищення рівня цифрової компетентності освітян, оскільки завдання педагога – формувати одну з ключових компетентностей учнів – інформаційно-комунікаційну. Означена компетентність, що передбачає впевнене та критичне застосування інформаційно-комунікаційних технологій для створення, пошуку, обробки, обміну інформацією на роботі, в публічному просторі та приватному спілкуванні, має стати наскрізною в усіх навчальних предметах та інтегрованих курсах освітньої програми закладу.

У родинному колі формувати навички безпечної поведінки в Інтернеті слід у довірливих партнерських взаєминах між дитиною та дорослими членами родини наступними шляхами:

- бесіди з дитиною щодо важливості персональної інформації, онлайн репутації, щодо профілактики загроз в Інтернеті та механізмів захисту від них;

- інсценізації ситуацій, які можуть трапитись з дитиною онлайн (спілкування з незнайомцями, контент, який налякав тощо);

- спільне визначення й дотримання сімейних правил/угод про умови користування Інтернетом та особистими пристроями, вікової відповідності змісту сайтів, ігор та застосунків, витоку конфіденційної інформації, яка стосується членів сім'ї;

- демонстрація батьками дитини, старшими братами й сестрами, іншими членами родини власного позитивного прикладу щодо екранного часу, безпечного й змістовного використання інтернет-мережі.

У закладі освіти формувати навички безпечної поведінки в Інтернеті в школярів доцільно шляхом заходів і занять, організованих освітянами у співпраці з представниками соціально-психологічних служб, соціальних служб, служб у справах дітей, правоохоронних органів, громадських організацій. Це такі

практико зорієнтовані освітні заходи як: навчальні тренінги, воркшопи, дискусії, бесіди з використанням ситуативних кейсів, квести, ділові ігри, челенджі, проектна діяльність, ігри-інсценізації та інші активні й інтерактивні методи й форми навчальної взаємодії учасників освітнього процесу. Бесіди з проблеми безпечного інтернет-користування можуть бути елементом кожного уроку/заняття зі школярами, якщо в його рамках передбачено використання цифрових технологій. На уроках з предметів «Інформатика», «Здоров'я, безпека та добробут», «Основи здоров'я», «Вчимося жити разом», «Основи правознавства» тощо проблема інтернет-безпеки має вивчатись систематично як окрема тема чи в межах вивчення інших тем освітньої програми. Захід з тематики безпечного інтернет-користування можна приурочити до видатних подій/дат. А саме: День захисту даних (28 січня), День безпечного Інтернету (другий вівторок лютого), Всесвітній день здоров'я (7 квітня), Міжнародний день протидії булінгу (4 травня), Міжнародний день захисту дітей (1 червня), Всеукраїнський тиждень протидії булінгу (вересень), Місяць кібербезпеки (жовтень), Європейський день захисту дітей від сексуальної експлуатації та сексуального насильства (18 листопада), Всеукраїнська Акція «16 днів проти насилля» (25 листопада – 10 грудня), День прав людини (10 грудня) тощо.

Важливо активно залучати здобувачів освіти та їх батьків до організації таких заходів і занять, підтримувати їх творчу ініціативу. Бесіди, лекції з запрошеними фахівцями, тренінги чи їх елементи доцільно використовувати також на батьківських зборах з метою формування у батьків компетентностей з інтернет-безпеки їх дітей.

З метою формування знань щодо безпечної поведінки у Всемережжі у закладі освіти також доцільно спільно розробити й оприлюднити правила користування мережею Інтернет. Ці правила можуть мати загальний характер та адресуватись усім учасникам освітнього процесу, або ж бути диференційованими, наприклад, за віковими категоріями учнів.



Наразі для освітян, здобувачів освіти та їх батьків розроблено потужну навчально-методичну базу з безпеки в Інтернеті. Це не лише посібники й брошури з правилами безпечного Інтернету, детальними інструкціями, як діяти в тій чи іншій небезпечній онлайновій ситуації, а ще освітні серіали, навчальні курси й готові до використання розробки уроків, тренінгів, вправ, ігор з відповідним методичним супроводом. На сайті щорічної Всеукраїнської науково-

практичної конференції [«Безпека дітей в Інтернеті: попередження, освіта, взаємодія»](#), що організовується кафедрою інформаційно-комунікаційних технологій та безпечного освітнього середовища комунального закладу «Кіровоградський обласний інститут післядипломної педагогічної освіти імені Василя Сухомлинського», є доступ до цих матеріалів. Так, тут розміщено інформацію про сутність актуальних інтернет-загроз, механізми звернення про допомогу й захист від загроз в Інтернеті, номери телефонів гарячих ліній, покрокові інструкції щодо дії керівників та педагогів закладів освіти, здобувачів

освіти та їх батьків у ситуаціях виникнення онлайн-загрози по відношенню до школяра. Також сайт містить відсортовані за віковими категоріями здобувачів освіти навчально-методичні кейси для дітей, їх батьків та освітян, розроблені командами платформи цифрової освіти ДІА, ГО «МІНЗМІН», CRDF Global спільно із партнерами ГО «Смарт освіта», дитячого фонду ООН ЮНІСЕФ, освітнього проєкту #stop_сехтинг тощо за підтримки Міністерства освіти і науки України, Міністерства цифрової трансформації України, Уповноваженого Президента України з прав дитини, офісу Добročесності Національного агентства з питань запобігання корупції, Центру протидії дезінформації при Раді національної безпеки і оборони України, Служби Безпеки України, кіберполіції. Також складовими кейсів є авторські розробки (ігри, вправи, вебквест, відеоматеріали, статті) з проблеми інтернет-безпеки. Кейси систематично поновлюються та доповнюються новими навчально-методичними матеріалами. Розглянемо окремі складові кожного з кейсів.



[Кейс «Для дошкільнят»](#) містить розробку уроку для дітей 4-6 років «Моя перша подорож безпечним онлайн-простором»; мультфільм та аудіоказку про безпеку дітей онлайн «Хаппі та її суперсила»; розробки ігор для малят з проблеми інтернет-безпеки; відеоматеріали й посібники для батьків та вихователів про безпеку дітей дошкільного віку в Інтернеті.



[Кейс «Для учнів 1-4 класів»](#) містить розробки уроків з безпеки в Інтернеті; мультфільм, аудіоказку та онлайн-інтерактиви за мотивами казки «Хаппі та її суперсила»; мультфільм «Корисні підказки 2. Увага! Інтернет!»; інтерактивну книгу «У мережі з САНГО»; топ-правила безпечного інтернет-користування для учнів початкової ланки освіти; онлайн-курс з кібербезпеки, відеоматеріали, посібники, ігри та вправи з інтернет-безпеки.



[Кейс «Для учнів 5-8 класів»](#) містить розробки уроків, виховних годин та тренінгів з безпеки в Інтернеті; робочий зошит для підлітків та посібник для вчителів «Інтернет, який ми хочемо»; відеоінструкції з налаштування приватності в соціальних мережах/месенджерах; освітній серіал «Про кібербулінг для підлітків»; топ-правила безпечного інтернет-користування для учнів середньої ланки освіти; онлайн-курс з кібербезпеки, посібники, ситуативні кейси, ігри та вправи з інтернет-безпеки.



[Кейс «Для учнів 9-11 класів»](#) містить розробки уроків, виховних годин та тренінгів з безпеки в Інтернеті; соціальний відеоролик про онлайн-грумінг; відеоінструкції з налаштування приватності в соціальних мережах/месенджерах; топ-правила безпечного інтернет-користування для юнацького віку; онлайн-курс з кібербезпеки, посібники, ситуативні кейси, робочі зошити, ігри, вправи та інший інтерактив з інтернет-безпеки.



[Кейс «Для батьків»](#) містить розробки ігор, вправ, шаблонів сімейних угод з безпеки в Інтернеті, які можна використовувати в родинному колі; соціальні відеоролики й освітні серіали для батьків про інтернет-загрози (небезпечний контент, секстинг, онлайн-грумінг, кібербулінг тощо); відеоінструкції з налаштування приватності дитини в соціальних мережах/месенджерах, налаштування технічних засобів батьківського Контролю на Android та iOS,

налаштування та розширення браузера, які допоможуть захистити дитину від інтернет-загроз; топ-правила безпечного інтернет-користування; посібники, поради для батьків з інтернет-безпеки дітей.



[Кейс «Інтернет-безпека під час війни»](#) містить авторські навчально-методичні матеріали з інформаційної грамотності та кібербезпеки дітей під час війни; розробки уроків «Доброчесність онлайн» для 7-11 класів від Центру протидії дезінформації при РНБО України та Офісу доброчесності НАЗК; розробку уроку для учнів 5-8 класів «(Не)безпека в час війни» від освітнього проєкту #stop_sexтинг; відеоматеріал від СБУ про шляхи залучення неповнолітніх українських

дітей російськими окупантами для розвідок військових позицій; авторський вебквест «Безпека в Інтернеті в умовах воєнного стану»; буклети від освітнього проєкту #stop_sexтинг «Онлайн злочини за участю дітей під час війни», «Протидія залучення дітей російськими військовими до протиправної діяльності через Інтернет», «Дезінформація та правила реагування на неї», «Дитинство під час війни. Які навички ми маємо дати дітям для їхньої безпеки?».



[Кейс «Розробки освітян Кіровоградщини»](#) містить сценарії заходів з тематики безпечного Інтернету, розроблені освітянами Кіровоградської області в рамках авторського дистанційного тренінгу «Організаційно-педагогічні умови формування безпечної поведінки школярів в Інтернеті».

В умовах очного формату навчання навчально-методичні матеріали, систематизовані в розглянутих кейсах, можуть стати помічниками освітян в організації

заходів та занять з формування у здобувачів освіти навичок безпечної поведінки в Інтернеті.

Під час дистанційного та змішаного навчання, за умов відсутності можливості організувати захід з проблеми інтернет-безпеки саме в очному форматі, формування навичок безпечної поведінки в Інтернеті в здобувачів освіти може здійснюватись за допомогою різноманітних цифрових інструментів.

Так, синхронну відеозустріч з представниками соціально-психологічних служб, соціальних служб, служб у справах дітей, правоохоронних органів, громадських організацій доцільно організувати, наприклад, за допомогою сервісів Zoom <https://zoom.us/> чи Google Meet <https://meet.google.com/>.

Розмістити для учасників освітнього процесу інформацію про сутність інтернет-загроз, правила інтернет-безпеки й механізми звернення про допомогу й захист від загроз в Інтернеті з номерами гарячих ліній та чат-ботами з кібербезпеки, доцільно на сайті закладу освіти, персональному сайті чи блозі освітянина.



Розмістити здобувачам освіти завдання й супровідні навчальні матеріали з можливістю зворотного зв'язку й оцінювання дозволяють безкоштовні освітні платформи Moodle та Google Classroom. Також найбільш популярні в Україні месенджери Viber та Telegram можуть стати непоганою альтернативою освітніх платформ або ж їх доповненням. Так, групи й спільноти у Viber та групи й канали в Telegram дозволяють здійснити обмін файлами різних форматів, опитування в режимі

вікторини, групові відеочати, обмін та збереження повідомлень, їх закріплення й швидкий пошук за типом. Так, до прикладу, автором створено та адмініструється Telegram-канал «Безпека дітей в Інтернеті: попередження, освіта, взаємодія» (<https://t.me/bezpekaditeivinterneti>), де для освітян систематично розміщується інформація про обласні, Всеукраїнські та Міжнародні заходи з безпеки в Інтернеті.

Чудовою альтернативою сайту, блогу чи освітньої платформи може слугувати умовно безкоштовний онлайн-сервіс Netboard <https://netboard.me/>, який дозволяє створювати безліч тематичних сторінок з підсторінками (рис. 1).



Рис. 1. Скриншот фрагменту авторської тематичної сторінки в Netboard, створеної для учнів 10-11 класів з теми «Безпека в Інтернеті»

Для кожної створеної тематичної сторінки можна обирати налаштування приватності. На створеній тематичній сторінці самостійно чи у співавторстві можна розміщувати будь-який вебконтент (текст, аудіо, зображення, відео, опитувальники, ігри й інший інтерактив), систематизувати його за розділами та підсторінками й поширювати для перегляду. Наприклад, на тематичній сторінці можна розмістити [Посібник з прав людини для Інтернет-користувачів та пояснювальний меморандум](#) в PDF-форматі, відеоролик [проєкту «Права людини та Інтернет»](#), візуалізовані за допомогою інфографіки правила безпечного Інтернету, подкаст, тест, гру й вебквест з проблематики інтернет-безпеки. Здобувачі освіти, перейшовши за покликанням, мають можливість переглянути вміст сторінки Netboard, завантажити її файли, взяти участь в тестуванні й пограти у вбудовані на сторінці ігри. Особливістю розглянутого сервісу є те, що він надає можливість адміністраторам (авторам) тематичної сторінки отримувати зворотний зв'язок у вигляді коментарів та вподобайок під кожним розміщеним матеріалом.

Пропонуємо ознайомитись з авторською тематичною сторінкою з проблеми безпечного інтернет-простору для учнів 10-11 класів, створеної в сервісі Netboard, а також авторським скринкастом з алгоритму її створення, перейшовши за покликанням чи QR-кодом.



[Авторська тематична сторінка «Безпека в Інтернеті», 10-11 клас](#)



[Світлана Єфіменко. Створюємо тематичну сторінку в netboard.me](#)

Ознайомити учнів із сутністю тих чи інших інтернет-загроз допоможе створена для дітей, дітьми чи разом з дітьми різноманітна наочність (інтелектуальні карти, інфографіка, інтерактивні плакати, буклети, презентації тощо). Наведемо приклад авторських інтерактивного плакату та інтерактивної презентації з тематики інтернет-безпеки (рис. 2, 3). Також, пропонуємо ознайомитись з означеними інтерактивними цифровими освітніми ресурсами та скринкастами з алгоритму їх створення, за допомогою покликання чи QR-коду.



Рис. 2. Скриншот авторського інтерактивного плакату «Інтернет-загрози», розробленого за допомогою сервісу Genially

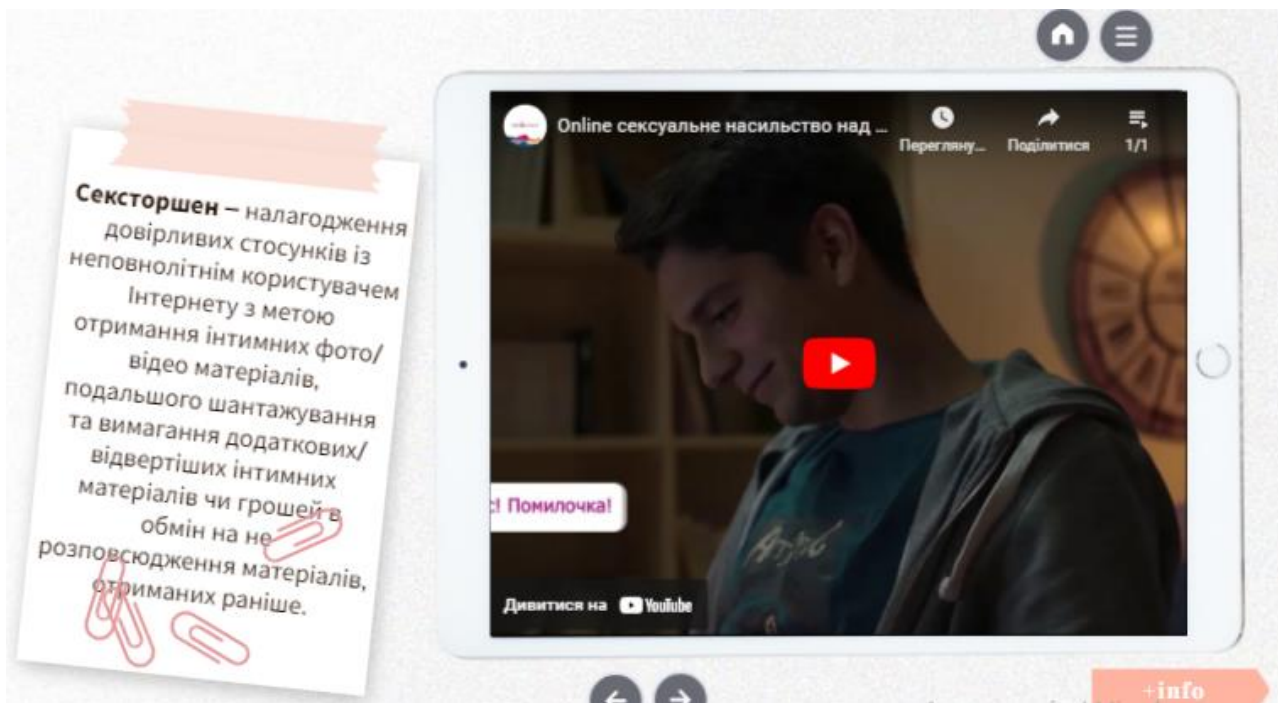


Рис. 3. Скриншот авторської інтерактивної презентації «Інтернет-загрози», розробленої за допомогою сервісу Genially



[Авторський інтерактивний плакат «Інтернет-загрози»](#)



[Світлана Єфіменко. Створюємо інтерактивний плакат в Genially](#)



[Авторська інтерактивна презентація «Інтернет-загрози»](#)



[Світлана Єфіменко. Створюємо інтерактивну презентацію в Genially](#)

Для інтерактивної взаємодії на відстані, з метою обміну думками, ідеями, досвідом з проблеми безпечного інтернет-користування, рекомендуємо використовувати умовно безкоштовний сервіс Conceptboard <https://conceptboard.com/>. Він дозволяє створювати безліч віртуальних дошок

досить великої площі та обирати для синхронної й асинхронної співпраці на дошці необхідні шаблони тла, блоків, схем, діаграм, таблиць, фігур, іконок та інших інструментів сервісу (але не більше 130 елементів на одній дошці у безкоштовному плані). Учасники взаємодії, перейшовши на онлайнкову дошку за покликанням, можуть спільно вбудовувати, редагувати й завантажувати контент різного формату (файли PDF, Google Docs, зображення, відео тощо), а також «прикріплювати» на полотні дошки стікери, використовувати стрілки, залишати один-одному коментарі (рис. 4).

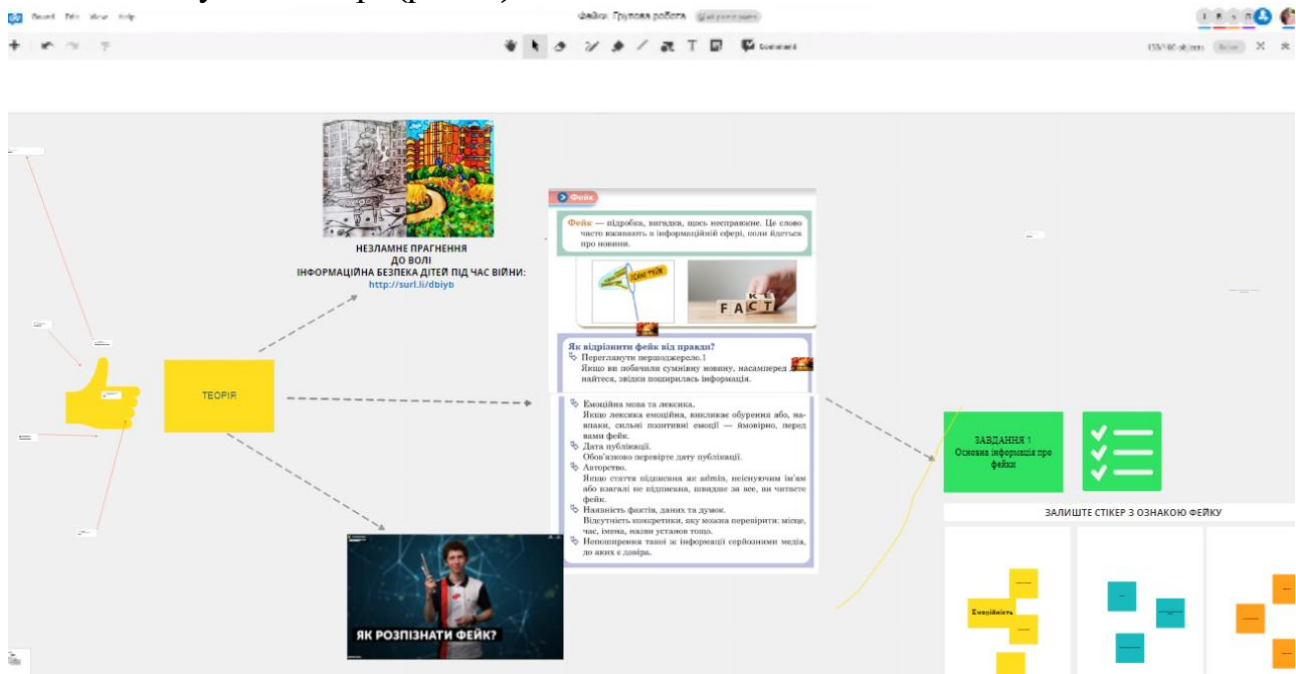


Рис. 4. Скриншот фрагменту віртуальної дошки Canva, яку було створено та використано під час онлайнкової взаємодії автора зі здобувачами освіти на занятті з теми «Безпека в Інтернеті: що потрібно знати учасникам освітнього процесу»

Аналогічні і, водночас, необмежені можливості з організації синхронної взаємодії на віртуальній дошці надає безкоштовна (за умови вибору під час реєстрації позиції «Canva для навчання») платформа графічного дизайну Canva https://www.canva.com/uk_ua/. Він пропонує великий банк зображень, анімацій, шрифтів, шаблонів, ілюстрацій та аудіо. За допомогою нього можна спільно в команді працювати у віртуальній дошці (рис. 5), а також створювати електронну газету, презентацію, слайд-шоу, відео, мапу думок, мозковий штурм, комікс, інфографіку, інтерактивний плакат, дидактичні картки, аркуші завдань та інший візуальний навчальний контент. Доступна як вебверсія, так і мобільна.



Рис. 5. Скриншот фрагменту віртуальної дошки Canva, яку автором було створено для здобувачів освіти та наповнено інформацією щодо інтернет-загроз

Jamboard <https://jamboard.google.com/> – це віртуальна інтерактивна дошка від Google з дуже зручним, простим інтерфейсом та можливістю наповнювати до 20 сторінок дошки невеликої площі різноманітним контентом (рис. 6). Призначена для мозкових штурмів, співпраці в синхронному чи асинхронному режимах. Має відповідний мобільний застосунок.



Рис. 6. Скриншот фрагменту віртуальної дошки Jamboard, яку було створено та використано для аналізу ситуативних кейсів під час онлайн-взаємодії автора зі здобувачами освіти на занятті з теми «Інформаційна безпека дітей під час війни»



Linoit <https://en.linoit.com> – умовно безкоштовний вебсервіс з інтуїтивним дуже простим інтерфейсом. Він надає можливість в синхронному чи в асинхронному режимах спільно створювати віртуальні дошки досить великої площі для розміщення та взаємобміну інформації різного формату: наліпки з текстом, зображення, відео, файли (рис. 7). Перейшовши за [покликанням](#) та QR-кодом, можна ознайомитись з авторським скринкастом щодо її створення.

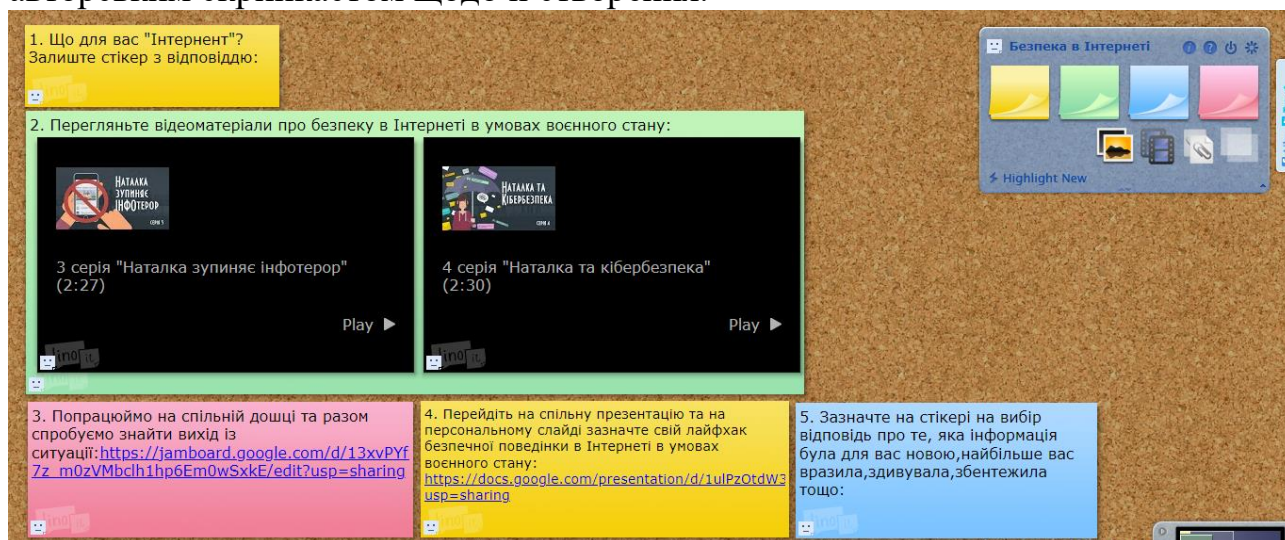


Рис. 7. Скриншот фрагменту віртуальної дошки linoit, яку було створено автором для онлайнової взаємодії зі здобувачами освіти на занятті з теми «Інформаційна безпека дітей під час війни»

На віртуальній дошці (як це продемонстровано на рис. 7) можуть бути закріплені стікери з покликанням на Google Docs <https://docs.google.com/document> чи Google Slides <https://docs.google.com/presentation> – безкоштовні онлайнві програми (застосунки), завдяки яким учасники взаємодії можуть спільно працювати над наповненням документу чи слайдів онлайнової презентації інформацією різного формату (рис. 8).

Де, кому і яку персональну інформацію я можу поширювати
(Поставте знак "+" чи "-" у кожну комірку)

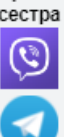
Твоя персональна інформація	Сторінка в соц.мережі 	Сторінка в соц.мережі 	Сторінка в соц.мережі 	Авторський YouTube-канал 	Батьки 	Брат/сестра 	Реальний друг,коханий  	Друг онлайн  	Твій варіант
Ім'я									
Прізвище									
Дата народження									
Номер телефону									
Адреса електронної скриньки									
Адреса проживання									
Геолокація									
Місце навчання									
Логіни й паролі від облікових записів, пристроїв									
Селфі в білизні									
Хобі, смаки, інтереси, вподобання									
Фото, де ти в гарній сукні, костюмі тощо									
Фото, де ти в купальнику									
Селфі в білизні									
Селфі без білизни									
Фото/відео на фоні твого помешкання									
Фото/відео на фоні твоєї школи									
Фото/відео в місцях, де ти любиш часто бувати									
Відео в реальному часі, де ти зараз перебуваєш									
Фото/відео з товаришем (коханим, братом, батьком...) військовим									
Фото біля об'єктів військового значення									

Рис. 8. Скриншот фрагменту Google документа, створеного автором для онлайнної взаємодії зі здобувачами освіти на занятті з теми «Інформаційна безпека дітей під час війни»

Наступний цифровий інструмент, який сприяє інтерактивній взаємодії під час онлайнного обговорення проблеми безпечного Інтернету – Mentimeter <https://www.mentimeter.com/>. Це умовно безкоштовний онлайнний сервіс, який в умовах тренінгового навчання дозволяє створити безліч інтерактивних презентацій з контентом (текст, зображення, відео) та вбудованими опитувальниками різних типів. Серед них: відкриті запитання, запитання з варіантами відповідей, анонімні запитання від аудиторії, лінійна шкала, сітка, мітки на мапі, гістограма, вікторина, правда чи брехня, визначення рейтингу,

визначення переможця, запитання зі словом-асоціацією для створення спільної тематичної хмаринки слів тощо. Презентацію з вбудованими опитувальниками можна використовувати як синхронно під час відеозустрічі, так і асинхронно, надавши учням доступ до неї за допомогою покликання чи QR-коду (рис. 9).



Чи потрапляли ви коли-небудь до пасток Інтернет-загроз?



Що означає для Вас поняття "безпечний Інтернет". Зазначте 3 слова-асоціації



Рис. 9. Скриншоти результатів опитування здобувачів освіти за авторським опитувальником з проблеми безпечного Інтернету, створеним в сервісі Mentimeter

Нижче наведено приклад авторського інтерактивного опитувальника, створеного в сервісі Mentimeter, а також покликання та QR-код на авторські скринкасти з алгоритму його створення.



[Приклад авторського інтерактивного опитувальника в Mentimeter](#)



[Світлана Єфіменко. Створюємо спільну хмаринку слів в #mentimeter](#)

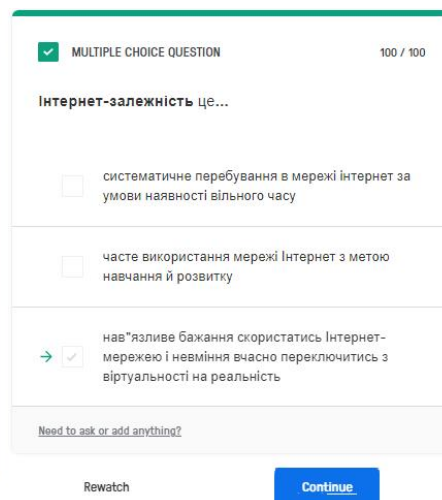


[Світлана Єфіменко. Створюємо інтерактивний опитувальник в #mentimeter](#)



З метою ефективного формування знань здобувачів освіти з проблеми інтернет-безпеки, пропонуємо використовувати готові відео або ж створювати власні відеоролики й розміщувати їх на каналі закладу освіти чи персональному каналі педагога в безкоштовному відеохостингу YouTube <https://www.youtube.com/>. За покликанням та QR-кодом наведено приклад авторського відео з проблеми інтернет-загроз, розміщеного на персональному YouTube-каналі автора: [«Засоби «цифрової дієти» як інструменти профілактики Інтернет-залежності»](#).

Edpuzzle <https://edpuzzle.com/> – безкоштовний онлайн-сервіс, що дає змогу створити інтерактивні відеоматеріали на основі звичайних відеороликів з YouTube. Інтерактивність забезпечується завдяки вбудованим у відео запитанням, відповівши на які, глядач може переглядати відеоролик далі (рис 10). Запитання можна формулювати як закритого, так і відкритого типу. Автор інтерактивного відеоматеріалу (педагог) має змогу переглянути результати опитування.



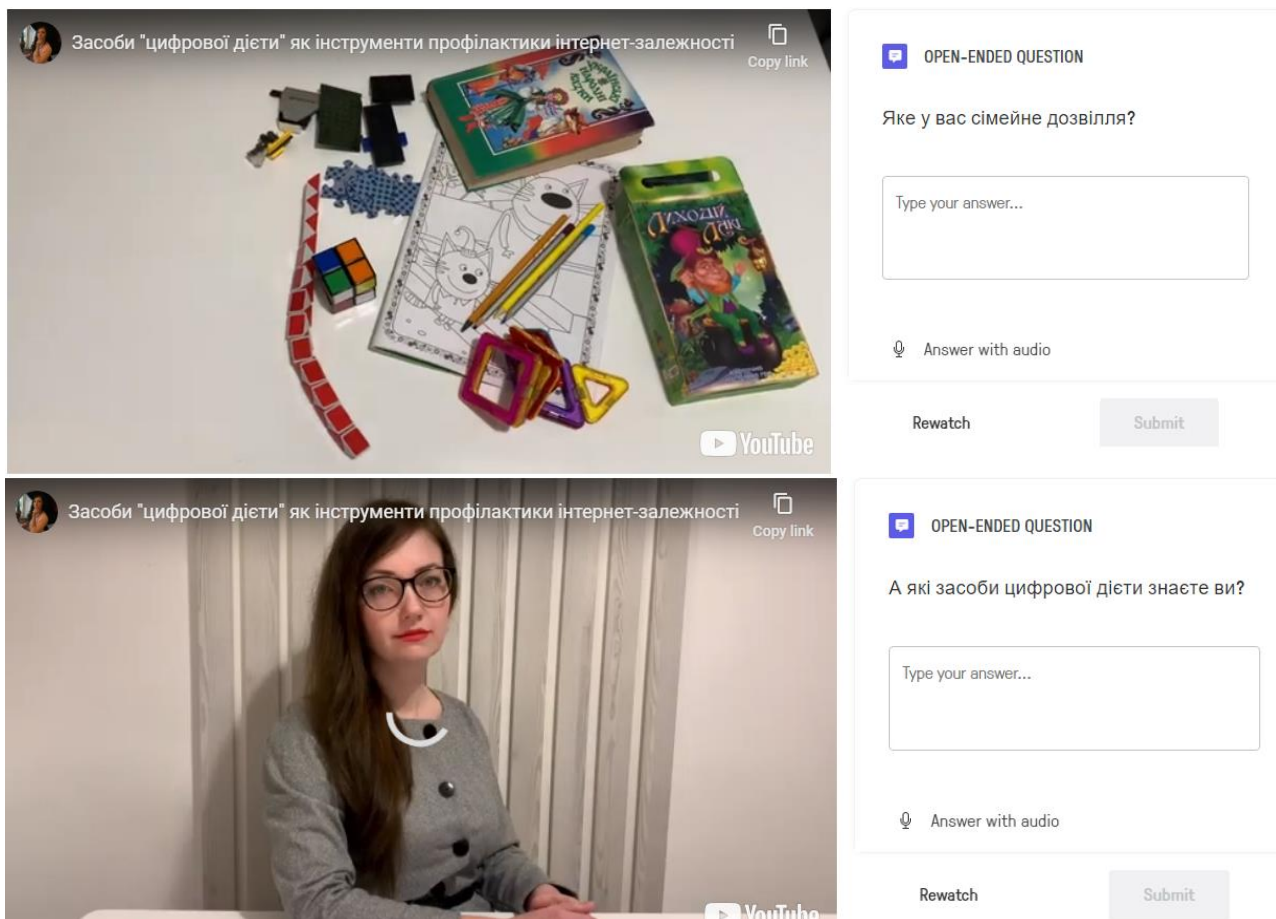


Рис. 10. Скриншоти фрагментів авторського інтерактивного відеоматеріалу з проблеми інтернет-безпеки, створеного в сервісі Edpuzzle

Нижче наведено приклад авторського інтерактивного відеоматеріалу, створеного в сервісі Edpuzzle, а також покликання та QR-код на авторський скринкаст з алгоритму його створення.



[Авторське інтерактивне відео, створене в сервісі Edpuzzle](#)



[Світлана Єфіменко. Створення інтерактивного відео в сервісі #edpuzzle](#)

Цікавим та практично орієнтованим завданням для учнів може слугувати освітній відеочелендж в соціальній мережі ТікТок. Його суть – зняти власне відео у Тік Тоці, наприклад, з авторським лайфхаком безпечного інтернет-користування. Приклади пізнавальних відео з цієї тематики розміщено на сторінці проекту stopsexting.ua у Тік Тоці.

За допомогою умовно безкоштовного багатофункціонального онлайнового сервісу Genially <https://app.genial.ly/> можна створювати різноманітні інтерактивні цифрові освітні ресурси для занять та заходів з інтернет-безпеки: презентації,

інфографіку, вебквести, ігри, віртуальні посібники тощо. Сервіс містить дуже велику кількість шаблонів. Він надає можливість працювати над розробкою у команді, а також використовувати готові ресурси з можливістю їх редагування. Безкоштовний план передбачає поширення ресурсів за допомогою покликання, а платний – ще й завантажувати роботу в PDF-форматі.

Зауважимо, що створюючи вебквест, важливо формулювати запитання закритого типу проблемного спрямування. Запитання можуть бути типу так/ні чи правда/вигадка (рис. 11).

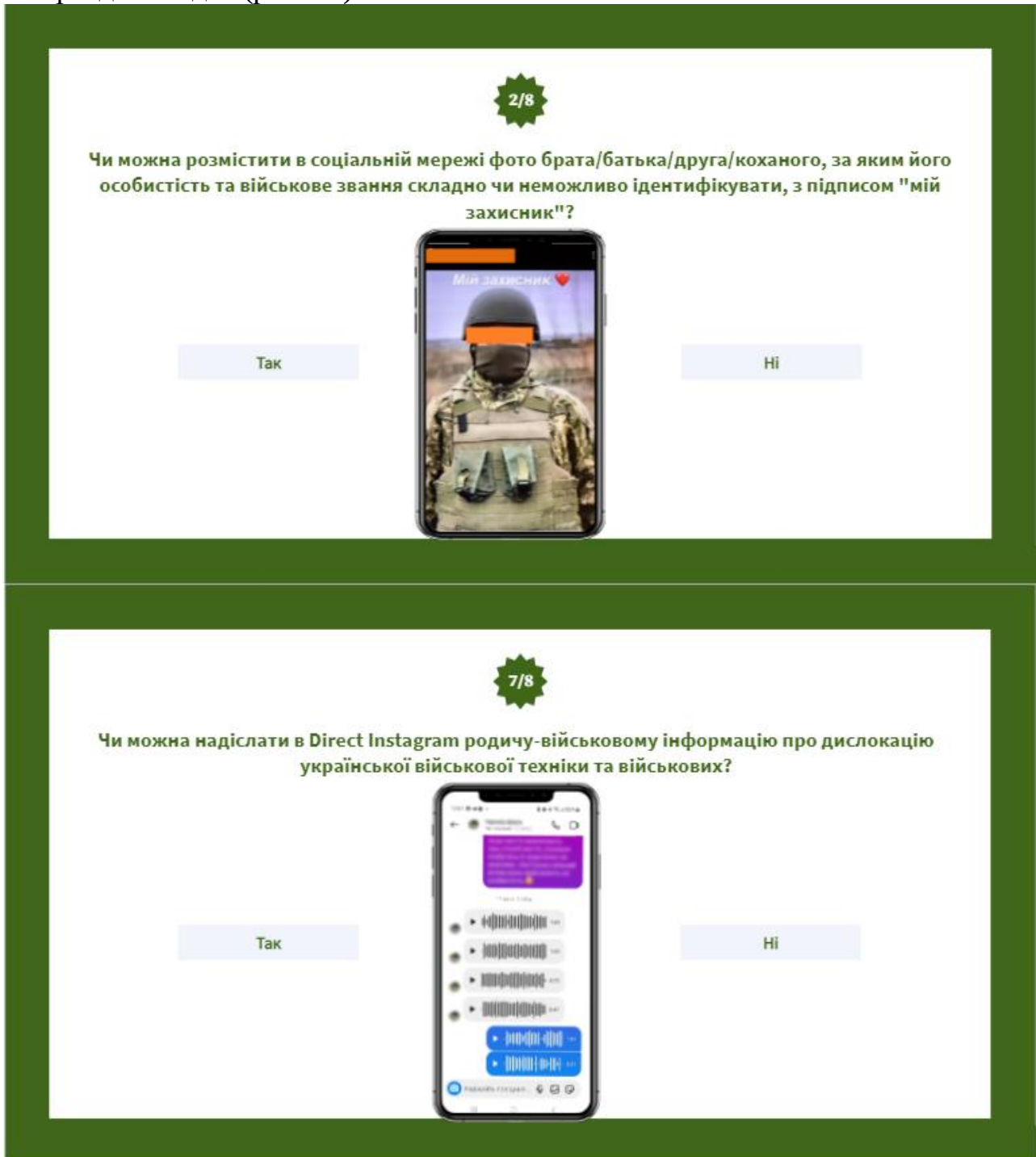
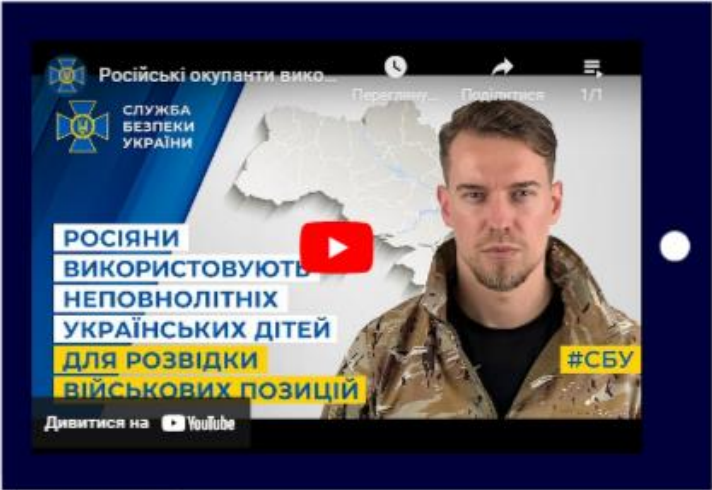


Рис. 11. Фрагменти авторського вебквесту «Безпека в Інтернеті в умовах воєнного стану», розробленого за допомогою сервісу Genially, що містять запитання типу так/ні

Запитання вебквесту також можуть містити більш розгорнуті відповіді (але закритого типу), працюючи з якими учень не лише здійснює рефлексію своїх компетентностей з безпечної поведінки в Інтернеті, а й активізує власне критичне мислення, дізнається нове з цієї теми (рис. 12). Використовувати вебквести доречно як в синхронному, так і в асинхронному режимах з обов'язковим подальшим обговоренням його змісту.

1/5

Переглянь відеоматеріал та дай відповідь на запитання. З якого віку настає відповідальність за кримінальні правопорушення, вчинені в рамках взаємодії з російськими військовими?



18 років

16 років

14 років

5/5

Яке з наведених нижче запитань, що ти можеш задавати собі, сприймаючи будь-яку інформацію в Інтернеті, НЕ Є ефективним у твоїх спробах з'ясувати, фейк це чи правда?



Хто поширює цю інформацію?	Навіщо поширюють цю інформацію?
Чи є в коментарях підтвердження правдивості цієї інформації іншими користувачами Інтернет-мережі?	Чи не надто привабливий, емоційний заголовок?
Чи мовиться про це на офіційних сторінках?	Чи є протиріччя в змісті інформації?

Рис. 12. Фрагменти авторського вебквесту «Безпека в Інтернеті в умовах воєнного стану», розробленого за допомогою сервісу Genially, що містять розгорнуті відповіді

Наведемо приклад авторських дидактичних ігор, розроблених в сервісі Genially. Ігри «Знайди пару» (рис. 13) та «Визнач відповідність» (рис. 14), сприяють формуванню знань здобувачів освіти з сутності понять «інтернет-загроза», «інтернет-залежність», «інтернет-шахрайство», «фішинг», «кібербулінг», «кібергрумінг», «секстинг», «сексторшен», «небезпечний

контент», «фейк», «кіберніоманія». Завдання першої гри передбачає визначення відповідності між терміном та визначенням інтернет-загроз, другої – між назвою та візуальним відображенням інтернет-загроз, з подальшим колективним обговоренням дій неповнолітніх інтернет-користувачів, які можуть призвести до виникнення зазначених у грі інтернет-загроз.

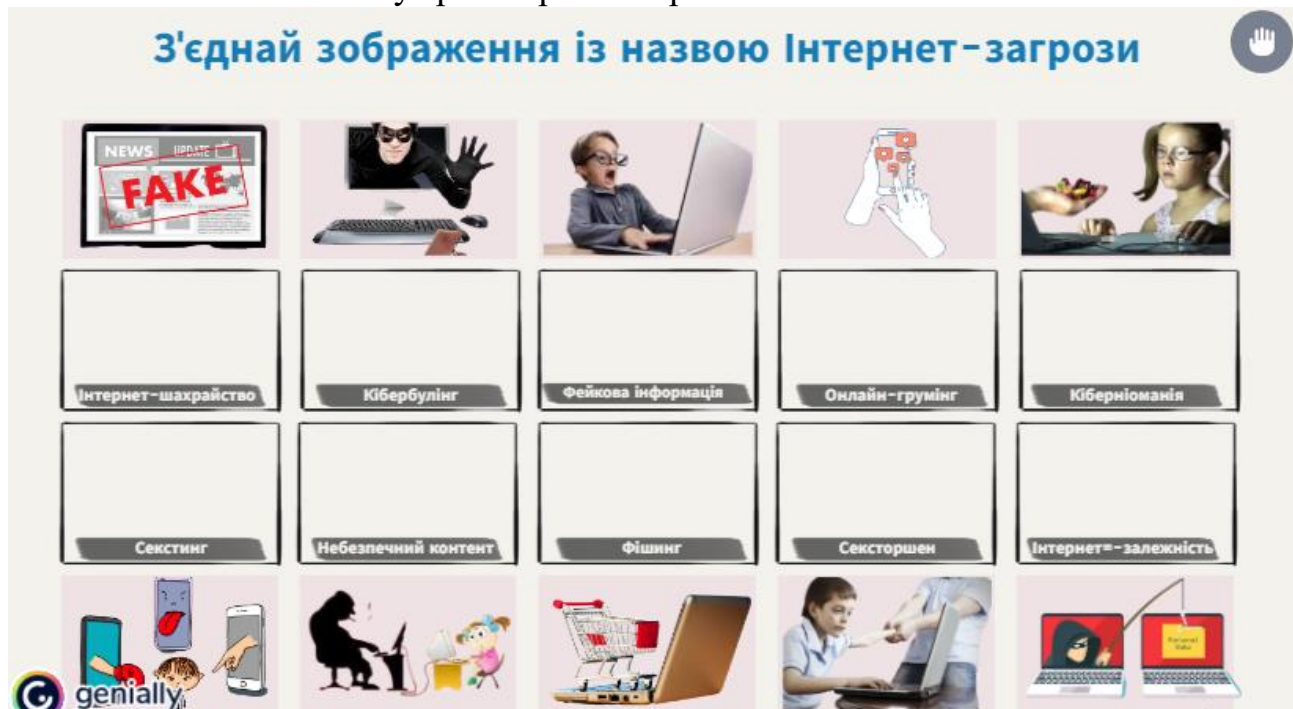


Рис. 13. Скриншот авторської гри «Знайди пару», розробленої за допомогою сервісу Genially



Рис. 14. Скриншот авторської гри «Визнач відповідність», розробленої за допомогою сервісу Genially

Нижче наведено покликання та QR-коди на авторські ігри та вебквест з проблеми інтернет-безпеки, створені у сервісі Genially та авторські скринкасти з алгоритму їх створення.



[Авторський вебквест
«Безпека в Інтернеті в
умовах воєнного стану»](#)



[Авторська гра «Знайди
пару»](#)



[Авторська гра «Визнач
відповідність»](#)



[Світлана Єфіменко.
Створюємо Web-квест у
#genially](#)



[Світлана Єфіменко.
Створюємо гру «Визнач
відповідність» в Genially](#)



[Світлана Єфіменко.
Створюємо гру «З'єднай
термін з його визначенням» в
онлайнному сервісі Genially](#)

Умовно безкоштовний онлайнний сервіс Wordwall <https://wordwall.net> дозволяє використовувати готові ресурси до занять з можливістю їх редагування, а також розробляти інтерактивні ігри різних типів. А саме: відповідники, сортування за групами, погоня в лабіринті, відповідні пари, вікторина, випадкове колесо, анаграма, діаграма з мітками, наведіть порядок, правильно, неправильно тощо. У платній підписці сервісу ще є можливість завантаження ігор у PDF-форматі. Розроблені в означеному сервісі ігри можуть стати невід'ємною складовою тренінгу чи іншого заняття з інтернет-безпеки.



Так, [гра «Розмісти у відповідні комірки Інтернет-загрози»](#) (рис. 15) сприяє формуванню знань здобувачів освіти з сутності понять «інтернет-загроза», «інтернет-залежність», «інтернет-шахрайство», «відеоігрова залежність», «кібербулінг», «секстинг», «сексторшен», «кібергрумінг», «небезпечний контент», «фейкова інформація», «кіберніоманія». Використовуючи означену гру в рамках заняття з інтернет-безпеки, доцільно запропонувати дітям обговорити колективно, які наслідки для інтернет-користувачів несуть ці загрози.

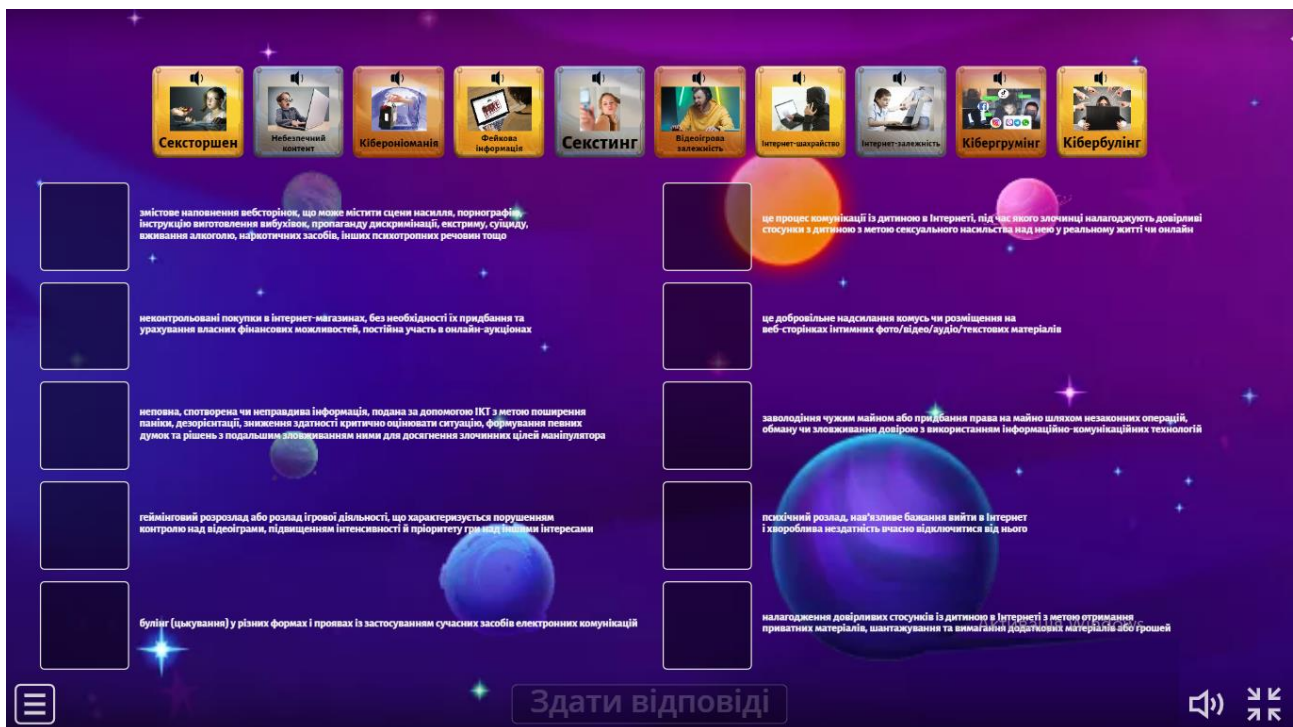


Рис. 15. Скриншот авторської гри «Розмісти у відповідні комірки Інтернет-загрози», розробленої за допомогою сервісу Wordwall



Гра з інтернет-безпеки «Правильно, неправильно» спрямована на формування знань здобувачів освіти з ознак «кібербулінгу» та механізмів захисту від нього. Завдання гри передбачають визначення правдивих та хибних тверджень щодо сутності та механізмів захисту від кібербулінгу з подальшим колективним узагальненням інформації, отриманої у грі (рис. 16).

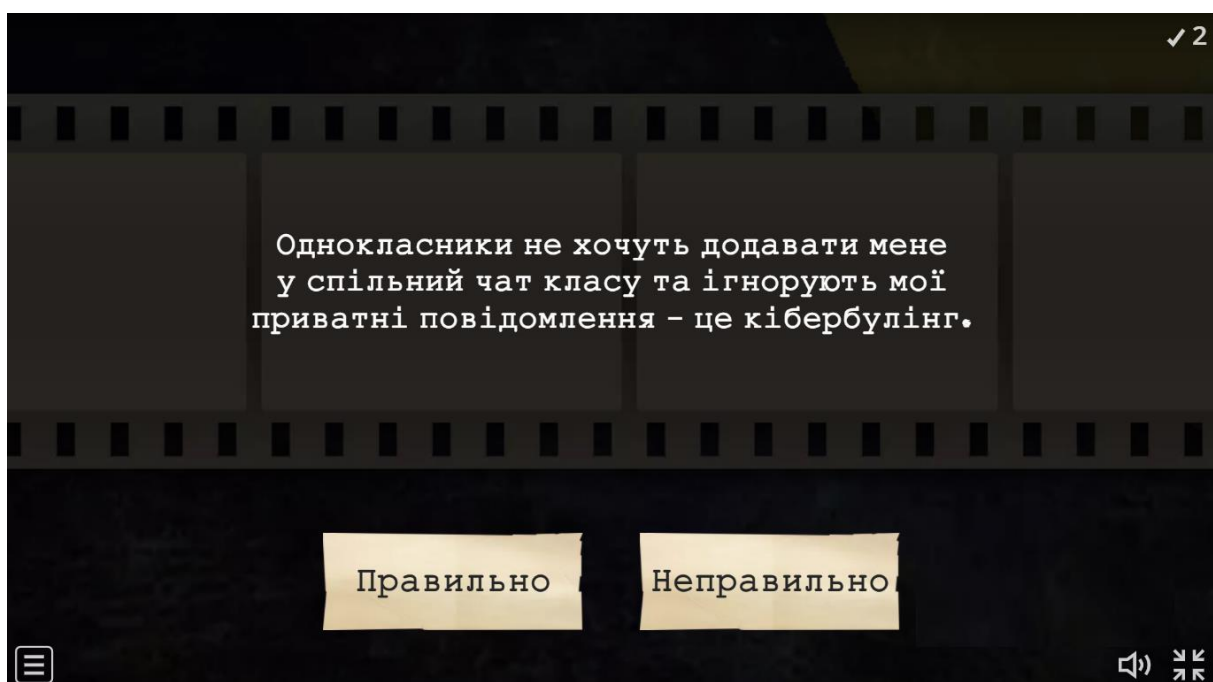


Рис. 16. Скриншот фрагменту авторської гри «Правильно, неправильно», розробленої за допомогою сервісу Wordwall



[Гра з інтернет-безпеки «Як діяти у випадку...»](#), на відмінну від попередніх ігор, використовується виключно під час очної чи синхронної зустрічі зі здобувачами освіти в форматі фронтальної роботи. Сенс гри полягає в тому, що педагог, натискаючи на кнопку «крутити», запускає колесо з секторами, а учень/мікрогрупа учнів чекають на своє запитання сектору, що зупиниться біля стрілки. Гра спрямована на розвиток критичного мислення й здатності

школярів в команді генерувати ідеї щодо ознак інтернет-загроз та шляхів виходу з проблемної ситуації в Інтернеті (рис. 17).



Рис. 17. Скриншот фрагменту авторської гри «Як діяти у випадку...», розробленої за допомогою сервісу Wordwall

Перейшовши за покликаннями чи QR-кодами, пропонуємо переглянути авторські скринкасти з алгоритму створення таких ігор.



[Світлана Єфіменко. Реєстрація та створення гри «Розмісти у відповідні комірки» за шаблоном «ВІДПОВІДНИКИ»](#)



[Світлана Єфіменко. Створюємо гру «Правильно, неправильно»](#)



[Світлана Єфіменко. Створюємо гру за шаблоном «Випадкове колесо» у #wordwall](#)

Онлайнний інструмент Rebus1 <http://rebus1.com/ua/> – безкоштовний сервіс з генерації класичних (вербальних) ребусів різними мовами, а також математичних (числових) ребусів. Сервіс дозволяє створити власний ребус та завантажити його на пристрій, а також використати готові ребуси з будь-якої тематики та для будь-якої вікової категорії учнів. Для генерації та розшифровування ребусів сервіс містить всі необхідні інструкції.

Авторські ребуси «Інтернет-загрози» (рис. 18), розроблені в означеному сервісі, сприяють формуванню знань здобувачів освіти з сутності понять «інтернет-загроза», «інтернет-залежність», «інтернет-шахрайство», «фішинг», «кібербулінг», «секстинг», «сексторшен», «кібергрумінг», «небезпечний контент», «небезпечне спілкування онлайн», «фейк», «кіберніоманія». Використовуючи ребуси на занятті/заході з інтернет-безпеки, доцільно запропонувати школярам довідатись про те, які інтернет-загрози поширені на сьогодні, розгадавши ребус, та обговорити колективно, чим небезпечні ці інтернет-загрози та чи потрапляли учні/їх знайомі у «пастку» тієї чи іншої інтернет-загрози, представлені у ребусі.



Рис. 18. Фрагмент завдання з ребусами, згенерованими автором у сервісі Rebus1



[Авторські ребуси «Інтернет-загрози»](#)



[Світлана Єфіменко. Генеруємо ребуси за допомогою сайту Rebus1](#)

Jigsawplanet <https://www.jigsawplanet.com> – безкоштовний ресурс для створення власних або використання готових пазлів, розроблених іншими користувачами. Онлайнві пазли можуть бути елементом заняття/заходу з інтернет-безпеки. Наприклад, авторська гра «Склади пазли», спрямована на формування знань здобувачів освіти з сутності різних видів інтернет-загроз, передбачає об'єднання здобувачів освіти у мікрогрупи. Завдання мікрогруп: скласти пазл та здогадатись, яку інтернет-загрозу він відображає, визначити її сутність, скласти банк ідей в межах мікрогрупи щодо правил безпечної поведінки в Інтернеті, дотримання яких допоможе не потрапити в халепу – «пастку» тієї чи іншої інтернет-загрози, відображеної на пазлі, обговорити колективно алгоритм дій та механізми захисту в ситуації, коли все ж втрапили в халепу конкретної інтернет-загрози (рис. 19).

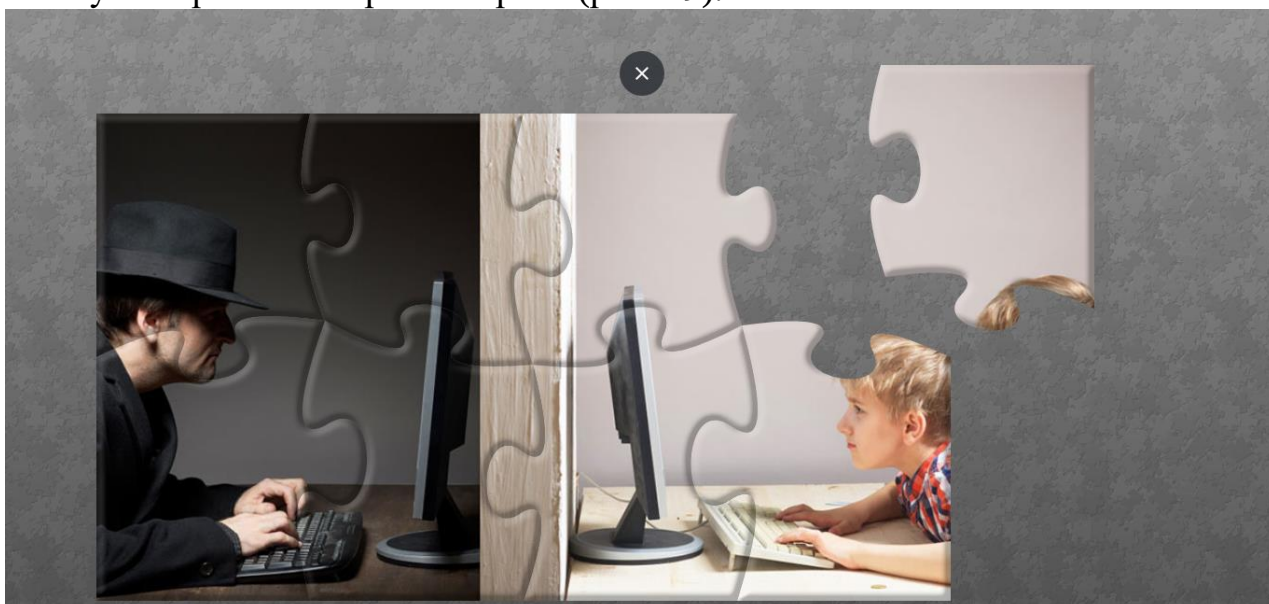


Рис. 19. Фрагмент авторської гри «Склади пазли», розробленої за допомогою ресурсу Jigsawplanet

Нижче наведено QR-коди на авторські пазли з проблеми безпеки в Інтернеті, розроблені в означеному сервісі для гри «Склади пазли».



[Пазл «Небезпечне спілкування онлайн»](#)



[Пазл «Кібербулінг»](#)



[Пазл «Небезпечний контент»](#)



[Пазл «Інтернет-шахрайство»](#)



[Пазл «Інтернет-залежність»](#)



[Пазл «Фейкова інформація»](#)



Перейшовши за [покликанням](#) та QR-кодом, можна ознайомитись з авторським скринкастом щодо створення пазлів за допомогою ресурсу Jigsawplanet.

«Розвиток дитини» <https://childdevelop.com.ua> – умовно безкоштовний сайт з генерації завдань та використання готових ресурсів до занять. Сайт містить розробки вправ з теми безпечного інтернет-користування (Розвиток дитини /Практичні завдання/Загальні компетенції/безпека), а також дозволяє згенерувати й завантажити на пристрій необмежену кількість власних вправ. Наведемо приклад авторських вправ, згенерованих в означеному сервісі.



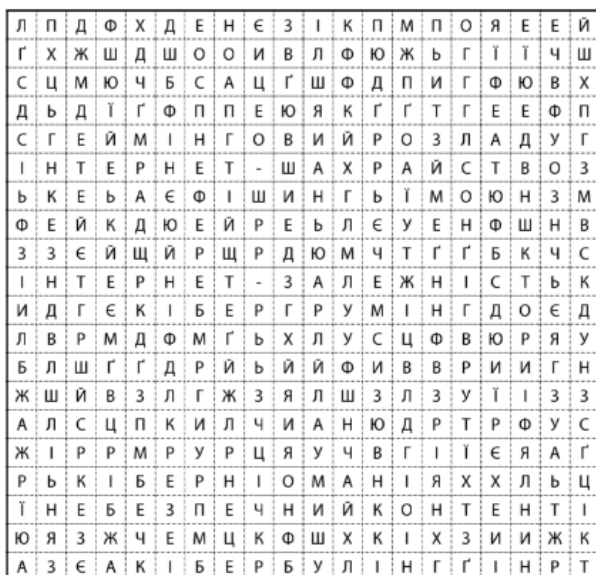
[Гра 1 «Знайди слова»](#) (рис. 20) спрямована на формування знань здобувачів освіти з сутності понять: «геймінговий розлад», «інтернет-шахрайство», «фішинг», «фейк», «інтернет-залежність», «кібергрумінг», «кіберніоманія», «кібербулінг», «небезпечний контент». Завдання гравців: з набору літер знайти слова – назви інтернет-загроз та пояснити їх сутність.



[Гра 2 «Знайди слова»](#) (рис. 20) спрямована на формування знань здобувачів освіти з сутності понять: «інформація», «геолокація», «контент», «конфіденційність», «спілкування», «мережевий етикет», «приватність», «цифровий детокс», «фото», «відео», «пост», «репост», які є ключовими серед правил безпечної поведінки в Інтернеті, зокрема в умовах воєнного стану. Завдання гравців: з набору літер знайти слова, які допоможуть пригадати правила безпечного інтернет-користування в умовах воєнного стану.

ЗНАЙДИ СЛОВА

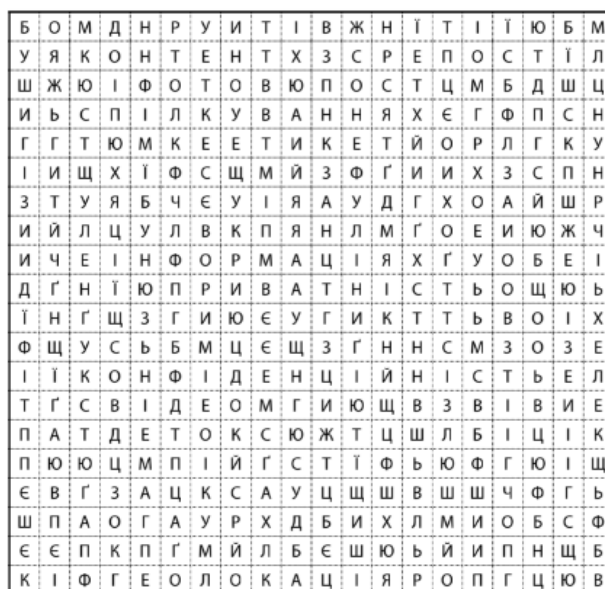
Знайди і обведи 9 слів головоломки.



СПИСОК СЛІВ: ГЕЙМІНГОВИЙ РОЗЛАД • ІНТЕРНЕТ-ЗАЛЕЖНІСТЬ • ІНТЕРНЕТ-ШАХРАЙСТВО • КІБЕРБУЛІНГ • КІБЕРГРУМІНГ • КІБЕРНІОМАНІЯ • НЕБЕЗПЕЧНИЙ КОНТЕНТ • ФЕЙК • ФІШІНГ (9)

ЗНАЙДИ СЛОВА

Знайди і обведи 12 слів головоломки.



СПИСОК СЛІВ: ІНФОРМАЦІЯ • ГЕОЛОКАЦІЯ • КОНТЕНТ • КОНФІДЕНЦІЙНІСТЬ • СПІЛКУВАННЯ • ЕТИКЕТ • ПРИВАТНІСТЬ • ДЕТОКС • ФОТО • ВІДЕО • ПОСТ • РЕПОСТ (12)

Рис. 20. Скриншоти авторських ігор «Знайди слова», розроблених за допомогою сайту «Розвиток дитини»



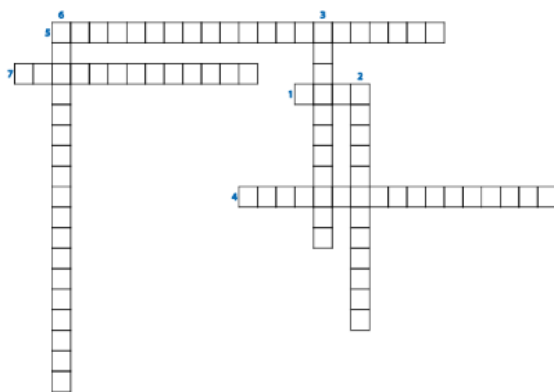
[Гра «Знайди види фейків»](#) (рис. 21) спрямована на формування знань здобувачів освіти з сутності поняття «фейк» та видів фейків: «пропаганда», «неохайна журналістика», «упереджені новини», «сатира», «видозмінений контент», «теорії змов», «чутки», «клікбейт». Завдання гравців: з набору літер знайти слова – назви різних видів фейкової інформації, обговорити сутність кожного з них та навести приклади в власного досвіду чи досвіду знайомих/друзів/родичів.



[Гра «Кросворд»](#) (рис. 21) спрямована на формування знань здобувачів освіти з сутності понять «небезпечне спілкування», «небезпечний контент», «кіберніоманія», «кібербулінг», «фейкова інформація», «геймінговий розлад», «кібергрумінг». Завдання гравців: розгадати кросворд, пояснити сутність та механізми захисту від інтернет-загроз, представлених у грі.

КРОСВОРД

Розгадай кросворд.

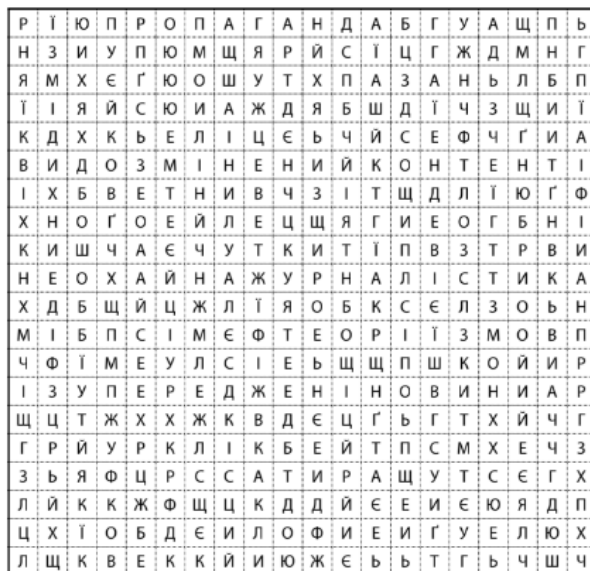


По горизонталі: 1. Неконтрольовані покупки в інтернет-магазинах, без необхідності їх придбання та урахування власних фінансових можливостей, постійна участь в онлайн-аукціонах. 4. Психічний розлад ігрової діяльності, що характеризується відокремленою залежністю, порушенням контролю над відокремленою діяльністю, підвищенням пріоритету гри над іншими інтересами та повсякденною діяльністю, а також продовженням грати та посилення його інтенсивності, незважаючи на виникнення негативних наслідків. 5. Змістове наповнення вебсторінок, що може заподіяти шкоду психічному, соціальному, фізичному чи матеріальному благополуччю користувача Інтернет-мережі. 7. Булінг (цькування) у різних формах і проявах із застосуванням сучасних засобів електронних комунікацій.

По вертикалі: 2. Заволодіння чужим майном або придбання права на майно шляхом незаконних операцій, обману чи зловживання довірою з використанням інформаційно-комунікаційних технологій. 3. Психічний розлад, наслідком якого є вихід в Інтернет і хвороблива нездатність вчасно відключитися від нього. Це явище може спричинити стан, у якому людина фокусуватиметься на віртуальному, а не реальному світі. 6. Процес комунікації із дитиною в Інтернеті, під час якого злочинці налагоджують довірливі стосунки з дитиною з метою сексуального насильства над нею у реальному житті чи онлайн.

ЗНАЙДИ ВИДИ ФЕЙКІВ

Знайди і обведи 8 слів головоломки.



СПИСОК СЛІВ: ПРОПАГАНДА • НЕОХАЙНАЖУРНАЛІСТИКА • УПЕРЕДЖЕНІНОВИНИ • САТИРА • ВИДОЗМІНЕНИЙКОНТЕНТ • ТЕОРІЗМОВ • ЧУТКИ • КЛІКБЕЙТ (8)

Рис. 21. Скриншоти авторських ігор «Кросворд» та «Знайди види фейків», розроблених за допомогою сайту «Розвиток дитини»



Гра «Анаграма» (рис. 22) спрямована на формування знань здобувачів освіти з сутності інструментів захисту в мережі Інтернет: «антивірус», «контент-фільтр», «аутентифікація», «приватність». Завдання гравців: з набору літер скласти слова, які означають інструменти захисту в мережі Інтернет, та пояснити сутність цих інструментів.



Учень: _____

Анаграма — безладна перестановка букв у слові, що створює інше слово. Розгадайте анаграми та запишіть відповіді у спеціально відведеному місці.

Анаграма

Анаграми

1. ТНАСРІИУВ
2. ІТНКНТ-ТРЬЛЕОФ
3. СТПНІРТВАИЙ
4. ТФІАЯКНИІТУАЦЕ

Відповіді

Рис. 22. Скриншот авторської гри «Анаграма», розробленої за допомогою сайту «Розвиток дитини»



Перейшовши за [покликанням](#) та QR-кодом, можна ознайомитись з авторським скринкастом щодо створення ігор за допомогою сайту «Розвиток дитини».

Продемонстровані авторські ігри, вправи та завдання не лише спрямовані на формування знань здобувачів освіти з сутності понять, які охоплює проблема безпечної поведінки в Інтернеті, а й сприяють формуванню вмінь учнів аналізувати, висловлювати власні думки й пропозиції в процесі генерації банку ідей щодо сутності інтернет-загроз та шляхів виходу з проблемних ситуацій, пов'язаних з інтернет-загрозами; формуванню вмінь працювати в команді, мислити творчо, критично, конструктивно; формуванню ціннісного ставлення до медіаграмотності, власного здоров'я (фізичного, психічного, соціального благополуччя), матеріального благополуччя та до безпечної поведінки в Інтернеті.

Виокремимо **організаційно-педагогічні умови** формування в учнів закладу загальної середньої освіти навичок безпечної поведінки в Інтернеті.

1. Забезпечення умов (організаційних, технічних) для безпечного використання мережі Інтернет.

2. Планування та реалізація в закладі загальної середньої освіти діяльності щодо запобігання й протидії будь-яким проявам дискримінації, булінгу, іншому насильству згідно з чинним законодавством.

3. Активна співпраця закладу освіти з представниками соціально-психологічних служб, соціальних служб, служб у справах дітей, правоохоронних органів, громадських організацій у веденні антибулінгової політики та організації заходів/занять з проблеми безпечної поведінки в Інтернеті.

4. Активна співпраця педагогів закладу освіти зі здобувачами освіти та їх батьками щодо організації заходів та занять з проблеми безпечної поведінки в Інтернеті, а також щодо забезпечення в родині безпечних умов інтернет-користування.

5. Систематична організація учасниками освітнього процесу заходів та занять з тематики безпечного інтернет-користування (наприклад, приурочених до видатних подій/дат).

6. Надання переваги практико зорієнтованим освітнім заходам з проблеми безпечної поведінки в Інтернеті (навчальні тренінги, воркшопи, дискусії, бесіди з використанням ситуативних кейсів, квести, ділові ігри, челенджі, проєктна діяльність, ігри-інсценізації та інші активні й інтерактивні методи й форми навчальної взаємодії учасників освітнього процесу), які, дійсно, сприяють відпрацюванню навичок безпечної поведінки в Інтернеті.

7. Наскрізне вивчення теми безпечної поведінки в Інтернеті, як складової інформаційно-комунікаційної компетентності, в усіх навчальних предметах та інтегрованих курсах освітньої програми закладу. Зокрема, використання бесід чи нагадувань (наприклад, щодо правил) з проблеми безпечного інтернет-користування як невід'ємного елементу кожного уроку/заняття зі школярами, якщо в його рамках передбачено використання цифрових технологій.

8. Спільна розробка й оприлюднення учасниками освітнього процесу правил користування мережею Інтернет. Ці правила можуть мати загальний характер або ж бути диференційованими, наприклад, за віковими категоріями учнів.

Під час організації заходів та занять з проблеми інтернет-безпеки в умовах очного, дистанційного чи змішаного навчання, пропонуємо скористатись наступними рекомендаціями:

- обирати спосіб формування знань та вмінь безпечного інтернет-користування відповідно до вікової категорії учнів (початкова ланка освіти – переважно ігрові методи, прослуховування аудіоказок, перегляд мультфільмів, бесіди, інсценізації тощо; середня й старша ланка – обговорення ситуативних кейсів, перегляд соціальних відеороликів, проєктна діяльність, челенджі, самостійне налаштування приватності й параметрів конфіденційності на своїх пристроях, ділові ігри, тренінги тощо);

- обирати цифровий інструмент (спільну віртуальну дошку, спільний Google документ/презентацію, опитувальник, онлайн-гру, інтерактивне відео, вебквест тощо) відповідно до поставлених цілей та завдань заняття/заходу, технічного забезпечення усіх учасників освітньої взаємодії, вікової категорії здобувачів освіти та їх цифрових навичок;

- використовувати як індивідуальні завдання, так і завдання для роботи в мікрогрупах, які надають можливість отримати зворотний зв'язок чи презентувати результат роботи (під час онлайн-взаємодії – інтерактивні відео, спільні документи й презентації, інтерактивні ігри й вебквести, віртуальні дошки, тематичні сторінки тощо);

- у групових очних, синхронних чи асинхронних завданнях чітко визначати кінцевий результат спільної діяльності та внесок кожного учасника взаємодії;

- застосовувати анонімні опитувальники на початку, впродовж чи по завершенню заняття/заходу для уточнення питань, що залишились не розкритими;

- для учасників, які з технічних чи інших причин не мали змогу бути присутніми на синхронному онлайн-занятті чи заході, надати можливість попрацювати над завданнями асинхронно, а також зробити для них запис екрану відеозустрічі для самостійного опрацювання;

- активно залучати дітей та їх батьків до організації заходів/занять з проблеми безпечного Інтернет-користування, підтримувати їх творчу ініціативу.

На шляху до розбудови безпечного і здорового освітнього середовища у Новій українській школі в закладі загальної середньої освіти має відбуватись планування та реалізація діяльності щодо запобігання й протидії будь-яким

проявам дискримінації, булінгу, іншому насильству згідно з чинним законодавством, а також створюватись умови для безпечного використання мережі Інтернет, у здобувачів освіти та інших учасників освітнього процесу мають формуватись навички безпечної поведінки в Інтернеті. Учасникам освітнього процесу варто завжди пам'ятати про те, що кожен користувач Всесвітньої павутини може бути як потенційною жертвою, так і потенційним джерелом небезпек й порушення прав людини в Інтернеті. А тому, перш ніж здійснювати ту чи іншу дію за допомогою Всемережжя, варто запитати себе, чи може ця дія будь-яким чином нашкодити вам, вашим близьким чи іншим користувачам Інтернету, нашій країні в цілому? Учасники освітнього процесу мають бути обізнаними зі своїх прав в Інтернеті та не порушувати права інших. Здобувачі освіти мають бути обізнаними з питань адміністративної та кримінальної відповідальності за правопорушення в мережі Інтернет (булінг із застосуванням інформаційно-комунікаційних технологій, пособництво державі-агресору як результат онлайн-взаємодії з російськими військовими, залучення неповнолітніх до виготовлення дитячої порнографії тощо), а також знати механізми звернення про захист і допомогу в разі потрапляння до пасток інтернет-загроз. Кожен учень має знати, що якщо до нього хтось звертається з проханням надіслати чи зробити щось неприйнятне, допомоги або виконати спеціальне завдання, шантажує, вимагає, погрожує, цькує чи вчиняє інші дії, які порушують його права й загрожують здоров'ю та/або матеріальному благополуччю, важливо не керуватись вказівками інтернет-злочинця, а повідомити про ситуацію дорослим, яким дитина довіряє (батьки, педагоги, психолог та ін.). Разом з тим ми – дорослі самі маємо бути обізнані з проблеми інтернет-безпеки, щоб знати, як допомогти дитині, якщо вона потребуватиме нашої допомоги. Якщо таких дорослих у близькому оточенні дитини немає, то звертатись за допомогою слід анонімно. Але ні в якому разі не залишатись сам на сам в небезпеці! Школяру разом з дорослим (або ж анонімно в разі відсутності дорослого, якому він може довіритись) слід зробити скриншот повідомлень та звернутися за допомогою до служби підтримки чи адміністрації соціальних мереж/сайту (наприклад, для блокування небезпечної сторінки); поліції (102) чи кіберполіції (callcenter@cyberpolice.gov.ua, тел. 0 800 505 170); національної дитячої гарячої лінії «ЛІА СТРАДА УКРАЇНА» (тел. 0 800 500 225, 772 або 116 111); порталів <https://report.iwf.org.uk/ua> та <https://stop-sexting.in.ua/send/> для видалення контенту, який зображає насильство над дитиною; чат-ботів «Кіберпес» (у [Вайбер](#) та [Телеграм](#)) та «Stop Sexting Bot» (в [Телеграм](#)); урядової консультаційної лінії з питань безпеки дітей в Інтернеті (тел. 1545, далі обрати «3»). Сповістити про матеріали, що містять порнографію з участю неповнолітніх та інше змістове наповнення, що порушує законодавство країни, можна за допомогою форми на головній сторінці вебсайту <http://skarga.ua/>. За правовою допомогою діти можуть звернутись до контакт-центру надання безоплатної правової допомоги (тел. 0 800 213 103), уповноваженого президента України з прав дитини (тел. 044 255 76 75), уповноваженого Верховної Ради України з прав людини (hotline@ombudsman.gov.ua). За кваліфікованою юридичною допомогою діти та/чи батьки дітей можуть звернутись до Українсько-

Гельсінської спілки з прав людини (тел. 044 383 9519, 094 928 6519). Звернутись зі скаргою до суду діти можуть самостійно з 14 років (до виповнення 14 років – батьки чи опікуни дитини). Після використання всіх національних механізмів правового захисту дитина може отримати міжнародну правову допомогу, зокрема, в Європейському суді з прав людини та Комітеті ООН з прав дитини.

Сформованість навичок безпечної поведінки в Інтернеті школяра характеризується сприйняттям себе в Інтернеті як потенційної жертви, спостерігача чи джерела небезпеки, зорієнтованістю у міжнародному й національному законодавстві щодо прав людини в цифрову епоху та механізмів їх захисту, визнанням Всесвітньої мережі значущим чинником розвитку, самореалізації, соціалізації й водночас загрозою благополуччю людини, умінням зберігати благополуччя під час роботи з цифровими пристроями й Інтернетом. Але, завдяки скоординованій взаємодії держави, громадськості й учасників освітнього процесу з питань створення безпечного інформаційного інтернет-простору, Всесвітня мережа визначатиметься її неповнолітніми користувачами, в першу чергу, як потенційне поле можливостей для реалізації прав та потреб.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абетка для директора. Рекомендації до побудови внутрішньої системи забезпечення якості освіти у закладі загальної середньої освіти. (Бобровський М.В., Горбачов С.І., Заплотинська О.О., Ліннік О.О. Рекомендації до побудови внутрішньої системи забезпечення якості освіти у закладі загальної середньої освіти, 2-ге видання, перероб. і доп. Київ, Державна служба якості освіти, 2021, 350 с.
2. Безпека дітей в Інтернеті: попередження, освіта, взаємодія : вебсайт. URL: <https://sites.google.com/view/safer-internet-day-koippo/>.
3. Безпека дітей в Інтернеті: попередження, освіта, взаємодія : збірник матеріалів І Всеукраїнської науково-практичної конференції, м. Кропивницький, 07-10 лютого 2022 року / уклад. С.М. Єфіменко; за заг. ред. Г.В. Скрипки. Кропивницький: КЗ «КОППО імені Василя Сухомлинського», 2022. 36 с.
4. Безпека дітей в Інтернеті: попередження, освіта, взаємодія: збірник матеріалів ІІ Всеукраїнської науково-практичної конференції, м. Кропивницький, 07-10 лютого 2023 року / уклад. С. М. Єфіменко; за заг. ред. Г. В. Скрипки. Кропивницький: КЗ «КОППО імені Василя Сухомлинського», 2023. 192 с.
5. Безпека дітей в Інтернеті: попередження, освіта, взаємодія : Telegram-канал. URL: <https://t.me/bezpekaditeivinterneti>.
6. Висвітлення інформації про заклад освіти в умовах воєнного стану. Освітній омбудсмен України : вебсайт. URL: <https://eo.gov.ua/vysvitlennia-informatsii-pro-zaklad-osvity-v-umovakh-voiennoho-stanu/2022/09/20/?fbclid=IwAR1msm6tvaGxvI4qUL5ACFyP-V9G-NXOheUXcsEGFVujLMWfaVz-ZvHPeKA>.
7. Єфіменко Світлана. Профілактика порушень прав людини в Інтернеті серед учасників освітнього процесу закладу загальної середньої освіти. Актуальні питання вдосконалення судово-експертної та правоохоронної діяльності : збірник матеріалів засідання №2 постійно діючої Міжнародної науково-практичної конференції (м. Кропивницький, 24 червня 2022 р.). Кропивницький: ТОВ «Центрально-Українське видавництво», 2022. 486 с. С.151 – 156.
8. Конституція України : Закон України від 28.06.1996 р. №254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/main/254%D0%BA/96-%D0%B2%D1%80#Text> (дата звернення: 11.08.2023).
9. Кримінальний кодекс України : Закон України № 2341-ІІІ від 05.04.2001. URL : <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення: 19.09.2023).
10. Навчальний мультсеріал «Доброчесність онлайн». НАЗК НАСР : youtube-канал. URL: https://www.youtube.com/watch?v=9mmV2888_KA&list=PLQCyS3bbFoFfXe8AUzgGodw8SOMiEO2Ep.
11. 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: 11.09.2023).

12.Посібник з прав людини для Інтернет-користувачів та пояснювальний меморандум (Рекомендація CM/Rec(2014)6 Комітету міністрів країнам-членам щодо посібника з прав людини для Інтернет-користувачів – пояснювальний меморандум). Перекладено українською мовою за виданням Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users – Explanatory Memorandum. К.: Інжиніринг, 2015. 56 с.

13.Права людини та Інтернет : youtube-канал. URL: <https://www.youtube.com/channel/UCeuQLmBXJMdjLl5lUEUQDlA> (дата звернення: 16.12.2022 р.).

14.Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 року №64/2022. URL: <https://www.president.gov.ua/documents/642022-41397> (дата звернення: 11.08.2023).

15.Про затвердження Порядку проведення інституційного аудиту закладів загальної середньої освіти : Наказ Міністерства освіти і науки України від 09 січня 2019 року №17. URL: <https://zakon.rada.gov.ua/laws/show/z0250-19#Text> (дата звернення: 03.09.2023).

16.Про інформацію : Закон України №2658-XII від 02.10.1992 р. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#n128> (дата звернення: 05.09.2023).

17.Про Освіту : Закон України №2145-VIII від 05.09.2017. URL: <https://zakon.rada.gov.ua/laws/show/2145-19#Text> (дата звернення: 10.09.2023).

18.Розвиток дитини : вебсайт. URL: <https://childdevelop.com.ua/>.

19.Російські окупанти використовують неповнолітніх українських дітей для розвідки військових позицій. Служба безпеки України : youtube-канал. URL: https://www.youtube.com/watch?v=IO6Siwgco-o&ab_channel=%D0%A1%D0%BB%D1%83%D0%B6%D0%B1%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8.

20.Сімейний Кодекс України : Закон України № 2947-XIV від 10.01.2002. URL : <https://zakon.rada.gov.ua/laws/show/2947-14#Text> (дата звернення: 19.09.2023).

21.Статут (Конституція) Всесвітньої організації охорони здоров'я від 22.07.1946. URL: <https://ips.ligazakon.net/document/MU46004>.

22.Цивільний кодекс України : Закон України № 435-IV від 16.01.2003. URL: <https://zakon.rada.gov.ua/laws/show/435-15/ed20230903#Text> (дата звернення: 19.09.2023).

23.Черних О.О. Онлайн: навч.-метод. посібн. К.: ВАІТЕ, 2020. 108 с.

24. #Stop_sexting : вебсайт. URL: <https://stop-sexting.in.ua/>.

25.Canva : платформа графічного дизайну. URL: https://www.canva.com/uk_ua/.

26.Conceptboard : вебсервіс. URL: <https://conceptboard.com/>.

27.Edpuzzle : вебсервіс. URL: <https://edpuzzle.com/>.

28.Genially : вебсервіс. URL: <https://app.genial.ly/>.

29.Google Docs: Google застосунок. URL: <https://docs.google.com/document>.

- 30. Jamboard : Google застосунок. URL: <https://jamboard.google.com/>
- 31. Jigsawplanet : вебсервіс. URL: <https://www.jigsawplanet.com>.
- 32. Linoit : вебсервіс. URL: <https://en.linoit.com>.
- 33. Mentimeter : вебсервіс. URL: <https://www.mentimeter.com/>.
- 34. Netboard : вебсервіс. URL: <https://netboard.me/>.
- 35. Rebus1 : вебсервіс. URL: <http://rebus1.com/ua/>.
- 36. Wordwall : вебсервіс. URL: <https://wordwall.net>.
- 37. YouTube : відеохостинг. URL: <https://www.youtube.com/>.

Світлана Єфіменко

Організаційно-педагогічні умови формування навичок безпечної поведінки школярів в Інтернеті

Навчально-методичний посібник

Підписано до друку 28.11.2023 р.
Формат 60х84 1/16. Папір офсетний. Гарнітура «Times New Roman».
Друк – принтер. Тираж – 100 прим.
Зам. № 422

КЗ «КОППО імені Василя Сухомлинського», вул. Велика Перспективна, 39/63,
Кропивницький, 25006

Віддруковано в лабораторії інформаційно-методичного забезпечення освітнього процесу
КЗ «КОППО імені Василя Сухомлинського», вул. Велика Перспективна, 39/63,
Кропивницький, 25006