

Матеріали учасників Всеукраїнської науково-практичної конференції

«Безпека дітей в Інтернеті:

попередження, освіта, взаємодія»



OPEN POST

Напрямок 8. Розвиток кіберграмотності педагога РОЗВИТОК КІБЕРГРАМОТНОСТІ СУЧАСНОГО ЗДОБУВАЧА ОСВІТИ.

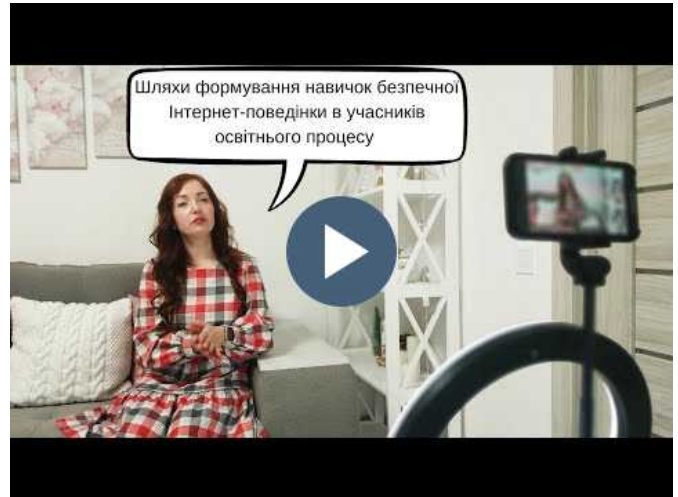
Тетяна БРОШЕВАН

Сучасний кіберпростір дає великі можливості для користувачів, ставить нові вимоги до їхнього рівня підготовки, але водночас несе загрози, які впливають на благополуччя (фізичне, психологічне, матеріальне та соціальне) підлітка [4, с.8].

Інформаційно-психологічна безпека особи та суспільства в цілому є складовою частиною кібербезпеки України. Постає проблема в її створенні та впливу фактів на індивідуальну психіку особистості. Володіючи певною інформацією, яку можна застосовувати для навчання та щоденного життя, забезпечує високий рівень кіберкультури [2, с.20]. Тому сучасний здобувач освіти повинен знати основні особливості, способи поширення та відомі приклади кіберзагроз, а також інструменти захисту домашньої мережі.

Розглянемо інтернет-загрози, що виникають на домашніх користувачів:

- ✓ бекдор – шкідливий програмний код для отримання доступу до робочої станції шляхом обходу аутентифікації, загроза надлеж зловмисникам можливість несанкціоновано та дистанційно управляти інфікованим пристроєм жертви;
- ✓ прихований майнінг – шкідливі програми для прихованого майнінгу належать до категорії шкідливого коду, призначеного для використання обчислювальної потужності пристрою користувача з метою видобутку криптовалют, при цьому, жертви не дають згоду і навіть не підозрюють про таку діяльність;
- ✓ кетфіншинг – це вид онлайн-шахрайства, коли людина або так званий кетфішер, створює фальшивий профіль у соціальній мережі чи на сайті знайомств з метою шахрайства чи обману;
- ✓ вішинг – вид телефонного шахрайства, під час якого зловмисники викрадають банківські дані або вилучають особисті



OPEN POST

Напрямок 5. Створення якісного безпечного українського контенту в мережі Інтернет: тренди, ролі, можливості.

ВИКОРИСТАННЯ ОНЛАЙН СЕРВІСІВ ДЛЯ СТВОРЕННЯ КОНТЕНТУ ДЛЯ НАВЧАННЯ У ДИСТАНЦІЙНОМУ ФОРМАТІ: ДОСВІД ЗАПОРІЗЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ

Олена БОЙКА, Юлія КАРПЮК

Реалії сьогодення змінюють формат навчання, починаючи з 2020 року українська освіта все більшою мірою переходить на навчання у дистанційному форматі. Особливо це актуально для регіонів які розташовані у зоні активних бойових, знаходяться біля таких територій та для громадян які мешають на тимчасово окупованих територіях. На превеликий жаль, Запорізька та Запорізька область розташовані в таких територіях, а, тому, питання надання освітніх послуг у дистанційному форматі стоїть дуже гостро.

Навчання повинно буде якісним та але й водночас дуже гостро стоїть питання не тільки якісного викладення матеріалу, але й мотивації та захоплення здобувачів освіти, формування та підтримання у них бажання вчитися. Одним з рішень цього завдання є викладення матеріалу та проведення контрольних заходів у цікавій та незвичайній формі, яка відрізняється від традиційних академічних форм.

Створення навчальних матеріалів за допомогою різноманітних онлайн сервісів може допомогти впоратись з цим завданням. Сучасний здобувач освіти відрізняється насамперед своєю діяльністю. Гаджети стали невід'ємною частиною нашого сучасного життя, а тому молодь краще сприймає такі форми набуття знань та навичок які використовують їх у якості допоміжних засобів. Здобувачі освіти охоче використовують різноманітні сервіси, додатки, сайти для опанування нових знань та навичок та для власного розвитку.

OPEN POST

Напрямок 6. Безпечне спілкування онлайн: ризики, правила, механізми звернення про допомогу й захист.

ПСИХОЛОГІЧНІ ОСОБЛИВОСТІ ДІТЯТИ ТА ПСИХОТРАВМУВАННЯ, ЯК ПЕРЕДУМОВА ВТЯГНЕННЯ ЇХ У КІБЕРЗЛОЧИННИ (ОНЛАЙН-ГРУМІНГ).

Юлія БОЙЧУК

Молодь у процесі свого дорослішання потребує певної моделі для наслідування. Тут важливу роль відіграє соціально-культурне середовище, тобто його суб'єкти, чий соціально-психологічний вплив може бути як позитивним, так і негативним. Розглядаючи зовнішні фактори, не можна оминути і внутрішні, такі як загальний психосексуальний розвиток та вікові особливості та новоутворення.

Лансаротська конвенція є першим міжнародно-правовим документом, що дає роз'яснення стосовно «домогання дітей в сексуальних цілях», що означає підготовку дитини до сексуального насильства, яка мотивована бажанням використати її для статевих цілей. Це може включати дружбу з дитиною, часто через дорослого, який надає себе за іншу молодшу особу, залучаючи дитину до обговорення інтимних питань, і поступово демонструючи дитині матеріали сексуального характеру для того, щоб зменшити опір або заборони стосовно сексуального насильства. Основним постулатом у сфері захисту дітей від сексуального насильства, які передбачає Конвенція, є зокрема криміналізація перегляду матеріалів сексуального насильства над дітьми та введення поняття грумінгу, що в свою чергу, кримінальним законодавством встановлює відповідальність за домогання дитини для сексуальних цілей. Тобто «грумінг» - це побудова в мережі Інтернет дорослим/групою дорослих осіб довірливих стосунків з дитиною (підлітком) з метою отримання її інтимних фото/відео з подальшим її шантажуванням та розповсюдження цих фото [1, с. 60]. Потрапивши в таку складну ситуацію, діти відчувають самотність, відчуженість та беззахисність, тому погоджуються на всі умови кривдників. Через таке психологічне пригнічення та страх дитини більшість випадків онлайн-грумінгу

OPEN POST

OPEN POST

**ПІТАННЯ ПІДГОТОВКИ МАЙБУТНІХ УЧИТЕЛІВ ІНФОРМАТКИ З
ПІТАНЬ БЕЗПЕКИ У КІБЕРПРОСТОРІ****Анотація**

У публікації йдеться про практичні прийоми підготовки майбутніх учителів інформатики до правильного розуміння питань сучасної інформаційної безпеки та використання отриманих знань у професійній діяльності під час навчання учнів. Акцент ставиться на співпрацю здобувачів освіти під час навчальної діяльності. Автором наведено приклади впровадження на практиці заходів, що надають необхідний рівень готовності майбутніх фахівців до діяльності за вказаним напрямом.

Ключові слова: професійна підготовка, безпека інформатики, інформаційна безпека, метод проєктів, ділова гра, рольова гра, інтернет-група.

Abstract

The publication deals with practical methods of preparing future computer science teachers for a correct understanding of modern information security issues and the use of the acquired knowledge in professional activities during the education of students. Emphasis is placed on the cooperation of students during educational activities. The author gives examples of measures tested in practice, which provide the necessary level of readiness of future specialists for activities in the specified direction.

Key words: Keywords: professional training of computer science teacher, information security, project method, business game, round table.

Актуальність теми та постановка проблеми. Як свідчать факти, сучасний етап розвитку шкільної освіти активно супроводжується та стимулюється мережею

Особливості виявлення, фіксації та розкриття правопорушень, вчинених відносно дітей з використанням мережі Інтернет.

**РОЗСЛІДУВАННЯ ПРАВОПОРУШЕНЬ, ВЧИНЕНИХ ВІДНОСНО
ДІТЕЙ В ІНТЕРНЕТІ ЯК ІННОВАЦІЙНИЙ НАПРЯМОК
КРИМІНАЛІСТИКИ**

Вікторія Яремчук

У сучасному світі велику кількість важливої інформації ми здобуваємо через мережу «Інтернет». Проте, серед правдивої інформації, що міститься у мережі, все частіше з'являється незаконна інформація. Дана ситуація призводить до порушення прав та законних інтересів громадян, особливо це стосується дітей. Їм досить складно розпізнати певні шахрайські дії в мережі інтернет. Тому у криміналістиці одним з нових напрямків є розслідування та розкриття кіберзлочинів.

Так, мережа Інтернет є одним з видів соціального простору та є широкою платформою для злочинної діяльності, що зумовлює виникнення нових способів вчинення кримінальних правопорушень, специфіку слідствознавства, вибір технічних засобів як для вчинення та приховування кримінальних правопорушень, так і для процедури їх виявлення та розслідування. В Україні забезпечення он-лайн безпеки громадян нашої країни покладється на кіберполіцію, що є одним зі структурних підрозділів Національної поліції, який діє у складі кримінальної поліції [1, с.115].

Так, у 2020 р. кіберполіцейські заблокували майже 30 тисяч шахрайських інтернет-послань і майже 9 тисяч фінансових операцій зловмисників. Злочинці продають неіснуючі товари на платформах оголошень або у соціальних мережах, вимагають передплату за товар, а після переведення коштів покупки блокуються. Популярним кримінальним правопорушенням є створення фішингових ресурсів, схожих на популярні Інтернет-магазини,

OPEN POST

OPEN POST

Напрямок 5. Створення якісного безпечного українського контенту в мережі Інтернет: тренди, ролі, можливості

**УКРАЇНОВИЙ ВІДЕОКОНТЕНТ ДЛЯ ДІТЕЙ: СУЧАСНІ
ТРЕНДИ ТА ТЕНДЕНЦІЇ**

Олена Кравченко

У дослідженні проаналізовано сучасні тренди та тенденції створення відеоконтенту для дітей в мережах YouTube та TikTok, представлено основні вимоги до якісного інтернет-сайту на контенту. Розглянуто класифікації особливості українського відеоконтенту, залежно від його формату та комунікатора. Встановлено, що український відеоконтент, створений дорослими комунікаторами, є переважно якісним та має високий потенціал для використання з навчальною і виховною метою.

Ключові слова: якісний контент, комунікатор, відеоканал, український YouTube, сучасні тренди.

Сучасні діти живуть в епоху становлення мережі Інтернет, вона стала важливою частиною їхнього соціального життя – навчання, розваг, спілкування. Діти дорослішають у світі, де онлайн-медіа стали невід'ємною частиною повсякденного життя: з інтернет-ресурсів діти й підлітки черпають знання про світ розширюють свій соціальний досвід, обирають зразки для наслідування й навіть аргументи для прийняття життєвих рішень [4, с.14].

Водночас проблема якісного українського дитячого контенту не була об'єктом спеціального наукового комплексного дослідження, що зумовлює новизну та актуальність роботи. Це питання розглядалося в контексті інших наукових проблем, зокрема у сфері соціально-психологічних особливостей впливу інтернет-простору на розвиток особистості дитини, маніпуляції свідомістю в умовах інформаційного суспільства, загрози безпеці дітей у соціальних мережах

Напрямок 7. Технологічні інструменти та рішення формування безпечного Інтернет-простору дитини.

**ФОРМУВАННЯ БЕЗПЕЧНОГО ЦИФРОВОГО ОСВІТЬОГО
СЕРЕДОВИЩА У ЗАКЛАДІ ОСВІТИ ЗАСОБАМИ
GOOGLE
WORKSPACE FOR EDUCATION**

Вікторія МАТЯШ, Володимир МАТЯШ, Лариса МІТЛЕНКО

Після сьогоднішніх останніх років, пов'язаних з карантинном, який запроваджено у зв'язку з поширенням гострої респіраторної інфекції, спричиненої коронавірусом COVID-2019, змусили перейти до дистанційної форми навчання більшість шкіл. Це змінило вимоги до рівня сформованості цифрових компетентностей у вчителів та учнів, до якості електронних освітніх матеріалів, до розроблення та наповнення персоналізованих, відкритих інформаційних платформ, що використовують під час дистанційного навчання. Гостро постала проблема формування цифрового освітнього середовища закладу освіти, яке відповідає сучасним вимогам, створює безпечні умови для навчання, для автоматизації обліку освітніх досягнень учнів, для створення та використання сучасних електронних освітніх ресурсів тощо [4, 5].

Метою даної роботи є опис структури цифрового освітнього середовища закладу загальної середньої освіти Новоградського ліцею №1 на платформі **Google WorkSpace for Education**.

Досліджено різні аспекти цифрового середовища закладу освіти присвячена низка наукових робіт (В.Ю. Біков, О.О. Грибок, М.І. Жалдак, Ю.О. Жук, І.В. Іванюк, В.В. Лапінський, О.М. Мельник, І.В. Момот, Н.В. Морзе, В.П. Олексюк, Н.В. Сорока та ін.). Проведені дослідження свідчать, що досі немає єдиного загальноприйнятого визначення цифрового освітнього середовища закладу загальної середньої освіти і узагальненої функціональної моделі такого середовища. З огляду на різні підходи можна стверджувати, що цифрове освітнє середовище школи – це складна багаторівнева цифрова система, яка послугує підсистемою забезпечення управлінської, навчальної та

OPEN POST

OPEN POST

Наприклад. Небезпечне спілкування онлайн: ризики, правила, механізми звернення про допомогу й захист.

СОЦІАЛЬНА МЕРЕЖА ТІКТОК. ЯК ЗАБЕЗПЕЧИТИ БЕЗПЕЧНЕ КОРИСТУВАННЯ

Катерина МАЛЬЦУКОВА

Досліджуючи сучасних дітей та соціальні мережі якими вони користуються, то безперечним лідером є TikTok. Згідно з даними дослідницької компанії Insider Intelligence, TikTok став третьою найбільшою соціальною платформою у світі за кількістю користувачів, обійшовши Snapchat та Twitter. Лідерами залишаються Instagram та Facebook. Така ж тенденція спостерігається і у 2022 році, згідно TechCrunch. За останні два роки кількість користувачів TikTok збільшилась — у 2020 році на 59,8% та ще на 40,8% у 2021. За прогнозами Insider Intelligence, у 2022 році ріст кількості користувачів на платформі сповільниться, але залишиться високим — 15,1%. Щодня аудиторія TikTok у 2022 році збільшиться до 755 млн. 3,57 млрд людей будуть заходити до соціальної мережі щодня, причому 82% з них — це 82% усіх користувачів інтернету у світі, йдеться у прогнозі Insider Intelligence. [1]

У всьому світі сьогодні 4,65 млрд користувачів соціальних мереж, це 58,7% всього населення планети. Якщо вважати, що соцмережами можуть користуватися люди від 13 років, приблизно три чверті усіх це вже роблять.

Користувачі проводять в середньому по 6 годин і 53 хвилини онлайн щодня. Типовий користувач інтернету зараз проводить в мережі понад 40% свого життя [2]

Через соціальні мережі відбувається не тільки дружнє спілкування чи розваги, а й навчання, погрози, цькування. Навчання, що відбувається у мережі Інтернет, потребує особливої уваги з метою його виявлення та протидії.

Напрям 5. Створення якісного безпечного українськомовного контенту в мережі Інтернет: тренди, ролі, можливості.

РОЛЬ МЕДІАГРАМОТНОСТІ ПЕДАГОГА ПРИ СТВОРЕННІ ЯКІСНОГО КОНТЕНТУ

Вікторія ЛЕБЕДЬВА

Медіатизоване суспільство епохи інформаційних технологій стрімко змінює середовище і форми спілкування, навчальний процес і систему освіти, джерела і методи отримання інформації, форми і способи подання результатів діяльності та прояви медіавторчості.

Перебуваючи в умовах інформаційно насиченого суспільства з відкритим доступом до будь-якої інформації дитина не може бути осторонь цих медіа потоків. Медіа потужно та суперечливо впливають на освіту молодого покоління. Саме сприйняття та оцінку зовнішнього світу дитина одержує із засобів масової інформації, які відночас є вагомим джерелом знань та освіти та виховання.

Тому надзвичайно велика відповідальність накладається на роль педагога, що організовує процес навчання, створює інформаційний контент, медіапродукти та формує особистісно значущі якості учня та його медіакультури, як основу подальшого самовизначення в глобальному інформаційному просторі.

У Концепції впровадження медіа-освіти в Україні зазначено, що «медіакультура – це сукупність інформаційно-комунікаційних засобів, що функціонують у суспільстві, знакових систем, елементів культури комунікації, пошуку, збору, виробництва і передачі інформації, а також культури її сприйняття соціальними групами та соціумом у цілому. На особистісному рівні медіакультура означає здатність людини ефективно взаємодіяти з мас-медіа, адекватно поводитися в інформаційному середовищі» [1].

Медіакомпетентність – рівень медіа-культури, що забезпечує розуміння особистістю соціокультурного, економічного і політичного контексту функціонування медіа, засвідчує її здатність бути носієм і передавачем медіа-

OPEN POST

OPEN POST

Напрям 5. Створення якісного безпечного українськомовного контенту в мережі Інтернет: тренди, ролі, можливості.

ВИКОРИСТАННЯ ОНЛАЙН-СЕРВІСІВ ДЛЯ СТВОРЕННЯ ОСВІТНЬОГО КОНТЕНТУ ЯК СКЛАДОВА ПРОФЕСІЙНОЇ КОМПЕТЕНТНОСТІ ВИХОВАТЕЛЯ ЗАКЛАДУ ДОШКІЛЬНОЇ ОСВИТИ

Ольга ВАЛЬТЕР

На сьогодні Професійний стандарт «Вихователь закладу дошкільної освіти» пунктом 5 визначає перелік трудових функцій сучасного вихователя:

- організація, забезпечення та реалізація освітнього процесу;
- участь у створенні, підтримці та розвитку здорового, безпечного та розвивального, інклюзивного освітнього середовища;
- партнерська взаємодія з учасниками освітнього процесу;
- професійний розвиток та саморозвитання [3].

Наразі акцентуємо увагу на функції, яка розкривається двома компетентностями: здатністю до самоосвіти протягом життя та інформаційно-комунікаційною. Розглянемо детальніше інформаційно-комунікаційну компетентність вихователя.



OPEN POST

OPEN POST

Напрям 4. Соціально-педагогічний вимір поведінки «цифрові сліди», «цифрові тіню».

ФОРМУЛА ПОЗИТИВНОГО ЦИФРОВОГО СЛІДУ

Альона ПЕЦУН

Кожна людина залишає свій слід в мережі Інтернет, який на відміну від сліду на снігу нікуди не зникне. Опублікована інформація може бути такою що компрометує особу або допомагає визначити типову поведінку.

Цифровий слід (або **цифровий відбиток**; **англ. digital footprint**) — сукупність інформації про відвідини та внесок користувача під час перебування у мережі. Класифікується 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 [1].

Складові цифрового сліду: фото, відео, голосова, текстова інформація. В сучасному світі висловлення свої думки часто використовують соціальні мережі. Лише секунди, щоб зруйнувати репутацію в Інтернеті. Навіть у разі анонімізації, яку допустила людина, ця особа може витратити місяці чи роки, намагаючись повернути довіру громадськості. Крім того, минуле може перешкоджати майбутнім успішним користувачів соціальних мереж на ринку праці, якщо їм потрібно шукати роботу [2]. Обережність є найкращим підходом до публікації контенту в Інтернеті.

Формула позитивного цифрового сліду: ДОСЛІДЖ + ОЦІНИ + ПІДКРЕСЛІ.

ДОСЛІДЖ, які уже є складові власного цифрового сліду. У нагоді стане інструмент Google Alerts, за допомогою якого можна налаштувати надходження оповіщення про появу власного прізвища та ім'я.

ОЦІНИ до яких наслідків можуть призвести висловлення та дії в мережі Інтернет. Дотримуйтеся мережевого етикету. Не варто робити речей, які не заохочуються в цивілізованому суспільстві – користуватися тюркськими

Напряг 3. Організаційно-педагогічні умови формування безпечної поведінки здобувачів освіти в Інтернеті.

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ПРОЦЕСУ ФОРМУВАННЯ БЕЗПЕЧНОЇ ПОВЕДІНКИ ЗДОБУВАЧІВ ОСВІТИ В ІНТЕРНЕТІ. PRO ET CONTRA

Ірина МАНЬКО

Ключові слова: здобувачі освіти, Інтернет, безпека, заклад освіти, держава, кіберполіція, нормативно-правова база, закон.

Мета статті провести аналіз нормативно-правової бази, що стосується забезпечення процесу формування безпечної поведінки дітей та підлітків у мережі Інтернет, визначити хто серед державних структур, закладів освіти чи інших організацій, має займатися цією проблематикою. Також, проілюструвати чи стосуються відповідні нормативно-правові документи конкретні безпеки дітей в мережі, та наскільки коректно вони застосовуються.

Постановка проблеми. Поширення комп'ютерної мережі Інтернет стала точкою невідворотності та дитини інструментом в процесі становлення сучасного інформаційного суспільства. Мережа Інтернет – це гучний майданчик без кордонів для обміну думками, пропаганди певних моделей поведінки, способу мислення, світогляду, цінностей тощо. Більше того, напевно не реально перебування людини у мережі акумулюється у реальні наслідки її дій у світі дійсному. Тож, не має сумніву, що ця сфера потребує нормативно-правового регулювання, як і на рівні окремих держав, так і на міждержавних рівнях. А визначені правила поведінки мають стосуватися кожного користувача чи категорії користувачів, і переслідувати за ним певний вид відповідальності чи обмежень. Однак, коли ми звужуємо коло дослідження, і пишемо для себе програмно дослідити саме український контекст, та конкретно питання залучення окремих державних структур у забезпечення процесу формування безпечної поведінки здобувачів освіти в Інтернеті, то потребуємо доказати більше зусиль, щоб зрозуміти, кому мають належати такі функції, яка

Напряг 2. Інформаційна безпека дітей під час війни. ІНФОРМАЦІЙНА БЕЗПЕКА УЧНІВ ПРИ ВИКОРИСТАННІ МЕРЕЖІ ІНТЕРНЕТ В ОСВІТНЬОМУ ПРОЦЕСІ

Олександр НИЧ

Інформаційна безпека – стан захищеності життя та важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвочасність та недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій [1].

Практично всі діти XXI століття мають свій персональний гаджет. Дуже зручно в будь-який час в будь-якому місці мати доступ до мережі Інтернет, соціальних мереж та до різної інформації. Але нажалі в Україні – війна. Часто лунають повітряні тривоги, доводиться ховатися в укриття. Дбаючи про своє життя ми дбаємо про власну безпеку, але ми не повинні забувати про інформаційну безпеку. Хоч для дітей Інтернет є середовищем для навчання, розваг і спілкування з друзями, але далеко не всі знають, що в Інтернеті існує низка небезпек і загроз.

Види небезпек: кібербулінг, як сучасна форма агресії, що набула поширення з появою мобільних телефонів, комп'ютерів та Інтернету; фішинг, як крадіжка персональних даних, наприклад логінів і паролів; жорстокі ігри; онлайніві казино; сайти, що пропагандують насилля; сайти сексуальних характеру; сайти магазинів ітм-послуг тощо.

Види загроз: загрози для особистої безпеки; загрози витоку персональної інформації; загрози для персональних комп'ютерів та мобільних пристроїв [3].

Отже, як захистити дітей під час війни в інформаційному просторі?

- Ні в якому разі не передавати своїх персональних даних і особистої інформації (особистий номер телефону чи номер батьків, де батьки працюють,

OPEN POST

Напряг 6. Небезпечне спілкування онлайн: ризики, правила, механізми звернення про допомогу й захист.

ІНТЕРНЕТ МОЖЕ БУТИ БЕЗПЕЧНИМ, А КОРИСТУВАЧ – ЗАХИЩЕНИМ

Наталія КВАЦІА

Дотримання кібергігієни нині стає питанням безпеки людини. Інтернет вже давно перестав бути тільки джерелом нових знань, він є також джерелом фейків, певних ризиків, кібер-загроз тощо. Та за правильного підходу інтернет може бути безпечним, а користувач захищеним. Захищений – значить об'язаний. Об'язаний з можливими ризиками, правилами роботи в мережі, з правовими аспектами протидії кіберзлочинності.

Діти, які отримали доступ до інтернету, отримали доступ до світу. Але світ так само отримав доступ до дітей, зокрема до їхніх, не завжди захищених, даних. За умов відсутності компетентностей безпечної поведінки в цифровому просторі може бути нанесена непоправна шкода здоров'ю та життю дитини. Тому освітянам варто робити все, щоб зробити шифрове освітнє середовище максимально безпечним. Під час дистанційного навчання зручним джерелом для ознайомлення з тематикою кібербезпеки може бути сайт ліцею, на якому згідно з методичними рекомендаціями має бути сторінка з безпечного інтернету.

Як адміністратор сайту Мартоніського ліцею [4], прийшла до ідеї створення не однієї сторінки, а окремого веб-сайту під назвою: «Інтернет може бути безпечним, а користувач – захищеним!» [1]. На ньому за матеріалами мережі зібрана інформація з інтернет-безпеки на допомогу класним керівникам, учням та батькам. Наразі доступним є такі сторінки:

- **Головна. Онлайн-курси з кібербезпеки.** На цій сторінці знаходяться опис і посилання на декілька курсів з кібербезпеки та медіаграмотності для учнів, вчителів, батьків. Курси від Prometis, Мінзміні, Чпана. Хочеться звернути особливу увагу на курс «Основи кібербезпеки для школярів» [7]. Учасниками якого можуть стати як учні, так і вчителі та батьки, а контент курсу – це

Напряг 6. Небезпечне спілкування онлайн: ризики, правила, механізми звернення про допомогу й захист.

ЧИ ГОТОВІ МИ НАРАЗІ ДО ПРОТИСТОЯННЯ КІБЕРБУЛІНГУ?

Тетяна ОВЧИННИК

Сьогодні Інтернет – це не тільки система комп'ютерних мереж, де зберігається неоскільки кількість різноманітної інформації, а й шлий віртуальний Всесвіт. Він використовується майже у всіх сферах діяльності людини, що значно полегшує наше життя. І наразі, в умовах надзвичайної ситуації, є гарна можливість продовжувати навчання у дистанційному форматі й в т.ч. спілкуватися за допомогою інтернет-мережі поза навчальним процесом. Звісно, переваг у користуванні Інтернетом достатньо, але є й інші бач, пов'язані із певними ризиками як для дорослих, так і для самої незахищеної категорії населення – дітей.

З явищем булінгу у дитинстві ми вже знайомі добре, проводимо активну роботу щодо запобігання його проявів, здійснюємо профілактику на виховних годинах, ведемо індивідуальні бесіди тощо. Крім того, в Україні активно розгорнута кампанія протидії булінгу, наприклад Всеукраїнська ініціатива, яка звертає увагу до цієї проблеми, максимально залучає до її вирішення освітян, батьків, громадських активістів, самих дітей та всіх небайдужих. Але, наразі суспільство зіткнулося із ще одним явищем пов'язаним із шакуванням саме в мережі – кібербулінгом, яке ввійшло в наше життя разом із розвитком соціальних мереж. Ми вважаємо, що дане явище потребує аналізу й роз'яснення та розповсюдження цієї інформації до широкого загалу.

Кібербулінг або інтернет-мобінг – це нова форма агресії, яка відбувається в Інтернеті. Нападник використовує соціальні мережі, електронну пошту, месенджери та інші засоби спілкування, щоб дошкулити, нашкодити та принизити людину [3].

OPEN POST

OPEN POST

Напрям 1. Соціально-педагогічний вимір поняття «права дитини в Інтернеті».

ЦИФРОВІ ПРАВА ТА ОНЛАЙН БЕЗПЕКА ДІТЕЙ В ІНТЕРНЕТІ Анна ДРАГАНЕЦЬ

Сучасне суспільство активно розвивається у сфері інформаційно-комунікаційних технологій. Інтернет вже не є новиною, та більшість людей є активними користувачами всесвітньої мережі «Інтернет», яку також називають «всесвітнє павутиння». Не лише доросле населення планети є її користувачами, але і діти різних вікових категорій, від наймолодших школярів до старшокласників. Зважаючи на такий ріст популярності мережі «Інтернет», постає питання безпеки в інтернеті, особливо важливим є питання безпеки дітей. Інтернет є глобальною мережею, яка охоплює величезні території і контролювати контент, який з'являється кожен день неможливо. Інтернет дає нам багато можливостей для навчання, роботи та спілкування, але в той же час він стає проблемою, адже в інтернеті спостерігається порушення прав людини. Саме тому питання цифрової безпеки дітей в інтернеті є дуже важливим.

З розвитком інформаційно-комп'ютерних технологій та входженням інтернету у всі ланки нашого життя, постало питання інтернет безпеки та дотримання прав людини в інтернеті. Найбільш вразливою категорією є діти, тому питання захисту їх прав в інтернеті постає гостро. Дослідженню даної проблеми приділяти увагу науковці, зокрема, одним із українських дослідників, який почав досліджувати питання взаємодії зку та прав людини став А.Пазюк, який висвітлює свої думки у праці «Права людини та інтернет» [3]. О. Черних досліджувала питання формування безпечної поведінки підлітків в інтернеті, як соціально-педагогічну проблему [4]. Володоська В., Двороний М. досліджували питання прав людини онлайн, та випустили посібник «Права людини онлайн: Порядок денний для України» [2].

Мета дослідження – дослідити сутність та зміст понять «цифрові права» та «права дитини в інтернеті».

OPEN POST

Напрям 8. Розвиток кіберграмотності педагога

МЕДІАГРАМОТНІСТЬ, ЯК УБЕЗПЕЧИТИ СВОЄ ЦИФРОВЕ ЖИТТЯ Олена ГОНЧАРУК

Анотація: у статті розглянуто питання про медіасвіту та медіаграмотність педагога, інформаційну безпеку під час використання інтернет ресурсів та застосувань, використання критичного мислення під час взаємодії з інформацією.

Ключові слова: медіаграмотність, інформаційна безпека, акаунти, Google, Facebook, Viber, інтернет, інформація, соціальна мережа.

Сучасний світ – це набір іконок соціальних мереж на вашому смартфоні. Один клік, і ви усюди! Ми – споживачі та творці контенту й різної інформації в мережі. А педагог – це місток між сучасним світом і дітьми, тому перш за все, він має розумітися у питаннях інформаційної освіти, вмінні оперувати інформацією, має розвинути інформаційну грамотність, вмінні розрізняти фейковий «маніпулятивний» контент, а також навчати дітей на онлайн програмах для спілкування, тобто володіти знаннями про медіаграмотності та медіагігієни. Головне правило сучасного світу: «шо потрапило у мережу, залишиться там назавжди!»

А що світ знає про вас? Яку ж позицію має зайняти педагог щодо соціальних мереж. Як убезпечити своє цифрове життя. Саме про це я хочу вам розповісти.

Ще у квітні 2016 року в Україні постановою преїдції Національної академії педагогічних наук було схвалено «Концепцію впровадження медіасвіти в Україні». Головна ідея концепції полягає в сприянні становленню ефективної системи медіасвіти в Україні.

Згідно з цією Концепцією, медіасвіта — частина освітнього процесу, спрямована на формування в суспільстві медіакультури, підготовку особистості до безпечної та ефективної взаємодії з сучасною системою масмедіа, як традиційними (друковані видання, радіо, кіно, телебачення), так і новітніми

OPEN POST

6. Небезпечне спілкування онлайн: ризики, правила, механізми звернення про допомогу й захист.

ОКРЕМІ НАПРЯМКИ МІНІМІЗАЦІЇ НЕБЕЗПЕКИ ДЛЯ ДІТЕЙ В ВІРТУАЛЬНОМУ ПРОСТОРІ Максім ГРИЦЕНКО

Сучасна дитина стає активним користувачем мережі інтернет буквально паралельно з засвоєнням вміння ходити. Батьки дозволяють малюкам дивитися розвиваючі сайти, мультки поступово привчаючи дитину до мережевого спілкування. З початком навчання у школі такий симбіоз дитини та інтернету стає нормою, завдяки інформатизації навчального процесу. Ще в 2019 році за даними міжнародного дослідницького проекту ESPAD, у 2019 році лише 6,7% опитаних підлітків в Україні не користувалися соціальними мережами [1]. Більше половини (55,4%) опитаних вважають, що проводять забагато часу в соціальних мережах. Практично половина дітей (23,9%) повідомили про те, що в нього посується настрої, коли не може провести час у соціальних мережах. Кожна друга дівчина (50,9%) та більше третини хлопців (35,7%) зазначили, що їхні батьки звертають увагу на витрачання забагато часу в соціальних мережах. (Серед усіх про це зазначили 43,6%). Такі проблеми притаманні всім віковим групам. Хоча за авторитетом діти поки ставлять на перше місце батьків, але Інтернет уже переїмг друзів, телебачення, книги і друковані ЗМІ. Серед 15-літніх дітей він вже потіснив батьків за ступенем довіри й частоти звернень. Також високі шанси, що найближчим часом, не витримавши найкороткішої конкуренції з віртуальним простором, батьки підуть б другий план і в старших підлітків. Павутиня стає місцем проживання для десятої частини опитаних: займає час, відлучений на школу, гуляння, харчування, сон. Діти проводять в Інтернеті від 5 до 10 годин на день, що служить надійним джерелом формування інтернет-залежності. 65 відсотків батьків не обмежують підлітків ні в часі, ні в темі їхніх подорожей у віртуальному просторі. Чим доросліше

OPEN POST

Напрям 3. Організаційно-педагогічні умови формування безпечної поведінки здобувачів освіти в Інтернеті

ПСИХОЛОГІЧНІ ОСОБЛИВОСТІ ПОВЕДІНКИ ПІДЛІТКІВ У МЕРЕЖІ ІНТЕРНЕТ

У межах публікації здійснено теоретичний аналіз особливостей поведінки підлітків в мережі Інтернет; виокремлено мотиви спілкування та специфічні особливості спілкування підлітків у мережі Інтернет.

Ключові слова: мережа Інтернет, соціальні мережі, підлітковий вік, спілкування підлітків, поведінка підлітків.

Сучасна людина стає свідком і активним учасником становлення інформаційного суспільства. Інтенсивні інформаційні та комунікативні потоки, які реалізуються за допомогою новітніх технологій (такі як Інтернет), створюють найважливіші навантаження на психічні процеси людини і її особистість. Вплив на психологію стоїть завдяки пошуку психологічних ресурсів, які могли б сприяти виваженому вибору навантажень і оптимізації процесів саморегуляції особистості [4].

Вивчення даної проблеми викликало достатній інтерес у вітчизняних вчених (О. Дроздов, Т. Карабин, В. Лоскутова, Л. Юр'єва), проте вони не враховували той факт, що більшість користувачів Інтернету складають підлітки. Цілком зрозуміло, що підлітковий вік – найнебезпечніший період щодо формування Інтернет-залежної поведінки (Дж. Річардсон). По-перше, для цього віку притаманне прагнення до пізнання всього нового, незвичайного (І. Кон), «почуття дорослості», яке виявляється у гіпертрофованій потребі самостійності, самоствердження, відмови від дитячої «моралі успіху» (Н. Максимова), бажання копіювати звички і способи поведінки старших, острах відстані від оновлєтків, здаватися в їхніх очах смішним (М. Кондратьєв, В. Мухіна). По-друге, вікові особливості

OPEN POST

ФОРМУВАННЯ КІБЕРГРАМОТНОСТІ МАЙБУТЬОГО ПЕДАГОГА
Світлана ДОЦЕНКО
Ван ЧЖЕН

Постійний розвиток цифрової трансформації та переведення більшості послуг в онлайн незвичні та потрібні! Проте важливо вміти захистити себе та свої персональні дані від кібератак та кіберзлочинів. Внаслідок пандемії СОУП-19, потім через російський напад і масштабну війну освітній сектор України перейшов майже повністю на дистанційне навчання та зіткнувся з широким спектром кіберзагроз: загрози на пристрої, загрози через людський фактор, крадіжка персональних даних, програм-вигоначі або зловмисне програмне забезпечення, фінансова вигода, шпигунство, фішинг, DDoS-атаки, загрози на SMS тощо [4]. Тому такою стала проблема формування кіберграмотності майбутніх педагогів як теми підготовки педагогічних працівників.

Раніше люди взаємодіяли в киберпросторі: земля, вода, повітря. З появою Інтернету з'явився ще один вимір – інформаційний (кіберпростір). Ідеться про мережу взаємозв'язаних між собою пристроїв. Загалом безпека – це стан захищеності від зовнішніх і внутрішніх загроз. А безпека в кіберпросторі – ваша особиста захищеність та безпека ваших пристроїв.

Якщо проблемою інформаційної безпеки вчені займаються вже давно, то проблема інформаційної безпеки вчителів з'явилася вже давно, бо проблема інформаційної безпеки вчителів залізається малодослідженою та актуальною в наш час. Особливо гостро стоїть проблема інформаційної безпеки у сфері освіти і зв'язку з переходом на дистанційне навчання та роботу в режимі онлайн. Відбувається масовий, глобальний вплив інформаційних технологій на людину [1].

Інформаційна безпека освітнього закладу – це комплекс заходів різного характеру, який спрямований на реалізацію двох шляхів: 1) захист персональних даних та інформаційного простору від несанкціонованого втручання, захисту

ЯК ВБЕРЕГТИ ДІТЕЙ ВІД НЕПРИСМНОСТЕЙ У СОЦМЕРЕЖАХ ПІД ЧАС ВІЙНИ.

Алла СКЕМСЬКА

Формування ключових та стійких компетенцій у дітей про безпечну поведінку під час війни та після її завершення – одне з головних завдань батьків та освіті. З 24 лютого 2022 року питання безпеки вишло на інший рівень. Нині воєнні ризики є частиною життя, тому маємо бути готовими захистити себе і дітей.

На сьогодні інтернет є безмежним простором для задоволення найрізноманітніших потреб дитини у навчанні й відпочинку, у комунікації з рідними, у самоствердженні й визнанні серед однолітків, в отриманні чергової порції інформації з фронту. Але варто пам'ятати, що за позначкою геолокації на пості чи фотографії в соціальній мережі чи одним повідомленням може ховатися серйозна небезпека. Особливо під час війни, коли інфопростір використовують окупанти для військових нападів на українські міста.

Як подбати про те, аби спілкування в інтернеті не завершилося для вашої дитини неприсмітцями і як подбати про інформаційну безпеку під час війни?

Загроза в Інтернеті – це ймовірність завдання збитків, заподіяних здоров'ю людини (фізичному, психічному, соціальному благополуччю) та (або) її майну (матеріальному благополуччю) внаслідок користування Інтернетом.

Розповсюджені загрози в Інтернеті: фейкова інформація, кібертунінг, сексторшес, секстинг, кібербулінг, інтернет-шахрайство, небезпечний контент, що містить порнографію та пропаганду насилля, екстриму, суїциду, заборонених речовин, інтернет-залежність, гемблінг та ін. В умовах війни, де активно діє інформаційний фронт, найбільш поширеною загрозою є фейкова інформація (від англ. fake – підробка). Така інформація є досить ефективним способом маніпуляції свідомістю шляхом надання неповної інформації,

OPEN POST

6. Небезпечне спілкування онлайн: ризики, правила, механізми звернення про допомогу й захист.

НЕБЕЗПЕКА СПІЛКУВАННЯ ОНЛАЙН. ЗВЕРТАННЯ ПРО ДОПОМОГУ Й ЗАХИСТ

Ніна АФАДСЬКА

Іновіації педагогічної освіти в сучасному інформаційному світі тісно сплелися із розвитком цифрових технологій та Інтернету. У статті розкривається зміст небезпек спілкування онлайн, звертання про допомогу й захист.

Ключові слова: Інтернет, безпечна поведінка школярів в Інтернеті, формування безпечної поведінки школярів в Інтернеті, спілкування, небезпека, онлайн.

Цифрові технології вже змінили світ. Молодь від 15 до 24 років є найбільшою групою інтернет-користувачів, і вже дошкільнята активно користуються мережею. Кожен третій інтернет-користувач – це діти й підлітки до 18 років.

Інтернет дедалі більше стає частиною життя дітей, і створює безліч ризиків для конфіденційності, добробуту та безпеки дітей. Новий звіт «Діти в цифровому світі» Дітячого фонду ООН (ЮНІСЕФ) проливає світло на небезпеку, створену цифровими технологіями сьогодні, пояснює, як захистити дітей та як краще підійти до проблеми «онлайн-залежності» дітей.

Мета. Формування навичок безпечної спілкування дітей у Інтернеті та інформувати до кого звертатися про допомогу й захист.

Завдання:

- дослідити позитивні і негативні наслідки Інтернету;
- сформулювати та засвоїти правила безпечної роботи в Інтернеті;
- проаналізувати поняття Інтернет-залежність та небезпеку спілкування онлайн;
- до кого звертатися про допомогу й захист.

OPEN POST

OPEN POST

II Всеукраїнська науково-практична конференція «Безпека дітей в Інтернеті: попередження, освіта, взаємодія»

Напряг 8. Розвиток кіберграмотності педагога.

ВИКОРИСТАННЯ СУЧАСНИХ ПРОГРАМ ДЛЯ ПРОВЕДЕННЯ ЗАНЯТЬ З УЧНЯМИ

Сьогоднішня потреба від нас адаптуватися до наших реалій. Потрібно проводити заняття з учнями на відстані, і матеріал має бути цікавим і захоплюючим. Тож постає питання як це зробити якісно?

Зараз як ніколи перед вчителем стоїть потреба у використанні Інтернет ресурсів для проведення занять, які б краще розкривали тему заняття і учні отримували необхідні знання. Головне в занятті це зацікавити учнів і розвинути бажання знову вийти з учителем на зв'язок. Запропоновані завдання мають не забирати багато часу у учня і давати високий рівень змістовних знань.

Сучасний педагог має відповідати наступним:

- бути сучасним (у підході до викладення свого предмету);
- весь час займатися самоосвітою;
- відповідати вимогам сучасності (використовувати різні Інтернет платформи для поглибленого викладання свого предмету).

Але не все залежить від самого вчителя, він потребує підтримки і від держави. Для того, щоб робота вчителя була кращою, використовуючи необхідні Інтернет ресурси потрібно створити відповідні умови:

- контент Інтернет ресурсів має бути саме українською мовою;
- необхідно розробити програмне забезпечення саме українського виробництва;
- безкоштовність і доступність навчальних програм;
- простий інтерфейс у використанні і він не має постійно оновлюватися, щоб не доводилося наново вчитися ним користуватися(особливо це не

OPEN POST

2. Інформаційна безпека дітей під час війни.

«Інформаційна безпека для дітей»

Федорина Марина

Викладач Гайворонського політехнічного фахового коледжу та комунального закладу «Гайворонський ліцей №2»

Анотація

В статті йдеться про основи інформаційної безпеки. Що таке фейк? Кому слід довіряти? Як перевіряти інформацію?

Напевне в 21 сторіччя війну в нашій країні не очікував ніхто.

Ця подія докорінно змінила життя всіх від мала до велика.

Українська молодь з перших днів війни на захист своєї Батьківщини. Дотримувалася до тероборони, волонтерства, допомагала.

Війна-це розруха, слези, сум, смерті, втрата даних.

І якби нам не хотілось вберегти наших дітей від війни нам це не вдасться. В кожній сім'ї хтось пішов до лав ЗСУ, хтось повернувся пораненим, а хтось загинув. Всі ми намагасьмо пришвидшити перемогу як на полі бою так і в тилу.

Завдання дорослих правильно доносити інформацію до дітей. Навчити їх в сучасних умовах правильно діяти підчас повітряної тривоги, під час комендантської години, при проходженні блок-постів, поводженні з невідомими предметами та речовинами. І ще одне з важливих питань про які необхідно говорити-це інформаційна безпека.

В умовах війни, де активно діє інформаційний фронт, найбільш поширеною загрозою є фейкова інформація (від англ. fake — підробка). За допомогою такої інформації відбуваються маніпуляції свідомістю шляхом надання неповної

OPEN POST

Секція 3 Організаційно-педагогічні умови формування безпечної поведінки здобувачів освіти в Інтернеті

ФОРМУВАННЯ У СТУДЕНТІВ НАВІКІВ БЕЗПЕЧНОЇ РОБОТИ В МЕРЕЖІ ІНТЕРНЕТ ПРИ ДИСТАНЦІЙНОМУ НАВЧАННІ.

Марія-Вікторія ПОЛЕЦЬ

Сьогодні, в умовах воєнного часу, найважливішим завданням, яке ставиться перед закладами освіти є створення безпечних умов навчання для здобувачів освіти і роботи для працівників. Вимоги до закладів освіти щодо організаційних заходів із цивільного захисту, техніки безпеки та охорони праці чітко окреслені і стандартизовані, а от питання забезпечення інформаційної безпеки учасників освітнього процесу при дистанційному навчанні ще ні.

Питання інформаційної безпеки та безпечної роботи в мережі Інтернет учасників освітнього процесу не нове і постає перед закладами освіти не один рік. Однак, зараз, з початком масового переходу закладів освіти на дистанційне навчання, а тим паче у воєнний час, ця проблема постала особливо гостро. При дистанційному навчанні фактично освітній процес перейшов в онлайн-формат: навчальні заняття та виконання домашніх завдань відбуваються засобами освітніх інтернет-платформ, інтернет-сервісів, віртуальних навчальних середовищ, мобільних додатків, спеціалізованого програмного забезпечення, тощо. Саме тому здобувачі освіти та педагоги повинні бути обізнані у питанні інформаційної безпеки та володіти навиками безпечної роботи в мережі Інтернет.

Для того, щоб сформувати вище вказані навички відповідно до ролі учасників освітнього процесу, закладам освіти необхідно опрацювати загальні рекомендації міжнародних і державних відомств, установ, спеціальних організацій (для прикладу, матеріали зібрані та структуровані Інститутом модернізації змісту освіти [1]), розробити методичні рекомендації та провести інструктажі з інформаційної безпеки та безпечної роботи у мережі Інтернет. При розробці рекомендацій та проведенні інструктажів треба обов'язково

OPEN POST

Юлія Британ,

канд. пед. наук, доцент кафедри

філологічних дисциплін та методики їх викладання,

Чернівецький обласний інститут післядипломної

педагогічної освіти імені К. Д. Ушинського

РЕСУРСИ БРИТАНСЬКОЇ РАДИ ДЛЯ ФОРМУВАННЯ НАВИЧОК БЕЗПЕЧНОГО КОРИСТУВАННЯ ІНТЕРНЕТОМ НА УРОКАХ АНГЛІЙСЬКОЇ МОВИ В НОВІЙ УКРАЇНСЬКІЙ ШКОЛІ

У тезах доповіді наводимо покликання на проаналізовані матеріали Британської Ради (за сайтом LearnEnglish Kids та LearnEnglish Teens), які спрямовані на одночасне ефективне вдосконалення у здобувачів освіти англійської комунікативної компетентності, формування навичок безпечного користування Інтернет-ресурсами та засвоєння правил коректного поводження в онлайн-середовищі.

Теоретичний аналіз досліджень доводить необхідність розширення проблеми безпеки користування Інтернет-середовищем на уроках англійської мови в контексті вимог Нової української школи (НУШ). У межах доповіді спираємося на наукові здобутки в галузі інформаційно-комунікаційних технологій, медіакомпетентності та медіаосвіти, зокрема актуальні фахові публікації Британської Ради (*The British Council*) та "Лабораторії медіаосвіти" (*Media Education Lab*), які підтверджують актуальність зазначеної проблеми.

Вважаємо за доцільне застосовувати такі матеріали з автентичних Інтернет-ресурсів на уроках англійської мови (АМ), які поряд із формуванням іншомовної комунікативної компетентності готують учнів до безпечного використання онлайн-ресурсів та до безпечної онлайн-взаємодії.

Для учнів початкової школи на сайті *LearnEnglish Kids* освітньої платформи Британської Ради наведено перелік методичних матеріалів для використання на уроках АМ. Розглянемо декі з них.

OPEN POST

Напрям 10. Особливості виявлення, фіксації та розкриття правопорушень, вчинених відносно дітей з використанням мережі Інтернет.

ДОВЕДЕННЯ ДО САМОГУБСТВА ДІТЕЙ-УЧАСНИКІВ «ГРУП СМЕРТІ»: ЗБИРАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

Аліна ГУТНИК

Мобільний телефон та Інтернет-з'язок стали невід'ємними атрибутами життя кожної людини. На сьогодні діти практично з пелюшок вміють користуватись різними гаджетами, вмикати ігри, записувати відео тощо. Велику популярність серед дітей завоювали соціальні мережі, через які діти не тільки комунікують, але й беруть участь у різних флешмобах та Інтернет-іграх. Проте, через свій вік діти не завжди можуть оцінити ризики і небезпеку такої участі. Зокрема з'являються нові небезпечні явища, такі як кіберсуїцидальність, психологічні маніпуляції, пов'язані з доведенням до самогубства через використання новітніх технологій (Гутник, 2021).

За період 2017-2021 рр. в Україні доступні надійні дані щодо загальної кількості дитячих самогубств та їх спроб, а також факти доведення до самогубства дітей іншими особами. Це пов'язано з тим, що офіційні статистичні дані різних суб'єктів (Держстату, Національної служби здоров'я, Офісу Генерального прокурора, Національної соціальної сервісної служби України, Управління ювенальної превенції Національної поліції України, Департаменту Національних «гарячих ліній» та соціальної допомоги ГО «Ла Страда Україна»), залучених до реагування на факти самогубств суттєво відрізняється. Водночас дитячі самогубства мають дуже низький рівень латентності, адже всі випадки кваліфікуються за ст. 115 КК або ч. 3 ст. 120 КК. Проте багато фактів суїцидальних спроб взагалі не фіксуються через те що ні батьки ні самі діти не звертаються за допомогою до психологів, медиків чи поліції що суттєво спотворює реальну картину рівня суїцидальної активності дітей [2, с. 18].

OPEN POST

Напрямок 2. Інформаційна безпека дітей під час війни
ЯК ВБЕРЕГТИ ДІТЕЙ ВІД НЕПРИСМНОСТЕЙ В ІНТЕРНЕТІ
Ірина КОВАЛЕНКО

Анотація: у статті розглянуто питання про інформаційну безпеку дітей під час війни, яка стосується захисту життєво важливих інтересів батьків і дітей. Безконтрольний доступ до Інтернету може мати негативні наслідки для дитини, тому робота у цьому напрямку для вихователя та батьків дуже важлива.

Ключові слова: інформаційна безпека, інтернет, інформація, сошмережа, інтернет – залежність.

Ми з вами вже не уявляємо свого життя без смарт телефону. Інформаційний простір дозволяє бути на зв'язку з рідними, дізнаватися останні новини з фронту, хоч якось знати про те, що відбувається навколо. Для дітей інтернет залишається світом розваг та спілкування з друзями. Працюючи у закладі дошкільної освіти, ми також часто маємо справу з новітніми гаджетами в роботі з дітьми. Наприклад, під час виконання роботи з малюками. Діти дошкільного віку не хочуть відлучатися від гаджет, якщо він вже у них є та намагаються покористуватися, якомога довше, заходять на небезпечні сторінки соціальних мереж. 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 інформацію використовують окупанти для військових нападів на українські міста.

Як захистити себе та дітей в інформаційному просторі під час війни?

Від чого варто захищати дитину.

Інформаційна безпека стосується захисту життєво важливих інтересів людини (і бізнесу глобально – суспільства, держави). Неправильна, неповна, невчасна інформація може нанести шкоду. Особливо вразливі у цьому контексті діти. Вони можуть не знати, яку інформацію можна викладати в мережу, а яку не варто. Навколи діти не можуть правильно зреагувати на матеріали з мережі з різних причин. Робота у цьому напрямку для вихователя та батьків дуже

OPEN POST

Напрямок 2. Інформаційна безпека дітей під час війни
БЕЗПЕЧНА ШКОЛА: ВИКЛИКИ СИСТЕМИ ОСВІТИ В УМОВАХ
СЬОГОДЕННЯ
Олена ТРЕТЬЯКОВА

Анотація. У статті розглянуто поняття, що таке безпечна школа, безпечний простір як захистити дітей в інформаційному просторі; засоби, які сприятимуть формуванню в учнів навиків онлайн-культури.

Ключові слова: безпека, безпечна школа, кібербулінг, учасники освітнього процесу, інформаційний простір.

Можливість отримати будь-яку інформацію не виходячи з дому – зараз це не фантастика, а реальність. І це стало можливим завдяки мережі «Інтернет». Окрім того, що інтернет дозволяє нам знайти потрібну інформацію, мережа «Інтернет» значно розширює коло нашого спілкування. І це стає можливим завдяки Viber, Telegram, Facebook.

Інтернет для наших учнів є важливою частиною життя. Те, що для нас, старшого покоління, є інновацією, для наших дітей – звична буденність. Вони швидко орієнтуються у віртуальному просторі, відкривають власні способи допущитися до новітніх можливостей інформаційно-комунікаційних технологій, винаходять свої уподобання, розвивають нові потреби. Часто все це залишається поза увагою дорослих, які не мають стільки часу, щоб пройтися туди ж шляхами інтернету, що і діти.

Інтернет на сучасному етапі його розвитку можна порівняти з Диким Заходом у той час, коли спить шериф. У чому ж головні небезпеки мережі «Інтернет»? Чим віртуальне інтернет-середовище відрізняється від реального? Від яких небезпек дорослі мають застерегти дитину, як допомогти та навчити захищати себе?

З метою надання інформації про небезпеку інтернету та формування в учнів навиків онлайн-культури варто використовувати в освітньому процесі такі інтернет-джерела:

OPEN POST

Напрямок 3. Організаційно-педагогічні умови формування безпечної
поведінки здобувачів освіти в Інтернеті

КІБЕРБЕЗПЕКА – ВАЖЛИВИЙ АСПЕКТ
ФОРМУВАННЯ ЦИФРОВОЇ ГРАМОТНОСТІ
СУЧАСНОГО ЗДОБУВАЧА ОСВІТИ

Ольга САМОФІЛОВА

Актуальність теми обумовлена проблемами, які виникають з проникненням глобальної мережі в усі сфери життєдіяльності сучасного суспільства. Інноваційні технології пропонують можливості кожному миттєво поринути у цифровий світ, просто натиснувши кнопку мишки. За допомогою комп'ютера або іншого пристрою, підключеному до Інтернету можна отримати небувалого рівня послуги та інформацію. Діти та підлітки стають користувачами цифрового онлайн-світу, який не має перешкод чи кордонів.

Однією з найгостріших проблем, яка турбує міжнародне співтовариство протягом останніх десятиліть у зв'язку з розвитком інформаційних технологій є злочинність у кіберпросторі – кібершахрайство [5], особистістю якого є ймовірність стати жертвою у власному будинку, на очах близьких людей. Кібершахраї знаходять своїх жертв, насамперед, серед дітей.

Людство потребує нових знань та вмінь, котрих не дають у закладах освіти.

Про актуальність та важливість теми свідчить значна кількість наукових праць: Бикова В.Ю., Бузова О.Ю., Деметієвської Н.П., аналіз яких дозволяє стверджувати, що проблеми кібербезпеки учасників освітнього процесу не зводяться лише до технічних аспектів захисту інформаційних ресурсів, у повному обсязі вони охоплюють такі види захисту, як правові, технічні, інформаційні, організаційні та психологічні, оскільки в останні роки населення

OPEN POST

Напрямок 3. Організаційно – педагогічні умови формування безпечної поведінки
здобувачів освіти.
ІНТЕРНЕТ І ДИТИНА.
Оксана МІРОНУК

Анотація: у статті подано інформацію про інтернет технології, війни привозати з комп'ютером і орієнтуватися в інтернет – просторі в сучасному суспільстві та використання комп'ютера дошкільному віці

Ключові слова: кіберграмотність, інтернет технології, інтернет простір, гаджети, цифрова компетентність, смарт дошка

Інтернет-технології стали природною частиною життя дітей і сучасної молоді. Неміння привозати з комп'ютером і орієнтуватися в інтернет-просторі в сучасному суспільстві можна порівняти з невмінням писати й читати. Комп'ютер є не тільки розвагою, але й способом спілкування, самовираження та розвитку. У кіберпросторі існує велика кількість спеціальних сайтів, адресованих дітям різного віку.

У час електроніки і інформатики ми швидко крокувати в ногу з технічним прогресом. Ми живемо в столітті інформації, в час, коли відбувається комп'ютерна революція і є свідками того, що комп'ютери вже зайняли мішні позиції в багатьох галузях сучасного життя, швидко проникають у заклади освіти і сім'ї. В сучасних умовах України комп'ютер є своєрідним «інтелектуальним зв'язком» і дозволяє людині вийти на новий інформаційний рівень.

Діти легко опановують різні технічні засоби й часто віддають перевагу іграм із гаджетами замість взаємодії з однокласниками. Тому важливо розуміти, що цифрова компетентність дитини – це не лише про технічні навички, а й про вміння користуватися гаджетами безпечно. Цифрова компетентність поєднує в собі сукупність знань, здібностей, особливостей характеру та поведінки, необхідних для того, щоб використовувати інформаційно-комунікаційні та

OPEN POST

Напрям 8. Безпечне спілкування онлайн: ризики, правила, механізми звернення про допомогу й захист.

ФОРМУВАННЯ МЕДІАГРАМОТНОСТІ СУЧАСНОЇ ДІТИНИ Наталія СОСНОВЕНКО

Сучасна людина постійно розвивається і вона не може бути остерою інформаційних медіапотоків. Більшість інформації вона отримує з мас-медіа, і головне питання полягає в тому, щоб визначити яка є найбільш релевантною. Постає питання, як у вирії мавіпулятивних технологій обрати достовірні ресурси. Важливо вміти працювати з інформаційним полем. Сьогодні вимагає від освітньої спільноти та батьків сприяти формуванню інформаційної культури. Важко переоцінити важливість вміння критично оцінювати інформацію, яку ми сприймаємо.

Медіа — це новий термін. Він походить від латинського mediūm — «посередник, середина». Слово «медіа» в українській мові — це буквально посередник між двома світами. «Медіа» містить у собі всі засоби комунікації для передачі інформації: відомлення, текст, музику або зображення [5].

Великий потік інформації призводить до того, що сучасна людина ризикує «потонути» в інформаційному морі. В сучасному світі важливо бути медіаграмотним та формувати культуру медіасприйняття у дітей. Що ж таке медіаграмотність? Сам термін означає здатність використовувати, аналізувати, оцінювати та передавати повідомлення у різних формах. Тобто фактично всі науковці сходяться на тому, що медіаграмотність — це набуті під час навчання навички аналізувати та оцінювати медіа. Канадський науковець і консультант з питань медіаграмотності Кріс Воренон вважає, що медіаграмотність — це результат медіаосвіти, вивчення медіа.

Медіаосвіта батьків, сьогодні, набуває все більшої актуальності, адже саме батьки повинні надати дітям можливість зрозуміти, як використовуватися мідіа в суспільстві, оволодіти навичками використання медіа в процесі

Напрям 4. Соціально-педагогічний вимір понять «цифрові сліди», «цифрові тіні».

«ЦИФРОВИЙ СЛІД» І «ЦИФРОВА ТІНЬ» ЯК ОСНОВНІ ЧИННИКИ ФОРМУВАННЯ ПОЗИТИВНОЇ ЦИФРОВОЇ РЕПУТАЦІЇ

Марина ОБІДЕННІКОВА

Щодня користувачі з власної волі вказують на онлайн - сторінках інформацію про себе: прізвище, ім'я, по-батькові, дату народження, сімейний стан, освіту, професію, місця, контактні телефони, адреси електронної пошти тощо. Таким чином, кожний користувач всевітньої павутини залишає після себе слід або цифровий відбиток. Він генерується під час перебування людини в цифровому просторі та дозволяє ідентифікувати користувача в Інтернеті. Проте, окрім «цифрових слідів», які люди залишають свідомо, є і така інформація, що заснована на прихованому зборі інформації без надання згоди користувача. Сукупність інформації, зібраною всевітньою мережею, формує цифрову репутацію людини.

Мета дослідження полягає в аналізі використання цифрового сліду і тіні як складових для формування позитивної цифрової репутації.

Цифровий слід являє собою сукупність інформації про відвідування сторінки у мережі, а також подання характеристик пристрою, за допомогою якого користувач здійснює вхід до Інтернету [1, с.91]. До того ж більшість програм на смартфоні вимагають доступ до списку контактів або вмісту календаря. Пошукові системи зберігають історію запитів, що можуть бути використані власниками Web-сайтів і рекламодавцями з метою ідентифікації та відстеження користувачів. Завдяки просторам мережі Інтернет щодня здійснюється безліч банківських переказів, створюються соціальні кампанії, відбувається процес навчання та спілкування. Публікації фотографій та текстів, репости, лайки сприймаються як прояви нашої особистості.

Цифрова тінь формується на основі зібраних мережею Інтернет даних користувача без його відома [1; 3]. Основним засобом формування цифрової тині є мобільні пристрої з камерою. Вони дозволяють людустві створювати

OPEN POST

УДК 347.121.1

Напрям 1. Соціально-педагогічний вимір поняття «права дитини в Інтернеті»

ПЕРСОНАЛЬНА ІНФОРМАЦІЯ ДІТИНИ В МЕРЕЖІ ІНТЕРНЕТ: ВИКЛИКИ СУЧАСНОСТІ

Тетяна Сергій

За останні тридцять років персональна інформація людини стала не тільки набором записів, статистичними даними або маркетинговим інструментом. Інформація про фізичну особу стала чи не найготовнішим джерелом суспільного пізнання, самопрезентації особи у сучасному соціумі, особистої ідентифікації та індивідуальності людини, організації спілкування, створення історії. Особливо це стало відчутним з появою та всевітнім розповсюдженням доступу до мережі Інтернет. Вочевидь, розуміння та регулювання обігу такої інформації повинна мати певну увагу як з боку держави, так і з боку суспільства в цілому.

І, якщо доросла людина, так чи інакше, володіє правовими механізмами захисту інформації стосовно себе, що може ширитися мережею, то діти становлять найуразливішу групу осіб, які фактично створюють незахищену персональну інформацію, що спричиняє у правовій системі держави грандіозний виклик.

Світове суспільство неодноразово вдавалося до визначення у міжнародних нормативно-правових актах певного обсягу персональної інформації дитини, але розвиток сучасних технологій шоразу випереджав законодавців.

Так, третім принципом Декларації прав дитини [1] встановлено, що дитині має належати від її народження право на ім'я і громадянство.

Статтею 8 Конвенції про права дитини [2] передбачено, що держави-учасниці зобов'язуються поважати право дитини на збереження індивідуальності, включаючи громадянство, ім'я та сімейні зв'язки, як

ОРГАНІЗАЦІЙНО-ПЕДАГОГІЧНІ УМОВИ ФОРМУВАННЯ БЕЗПЕЧНОЇ
ПОВЕДІНКИ ЗДОБУВАЧІВ ОСВІТИ В ІНТЕРНЕТІ

Громова Ольга Сергіївна
учитель фізики та математики
КЗ «Лозуватський ліцей»
Колчанівської територіальної громади
Кіровоградської області

В одному виступі висвітлюється особистий досвід роботи вчительки фізики та математики Громової Ольги Сергіївни з теми «Безпека дітей в Інтернеті». Податиться думки про роль вчителів та батьків у формуванні умов безпечної поведінки здобувачів освіти в Інтернеті.

З кожним новим поколінням зростає рівень проникнення Інтернету в сім'ї. На сьогодні внаслідок доступності Інтернету в Україні більшість шкіл працюють дистанційно і все більше дітей користуються Інтернетом для спілкування, пошуку інформації, ігор, завантаження мультимедійного контенту. Але з розширенням можливостей в онлайн збільшується і кількість ризиків. Чи ж роль та обов'язок у забезпеченні безпеки дітей в Інтернеті? Думку про те, що навчати дітей безпеці в Інтернеті повинні вчителі, розділяють 95% батьків і лише 13% самих вчителів.

Все частіше батьки і педагоги говорять про негативний вплив Інтернету на психологічний, емоційний та фізичний стан здоров'я школярів і сходяться на думці, що Інтернет більшою мірою відволікає школярів, ніж навчає.

За результатами педагогічних (Н. Анохіна, Н. Уїллард, Л. Сорочіна), психологічних (О. Войсунський, Т. Наумова, В. Фатурова), соціологічних (О. Горощко, С. Ковоплишків, Н. Коритнікова) досліджень доведено, що найбільш вразливими користувачами Інтернет-мережі є підлітки 13-15 років, які здійснюють пошукову, пізнавальну, комунікативну, ігрову, дозвілєву,

OPEN POST

OPEN POST

Напряг 7. Технологічні інструменти та рішення формування безпечного Інтернет-простору дитини.
БЕЗПЕКА ДІТЕЙ У ВІРТУАЛЬНОМУ СВІТІ: ЗАКОРДОННИЙ ДОСВІД
Ольга ЛУНГОЛ, Олександр РОЗУМЕНКО

Питання безпеки у віртуальному світі є актуальною проблемою сьогодення. Майже кожен третій користувач Інтернету є дитиною [1]. Діти виходять в Інтернет у все молодшому віці за допомогою різноманітних гаджетів. Молоде покоління проводить все більше часу в цифровому світі, переглядаючи соціальні мережі, граючи в онлайн-гри, користуючись мобільними додатками, дивлячись відео тощо. Особливо актуальна проблема в тому, що дуже часто перебування дітей у віртуальному просторі відбувається без нагляду дорослих. Молоде покоління може зіткнутися зі шкідливим вмістом і поведінкою у мережі Інтернет, такими як кібербулінг, кіберзалякування, сексуальні домагання, порнографічне володіння, шахрайство, маніпуляції тощо. Зважаючи на те, що в Інтернеті простір розширюється, в ньому з'являється все більше користувачів, зростає ризик, тому необхідні ефективні дії щодо запобігання небезпек віртуального світу для дітей.

Віртуальний простір не має фізичних меж. Тому важливим є вивчення міжнародного досвіду щодо забезпечення безпеки дітей в мережі Інтернет. Так, важливим кроком на міжнародній арені є розробка European strategy for a better internet for kids (BIK+) [2] – Стратегії кращого Інтернету для дітей (BIK+), яка ухвалена 11.05.2022 року і має на меті забезпечення захисту, поваги та розширення можливостей дітей в Інтернеті в новому Цифровому десятилітті відповідно до Європейських цифрових принципів [2]. BIK+ має на меті реалізацію трьох основних принципів: безпечний цифровий досвід, щоб захистити дітей від шкідливого та незаконного онлайн-контенту, поведінки, контактів і ризиків молодих користувачів, а також покращити їх онлайн добробуту через безпечне цифрове середовище, яке відповідає віку та створене таким чином, щоб поважати інтереси дітей; розширення цифрових

Напряг 2. Інформаційна безпека дітей під час війни.
БЕЗПЕКА ДІТЕЙ У ЦИФРОВОМУ ПРОСТОРІ В УМОВАХ ВОЄННОГО СТАНУ

Марина БАГАУТДІНОВА, Ольга ЛУНГОЛ

Необмежений доступ до Інтернет-ресурсів надає дітям і молоді широкі можливості отримання нової інформації, вивчення культури, спілкування з однодумцями незалежно від фізичного місцезнаходження, доступ до цифрових розваг, можливості розвитку, творчості, реалізації креативності тощо. Однак поряд з багатьма надзвичайними перевагами відкритого доступу до неоскнених ресурсів цифрового світу, з'являється багато небезпек. Інтернет і пов'язані з ним технології сприяють створенню та розповсюдженню неприйнятних для дітей контенту і надають зловмисникам значні нові можливості для встановлення контактів з дітьми в Інтернеті. У зв'язку із збільшенням небезпек у віртуальному світі через контакти, пов'язані із воєнним станом на території нашої країни, за останній час збільшився об'єм небезпечного контенту, що загрожують життю молодого покоління. Зокрема, фахівці Міністерства освіти і науки рекомендують батькам встановити контроль за використанням Інтернету на дітей та розробляють рекомендації для проведення додаткових профілактичних заходів з боку закладів освіти серед дітей та інформування батьків [1]. Актуальність проведення подібних заходів зумовлена збільшенням тривалості перебування дітей в Інтернеті, до того ж в переважній більшості випадків без контролю дорослих. Цьому ще сприяло введення дистанційного або змішаного навчання спочатку через глобальний вплив коронавірусної інфекції COVID-19, а далі – вислідок повномасштабного вторгнення росії на територію України. Тому, важливо створити умови, за яких у молодого покоління будуть формуватися навички безпечної поведінки в Інтернет-просторі.

Існує низка потенційних небезпек в Інтернеті для дітей, але серед найактуальніших ризиків, з якими стикається більшість дітей ми виділимо:

OPEN POST

OPEN POST

Напряг 2. Інформаційна безпека дітей під час війни.

ІНФОРМАЦІЙНА БЕЗПЕКА ДІТЕЙ ПІД ЧАС ВІЙНИ: ДЕЯКІ АСПЕКТИ ТА ПЕРСПЕКТИВИ ПРОТЯГІ НЕГАТИВНИМ ВПЛИВАМ
Тетяна ПАВЛЕНКО

3 квітня 2019 року світ стикнувся з драматичними подіями, пов'язаними зі швидкою появою та розповсюдженням нового коронавірусу, що привело до масової ізоляції людей по всьому світу, а відтак одним з найбільш поширених способів комунікації серед людей в цілому, і серед дітей та підлітків зокрема, стали соціальні мережі. І якщо з початку 2022 року ситуація у світі щодо ізоляції людей практично кардинально змінилася, у зв'язку зі зняттям «коронавірусних обмежень», то Україна стикнулася зі ще більшим викликом – відкритою збройною агресією Російської Федерації (далі – РФ) проти України. Що знову привело до того, що більшість соціальних контактів як дорослих, так і дітей та підлітків втрачається. Особливо це стосується саме дітей та підлітків, адже вони вимушені разом з батьками покинути своє звичне життя та переїжджати або до інших регіонів України, або до інших країн, а відтак відбувається втрата звичного способу спілкування. Крім того, дітям, які перебувають в Україні далеко не завжди безпечно перебувати на вулицях, що знову ж таки тягне за собою втрату «оживого» спілкування, навчальний процес переважно відбувається у дистанційному форматі. Соціальна, інформаційна, економічна напруга, у якій перебувають батьки, наважд, досить часто приводить до того, що левову частину вільного часу діти проводять саме у мережі Інтернет, до того ж переважно без контролю з боку батьків. Безумовно, що у сучасних умовах без використання мережі Інтернет ми не можемо уявити своє життя. Саме у режимі онлайн виконуються важливі для реального життя завдання (діти мали можливість навчатися під час карантину і мають таку можливість під час війни (хоча зараз така можливість і супроводжується ризиком перехоод, оскільки, саме під час занять не завжди є світло, стабільний Інтернет

¹ За даними ЮНІСЕФ станом на 12 квітня 2022 року 7,1 мільярд осіб в Україні, зокрема 2,8 мільярд дітей, є активними користувачами Інтернету [1, с. 3].

OPEN POST

OPEN POST

6. Небезпечне спілкування онлайн: ризики, правила, механізми звернення про допомогу й захист.

ЗАБЕЗПЕЧЕННЯ ПСИХОЛОГІЧНОГО СУПРОВОДУ УЧАСНИКІВ ОСВІТЬОГО ПРОЦЕСУ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

Людмила САВЧЕНКО, Тимур САВЧЕНКО, Дарина САВЧЕНКО

Увага до освіти та виховання дітей, захисту та дотримання прав завжди були серед пріоритетів Української держави. Ідеї розвитку, миру, патріотизму, демократії, верховенства права, недискримінації, справедливості, поваги до особистості, любові до рідних та близьких, самореалізації та служіння країні та народові є стержнем навчального та виховного процесів, так само, як і фактова відповідь на вимоги та виклики, з якими стикається суспільство.

Таким викликом для України на початку 2014 року стали анексія Автономної Республіки Крим та окупація територіями утримуваними за підтримки Російської Федерації територій Донецької та Луганської областей. 24 лютого 2022 року Російська Федерація розпочала новий етап воєнної агресії проти України, повномасштабний вступ війни виснажує нас фізично та психологічно. Попри те, що наша психіка здатна адаптуватися під будь-які складові, кожен день бойових дій у рідній країні пережити надзвичайно складно. У цей непростий час варто підтримувати себе, рідних та близьких. Це життєво необхідно для того, щоб зберегти здоров'я – фізичне та психологічне.

Психологічний стан та психічне здоров'я під час військових дій є вкрай важливим. Багато людей переживають виснаження, спустошення, втому, відчувують тривогу й паніку, екстремальну ситуацію. Сьогодні всі учасники освітнього процесу більш, ніж будь-коли раніше, потребують психологічної підтримки і допомоги. Одним із важливих пріоритетів в діяльності закладів освіти є забезпечення психологічної стійкості учасників освітнього процесу, які страждають від російської воєнної агресії, та емоційна підтримка.

6. Небезпечне спілкування онлайн, ризики, правила, механізми звернення про допомогу й захист.

ОНЛАЙН РИЗИКИ У ВІРТУАЛЬНОМУ СЕРЕДОВИЩІ
Світлана НАРОЛЬСЬКА
Владислав НАРОЛЬСЬКИЙ

У зв'язку з глобальним впливом COVID-19 та війною в Україні освітній процес у закладах освіти перейшов на дистанційну та змішану форму навчання, і молоді проводять дедалі більше часу в Інтернеті.

Інтернет - це важливий чинник соціалізації сучасної дитини, взаємодія з яким неоднозначно впливає на її здоров'я та соціальне становлення.

Сьогодні Інтернет-мережа стає для підлітків тим соціалізаційним простором, у якому вони задовольняють потреби самостійності, самоствердження, розширення соціальних контактів. Разом з багатьма перевагами Інтернет-мережа містить значну кількість ризиків, з якими стикається молодь під час своєї діяльності в віртуальному просторі. Саме молодь є однією з малозахисних шпильок цієї ситуації.

Міністерство освіти і науки надзвичайно стурбоване трагічними подіями, що сталися з підлітками через небезпечні ігри в соціальних мережах. Цифрове середовище, дійсно, є небезпечнішим, ніж здається, адже, підлітки можуть сприяти своїю активність у соціальних мережах як гру та не розуміти наслідків своїх дій, що може призводити до катастрофічних випадків. Саме, створення безпечного освітнього середовища, зокрема в Інтернеті, формування навичок цифрової грамотності та поведінки у підлітків у Всесвітній мережі, соціально-емоційна грамотність є важливими завданнями для Міністерства.

Використовуючи Інтернет для спілкування у соціальних мережах, підлітки можуть зіштовхнутися з різноманітними ризикованими чинниками, такими як:

- Ризик взаємозв'язку: доступність персональної інформації під зворотного зв'язку.



Напрямок 5. Створення якісного безпечного українського контенту в мережі

Інтернет: тренди, ролі, можливості.
СТВОРЕННЯ ЯКІСНОГО БЕЗПЕЧНОГО УКРАЇНСЬКОГО КОНТЕНТУ ЗА ДОПОМОГОЮ БЛОГІВ, ЮТУБ-КАНАЛІВ, ТЕЛЕГРАМ-КАНАЛІВ, СОЦІАЛЬНИХ МЕРЕЖ
Оксана КІЗИМЕНКО

Наше сьогоднішнє та майбутнє – це життя та праця в новому цифровому суспільстві, у якому володіння ІКТ є запорукою успіху. Перед учителем регулярно постає питання: як зацікавити учнів темою, як краще пояснити матеріал, якими способами розвивати навички учнів, як зробити навчання ефективним. Раніше учні озброювалися лише системою знань, умінь і навичок, зараз – повинні бути підготовлені до життєдіяльності, здатні активно і творчо працювати, діяти, саморозвиватися. Для покращення якості знань учнів час вимагає пошуку нових шляхів навчання.

Організація роботи з дітьми в час дистанційного та змішаного навчання набула нових форм. Завданнями освіти стали блоги, ютуб-канали, телеграм-канали, соціальні мережі, освітні проєкти «На Урок» та «Всесвіта». Саме там вчительська спільнота розширює матеріал: актуальну інформацію, розробки заходів, виховні години, квести, флешмоби, акції, челенджи, фотоконкурси тощо. Під час проведення такої роботи передбачені різні форми: індивідуальні, парні, групові.

Одним із головних пріоритетів сучасної освітньої політики стало формування в сучасній молоді національних суспільно-державних цінностей як цінностей підприжиття української ідентичності. У цей нелегкий час, коли війна принищує щастя дитинства, учні беруть активну участь у різних заходах:

- Міжнародному багатожанровому онлайн-проєкті «Діти за мир»;
- Всеукраїнському конкурсі «Ми з Україною»;

OPEN POST

OPEN POST

Напрямок 3. Організаційно-педагогічні умови формування безпечної поведінки здобувачів освіти в Інтернеті.

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ПРОЦЕСУ ФОРМУВАННЯ БЕЗПЕЧНОЇ ПОВЕДІНКИ ЗДОБУВАЧІВ ОСВІТИ В ІНТЕРНЕТІ. PRO ET CONTRA

Ірина МАНЬКО

Ключові слова: здобувачі освіти, Інтернет, безпека, заклад освіти, держава, кіберполіція, нормативно-правова база, закон.

Мета статті провести аналіз нормативно правової бази, що стосується забезпечення процесу формування безпечної поведінки дітей та підлітків у мережі Інтернет, визначити хто серед державних структур, закладів освіти чи інших організацій, має займатися цією проблематикою. Також, проілюструвати чи стосуються відповідні нормативно-правові документи конкретно безпеки дітей в мережі, та наскільки коректно вони рекомундації.

Постановка проблеми. Проблема безпеки в комп'ютерній мережі Інтернет стала тодією невідомістю та дитиним інструментом в процесі становлення сучасного інформаційного суспільства. Мережа Інтернет – це гібридний майданчик без кордонів для обміну думками, пропаганда певних моделей поведінки, способу мислення, світогляду, цінностей тощо. Більше того, начебто не реальне перебування людини у мережі акумулюється у реальні наслідки її дій у світі дійсному. Тож, не має сумніву, що ця сфера потребує нормативно-правового регулювання, як і на рівні окремих держав, так і на міждержавних рівнях. А визначені правила поведінки мають стосуватися кожного користувача чи категорії користувачів, і переслідувати за ним певний вид відповідальності чи обмежень. Однак, коли ми звужуємо коло дослідження, і питаємо для себе прагнемо дослідити саме український контекст, та конкретно питання залучення окремих державних структур у забезпечення процесу формування безпечної поведінки здобувачів освіти в Інтернеті, то потребуємо докласти більше зусиль, щоб зрозуміти, кому мають належати такі функції, яка



Напрямок 2. Інформаційна безпека дітей під час війни.
ЩОДО ОКРЕМИХ ПИТАНЬ ПРОТІДЦІ ВІТЯГВАННЯ НЕПОВНОЛІТНІХ У ПОСОБИЩІ ВІЙСЬКАМ АГРЕСОРА НА ТЕРИТОРІЇ УКРАЇНИ

Марія Д'ЯЧКОВА, Владислав СІДОРЧУК

Наше дослідження ми вирішили присвятити дітям (під дітьми ми розуміємо осіб до досягнення ними 18-річного віку, окрім рідких випадків емансипації), які невинувато стають заручниками втягнення їх у вчинення кримінальних правопорушень, в тому числі і у тяжкі чи особливо тяжкі злочини військових країни агресора. Особливістю даної ситуації є те, що особи до 18 річного віку в силу особливостей психіко-фізіологічного розвитку, на фоні частих дезінформаційних впливів, не в змозі повною мірою оцінювати особливості ситуації в яку вони потрапили і можливі кримінально-правові наслідки своїх дій. А отже, важко буде ефективно протидіяти або намагатися протидіяти незаконному впливу який здійснюється на них.

Варто зазначити, що з урахуванням способу взаємодії військових країни агресора, можна виділити наступні можливі види взаємодії їх з дітьми:

- прямий вплив на дітей з метою втягнення їх для пособництва військовим країни агресора. Здійснюється безпосередньо шляхом спілкування і вербального впливу на дітей.
- опосередкований вплив на дітей з метою втягнення їх для пособництва військовим країни агресора. Здійснюється опосередковано за допомогою засобів зв'язку.

Зв'язуючи на обмеженість роботи певним об'ємом, а також на напрям конференції нами було прийнято рішення охарактеризувати опосередкований вид впливу на дітей з метою втягнення їх для пособництва військовим країни агресора. Щодо наявності відповідної проблематики, то вона висвітлювалась на офіційних ресурсах Служби безпеки України: «СБУ звертається до всіх батьків

OPEN POST

OPEN POST

Напряг 2. Інформаційна безпека дітей під час війни.

Цифрова гігієна

Катерина Деченко

Формування ключових та стійких компетенцій у дітей про безпечну поведінку під час війни та після її завершення – одне з головних завдань батьків та освітян.

З 24 лютого 2022 року питання безпеки вишло на інший рівень. Нині воєнні ризики є частиною життя, тому мислячи про готовність захистити себе і дітей.

Освітній проєкт #stop_sexting створив уроки щодо безпечної поведінки під час війни трьох категорій. Такі уроки були представлені під час вебінару «Ключові навички дітей шкільного віку у воєнні часи. Як навчити дітей безпечної поведінки». До такої роботи було залучено понад 2 тис. учителів з усіх куточків України.

#stop_sexting – найбільш актуальний проєкт щодо захисту дітей в Інтернеті. Тому, слід визначити, чи це інформаційна безпека?

Інформаційна безпека (InfoSec) – це стан захищеності, набір процедур та інструментів, які захищають усю делікатну інформацію від неавторизованого використання, несанкціонованого доступу, псування або знищення.

Загроза інформаційної безпеки – сукупність умов і факторів, що створюють небезпеку порушення інформаційної безпеки. Під загрозою розуміється потенційно можлива подія, дія, процес або явище, які можуть призвести до заподіяння шкоди чим-небудь інтересам.

Інформаційний простір дозволяє бути на зв'язку з рідними, дізнаватися 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.



OPEN POST

Напряг 2. Інформаційна безпека дітей під час війни.

ІНФОРМАЦІЙНА ВІЙНА: ЯК ВИТІТИ ІЗ НЕЇ ПЕРЕМОЖЦЕМ?

Яна СУДАК

Усі ви мабуть звикли, що інтернет наш друг? Ми йдемо туди, щоб знайти необхідну інформацію: правило з української мови, формулу з математики, поспілкуватися з друзями в чаті, подивитися цікаве відео у YouTube чи TikTok, або ж потрапити на онлайн-урок. А останній часом ми йдемо туди аби дізнатися останні новини: чи наступають вже наша Збройні Сили та коли закінчиться війна?

Однак є одна важлива річ, яку нам усім потрібно пам'ятати: під час війни інтернет також стає полем бою. Подібно до реального поля бою тут відбуваються ворожі атаки, які мають назву ІПО (інформаційно-психологічно спецоперація).

Якщо ви в пам'яті та не можете відірватися від новин, або навпаки переповнені ейфорією, то ви – ціль інформаційної атаки від удару агресора.

Дружі, в цей складний час варто спостерігати за своїм моральним станом. Від бойового духу залежить те, як ви фізично будете переносити стрес!

Наразі війна відбувається не лише за допомогою зброї на землі, воді та у повітрі, а й на полі бою соцмереж та всього інформаційного простору.

Ворог проводить їх у різних соцмережах, телеграм та ютуб-каналах аби дезінформувати нас з вами. Дяк чого ворог це робить? І навіщо йому атакувати дітей? – заштегає ви. Таким чином ворожі операційні спецпроєкти вирішують справжні оперативні задачі. Наприклад, підкачуючи інформацію про непереможність російської армії, чи про загрозу ракетних ударів. Він намагаться нас залкати. А вже, з деморалізованим суспільством воювати набагато легше.

За останні вісім років український інформаційний простір зазнав певних покривень – більшість ЗМІ та медіа агресора були зруйновані для трансляції в Україні. Отже мовлення зі злочинними меседжами проти української



OPEN POST

Напряг 2. Інформаційна безпека дітей під час війни.

КІБЕРБЕЗПЕКА ТА ОТРИМАННЯ НЕДОСТОВІРНОЇ ІНФОРМАЦІЇ (ФЕЙКІВ) В УМОВАХ ВІЙНИ

Людямила САВЧЕНКО, Ангеліна СІНЧЕНКОВА, Ганна ОТИЦЬ

Сьогодні Україна переживає нелегкий період у забезпеченні національної безпеки, проходячи через купу загроз, пов'язаних із гібридною війною, де часто використовуються прийоми дезінформації та поширюються фейкові новини з метою дестабілізації ситуації в країні. Інформаційне вторгнення, маніпуляції, застосування соціально-психологічного впливу є серйозною загрозою як головним засадам демократичного суспільства, так і особистій інформаційно-психологічній безпеці громадян, у тому числі – загрозою є застосування фейків з метою політичного впливу та здійснення політичних завдань.

На сьогодні інформація є не тільки можливістю передачі знань, подій, описати емоції або почуття, не потонути в інформації, яка може не лише маніпулювати свідомістю, а й вбивати, адже за допомогою інформації можна зробити певні наші, думки, ментальність – це дозволяє формувати негативне та вороже ставлення до подій, особистостей, а також думок тощо. Саме в період військової агресії Російської Федерації у 2022 році та війни з Україною, інформація набуває важливого та смертельного значення. Інформація – це надзвичайний інструмент та механізм маніпулювання будь-якими подіями, наслідками подій, суспільною думкою, формувати та впливати на певну оцінку подій тощо.

Інтернет і гаджети – це можливість бути на зв'язку зі своїми рідними та друзями. Діти та підлітки зараз проводять багато часу в інтернеті, зокрема у соцмережах, дивляться улюблених блогерів, спілкуються з однолітками.

Проте, тут на них може чатувати небезпека. Українці думають, що досконалим знають методи російської пропаганди. Але «розп'яті хлопчики» залишилися у минулому. Нині використовується вичищеніша інформаційна зброя. Відшукати болючу тему, сформувати у суспільстві протилежні погляди, знайти людей, які їх поділяють, та підбурювати їх один проти одного.



OPEN POST

Напряг 2. Інформаційна безпека дітей під час війни

ІНФОРМАЦІЙНИЙ ПРОСТІР ДІТЕЙ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

Ольга РОХМАЦЬ

Приблизно 82% українців користуються Інтернетом хоча б раз на тиждень, із них 78% щодня чи майже щодня [3]. Інформаційна безпека стосується захисту життєво важливих інтересів людини (і більш глобально – суспільства, держави). Неправдива, неповна, невчасна інформація може нанести шкоду.

Нині, коли на території України ведуться повномасштабні бої, війна триває і в Інтернеті. У складні для нашої країни часи важливо захищати себе не лише фізично, а й інформаційно. В умовах війни росії проти нашої держави ми дуже часто стикаємось з фейками, дезінформацією, інформаційними атаками. Ворог також може перехоплювати повідомлення в чаті й групі, щоб дізнатися інформацію, зламувати акунти, а в умовах війни передбачає ослаблення моральних і матеріальних сил громадянина, а також посилення власних інформаційних сил. Усе це окупанти роблять для того, щоб українці втратили віру в перемогу й опустити руки, тому шкідлива спільнота має пам'ятати про свою кібербезпеку.

На сьогодні потік інформації настільки потужний, що дорослим людям часом буває дуже складно орієнтуватися в новинах, а про дітей – годі й казати. Саме тому надзвичайно важливо навчити шкільну спільноту відповідально і свідомо споживати інформацію так, щоб не наразити себе та інших на небезпеку, не стати жертвою обману, відділити корисну інформацію від непотрібної чи шкідливої.

В ході інформаційної війни використовуються пропагандистські засоби, що впливають на свідомість людини ідеологічного та емоційного характеру. Інформаційні війни безпосередньо не призводять до кровопролиття або



OPEN POST

Напрямок 4. Соціально-педагогічний вивір понять «цифрові сліди», «цифрові тіні».

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ ЦИФРОВИХ СЛІДІВ ТА ЦИФРОВИХ ТІНЕЙ ДІЯЛЬНОСТІ ДІТЕЙ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Дмитро ДОЦЕНКО

Цифрові сліди та тіні діяльності дітей все частіше стають предметом дослідження та уваги освітян та батьків. Зі зростанням доступу до Інтернету та цифрових медіа з'являються такі загрози, як кібербулінг, онлайн-шкрявство та небезпечний контент. Крім того, навчання дітей безпечно використовувати цифрові пристрої є довгим та складним процесом. Багато часу потребує вивчення безлічі додатків, веб-сервісів та платформ, які можуть бути використані в освітній діяльності. Тому актуальним сьогодні є використання технологій штучного інтелекту (ШІ) для розв'язання значущої проблеми.

Аналіз наукових досліджень свідчить, що інноваційні технології штучного інтелекту використовують різні алгоритми та підходи для моніторингу поведінки дітей в Інтернеті та автоматичної оцінки потенційних ризиків або загроз. Завдяки використанню алгоритмів штучного інтелекту можна швидко аналізувати великі масиви даних, які отримані під час онлайн-активності. Зазначені алгоритми допомагають ідентифікувати потенційно ризиковану поведінку або інтереси (кібербулінг, спокливання небезпечного контенту тощо). Крім того, алгоритми штучного інтелекту також дають можливість отримати уявлення про наміри користувачів шляхом відстеження мовних або візуальних тенденцій на основі аналізу коментарів або публікацій у відеохостингах.

Метою статті є огляд технологій штучного інтелекту та їх використання для оцінки цифрових слідів і тіней, що залишаються від діяльності дітей в інформаційному просторі.

OPEN POST

Напрямок 3. Організаційно-педагогічні умови формування безпечної поведінки здобувачів освіти в Інтернеті. ФОРМУВАННЯ БЕЗПЕЧНОЇ ПОВЕДІНКИ ПІДЛІТКІВ В ІНТЕРНЕТІ

Наталія ГРЯЗНОВА

Сьогодні неможливо уявити освічену людину, яка не володіє навичками роботи в Інтернеті, не використовує основні служби глобальної мережі, адже знання і уміння, що дають змогу пильно використовувати світовий інформаційний простір, є чи не найважливішою складовою інформаційної культури. Нині Інтернет став явищем загальнонаціональної культури – явищем зі своїми законами і правилами, неперерешеними перевагами та немінучими недоліками.

Нові інформаційні технології збільшують можливості школярів у пошуку навчальної інформації, культурного самовдосконалення, ознайомлення з традиціями різних країн, спілкування, обговорення своїх проблем тощо. Сьогодні Інтернет-мережа стає одним з основних соціалізаційних простором, у якому вони задовольняють свої потреби в самостійності, самоствердження, розширення соціальних контактів.

Тому проблема безпеки особистості в Інтернет-мережі залишається не менш актуальною. Адже Інтернет буває не лише приємним і корисним, але й становить потенційну небезпеку не тільки для комп'ютера й інформації, яка зберігається на ньому, а й для користувача, і особливо школяра в умовах дистанційного навчання, коли в мережі він проводить ще більше часу, а відтак і ще більше наражається на небезпеки: велику кількість спаму, неправдивої та недостовірної інформації; залучення через спілкування в Інтернет-мережі до асоціальних організацій; використання персональних даних користувачів Інтернет-мережі; відвідування сайтів агресивної та аутоагресивної спрямованості; залучення до онлайн-ворно індустрії; розповсюдження фото та відеофайлів із зображенням порнографії та насильства; неможливість видалення персональної інформації зі сторінок соціальних мереж, сайтів для знайомств та сайтів з «дорослим контентом»; спілкування та зустрічі з

OPEN POST

Напрямок 2. Інформаційна безпека дітей під час війни.

ІНФОРМАЦІЙНА БЕЗПЕКА ДІТЕЙ ПІД ЧАС ВІЙНИ: ДЕЯКІ АСПЕКТИ ТА ПЕРСПЕКТИВИ ПРОТЯГІ НЕГАТИВНИМ ВПЛИВАМ

Тетяна ПАВЛЕНКО

З кінця 2019 року світ стикнувся з драматичними подіями, пов'язаними зі швидкою появою та розповсюдженням нового коронавірусу, що призвело до масової ізоляції людей по всьому світу, а відтак одним з найбільш поширених способів комунікації серед людей в цілому, і серед дітей та підлітків зокрема, стали соціальні мережі. І якщо з початку 2022 року ситуація у світі щодо ізоляції людей практично кардинально змінилася, у зв'язку зі зняттям «коронавірусних обмежень», то Україна стикнулася зі ще більшим викликом – відкритою збройною агресією Російської Федерації (далі – РФ) проти України. Що знову призвело до того, що більшість соціальних контактів як дорослих, так і дітей та підлітків втрачається. Особливо це стосується саме дітей та підлітків, адже вони вимушені разом з батьками покинути своє звичне життя та переїжджати або до інших регіонів України, або до інших країн, а відтак відбувається втрата звичного способу спілкування. Крім того, дітям, які перебувають в Україні далеко не завжди безпечно перебувати на вулицях, що знову ж таки тягне за собою втрату «оживого» спілкування, навчальний процес переважно відбувається у дистанційному форматі. Соціальна, інформаційна, економічна напруга, у якій перебувають батьки, наваждь, досить часто приводить до того, що левову частину вільного часу діти проводять саме у мережі Інтернет, до того ж переважно без контролю з боку батьків. Безумовно, що у сучасних умовах без використання мережі Інтернет ми не можемо уявити своє життя. Саме у режимі онлайн виконуються важливі для реального життя завдання (діти мали можливість навчатися під час карантину і мають таку можливість під час війни (хоча зараз така можливість і супроводжується ризиком перехоод, оскільки, саме під час занять не завжди є світло, стабільний Інтернет

¹ За даними ЮНІСЕФ станом на 12 квітня 2022 року 7,1 млн осіб в Україні, наразі 2,8 млн дітей, є внутрішньо переміщеними особами [1, с. 3].

OPEN POST

Напрямок 5. Створення якісного безпечного українського контенту в мережі Інтернет: тренди, ролі, можливості.

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ УКРАЇНОМОВНОГО КONTENTУ В МЕРЕЖІ ІНТЕРНЕТ

Єлизавета ОРЛОВА, Ольга ЛУНГОЛ

Підлі 2022 року на території України стали поштовхом до масового переходу населення країни на використання української мови як у фізичному світі, так і у віртуальному. Дерусифікація громадського простору, стрімкий розвиток і популярність українського культурного продукту свідчать, що багато громадян України переосмислили й усвідомили важливість національного самовизначення у тому числі й через мову, рівень підтримки якої в суспільстві зростає чи не найбільше за роки незалежності України [1]. Відкритий воєнний напад росії на Україну сприяв більш активному обговоренню мовного питання як у спільноті, так і на державному рівні. Більшість українських блогерів, зокрема телебачення та журналістика, які до 2022 використовували російську мову, почали активно перемикатися на спілкування українською.

В Україні з 16 липня набудли чинності норми закону «Про забезпечення функціонування української мови як державної», що передбачають збільшення присутності української мови в публічному просторі, у тому числі в мережі Інтернет. Ці норми стосуються сфери культури й розваг, туристичного напрямку, книговидавництва та роботи книгарень, створення та демонстрування фільмів у кінотеатрах і на телебаченні тощо [2; 3]. Зокрема, з літа 2022 року всі фільми та серіали на телеканалах України мають транслювати державною мовою. Отже, фільми, створені іноземною мовою, мають показувати з дубляжем або озвучкою українською мовою. В той же час, на стрімінгових платформах разом з українськомовними версіями, фільми можуть містити аудіодоріжки іноземними мовами. Аналіз мови серіалів, проведений Секретаріатом Уповноваженого із захисту державної мови [2], засвідчив, що з 43 серіалів, які демонструвалися на 5-ти провідних телеканалах України з 1 по

OPEN POST

Напряг 6. Безпечне спілкування онлайн: ризики, правила, механізми звернення про допомогу й захист.

КОМУНІКАЦІЙНІ ЗАГРОЗИ БЕЗПЕЦІ ДІТНИНІ В ЦИФРОВОМУ СЕРЕДОВИЩІ Ірина ЛУБЕНЕЦЬ

Інтернет є невід'ємною частиною життя сучасного суспільства загалом та дітей, зокрема. Цифрове середовище має значний потенціал для розвитку та самореалізації особистості дитини. За допомогою ресурсів відкритих цифрових сховищ бібліотек, музеїв, сайтів освітнього, пізнавального та розважального характеру сучасні школярі мають можливість завантажувати оцифровані книги, музику, фотографії та ін. Завдяки новітнім технічним засобам діти навчаються, спілкуються з друзями та відпочивають. Інтернет для них є частиною життя, а віртуальний світ – засобом соціалізації. На жаль, офіційні статистика стосовно кількості дітей в Інтернеті відсутня, але згідно даних різних досліджень, найбільш активними інтернет-користувачами є неповнолітні [1, С.82; 2]. Більше того, Інтернет стрімко молодшає, а в сучасній Україні діти 4-6 років активно ним користуються, а сучасні гаджети грають роль цифрової няні. Хоча лише декілька років тому, вік інтернет-користувачів становив – 10 років [3, С.26]. Слід відмітити, що особливо різке збільшення кількості дітей, які вперше придбалися до онлайн-світу, щоб одержувати допомогу в навчанні та підтримувати соціальні взаємодії відбулось у період глобальної пандемії COVID-19 [4, С. 6].

Незважаючи на всі позитивні сторони, що надає цифрове середовище, не можна ігнорувати існування негативної складової. По-перше, це проблема, пов'язана із повним зануренням дитини у віртуальний світ, що є наслідком залежності від гаджетів та постійної онлайн-присутності, адже діти нерідко проводять в цифровому середовищі близько 5 годин, а деякі – завжди перебувають «онлайн» [5, С. 156].

По-друге, перебуваючи постійно «онлайн», піддаються ризик зіткнення з деякими загрозливими віртуального світу: від кібервильства, шахрайства та розповсюдження наркотичних речовин до тролінгу, секстингу та схизми до самотубства.

OPEN POST

Напряг 2. Інформаційна безпека дітей під час війни

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПІД ЧАС ВІЙНИ НА ОСНОВІ ЗАСТОСУВАННЯ ПЛАТФОРМИ МІЖУА ВІД КІБЕРПОЛІЦІЇ УКРАЇНИ Олександр СМІРНОВ

Інформаційна безпека дітей під час війни набуває особливої важливості. Безпека в Інтернеті, перш за все, починається вдома з батьків, які навчають своїх дітей про безпеку, які підстерігають онлайн. Реальність така, що багато дітей і підлітків краще, ніж їхні батьки, знайомі з кіберсвітом і різними програмами, які існують. Вони просто все не сприймають швидше. І, на жаль, батьки часто або не розуміють, або не знають, що їхні діти та підлітки роблять у цих програмах. І враховуючи, що споживання дітей і підлітків в Інтернеті відбувається практично на кожній онлайн-платформі, дуже важливо, щоб ви та ваші діти розуміли ризики, які існують в Інтернеті [1].

У даній роботі визначено основні методи кібератак і загрози та розглянуті наступні виклики інформаційної безпеки дітей та підлітків:

- Кіберзалучення (Кібербулінг)
- Кіберпереслідування.
- Доксінг (Doxxing).
- Шахрайство з шантажем (сексуальні вимоги).
- Крадіжка кредитної картки.
- Неправильні обмін інформацією.
- Розумні іграшки та підключені пристрої.
- Онлайн-догляд (онлайн-спокуса).
- Крадіжки особистих даних.
- Порнографія помсти (порнографія без згоди).
- Причлонування та шпигунство через веб-камеру.

Далі у роботі розглянуті тактики, яку використовують кіберзлочинці, щоб приховати або замаскувати свою особу та питання соціальної інженерії, її методи протидії їй.

OPEN POST

Напряг 8. Розвиток кіберграмотності педагога.
ШЛЯХИ ТА ДЖЕРЕЛА ВДОСКОНАЛЕННЯ КІБЕРГРАМОТНОСТІ
СУЧАСНОГО ПЕДАГОГА: ДЛЯ ЧОГО МЕНІ ЦЕ ПОТРІБНО?

Тіля САВІСЬКО

Питання кіберграмотності сучасного педагога в умовах дистанційної та змішаної форми навчання постає дуже гостро, адже на кожного вчителя-предметника, а не лише на вчителя інформатики, покладається велика відповідальність: педагог повинен вміти відрізнити офіційні джерела інформації і фейкові, фішингові матеріали, мати вміння критично оцінювати отриману інформацію та розпізнавати ПІСО; правильно та швидко реагувати на інформаційні «вкляди» шахрайського вмісту та вміти захистити себе та здобувачів освіти від можливих ризиків і небезпек у кіберпросторі.

Сучасна освіта робить непевнені кроки у напрямі поінформованого здобувачів освіти та педагогів про поняття інформаційної безпеки, критичного мислення та загрози Інтернету, зокрема, вивчення цих знань та вмінь діючі навчальні програми з інформатики не надають належного мізеру уваги, адже маєтись на увазі, що інформаційно-комунікаційна компетентність здобувачів освіти формуєть на кожному уроці. Проте, в реалії сьогодні, цього не достатньо. Коли система освіти залежна від неперезабуваних чинників, таких як: відключення електроенергії, часті повітряні тривоги, нестабільний доступ до Інтернету, вчитель намагається максимально швидко опрацювати навчальний матеріал, а на формування наскрізних змінь часу не вистачає. Стрімкий розвиток в галузі цифрового громадянства, поява нових технологій обумовлює і постійну появу все нових небезпек.

Ще однією перешкодою на шляху до формування інформаційної культури та кіберграмотності суспільства є те, що значна частина вчителів-предметників, які освоїли ІКТ на рівні мінімального базового рівня, не спроможні формувати в учнів зазначені компетентності, адже самі не володіють ними в необхідному обсязі, в той час, як саме ці навички є одними з ключових для спеціаліста, якого хочуть бачити роботодавці.

OPEN POST

Напряг 6. Безпечне спілкування онлайн: ризики, правила, механізми звернення про допомогу й захист

ВПЛИВ ПОРНОГРАФІЧНОЇ ПРОДУКЦІЇ НА МОЛОДУ ОСОБУ ТА ДЕЯКІ ПІДХОДИ У ПРОТИДІ АГРЕСИВНОМУ СЕКСУАЛЬНОМУ КОНТЕНТУ В ІНТЕРНЕТ-МЕРЕЖІ

Тарас ВАЙДА

Актуальність проблеми. У сучасних умовах поряд із значним позитивним значенням медіаресурсів у публічній діяльності особи (освітній, науковий, соціально-комунікативній, дозвілєвій та ін. сферах), а також активним використанням можливостей інтернету у різноманітних галузях виробництва українське суспільство стає свідком непоодиноких випадків негативного впливу сексуального інтернет-контенту на психіку чи навіть на деформацію моральної поведінки окремих його користувачів – доведення до самогубства малолітніх користувачів мережі, вбивств, вступання їх до «груп смерті», використання персональної фотографії в Інтернеті як способу шантажування людини, зокрема, порнопомсти, сексуального насильства, розповсюдження дитячої порнопродукції тощо.

Підтвердженням цієї точки зору багатьох вчених на підставу проблему та об'єктивного існування вищезазначеної негативної тенденції в українському суспільстві є той факт, що Україна, котра, зокрема, займає дев'яте місце в Європі за кількістю користувачів інтернету, посіла одинадцяте місце в рейтингу країн світу із найбільшою кількістю порносайтів. За даними американської компанії «MetaCler», яка склала цей рейтинг, в Україні 1,1 мільйонів сайтів такого спрямування. Лідером за кількістю сторінок для дорослих виявились США з 428 мільйонами сайтів (60% світового порноконтенту). До трійки лідерів рейтингу увійшли також Нідерланди (187 млн сайтів) і Великобританія (52 млн сторінок). У першій десятці опинилися Франція, Канада, Японія, Австралія, Британські Віргінські острови та Чехія. Росія посіла 18 місце в рейтингу з 638 тисячами порносайтів [1, с. 5].

OPEN POST

Напряж 5. Створення якісного безпечного українського контенту в мережі

Інтернет: тренди, ролі, можливості

**ФОРМУВАННЯ ЛІНГВОКУЛЬТУРОЛОГІЧНОЇ КОМПЕТЕНТНОСТІ
ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ ЗА ДОПОМОГОЮ ЯКІСНОГО
БЕЗПЕЧНОГО УКРАЇНЬСЬКОГО КОНТЕНТУ В МЕРЕЖІ ІНТЕРНЕТ**
Ірина ДАВИДЧЕНКО

На виконання Указу Президента України №64/2022 «Про введення воєнного стану в Україні», затвердженим Законом України «Про затвердження Указу Президента України «Про введення воєнного стану в Україні» від 24 лютого 2022 року №2102-IX» навчання здобувачів вищої денної та заочної форм навчання та проходження практики в закладах вищої освіти здійснюється у дистанційному (синхронному) або дистанційному (асинхронному) режимі віддалено з допомогою цифровізації.

Сьогодні в Україні відбувається швидке поширення використання інформаційного простору, сучасних технологій змішаного, дистанційного та електронного навчання. Також у сучасних умовах виникає потреба в отриманні вищої освіти дистанційно, що дає змогу навчатися без відриву від виробництва.

Одним із головних факторів, що прискорює формування і розвиток інформаційного суспільства, є Інтернет. Він став не лише глобальним засобом комунікацій без територіальних і національних кордонів, але й ефективним інструментом здобування освіти, досліджень, впливу на аудиторію.

Заклади освіти в Україні все частіше використовують сторінки у соціальних мережах для здобуття освіти. Здобувачі освіти проводять багато часу у таких мережах як Facebook, Instagram, TikTok. Безпека понад усе, тобто всі платформи намагаються посилювати правила конфіденційності та збереження користувацьких даних. Соціальні мережі стали каналом, де особистості транслюють свої успіхи у досягненні шлей сталого розвитку.

OPEN POST

2022 рік

Комп'ютерний заклад «Кіровоградський обласний інститут
підвищення кваліфікації освіти Ізени Василів Сухомлинського»
Кіровоградський науково-дослідний
експертно-криміналістичний центр МВС України
Центр інноваційних технологій навчально-наукового інституту
права, психології та інноваційної освіти Національного університету
«Львівська політехніка»
Громадська організація «Вікмедіа Україна»

I Всеукраїнська науково-практична конференція
**«БЕЗПЕКА ДИЦІТАЛЬНИХ КОМУНІКАЦІЙ ІНТЕРНЕТІ:
ПОПЕРЕДЖЕННЯ, ПРОБЛЕМИ, ВЗАЄМОДІЯ»**

<https://conf.org.ua>

07-10 лютого 2022 року

Кропивницький
2022

OPEN POST

Links

#	Summary	Type	Link
1		Video	https://youtu.be/263MxpWbkWw
2		Video	https://youtu.be/2F6DGv1oMXM
3		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/7f4cc343ca0a8b800cf6321d8ab224b1.docx
4		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/172c639996ea0ec1e93bdbb2229470b1.docx
5		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/ed73fb60c7828239465c57d80de3999b.docx
6		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/1a632fb5b4f12ef6fa5be57358d13f2d.doc
7		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/68237e03ed8c4f95405d9f36ff718ec9.doc
8		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/2120ad06058c0f1e7c6b95befc80b3e5.docx
9		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/19015054c8b75013e7638e25efe4043b.doc
10		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/96d1facc89976603e2ce13c43e867218.doc
11		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/0d3750010c345d09e2d71d97b8089bac.docx

12		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/1ad582b6b879a722cee6304b2e12d907.docx
13		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/cdaff1339751653ac4c510ee17de1b11.docx
14		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/c2d00cefbf2a1c97661b93b82ea87343.docx
15		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/2178bdac0f5d4fa214ee4a4cf424b341.docx
16		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/ac57d0b29990d62083d7f78f21959542.docx
17		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/bc435c4c04b4e723e8aa1c11d6a12d39.docx
18		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/361539880c2c42df241012849bcf5741.docx
19		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/6d7e06b51dbbe43e5f1c4f13ffd6a3a4.docx
20		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/af27592ae3a8e368258a3a8a5c2f4fa4.docx
21		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/bfb005bfb58993d538e56b6cdcb57756.docx
22		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/

			published/207673/files/d9bfbbaa289e368a1f424c6627733fc0.docx
23		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/11ed925fc29b4da025c3fa4664b68b55.doc
24		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/564c0b5fb0d067a5092ff870ae5f49a7.docx
25		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/8127e0867c0b9e61c4973e3aca4ac188.docx
26		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/bcac5f50dea859e2db7ae9d9d5d09aed.docx
27		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/f318c2c8747e1f458a215414053125ff.docx
28		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/c2b93dcbd9067cee90baf24305fb3cbb.docx
29		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/fdb433a906e900af1d35e0455de43be5.docx
30		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/ed8f49a956138414ecee76f2b0b5f682.docx
31		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/3d1aa9d0eb9714b3b88a78eb0cebba2f.docx
32		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/6a037dcad6f4b5d2b4c622bef821d51

			4.docx
33		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/c8dee5465c1406bd8d6e42b6aab80ba8.doc
34		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/0e5569474b170f781b8178790f1afd2f.docx
35		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/e9359ce55c6f33b9817fe55d66d0d96a.docx
36		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/f9d7b0422758b8765ca8676a03430d73.docx
37		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/648fa45086f9a4cea6e3684cbf91df93.docx
38		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/555a99ed7d63ea333c95b12569f8e696.docx
39		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/6b4de1cb5b3b1cc24a3cc5ea9cad43cc.doc
40		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/4c817546a2ed8d84d1c16fd03eea8a67.docx
41		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/8b4dc22a28a5d89f64fc0c37c3c8819.docx
42		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/7c7db6aae29fea470e7a4aee6d12c481.docx

43		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/f2a1b3cb18d93775b1e8e9978751a5eb.docx
44		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/68c3d2c56b0e474406c9a41ec6b02e72.docx
45		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/f85a8da197b4aa8df51d665c79a266c5.docx
46		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/c23de59d00bcf154a32553e5de7a0936.docx
47		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/5d9e1bcc256542ea14a6dedc54937f0b.doc
48		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/d989e63b39a15bc72bf48f08d307235b.docx
49		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/9260c16dbec7ede756f99120bdd33576.docx
50		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/b81405b1af58c529989653ec3cf766d5.docx
51		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/53c5659605cd3f2882fc1d9bea89a7b7.docx
52		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/c303cc38e3dfb736674b0de1ff9892c9.docx
53		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/

			published/207673/files/3d76ee823e4e57b26257c2cb279c4003.docx
54		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/0dcbe6f0cb11e07a602b6c7df14a46e1.docx
55		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/a5bac652229285a9f338fd3a69c98a8e.docx
56		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/a24eec547f8bd8520bee1e23dba54ddc.docx
57		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/ac6c338e68c4e2a2a4ae82333fe4a8e2.docx
58		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/827821637e73e185e3a4c1bc7dd9fed7.docx
59		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/784e90e9d4afb06d007ec7c04c0c7456.doc
60		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/8996868e9bb5c9f781cf9d1d91534a15.docx
61		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/25a067fecfd19fb5fa5bb987d28dcab9f.doc
62		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/files/bc4175b705f8ecbbcbb662ddee2cfd3b.docx
63		Document/ Media	https://netboardme-cf1.s3.amazonaws.com/published/207673/

			files/2ec7b546a12c7b606f8750a0e1057d13.pdf
--	--	--	--