



БІБЛІОТЕКА ТА ІНФОРМАЦІЙНА ГІГІЄНА В УМОВАХ ВІЙНИ

Методичний поради́ник бібліотекаря

Випуск 10



Чернігівська обласна універсальна наукова бібліотека
імені Софії та Олександра Русових

**БІБЛІОТЕКА ТА ІНФОРМАЦІЙНА ГІГІЄНА
В УМОВАХ ВІЙНИ**

Методичний poradник бібліотекаря

Вип. 10

Чернігів
2024

Укладач Ольга Шурубенко

Бібліотека та інформаційна гігієна в умовах війни : метод. poradник бібліотекаря / Черніг. ОУНБ ім. Софії та Олександра Русових ; уклад. О. Шурубенко ; відп. за вип. В. Примаєв. – Вип. 10. – Чернігів, 2024. – 35 с.

У методичному poradнику бібліотекаря розповідається про вплив інформації на якість нашого життя та здоров'я в умовах війни. Дається визначення поняття «інформаційна гігієна», наводяться правила, які допоможуть ефективніше фільтрувати інформацію під час війни, та поради як вберегтися від шахрайських дій в соціальних мережах.

У poradнику подано перелік інтернет-ресурсів, які дозволять безкоштовно поглибити знання з теми «Інформаційна гігієна» й надалі реалізувати їх на базі своєї бібліотеки, а також представлено досвід роботи бібліотек України в цьому напрямі.

Рекомендовано для бібліотекарів публічних, міських та сільських бібліотек.

ЗМІСТ

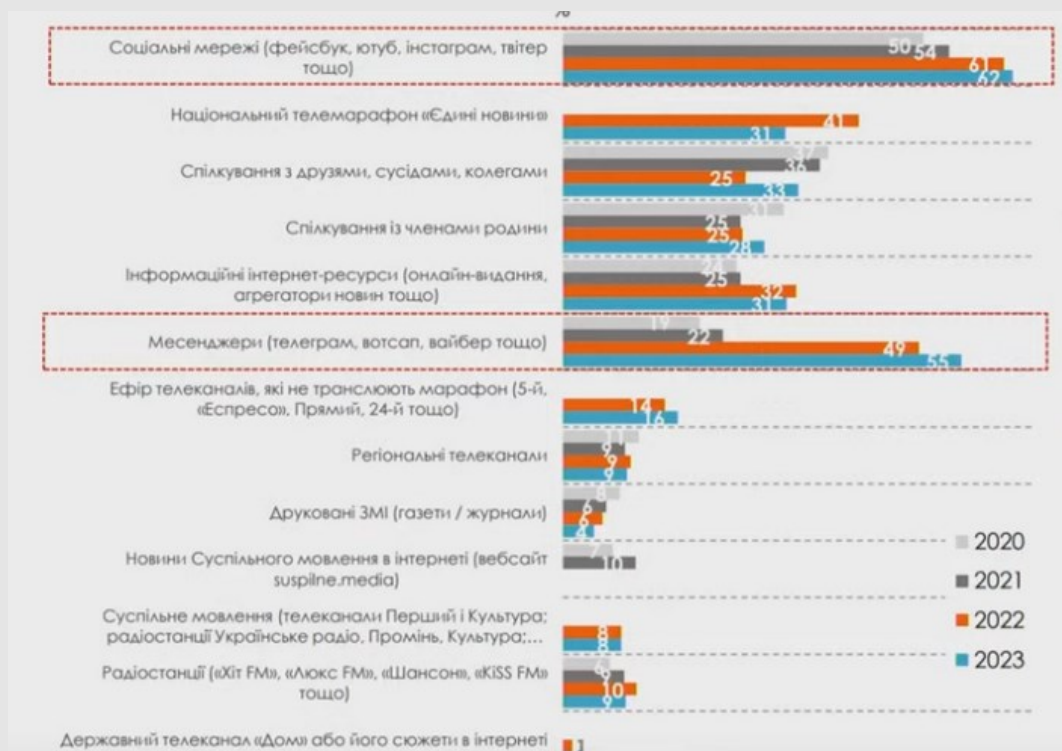
Звідки ми споживаємо інформацію?.....	5
Інформаційна гігієна як фактор збереження ментального здоров'я.....	7
Шахрайство у соціальних мережах: чи можна вберегтися?.....	16
Де вдосконалювати свої знання про інформаційну гігієну?.....	24
Досвід вітчизняних бібліотек.....	28
Джерела.....	32

ЗВІДКИ МИ СПОЖИВАЄМО ІНФОРМАЦІЮ?

Загальновідомим є той факт, що наш мозок запам'ятовує все, з чим доводиться мати справу. Інформація – це свого роду їжа для розуму, яку потрібно вибирати так само ретельно, як і продукти. Різноманітні новини, заголовки статей, картинки – все це накопичується у нашому мозку та призводить до інформаційного перенасичення, нервової напруги та хронічного стресу. Тож до споживання інформації треба ставитись критично.

Старша наукова співробітниця Інституту соціології НАН Марта Наумова розповіла, що за результатами щорічного дослідження «Індекс медіаграмотності української аудиторії» основним джерелом отримання суспільно-політичної інформації для українців у період воєнного стану є соціальні мережі і месенджери (Telegram, WhatsApp, Viber), а телебачення поступово втрачає свої позиції. Якщо говорити про «Єдиний телемарафон», то у 2022 році його дивилися 41% респондентів, а у 2023 році – тільки 31% опитаних. У віковій групі 18-65 років лише 32% опитаних відповіли, що дивилися телебачення останнього тижня, а головними джерелами інформації вказали соцмережі і месенджери. Ключовим джерелом інформації телебачення залишається для пенсіонерів.

За словами Марти Наумової, згідно з отриманими результатами, медіаграмотність 3% українців є низькою, у 21% – нижча за середню, 62% респондентів мають вищий за середній рівень медіаграмотності, 14% – високий.



Також результати дослідження свідчать про те, що у порівнянні з 2022 роком у 2023-му зросла кількість споживачів суспільно-політичного контенту в месенджерах (49% і 55%). З 25% до 33% зросла кількість аудиторії, яка отримує інформацію про суспільно-політичні новини у спілкуванні з друзями, сусідами, колегами.

Цінність актуальної інформації, особливо у критичних ситуаціях (повітряні тривоги, ворожі наступи тощо), важко переоцінити. Іноді вона може врятувати життя. Українці це знають не з чуток. Однак постійна перевірка сповіщень у соцмережах і Telegram-каналах може завдати шкоди здоров'ю – викликати інформаційну залежність, яка більш загострюється в умовах війни.

Результати опитування Київського міжнародного інституту соціології у 2023 році на замовлення Програми розвитку ООН (UNDP) в Україні за підтримки Швеції й у партнерстві з Міністерством цифрової трансформації України свідчать, що кількість українців, які щоденно користуються інтернетом, протягом року зросла з 72% до 80%. Починаючи з 2021 року цей показник збільшився на понад 10%. Ще 11% українців у 2023 році користувалися інтернетом нерегулярно: 2-3 години на тиждень і рідше. Не користувалися інтернетом узагалі 9% респондентів. За два роки (2021–2023) частка останніх зменшилася на 5%.

Отже, з досліджень бачимо, наскільки важливим є для нас інтернет, а особливо доступ до інтернету в період війни. Але під час користування інтернетом з метою споживання інформації треба пам'ятати про хворобу сучасного суспільства – інформаційну залежність.

ІНФОРМАЦІЙНА ГІГІЄНА ЯК ФАКТОР ЗБЕРЕЖЕННЯ МЕНТАЛЬНОГО ЗДОРОВ'Я

Здавалося б, ми все знаємо про інформаційну гігієну, вміємо відрізнити правду від брехні у медіапросторі, не ведемося на маніпулятивні дописи і т. д. Але чи це дійсно так?

Міністерство охорони здоров'я України оприлюднило інформацію про те, як впливає інформаційне середовище на психічне здоров'я людини. Постійна інформаційна напруга спричиняє порушення психологічного добробуту, безсоння, підвищений артеріальний тиск, пригнічений стан, депресивні та тривожні розлади, які ускладнюють якість життя, негативно впливають на емоції, а з часом і на фізичне здоров'я. Особливо відчутний взаємозв'язок між інформацією, яку ми щодня споживаємо, та психологічним здоров'ям у період війни. Численні публікації у різноманітних пабліках про наступи ворога, про масштабні обстріли, їхні наслідки, переживання за рідних, постійні сирени спонукають нас жити в стані хронічного стресу.

Що ж таке стрес?

До стресу можна або адаптуватись, або ж усунути його причину. Оскільки зупинити війну зараз ми

Стресом називають реакцію організму, яка виникає як відповідь на фізичну чи розумову напруженість або ж загрозу для життя. Під час війни поєднуються всі ці фактори, що значно ускладнює ситуацію.

не можемо, українцям доводиться пристосовуватись до нових реалій, і, зокрема, до того, що стрес тепер буде постійно присутній у нашому житті. Проте боротись із ним необхідно.

Одним зі способів боротьби зі стресом є захист від шкідливої інформації. Під час війни люди набагато частіше стежать за новинами, адже часто від цього залежить їхнє життя. Проте надмірна зацікавленість може перерости у своєрідну залежність. Також небезпечно черпати інформацію із неперевіраних джерел. Вони часто транслюють фейки, що збільшує тривожність та погіршує і так порушений ментальний стан. Для того, щоб черпати інформацію з правдивих джерел, треба орієнтуватися в цьому потоці – дбати про інформаційну гігієну.

Інформаційна гігієна – це фільтрація потоку отримуваної інформації, що допомагає не засмічувати голову фейками, протистояти шахрайству та не робити непотрібних помилок у момент паніки. Метою інформаційної гігієни є зниження негативного впливу інформації на психічний, фізичний і соціальний стани.

Термін «інформаційна гігієна» прийшов в ужиток у зв'язку з розвитком інформаційних технологій та набуттям людьми майже необмеженого доступу до потоків різного роду інформації. Адекватні реакції на будь-які новини і події, перевірка відомостей на предмет достовірності та дотримання простих правил цифрової безпеки є запорукою вдалої інформаційної гігієни.

Завдяки інтернету є безліч способів та інструментів, які дозволяють вплинути на емоційний стан людини, зробити її залежною, маніпулювати її свідомістю: це соціальні мережі (фейсбук, інстаграм, тікток, телеграм, твіттер...), іноземні медіа, блогери-інсайдери, ІПСО та багато інших. Такі терміни, як «інформаційна війна», «спеціальні психологічні операції», «пропаганда» чули всі. Але далеко не всі розуміють, як самих українців використовують для цих процесів та як наша поведінка ненавмисно стає допоміжним інструментом для ворога.

Подумаєте, до чого тут бібліотеки? Все просто: бібліотеки – це чудове місце для проведення тренінгів з медіаграмотності, адже жертвою інформаційних атак ворога може стати кожен українець, який користується інтернетом, читає друковані ЗМІ, дивиться ТБ. Найчастіше до маніпуляцій схильні люди похилого віку, діти та всі, хто не підходить критично до аналізу того чи іншого контенту. Тож першочергове завдання бібліотек – прищепити користувачам книгозбірні, жителям громади розуміння основ інформаційної гігієни, навчити критично ставитись до інформації, яка шириться просторами інтернету.

У січні 2023 року волонтерська ініціатива «Як не стати овочем» оприлюднила результати 4-ї хвилі дослідження рівня інформаційної гігієни українців у соціальній мережі «Фейсбук». Досліджувалися дописи, які українці опублікували в червні-вересні 2022 року.

Згідно з дослідницьким підходом дописами, які порушують інформаційну гігієну вважалися:

- ♦ публікації матеріалів з посиланням на сайти-сміттярки, Facebook-сторінки сміттярки, Facebook-групи сміттярки;
- ♦ фейки, які визначені фактчекерськими компаніями;

Сміттярки – це ресурси, які імітують онлайн-медіа чи/та інформаційну сторінку. Вони публікують новину не дотримуючись журналістських стандартів, перекручують та маніпулюють фактами.

Фактчекінг – це перевірка фактів та тверджень, які викликають сумнів, на точність та правдивість.

Фактчекери – це «сапери», які знешкоджують інформаційні «міни».

- ♦ посилання на матеріали, які містять маніпулятивну інформацію;
- ♦ тести, флешмоби, ігри та інші форми розважального характеру, проходячи які, людина дає доступ до своїх даних чи які є інструментом збору даних про людину в обхід фейсбуку.

Відсутність порушень цих параметрів вважалася дотриманням базової інформаційної гігієни.

За результатами дослідження бачимо, що дописи з порушенням інформаційної гігієни та з тематичними порушеннями публікували переважно українці старші 46 років. Крім того, показник по Україні за 2022 рік вищий (63% і 49%), ніж був у 2021-му (51% і 30%). Кожен другий користувач українського фейсбуку все ще поширює повідомлення, які підсилюють інформаційні операції ворога. Це в умовах, коли соціальні мережі є джерелом новинної інформації для 74% українців.

	Публікували дописи з порушеннями інфогігієни				Публікували дописи з тематичними порушеннями		Поширювали лінки на медіа з "білого списку ІМІ"	
	1' 2020	2' 2020	2021	2022	2021 - ковід	2022-ІПСО	2021	2022
25-35	46%	64%	42%	57%	24%	44%	7%	2%
36-45	52%	74%	52%	63%	29%	48%	10%	19%
46-55	61%	81%	59%	70%	36%	56%	11%	22%
56+	71%	85%	65%	74%	37%	57%	14%	26%
Україна	54%	73%	51%	63%	30%	49%	10%	20%

Такий вигляд мають цифри по регіонах України:

	Публікували дописи з порушеннями інфогігієни				Публікували дописи з тематичними порушеннями		Поширювали лінки на медіа з "білого списку ІМІ"	
	1' 2020	2' 2020	2021	2022	2021 - ковід	2022-ІПСО	2021	2022
Захід	57%	74%	52%	67%	30%	55%	13%	21%
Південь	58%	75%	56%	61%	35%	43%	5%	19%
Північ	48%	69%	42%	58%	27%	44%	11%	17%
Схід	60%	77%	40%	67%	19%	51%	7%	19%
Центр	51%	72%	57%	64%	31%	50%	9%	20%
Київ	41%	62%	35%	54%	22%	44%	13%	19%
Україна	54%	73%	51%	63%	30%	49%	10%	20%

Як бачимо, серед жителів Північного регіону кожен другий порушує інформаційну гігієну у фейсбуці.

Цікаво подивитися і на дані дослідження в розрізі видів порушень та вікової категорії користувачів.

Згідно з результатами найбільше користувачі фейсбуку, незалежно від віку, поширювали ІПСО (група дописів, які були з порушенням інфогігієни та їх тематика збігалася з меседжами, які поширював ворог) (44–57%). Користувачі старші 36 років активно поширювали маніпулятивну інформацію (46–57%), сміттярки (36–48%) та тести (26–30%). З огляду на наявну інформацію, найбільше про інформаційну гігієну дбають молоді люди (25–35 років).

Публікували дописи з порушеннями інфогігієни	Україна		25-35		36-45		46-55		56+	
	2021	2022	2021	2022	2021	2022	2021	2022	2021	2022
Порушники										
- тести	15%	25%	11%	2%	15%	26%	18%	31%	23%	30%
- сміттярки	29%	36%	21%	3%	30%	36%	35%	39%	40%	48%
- фейки ПРОмарковані Fb	10%	6%	7%	0%	10%	6%	13%	7%	16%	11%
- фейки НЕ промарковані Fb	19%	6%	13%	0%	17%	5%	26%	8%	33%	11%
- маніпулятивна інформація	31%	48%	26%	4%	33%	46%	37%	55%	38%	57%
- порушення про Ковід	30%		24%		29%		36%		37%	
- ІПСО		49%		44%		48%		56%		57%
Білі медіа	10%	20%	7%	2%	10%	19%	11%	22%	14%	26%

Такий вигляд мають дані дослідження в розрізі видів порушень за регіонами:

Публікували дописи з порушеннями інфогігієни	Україна		Захід		Південь		Північ		Схід		Центр	
	2021	2022	2021	2022	2021	2022	2021	2022	2021	2022	2021	2022
Порушники												
- тести	15%	25%	17%	30%	16%	21%	10%	21%	14%	26%	17%	27%
- сміттярки	29%	36%	33%	39%	30%	38%	21%	29%	14%	41%	36%	35%
- фейки ПРОмарковані Fb	10%	6%	12%	7%	12%	5%	8%	5%	7%	5%	11%	6%
- фейки НЕ промарковані Fb	19%	6%	20%	9%	24%	5%	15%	4%	10%	4%	22%	7%
- маніпулятивна інформація	31%	48%	31%	51%	35%	44%	27%	45%	29%	48%	33%	49%
- порушення про Ковід	30%		30%		35%		27%		19%		31%	
- ІПСО		49%		55%		43%		44%		51%		50%
Білі медіа	10%	20%	13%	21%	5%	19%	11%	17%	7%	19%	9%	20%

Орієнтуючись на результати цього дослідження, бібліотекарі можуть визначити види порушень інфогігієни, відібрати вікову категорію аудиторії і відповідно до отриманих даних підготувати теоретично-практичні курси, які допоможуть орієнтуватися у загальному потоці інформації, незалежно від того, де ця інформація зустрічається – у соціальних мережах, ЗМІ тощо.

У деяких бібліотеках області, переважно центральних, подібна робота проводилась. Наприклад, у Сновській публічній бібліотеці в межах проєкту «Бібліотека – територія жіночої синергії» відбувся захід «Медіаграмотність жінок – вимога сучасного світу», де учасниці навчилися розпізнавати дезінформацію та фейки серед сотень дописів, які кожного дня зустрічаються в інтернеті. А в Корюківській публічній бібліотеці провели в ігровій формі зустріч для дітей зі старшим інспектором з дотримання прав людини Корюківського РВП ГУНП, на якій дітлахи дізналися про те, як потрібно користуватися мережею Інтернет, які небезпеки в ній існують, як діяти, коли пишуть повідомлення незнайомці та ін.

Про інформаційну гігієну своїх користувачів мають дбати всі бібліотеки, а не лише центральні чи публічні. На базі великих бібліотек здебільшого діють цифрові хаби, метою яких є підвищення рівня медіаграмотності, а от сільські бібліотеки до цього процесу залучені не всі. Сьогодні сільська бібліотека залишається фактично єдиним осередком культури, де можна не лише взяти книжку, а й поспілкуватися. Тож хто як не бібліотекар має навчити жителів громади дбати про інформаційну гігієну, а разом і про ментальне здоров'я. Нині у селах все більше людей старшого віку активно користуються смартфонами та іншими гаджетами, зареєстровані у фейсбуці, телеграмі, вайбері, переглядають тіток, ютуб, коментують дописи,

ставлять вподобайки чи дизлайки, поширюють різний контент на власних сторінках, розповідають про побачене чи прочитане сусідам, друзям. Важливо, щоб користувачі інтернету не поширювали неправдиву інформацію, а підходили до її споживання критично. Дуже часто можна зустріти, що у фейсбуці поширюють сльозливі дописи про хворих дітей, поранених захисників тощо для збору коштів на лікування, не усвідомлюючи, що це працюють шахраї. А той хто поширює подібний контент невільно стає співучасником злочину, адже допомагає розповсюдити інформацію, збільшити просування допису та зарахування на банківські реквізити шахраїв.

Медіаекспертка Оксана Мороз розповідає про **7 базових правил**, які допоможуть ефективніше фільтрувати інформацію під час війни:

1. Визнати.

Формування інформаційної гігієни починається, перш за все, з усвідомлення та розуміння проблеми – далеко не кожен українець може відрізнити правду від брехні в інформаційному просторі.

Невміння фільтрувати інформацію є чудовим підґрунтям для впливу на мислення та поведінку українців. Невизнання проблеми штовхає людину на сприйняття будь-якої інформації з ворожих інформаційних сайтів-сміттярок (ресурсів, які маскуються під медіа) як правдивих.

2. Зрозуміти розрізненість інфополя.

Нас оточує великий масив різноманітної інформації – правди й брехні. Це можуть бути:

- ♦ Реальні новини й ті, які вигадали заради хайпу. Скажімо, під час повітряної тривоги вкидають інформацію про прильоти. Відразу тисячі репостів. Місцева влада потім спростовує інформацію, але медійна задача хайповика вже виконана – вподобайки, поширення, коментарі.
- ♦ Фейки та ворожі інформаційні спецоперації.
- ♦ Наші інформаційні спецоперації. Так, українці, які споживають російськомовний контент, можуть потрапити під їхній перехресний вогонь.
- ♦ Інформація, яку ми транслюємо міжнародним партнерам: і там точно інші акценти, ніж ті, які потрібні для української аудиторії.
- ♦ Політичні ігри вітчизняних та західних політиків.

- ♦ Канонічні українські сварки з будь-якого приводу. Вони добре допомагають ворогу, вказуючи на больові точки суспільства.

В умовах гібридної війни ми маємо навчитися спершу аналізувати інформацію, а вже потім на неї реагувати. Перш ніж цілковито довіряти побаченому, почутому чи прочитаному, поставте собі кілька запитань: чому я це бачу? Хто це транслює? Якої мети хоче досягти?

3. Білий список.

Мінімізувати вплив інформаційних вірусів на нас зможе правильно сформований та регулярний у використанні інформаційний трафарет. Щоб його створити, необхідно вибрати три-п'ять медіа з «Білого списку» Інституту масової інформації (<http://surl.li/gxvqt>). Читайте новини та аналітику в них. Лише зрозумівши об'єктивну реальність, переходьте на інші інформаційні канали, де немає стандартів і фільтрування інформації.

Якщо ж вам надіслали посилання на матеріал, що містить заголовок «СЕНСАЦІЯ! ШОК! ПЕРЕШЛІТЬ, БУДЬ ЛАСКА, КОМУСЬ!», «ТЕРМІНОВО!», «БУДЬ ПЕРШИМ, ХТО ДІЗНАЄТЬСЯ!» чи будь-які інші виражені емоції, перевірте, чи є ця інформація на ресурсах із «Білого списку». Якщо це справді сенсаційна інформація, а не фейк, ви точно її там знайдете.

4. Аудит.

Виконайте аудит свого інфополя. Видаліть канали, які вами маніпулюють.

- ♦ Facebook – перегляньте список ваших друзів і сторінок, на які підписані. Відпишіться від сторінок, які зламали, сміттярок і тих, що не відповідають вашим інтересам.
- ♦ YouTube – перегляньте відео, які відеохостинг рекомендує вам. Натисніть «Не цікавить» (справа за трьома крапками), якщо відео не відповідають вашим інтересам чи є сміттярками.
- ♦ Google – встановіть український інтерфейс і гугліть українською. Це мінімізує вплив російських сайтів, що можуть містити фейкову інформацію.
- ♦ Viber – перегляньте чати та спільноти, до яких ви додані. Відпишіться від ресурсів-сміттярок.
- ♦ Telegram – перегляньте канали, на які підписані. Відпишіться від анонімних каналів та ресурсів-сміттярок.

- ♦ Вікіпедія – не використовуйте російську версію.

5. Не допомагати ворогу.

Рф постійно моніторить українське інформаційне поле, шукає слабкі місця у суспільстві, а коли знаходить – завдає на їх основі тріщин. Точки болю – це дискусійні теми, які для нас зараз важливі: мова, переселенці тощо. Перш ніж поширити якусь інформацію, треба добре подумати і відповісти на запитання: «Чи зашкодить це країні?» Якщо відповідь ствердна, – не публікуйте.

Якщо ж під впливом емоцій ви все ж опублікували шкідливу інформацію, не соромтесь видалити пост, аби його поширило якомога менше людей.

Пам'ятайте, що ніколи не пізно видалити пост. Ніколи не пізно написати спростування. Жодні лайки та охоплення не варті роботи на розкол країни чи дезорієнтацію людей.

6. Розпізнавання фейків.

Фейки швидко ширяться в інформаційному просторі. Навіть людина з достатньо розвиненим критичним мисленням може легко попастися на неправдиву інформацію, коли читає «по діагоналі», просто гортає стрічку в соціальних мережах, споживаючи інформацію фоном під час буденних справ.

Існує кілька простих правил, які допоможуть запобігти поширенню фейкових новин у соцмережах:

1. Якщо у тексті наведені посилання – не лінуйтеся переходити за ними.

Саме за посиланням має бути першоджерело: інформація з перших уст, фото-докази, цитати пресслужб. Якщо посилання веде на сторінку, що не існує, фейковий сайт або тільки на головну сторінку сайту, а не на джерело, то є велика ймовірність, що ви натрапили на фейкову новину. Також слід замислитися, якщо першоджерело веде на сайт, який ніяк не може належати до новини начебто про нашу українську буденність (так, наприклад, новина у фейсбуці про те, що під Пирятином перевернулися чотири фури з кукурудзою навряд буде мати першоджерело на сайті, домен якого зареєстрований у Казахстані). Тож якщо жодне інше надійне джерело не повідомляє про ці події, скоріше за все, новини є неправдивими.

2. Обов'язково звертайте увагу на дату публікації.

Емоційні тексти, написані декілька років тому, дуже часто «випливають» у сучасному інформаційному просторі завдяки цікавості інтернет-користувачів, яка не згасає.

3. Читайте більше, ніж заголовок та передмову статті.

Саме так ви зможете оцінити співвідношення заголовок-публікація на предмет відповідності, об'єктивної подачі інформації, правдивості джерела. Адже найпоширеніший прийом – винести неправду в заголовок, таким чином заманюючи читача на сторінку чи сайт.

4. Дотримуйтесь правил інформаційної гігієни.

Є всі підстави сприйняти новину, статтю чи допис у соцмережі як фейковий, якщо:

- ♦ «б'є» не на об'єктивність з цифрами та фактами, а на емоції, має маніпулятивні риси («емоційний», «шоковий заголовок», жахливі подробиці, картинка, яка не має відношення до тексту, але несе емоційне навантаження);
- ♦ допис чи стаття розміщені на «сайтах-сміттярках»;
- ♦ джерело анонімне або неодноразово помічене у розповсюдженні фейків;
- ♦ допис, новина, стаття і т. д. апелює до конспірологічних теорій, а думка чи оцінка подається як факт;
- ♦ є посилання на ВКонтакте, Однокласники, МойМир тощо серед посилань на офіційні сторінки у соціальних мережах, редакційна пошта на серверах Яндекс, Майл.ру, Рамблер тощо.

5. Як написано не менш важливе, ніж ЩО написано.

Одним з неочевидних ярликів, які можуть нам сигналізувати, що перед нами фейкова інформація – граматичні, орфографічні та синтаксичні помилки. Крім того, досить часто у фейкових новинах можна зустріти фрази, які явно перекладені Google-перекладачем або слова з російськими «ъ» замість апострофа.

6. Фейкова публікація здебільшого висвітлює тільки один погляд.

Журналіст насправді може реально полінуватися знайти ще одного експерта або розраховувати на те, що він достатньо розкрив тему у своєму тексті, але критично мисляча людина має подумати, перш ніж сприймати на віру будь-яку інформацію, тим більше перед подальшим її поширенням. У достовірних виданнях щонайменше два джерела новини: інформаційні агентства та реальні свідки подій.

7. «Дута» експертність має насторожити.

Посилання у публікації на експертну думку – це супер. Але не дуже гарно виходить, якщо експерт виявляється анонімом з фейсбуку або просто видуманим героєм.

Якщо посилання веде на незрозумілу сторінку в соцмережах, або ви не можете знайти ніяку конкретну інформацію про людину чи установу, яку вона представляє – перед вами скоріш за все фейк.

8. Не будьте занадто самовпевненими!

Відповідно до дослідження, проведеного Університетом Юти (США) та опублікованого в журналі «Proceedings of Nation Academic of Sciences» щодо сприйняття фейків у ЗМІ та соцмережах, близько 90% людей, які оцінили себе як особу з високим рівнем критичного мислення, показали гірші результати, ніж ті, хто оцінив свій рівень критичного мислення як середній. Крім того, занадто самовпевнені люди з більшою ймовірністю зайдуть на небезпечний сайт та будуть постити фейки, ніж ті, у кого все в порядку з рівнем самовпевненості.

7. Не брати інформацію з російських джерел.

Усі російські медіа прямо чи опосередковано підігрують російській пропаганді. Тому якщо ви хочете дізнатися «що там на росії», то краще прочитати іноземні медіа чи українські з «білого списку».

Дотримуючись цих правил, можна навчитися сортувати інформацію, яку нам нав'язують, дбати про психологічний добробут та емоційний комфорт, зменшити вплив інфополя на наше самопочуття, а отже, зменшити рівень стресу.

ШАХРАЙСТВО У СОЦІАЛЬНИХ МЕРЕЖАХ:

ЧИ МОЖНА ВБЕРЕГТИСЯ?

З кожним роком все більше українців реєструється у соціальних мережах. Цифровий простір стає не тільки зручним місцем для знайомств, спілкування, здійснення покупок чи ведення бізнесу, а й одним з улюблених місць для шахраїв та злочинців. Особливо популярним і масовим стає шахрайство у соцмережах. У цьому розділі ми спробуємо розібратися, які поширені небезпеки нас можуть спіткати у соцмережах.

1. Фейкові облікові записи.

У січні-березні 2022 року Facebook видалив 1,6 млрд фейкових акаунтів. За допомогою сучасних програмних засобів інтернет-ділки за лічені хвилини створюють тисячі фейкових сторінок користувачів, збираючи з них армію. Її використовують для просування в соціальній мережі політичних наративів, формування потрібної суспільної думки, просування соціальних сторінок приватних компаній, накручування «лайків», виманювання персональних даних, залучення людей до інвестування з елементами шахрайства. Ця цифра не найбільша в історії компанії. У четвертому кварталі 2021 року Facebook видалив 1,7 млрд фейкових акаунтів. Це при тому, що активними користувачами мережі (принаймні одне відвідування на день) є 2,5 млрд людей.

Хто і навіщо створює фейкові акаунти?

В Україні Facebook є одним з найбільш популярних сайтів за охопленням аудиторії та серед мобільних застосунків. За даними маркетингового агентства «Кантар Україна», у травні 2022 року соцмережа посідала четверте місце в переліку 25 провідних сайтів України за охопленням аудиторії – охоплювала 45% інтернет-користувачів країни.

Інструменти для створення бот-мереж і самі бот-мережі зазвичай створюють і застосовують команди досвідчених веброзробників, тобто спеціалістів у сфері розробки зовнішніх та внутрішніх компонентів вебресурсів, які володіють мовами програмування HTML, Java, Javascript, PHP, CGI та Perl.

Зловмисники створюють облікові записи, які імітують реальних користувачів або вигадують псевдоніми, щоб викликати довіру в інших користувачів соцмереж та взаємодіяти з ними у своїх цілях. Також шахраї в інтернеті можуть створювати дублікати профілів ваших друзів або родичів, щоб втертися у довіру та підштовхнути

до небезпечних дій, наприклад, надання своєї конфіденційної інформації чи переказу коштів.

В умовах війни мережі ботів застосовують переважно на замовлення українських політичних сил, спецслужб країни-агресора та її агентів.

Вони роблять це для дискредитації політичного керівництва України, дій ЗСУ, виправдання російської агресії, нав'язування кремлівських наративів, поширення панічних настроїв та проведення інформаційно-психологічних операцій, направлених на придушення волі населення до спротиву окупантам.

Як виявити фейкові акаунти?

Для виявлення фейкових акаунтів передусім слід перевірити зображення профілю. Профіль має ознаки підробки, якщо в ньому відсутнє фото, є тільки один знімок, на світлині профілю зображені квіти, тварини або логотипи.

Далі треба поставити «другу» кілька запитань. Чому він хоче бути вашим другом? Як він про вас дізнався? Чи є у вас спільні друзі? Кого з них ви знаєте особисто? Зазвичай фейковий акаунт на запитання не відповідає.

Після цього потрібно переглянути стрічку «друга». Якщо користувач публікує багато посилань на сайти з великою кількістю реклами, то обліковий запис призначений для реклами і, ймовірно, цей акаунт підроблений.

Справжні користувачі соцмереж діляться різним контентом, наприклад, власними думками, розповідями, жартами, музикою, відео, фото.

У зв'язку з воєнними діями, зборами, які проводять волонтери та військові, у соціальних мережах, зокрема у фейсбуці, з'явилося безліч фейкових акаунтів-двійників. Популярними серед шахраїв є фейкові акаунти медійних військових.

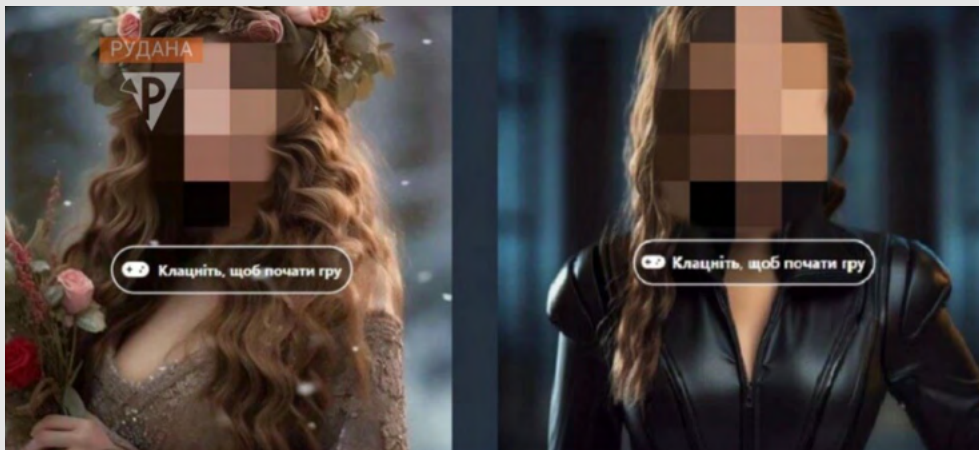
2. Обман під час взаємодії та спілкування.

Доволі часто шахраї надсилають користувачам соцмереж повідомлення про виграш цінних призів або участь у вигідних акціях, які вимагають від вас поділитися особистою інформацією чи внести певну суму коштів для отримання такого «призу». Також зловмисники можуть намагатися вивчити вас і ваші звички через публікації та взаємодії в соцмережах. Потім вони використовують цю інформацію для створення переконливих сценаріїв обману.

Загрозу для користувачів становлять і різноманітні тести та ігри. Веселі тести у фейсбуці на кшталт «Яка ти принцеса Діснея?» і «На кого зі знаменитостей ти

схожа?» не просто видають досить сумнівні результати, а й збирають приватну інформацію про користувачів. Додаток отримує повний доступ до всіх даних на фейсбуці – вік, стать, список друзів, адреса електронної пошти, геолокація, публікації в хроніці і всі фотографії. Причому все це – безкоштовно і назавжди, з можливістю зберігати цю інформацію де завгодно і кому завгодно передавати.

За схожим принципом у фейсбуці активно шириться гра My Puzzles, яка за допомогою штучного інтелекту перетворює фото людини на казкового персонажа. Сенс гри – скласти пазли й побачити картинку, згенеровану штучним інтелектом, де зображено вас в образі якогось героя. Такі ігри дуже часто викликають інтерес публіки, адже кожному цікаво побачити, як штучний інтелект нас зобразить.



Тобто, щоб зіграти в ці пазли, вам потрібно буде надати грі дані про себе, як мінімум ваше фото та ім'я. Потенційно ці дані можуть бути передані іншим програмам, зокрема комерційним, які відстежують ваші вподобання.

Торік на тлі успіху голлівудського фільму «Барбі» особливо відомим став застосунок BaiRBIE.me, який перетворював фото користувача на ляльку Барбі чи Кена. Програма працювала безкоштовно, але щоб отримати фото без водяного знака потрібно було заплатити \$2. Під час створення знімка користувача просили завантажити портретну фотографію, а також вказати адресу електронної пошти. Тоді мінцифри Польщі визнали цей застосунок небезпечним, адже він збирав величезну кількість персональних даних. Штаб інформаційних та кібернетичних сил Армії Чехії також попереджав мешканців про потенційну небезпеку, яку представляє цей додаток. Отже, інструмент BaiRBIE.me не відповідає вимогам Регламенту ЄС щодо захисту персональних даних, а тому неясно, що його творці будуть робити із зібраними даними.



Ще один варіант, коли вам надходить повідомлення від «служби підтримки Фейсбук» чи Інстаграм. У тексті йдеться, що за вашим акаунтом помічені проблеми і для їх вирішення потрібно негайно перейти за посиланням та ввести свій логін і пароль. Після виконання цих дій доступ до акаунту буде втрачено.

У чому небезпека ігор у Facebook?

Ігри у фейсбуці можуть становити потенційну небезпеку, коли йдеться про захист персональних даних, якщо не дотримуватися обережності та не бути обізнаним користувачем.

Основні проблеми:

1. Можливість збору особистих даних. Деякі ігри можуть використовувати неправомірні методи для збору особистих даних користувачів. Розробники можуть використовувати ці дані для маркетингових цілей або для шахрайства.

2. Ризик вірусів та шкідливих програм. Маловідомі розробники можуть створювати ігри, що містять віруси або інші шкідливі програми, які можуть завдати шкоди комп'ютеру чи смартфону, або особистій інформації користувача.

3. Спам та фішинг. Деякі ігри можуть використовувати надмірну кількість спаму або спроб фішингу для отримання конфіденційної інформації.

3. Небезпечний «заробіток» у соцмережах.

Поширеними стали випадки, коли зловмисники пропонують здати в оренду акаунт Facebook або іншої соцмережі. За це обіцяють користувачу прибуток у розмірі 10-20 доларів на день. Проте найчастіше такий спосіб «заробітку» призводить до втрати вашого особистого акаунту, а інколи і грошей, особливо, якщо до вашого облікового запису прив'язана банківська картка.

Популярним є і «заробіток» у соцмережах та телефонних месенджерах (Viber, Telegram, WhatsApp). Розрахований він на шукачів легких грошей. Аферисти

можуть пропонувати чималий заробіток за написання коментарів у соцмережах, поширення повідомлень у сторіс, перегляди відео в тіктоці, бронювання номерів у готелях тощо. Аферисти просять одразу реквізити банківської карти та надсилають кошти нібито за перші виконані завдання – 100-200 грн. Увійшовши в довіру, швидко пропонують подвоїти заробіток, довірливі мешканці надсилають чималі суми коштів. Дехто надсилав 130 тис. грн. Після того, як кошти надходять на рахунок шахраїв, вони обривають контакти.

4. Поширення шкідливих посилань.

Шахраї часто-густо використовують соціальні мережі для поширення шкідливих посилань, що містять віруси або шкідливі програми, які можуть наразити на небезпеку ваш обліковий запис або поцупити особисту інформацію.

Ці посилання можуть бути різних видів: чи то повідомлення, публікації або навіть коментарі. Необхідно остерігатися будь-яких посилань, які виглядають підозріло, особливо якщо їх надсилає незнайома вам людина. Щоб переконатися в безпеці посилання, ви повинні взяти за правило завжди наводити курсор на неї, перш ніж натиснути. Крім того, ви можете використовувати онлайн-сервіси для перевірки посилань, як-от «Безпечний перегляд» від Google.

Подібні програми виявляють шкідливі посилання, а отже захищають вас від ризику стати жертвою шахрайства.

Наприклад, шахраї у Facebook масово тегають публічні сторінки та надсилають користувачам спам-повідомлення з текстом: «Подивіться, хто загинув у ДТП, я думаю, ви його знаєте, так шкода...» Наприкінці повідомлення міститься посилання. Якщо за ним перейти, то можна втратити доступ до свого акаунту та стати жертвою шахраїв. Якщо ви отримали таке повідомлення, потрібно надіслати скаргу на допис і заблокувати джерело його розповсюдження!

Таке шахрайство називають фішингом. Як стверджує поліція, найчастіше аферисти, які займаються фішингом, видають себе за банки чи інші установи, щоб змусити жертву заповнити фальшиву форму та отримати дані облікових записів.

Фішинг — це один з різновидів шахрайства в інтернеті з метою отримання незаконного доступу до конфіденційних даних користувачів.

Як уникнути шахраїв у соціальних мережах?

Шахрайство в соціальних мережах є серйозною загрозою, яка може вплинути на фінансову безпеку, репутацію та приватність користувачів. Фактично, якщо ви є користувачем таких соціальних мереж, як Facebook, Twitter, Instagram або Tiktok, ви вже в небезпеці. Щоб зменшити ризики і не стати жертвою шахраїв у інтернеті, треба дотримуватися **кількох порад**:

1. Використовуйте надійний пароль.

Надійний пароль – запорука безпеки ваших соціальних мереж та інших облікових записів в Інтернеті від несанкціонованого доступу.

Експерти у сфері кібербезпеки стверджують, що надійний пароль має містити щонайменше 12 символів, цифр, а також має поєднувати у собі символи верхнього та нижнього регістрів (великі та малі літери).

Ба більше, ви повинні уникати використання таких поширених та банальних паролів, як, наприклад, «123456» або «Пароль», оскільки зламати їх для шахрая надто просто.

2. Увімкніть двофакторну автентифікацію.

Двофакторна автентифікація – це один з елементів, який створює додатковий захист для ваших облікових записів у мережі.

Крім пароля, він передбачає ще один спосіб ідентифікації. Це може бути код, що надсилається на номер телефону; дзвінок на мобільний; лист на e-mail; відбиток пальця. Це значно ускладнює отримання несанкціонованого доступу до вашого облікового запису, навіть якщо шахрай має пароль.

Як встановити двофакторну автентифікацію:

1. Увійдіть у потрібний акаунт (наприклад, Facebook, Telegram, Google чи ін.)
 2. Зайдіть у розділ меню «Налаштування», а потім «Безпека».
 3. Оберіть пункт із налаштуваннями двофакторної автентифікації, якщо така функція є (зверніть увагу, може називатися також «двоетапна перевірка»).
 4. Виконайте всі необхідні дії за запропонованою інструкцією.
- ### ***3. Захистіть особисту інформацію.***

Розміщення зайвої особистої інформації у соціальних мережах може зробити вас уразливими для шахраїв в інтернеті, а також може призвести до крадіжки ваших особистих даних. Тому дуже важливо обмежити кількість особистої інформації,

якою ви ділитесь в інтернеті. Не варто ділитися своїм місцезнаходженням, планами на день, особистою інформацією про своїх друзів та родичів або будь-якою іншою інформацією, яка може бути корисною для шахраїв та злочинців. Не варто також відкривати своє повне ім'я, дату народження, адресу, номер телефону, фотографії ваших документів та інші подібні дані.

Наприклад, зловмисники можуть спробувати розшифрувати пароль, використовуючи ім'я вашої дитини або домашньої тварини. У зв'язку з цим дуже важливо стежити за тим, що ви публікуєте у соціальних мережах.

4. Остерігайтесь фейкових акаунтів.

Шахраї та кіберзлочинці можуть отримати доступ до конфіденційної інформації, створюючи фальшиві профілі у соціальних мережах.

Видаючи себе за іншу людину, вони можуть надсилати вам запити на додавання до друзів або надсилати повідомлення з метою ошукати вас та змусити поділитися своєю особистою інформацією. Тому вкрай важливо з обережністю ставитись до того, з ким ви спілкуєтесь у соціальних мережах.

Отримавши запит на дружбу або повідомлення від незнайомця, перевірте його профіль на наявність підозрілих дрібниць та деталей, які можуть вказати на його фальшивість. Наприклад, типовими ознаками фейкових сторінок є: відсутність фотографії профілю, активності у стрічці або друзів.

5. Перевірте налаштування конфіденційності.

Більшість соціальних мереж дозволяють налаштувати параметри конфіденційності. Там ви можете керувати тим, хто може бачити ваші публікації та інформацію про ваш профіль.

Ретельно відрегулювавши конфіденційність, ви гарантуєте, що вашу інформацію побачать тільки ті люди, яким ви довіряєте.

6. Регулярно відстежуйте свої облікові записи.

Періодично спостерігаючи за своїми сторінками у соціальних мережах, ви з легкістю зможете виявити будь-яку підозрілу активність чи сторонній доступ до вашого профілю.

Якщо, наприклад, хтось входить до вашого облікового запису з незнайомого місця або залишає коментарі та надсилає повідомлення сумнівного характеру та змісту

вашим друзям, вам слід негайно змінити пароль та повідомити про це службу підтримки вашої соціальної мережі.

7. Використовуйте VPN.

Використання VPN (з англ. «Віртуальна приватна мережа») може підвищити безпеку вашої діяльності в Інтернеті. VPN шифрує ваше інтернет-з'єднання, що ускладнює перехоплення ваших даних. Таким чином ви почуватиметеся у більшій безпеці.

8. Не втрачайте пильності.

Зрештою, дуже важливо тримати руку на пульсі у світі цифрових технологій. Онлайн-шахраї та кіберзлочинці постійно шукають нові способи щось поцупити та когось ошукати.

Коли щось здається вам надто гарним, щоб бути правдою, то, швидше за все, так воно і є. Шахраї не прогавлять жодного шансу нажитися на вашій необачності.

Тому, будучи пильними та уважними, ви залишаєте зловмисників біля розбитого корита, тим самим позбавляючи їх стимулу до пошуку нових схем шахрайства.

ДЕ ВДОСКОНАЛИТИ СВОЇ ЗНАННЯ ПРО ІНФОРМАЦІЙНУ ГІГІЄНУ?

Бібліотечні працівники України розуміють важливість інформаційної гігієни для українського суспільства, особливо в умовах воєнного стану. Тому на базі бібліотек проводяться відповідні заходи для дітей, дорослих та бібліотечних працівників. Проте перш ніж навчати когось, бібліотекарям треба поглибити власні знання з цієї теми. Тож розглянемо кілька ресурсів, які дозволять безкоштовно поглибити наші знання з теми «Інформаційна гігієна».

Платформа онлайн-освіти в Україні Prometheus. У партнерстві з найкращими лекторами, провідними компаніями та міжнародними організаціями на платформі створено онлайн-курси з найбільш популярних тем. Кілька курсів присвячено і темі «Інформаційна гігієна»:

- ♦ **«Інформаційна гігієна. Як розпізнати брехню в соцмережах, в інтернеті та на телебаченні».** На цьому курсі ви зрозумієте, як не потрапити на гачок маніпуляторів в інтернеті, у соцмережах та онлайн-ЗМІ.

Також на курсі ви дізнаєтеся:

- як руйнувався інформаційний імунітет українців та які наслідки це має для держави та людей;
- про нову роль інформації в цифрову еру;
- хто, як і навіщо створює інформаційні віруси;
- як маніпулюють на телебаченні, в онлайн-медіа, Facebook, YouTube, Google, Telegram, Viber, Вікіпедії;
- як споживати інформацію безпечно та навчати цього інших.

Фейків та маніпуляцій тисячі, вивчати їх – це окрема професія, а ось каналів їх створення та поширення десятки. Для того, щоб суттєво зменшити ризики підхопити інформаційний вірус, не обов'язково тільки перевіряти факти, достатньо розуміти, як вони розповсюджуються.

Обсяг курсу – 45 годин (загальна тривалість відеолекцій – 4 години).

Більш детально ознайомитись з курсом можна за посиланням: https://prometheus.org.ua/course/course-v1:Prometheus+IH101+2021_T3.

- ♦ **«Інформаційна гігієна під час війни».** Мета курсу – навчити базової інформаційної гігієни під час війни – основ фільтрування інформації та розпізнавання брехні.

У курсі ви дізнаєтесь:

- Як формується інформаційне поле під час активної фази війни?
- Чи є правда та де її шукати? Про специфіку українських, іноземних та російських медіа.
- Як працює класична російська пропаганда?
- Що таке інформаційно-психологічні спецоперації та як вони працюють?
- Як росіяни використовують Telegram, блогерів-інсайдерів та «хороших росіян» для досягнення своїх цілей?
- Яких правил інформаційної гігієни слід дотримуватись під час війни?

Обсяг курсу – 15 год (загальна тривалість відеолекцій – 2 години). 0,5 кредиту ЄКТС.

По закінченні курсу видається Сертифікат про успішне завершення навчання зі вказаною кількістю годин.

Більш детально ознайомитись з курсом можна за посиланням: https://prometheus.org.ua/course/course-v1:Prometheus+IHWAR101+2022_T2.

- ♦ **«Медіаграмотність: як не піддаватися маніпуляціям?»** – це онлайн-курс, який навчає відрізняти правду від брехні в нинішньому світі. Ця навичка вкрай необхідна, адже ми живемо в часи справжнісінької навали різноманітної інформації. А в час війни медіаграмотність необхідна для захисту свого життя. Адже ворог веде проти нас війну не лише на полі бою, він намагається вразити нас в інформаційному просторі. Його завдання: поширити зневіру, підірвати підтримку партнерів, посіяти паніку, створити в кожного українця враження, що війну ми програємо або й уже програли.

До курсу залучені експерти із різних організацій та з різним бекграундом, щоб курс справді був всеохопним та вичерпним.

На курсі ви:

- дізнаєтесь, чому і як медіаграмотність допомагає в ухваленні найкращих рішень;
- ознайомитеся з найкращими практиками для розвитку рівня критичного мислення;
- опануєте алгоритм перевірки якості контенту українських та закордонних медіа;
- навчитесь досліджувати експертність авторів, джерел інформації, зокрема телеграм-каналів;

- засвоїте цифрові інструменти для швидкої та ефективної перевірки достовірності фото та відео;
- ознайомитеся з ключовими наративами й тактиками російської пропаганди, аби протидіяти їм;
- навчитеся визначати маніпулятивний медіаконтент, розрізняти дезінформацію, шкідливі пропагандистські наративи;
- дізнаєтеся, як самостійно створювати якісний контент та уникати блокувань у соцмережах.

Розрахований курс на 30 годин (1 кредит ЄКТС). Пройти курс можна безкоштовно, онлайн, опановується дистанційно і самостійно.

Виконавши всі обов'язкові завдання курсу, користувач чи користувачка отримує сертифікат про успішне завершення навчання. Автентичність сертифіката можна перевірити за посиланням на ньому. Усі видані сертифікати внесено до реєстру.

Більш детально ознайомитись з курсом можна за посиланням: https://prometheus.org.ua/course/course-v1:Prometheus+MEDIA_L101+2022_T3.

Сімейний курс з інфогігієни. Це серія коротких відео з прикладами із нашого щоденного життя. Тут говорять не лише про медіаграмотність для дітей, а й пояснюють, які небезпеки чекають нас в YouTube, TikTok, медіа, Вікіпедії, Telegram, Facebook. А ще діляться порадами, як розпізнати російські інформаційні операції та інші пастки. Тому за кілька годин ви зрозумієте, як захистити себе від інформаційних вірусів – фейків та маніпуляцій.

Цей курс створили фахівці з понад 20-річним досвідом у своїй справі: Оксана Мороз – дослідниця медіаполя, експертка з інфогігієни та засновниця ініціативи «Як не стати овочем»; Гольцберг Катерина – дитяча та сімейна психологиня, яка має багаторічну практику в освітній сфері і є президенткою професійної Асоціації дитячих аналітичних психологів.

Зокрема, за посиланням (<https://salo.li/006604d>) можна переглянути відео на такі теми: «4 причини, чому українців легко обдурити онлайн», «Передай це повідомлення у Viber 10 друзям та інша дурість», «Боти. База, яку варто знати про фейкових людей», «Коротко про пастки в YouTube, Google, TikTok, Вікіпедії», «Коротко про пастки в Facebook та Instagram», «Коротко про пастки в Telegram та Viber»,

«Онлайн-медіа (не)можна довіряти», «Псевдоексперти та корисні ідіоти», «Як маніпулюють з допомогою фільмів, книг, серіалів», «Фіксики, Смішарики, Синій трактор: українських дітей виховували мультики рф?»»

Вебінар «Інформаційна гігієна під час війни. Базові правила». На YouTube-каналі Центру цифрової освіти та медіакультури розміщено вебінар «Інформаційна гігієна під час війни. Базові правила». Під час вебінару розглядалися такі питання: «Українці та інформація в цифрову еру (дослідження). Як цим користуються ворог та маніпулятори», «Чи є правда під час війни та де її шукати? Українські та іноземні медіа», «Актуальні загрози в інформаційному полі: як розпізнати та зрозуміти», «Хороші росіяни» корисні для України? Дослідження», «Правила інфогігієни під час війни».

Переглянути вебінар можна за посиланням: <https://www.youtube.com/watch?v=G5UBTCsZRYQ>.

Переглянувши ці ресурси, ви здобудете знання, підтверджені сертифікатами, про інформаційну гігієну та на їх основі зможете підготувати тренінг з цієї теми для жителів вашої громади.

ДОСВІД ВІТЧИЗНЯНИХ БІБЛІОТЕК

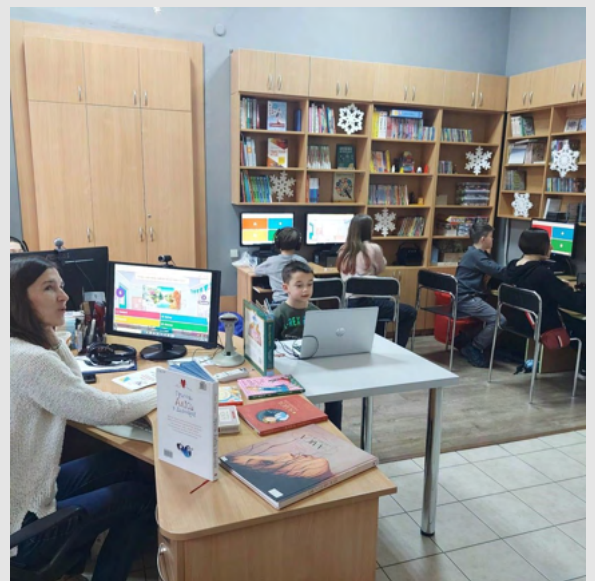
У Львівській обласній бібліотеці для дітей за підтримки Відділу преси, освіти та культури Посольства США в Україні було реалізовано проєкт *інформаційно-психологічної безпеки дітей та підлітків «П'ята стихія»*. Почали працювати над проєктом ще у 2022 році, зараз він в межах гранту вже завершений, але бібліотекарі продовжують самостійно працювати над ним і досі.

Метою проєкту, як зазначають організатори, є подолання інформаційної нерівності, виховання інформаційної грамотності й критичного мислення, протидія шкідливим інформаційним впливам, прищеплення навичок інформаційної гігієни та кібербезпеки, посилення інформаційної та психологічної стійкості громадян до пропаганди та дезінформації.

Результатом проєкту стало масштабне залучення дітей до навчання інформаційної та комп'ютерної грамотності, навчання та практичні заняття для бібліотекарів України, підготовка електронного збірника навчальних занять, розроблених бібліотекарями – учасниками проєкту.

Проєкт «П'ята стихія» Львівська обласна бібліотека для дітей створила для дітей та підлітків від 8 до 15 років, які постраждали від російської агресії. Бібліотека організувала навчання для евакуйованої молоді зі Сходу та Півдня та львівських підлітків, щоб допомогти ВПО вдало інтегруватися у місцеве середовище. У межах проєкту відбувалися заняття з протидії дезінформації, уроки української мови та програмування.

Навчання проходило у двох категоріях: це діти 8-10 років і підлітки від 11 до 17 років. Крім того, у своїх вікових групах діти були поділені на групи, відповідно від рівня знань. Результатом проєкту стала підготовка дітей і підлітків до грамотного, виваженого і критичного споживання та оцінювання інформації, вироблення психологічної та інформаційної стійкості до дезінформації і фейків. Завдяки заняттям всі учасники отримали навички безпечної поведінки в Інтернеті, навчилися розпізнавати фейки. Крім цього, діти значно підвищили свій рівень володіння комп'ютерами,

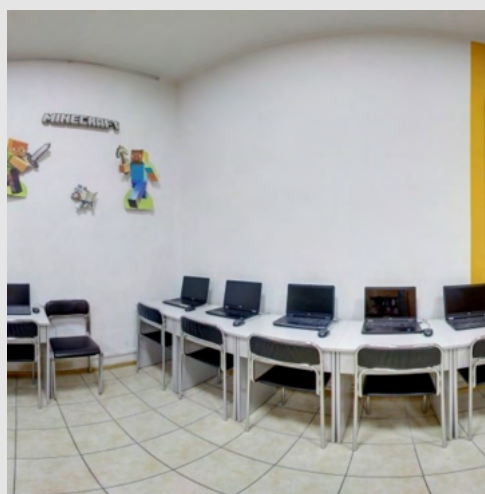


навчилися програмувати, дізнались про сучасні ІТ-тренди на лекторії, брали участь у майстерках з 3D-друку. В межах реалізації проєкту відбулися:

1. Навчальні курси для дітей 8-15 років з такої тематики:

- 3D-моделювання
- Scratchновачок
- Курс розмовної англійської
- Курс програмування «JAVA»
- Курс програмування «PYTHON»
- Курс програмування «HTML+CSS»

Всього відбулося 91 заняття, навчання пройшов 81 учасник.



2. ІТ-лекторій, тематика занять:

- Хто такі чатботи або як навчити програму розмовляти
- Безпечно в інтернеті – 8 занять
- Медіаграмотність
- Створення мобільних додатків
- Кібербезпека
- Створення модів для майнкрафт
- Професія графічний дизайнер

Всього відбулося 25 лекцій, в яких взяли участь 484 людини.

3. Для підлітків 10-13 років відбулись психологічні тренінги з психологом з циклу Softskills: ефективні комунікації, як стати лідером, робота в команді тощо. Всього проведено 7 тренінгів в яких взяло участь 122 учасники.

4. Відбулось 3 вебінари для працівників бібліотек України. Тематика вебінарів:

- Як не загубитися в п'ятій стихії?
- Інформаційні технології як засіб підвищення мотивації до читання
- Ефективна комунікація. Розповідай про себе так, щоб тебе почули і зрозуміли.

Вебінари відбувались онлайн у стримінговому режимі. Їх відвідало 350 бібліотекарів. За матеріалами проєкту створено збірку матеріалів «Як не загубитися в п'ятій стихії».

Також бібліотека розповсюдила апробовані практики для впровадження в бібліотеках України під час проведення вебінарів. Всього за час дії проєкту навчання пройшли: 81 дитина, 484 дитини взяли участь в ІТ-лекторії, 650 бібліотекарів пройшли навчання на вебінарах. Всього участь у заходах проєкту взяло 1215 людей, з них 522 – офлайн.

За цей проєкт бібліотека отримала міжнародну премію EIFL Public Library Innovation Award. У межах премії бібліотеці нададуть 1500 доларів, кубок, сертифікат, рекламу через вебсайт EIFL та широку мережу контактів.

Бібліотекарі відділу інформаційно-бібліографічних послуг та краєзнавства Кіровоградської обласної бібліотеки для юнацтва ім. Є. Маланюка для студентів міського медичного фахового коледжу ім. Є. Й. Мухіна в рамках Школи інформаційного комфорту провели **медіа-інформ з елементами тренінгу «Інформаційна безпека під час війни»**. Під час заходу студенти аналізували зміни, що відбулися останнім часом у споживанні інформації, сканували власне медіаполе; на конкретних прикладах переконалися, наскільки важливо вміти ідентифікувати й контролювати власні емоції; обговорили, чому важливо перевіряти інформацію, та як орієнтуватися в інформаційному просторі. Методом мозкового штурму студенти навчилися розрізняти правдиву, помилково хибну та навмисно неправдиву інформацію під час війни.

Фахівці Державної науково-педагогічної бібліотеки України імені В. О. Сухомлинського НАПН України у 2023 році в рамках відзначення міжнародного Дня безпечного інтернету провели методичний івент **«Інформаційна безпека дітей під час війни»**, ознайомитися з яким можна за посиланням: <https://www.youtube.com/watch?v=pwgmFaZBjNc>.

В рамках Школи професійного навчання група фахівців Житомирської обласної бібліотеки для дітей та юнацтва протягом березня-квітня 2023 року взяла участь в навчальному курсі **«Інформаційна гігієна під час війни»**. Курс охоплює 4 модулі:

- «Інформаційне поле під час війни»
- «Як працює російська пропаганда»
- «Інформаційно-психологічні спеціальні операції»
- «Базові правила інформаційної гігієни».

Тренерка курсу – Галина Козаченко, головний бібліотекар науково-методичного відділу Житомирської ОУНБ імені Олега Ольжича.

На початку та наприкінці навчання учасниці пройшли вхідне та вихідне тестування базових та отриманих на курсі знань і навичок інформаційної безпеки. За результатами проходження курсу учасниці отримали сертифікати Регіонального тренінгового центру для бібліотекарів.

Тренінги побудовані за структурою відеокурсу «Інформаційна гігієна під час війни» освітнього онлайн-ресурсу «Prometheus» (про який згадувалося у попередньому розділі).

Бібліотека-філія сімейного читання № 11 ЦБС Шевченківського району м. Харкова пропонує до уваги своїх читачів онлайн-тренінг з інформаційної безпеки **«Інформаційна гігієна в інтернет-середовищі»**, який можна переглянути онлайн за посиланням: <http://surl.li/npmeod>.

У цьому розділі представлена лише частина досвіду роботи бібліотек України у напрямі інформаційної гігієни. Проте і цей досвід, і поданий у пораднику матеріал, і вказані ресурси з теми «Інформаційна гігієна» дозволять всім зацікавленим бібліотечним фахівцям поглибити свої знання та на їх основі підготувати відповідні заходи (тренінги, вебінари, лекції та ін.) для навчання, наприклад, сільських бібліотекарів (для публічних / центральних бібліотек), жителів своїх громад.

ДЖЕРЕЛА

1. 8 дієвих способів розпізнати фейкову інформацію // Громадський простір. – Електрон. текст. дані. – 2021, 30 серп. – Режим доступу: <http://surl.li/efshxs> (дата звернення: 31.07.2024). – Назва з екрана.
2. Вплив інформаційного середовища на психічне здоров'я та благополуччя // Міністерство охорони здоров'я України. – Електрон. текст. дані. – Режим доступу: <http://surl.li/rgnwmu> (дата звернення: 31.07.2024). – Назва з екрана.
3. 10 простих способів захиститися від шахрайства у соціальних мережах. Швидше за все, ви їх не застосовуєте // NEW VOICE. – Електрон. текст. дані. – 2023, 3 жовт., 04:40. – Режим доступу: <http://surl.li/gupmxv> (дата звернення: 31.07.2024). – Назва з екрана.
4. Дослідження рівня інфогігієни українських користувачів Facebook (4-а хвиля) : стаття, результати дослідження // #Якнестатиовочем. – Електрон. текст. дані. – 2023, січ. – Режим доступу: <https://www.oksanamoroz.com/doslidzhennya> (дата звернення: 31.07.2024). – Назва з екрана.
5. Звіт про роботу КЗЛОР «Львівська обласна бібліотека для дітей» у 2023 році. – Львів. – 2024. – Режим доступу: <https://lodb.org.ua/assets/files/zvit-golovnyj-2023.pdf> (дата звернення: 31.07.2024). – Назва з екрана.
6. Індекс медіаграмотності українців віком від 66 років майже на 30% нижчий від загального : дослідження // Укрінформ. – Електрон. текст. дані. – Режим доступу: <http://surl.li/uoeebc> (дата звернення: 31.07.2024). – Назва з екрана.
7. Інформаційна безпека під час війни // Кіровоградська обласна бібліотека для юнацтва ім. Є. Маланюка. – Електрон. текст. та зображув. дані. – Режим доступу: <https://lib.kr.ua/?p=51868> (дата звернення: 31.07.2024). – Назва з екрана.
8. Інформаційна гігієна під час війни. Базові правила / Центр цифрової освіти та медіакультури // YouTube. – Електрон. текст. та відеодані. – 2023, 8 лют. – Режим доступу: <http://surl.li/gsmkoz> (дата звернення: 31.07.2024). – Назва з екрана.
9. Інформаційна гігієна під час війни : навч. курс // Prometheus. – Електрон. текст. дані. – Режим доступу: <http://surl.li/rsdnax> (дата звернення: 31.07.2024). – Назва з екрана.

10. Інформаційна гігієна. Як розпізнати брехню в соцмережах, в інтернеті та на телебаченні : навч. курс // Prometheus. – Електрон. текст. дані. – Режим доступу: <http://surl.li/edywpe> (дата звернення: 31.07.2024). – Назва з екрана.

11. Користувачі публікують фото в стилі Барбі та Кена, згенеровані нейромережею. Але до неї є багато питань / ред. В. Ворожко // MC.today = Media for Creators. – Електрон. текст. дані. – 2023, 26 лип. – Режим доступу: <http://surl.li/zgriju> (дата звернення: 31.07.2024). – Назва з екрана.

12. Масюк М. Львівська обласна бібліотека для дітей отримала міжнародну премію за проект для ВПО / Марія Масюк // ZAXID.NET. – Електрон. текст. та зображув. дані. – 2024, 26 січ., 14:12. – Режим доступу: <http://surl.li/bzgyki> (дата звернення: 31.07.2024). – Назва з екрана.

13. Медіаграмотність: як не піддаватися маніпуляціям? : навч. курс // Prometheus. – Електрон. текст. дані. – Режим доступу: <http://surl.li/tcbmaz> (дата звернення: 31.07.2024). – Назва з екрана.

14. Методичний івент «Інформаційна безпека дітей під час війни» / ДНПБ України ім. В. О. Сухомлинського // YouTube. – Електрон. текст. та відеодані. – 2023, 7 лют. – Режим доступу: <http://surl.li/rsqnsf> (дата звернення: 31.07.2024). – Назва з екрана.

15. Мороз О. Інформаційна гігієна під час війни: 7 базових правил / Оксана Мороз // Освіторія Медіа. – Електрон. текст. та зображув. дані. – Режим доступу: <http://surl.li/vcaxpj> (дата звернення: 31.07.2024). – Назва з екрана.

16. Некрасов В. Фейкові друзі. Чому соцмережі заповнили шахраї і як з ними боротися / Всеволод Некрасов // Економічна правда. – Електрон. текст., зображув. та граф. дані. – 2022, 13 серп., 10:30. – Режим доступу: <http://surl.li/cscwpy> (дата звернення: 31.07.2024). – Назва з екрана.

17. «П'ята стихія» // Львівська обласна бібліотека для дітей. – Електрон. текст. та зображув. дані. – Режим доступу: <http://surl.li/dzkjes> (дата звернення: 31.07.2024). – Назва з екрана.

18. Сімейний курс з інформаційної гігієни / Як не стати овочем // YouTube. – Електрон. текст. та відеодані. – Режим доступу: <http://surl.li/zoeeqn> (дата звернення: 31.07.2024). – Назва з екрана.

19. Соцмережі витісняють телебачення як джерело інформації : дослідження // Укрінформ. – Електрон. текст., зображув. та граф. дані. – 2024, 22 квіт., 19:08. – Режим доступу: <http://surl.li/zlbfwk> (дата звернення: 31.07.2024). – Назва з екрана.

20. Українці стали частіше користуватися інтернетом, 80% – онлайн щодня: соціопитування // United Nations Development Programme. – Електрон. текст. та зображув. дані. – 2024, 26 січ. – Режим доступу: <http://surl.li/turndd> (дата звернення: 31.07.2024). – Назва з екрана.

21. Шахрайство у соцмережах: як уберегтися? // TransferGo. – Електрон. текст. дані. – 2023, 8 серп. – Режим доступу: <http://surl.li/pclbbk> (дата звернення: 31.07.2024). – Назва з екрана.

22. Що таке двофакторна автентифікація, і як вона працює? // Державна служба спеціального зв'язку та захисту інформації України. – Електрон. текст. дані. – Режим доступу: <http://surl.li/ucozyb> (дата звернення: 31.07.2024). – Назва з екрана.

14000 м. Чернігів, просп. Миру, 41,
Чернігівська ОУНБ імені Софії та Олександра Русових,
науково-методичний відділ.
Тел.: (0462) 77-45-44
E-mail: metodvid@ukr.net