



Антон ШИМАНЮК,
вчитель інформатики Судилківського ліцею Шепетівського району

Інформаційна гігієна в епоху діпфейків: практичні аспекти кібербезпеки для учнів НУШ

Анотація

У статті розглянуто актуальні питання формування цифрової стійкості учнів у середовищі Нової української школи (НУШ) в умовах стрімкого розвитку технологій штучного інтелекту. Підвищену увагу приділено феномену діпфейків як одній із ключових загроз сучасній кібербезпеці та медіагігієні. Також запропоновано методичні рекомендації та практичні вправи для уроків інформатики, спрямовані на розвиток навичок критичного аналізу візуального та аудіоконтенту. Окреслено алгоритми верифікації інформації та захисту персональних даних підлітків у соціальних мережах. Матеріали статті мають практичне спрямування та можуть бути використані вчителями інформатики, класними керівниками та адміністрацією закладів освіти для підвищення рівня кіберкультури учнів.

Ключові слова: кібербезпека, штучний інтелект, діпфейк, медіагігієна, Нова українська школа, цифрова грамотність.

Вступ

Сучасне інформаційне суспільство характеризується стрімким розвитком цифрових технологій, зокрема систем штучного інтелекту, які активно використовуються у створенні мультимедійного контенту. Одним із найбільш дискусійних явищ останніх років стали технології *deepfake*, що дозволяють створювати реалістичні, але фальсифіковані відео- та аудіоматеріали.

У контексті освітньої реформи НУШ важливого значення набуває формування інформаційної культури та критичного мислення учнів. Сучасні школярі активно користуються соціальними мережами, цифровими платформами та мобільними додатками, що робить їх потенційно вразливими до інформаційних маніпуляцій, кібербулінгу та поширення фейкових новин.

Враховуючи зазначені виклики, актуальним є дослідження ефективних методів інтеграції медіаграмотності та кібербезпеки в навчальний процес. Особлива увага приділяється використанню інтерактивних вправ, кейсів та технологій аналізу медіа, що моделюють реальні загрози цифрового середовища. Отож, стаття спрямована не лише на опис проблеми, а й на пропозицію практичних рішень, які можуть бути застосовані у реальному освітньому процесі. Запропоновані підходи окреслюють поєднання наукового аналізу та педагогічної практики.

Саме тому питання інформаційної гігієни та кібербезпеки повинні стати невід'ємною складовою освітнього процесу, зокрема на уроках інформатики, оскільки без-

пека в сучасному інформаційному суспільстві розглядається як важлива соціально-гуманітарна категорія, що пов'язана із захистом особистості та інформаційного простору [11].

Аналіз останніх досліджень і публікацій

Проблема інформаційної безпеки та медіаграмотності у цифровому середовищі активно досліджується як українськими, так і зарубіжними науковцями. Значна увага приділяється впливу технологій штучного інтелекту на інформаційний простір та ризикам, пов'язаним із поширенням діпфейків [5].

Питання розвитку цифрової грамотності та інформаційної культури учнів розглядаються у працях українських дослідників В. Бикова, Н. Морзе, О. Кузьмінської, які підкреслюють необхідність формування цифрових компетентностей як складової сучасної освіти [1, 2].

Цифрова трансформація суспільства потребує нових підходів до навчання, зокрема інтеграції медіаграмотності та кібербезпеки у зміст навчальних дисциплін [4].

Сучасні дослідження також демонструють важливість освітніх програм, спрямованих на розвиток цифрової грамотності. Зокрема, результати експериментального дослідження серед школярів показали, що після проходження спеціальних навчальних воркшопів з тематики штучного інтелекту та медіабезпеки учні демонструють підвищений рівень обізнаності щодо ризиків синтетичного медіаконтенту, включно з діпфейками [8].

Дослідження у сфері медіакомунікацій показують, що стрімке поширення таких технологій може підірвати довіру до медіа, посилювати дезінформацію та створювати нові форми кібербулінгу [9].

Незважаючи на значну кількість досліджень у сфері цифрової грамотності та інформаційної безпеки, питання формування навичок інформаційної гігієни учнів у контексті поширення діпфейків потребує подальшого вивчення. Актуальним є розроблення практичних методик та навчальних вправ, які можна інтегрувати у навчальний процес НУШ.

Мета статті

Метою статті є аналіз проблеми поширення діпфейків у цифровому середовищі та визначення практичних методів формування інформаційної гігієни і навичок кібербезпеки в учнів НУШ. У статті також запропоновано практичні вправи та методичні рекомендації, спрямовані на розвиток навичок критичного аналізу медіаконтенту та безпечної поведінки учнів у цифровому середовищі.

Основний виклад матеріалу

1. Діпфейки як виклик інформаційній безпеці

Термін *deepfake* (діпфейк) виник на перетині понять *deep learning* (глибинне навчання) та *fake* (підробка). Це продукт генеративного штучного інтелекту, що базується на використанні генеративно-змагальних мереж (GAN). Механіка цієї технології полягає у взаємодії двох алгоритмів: один створює контент (генератор), а інший намагається відрізнити його від реальності (дискримінатор). Цей цикл повторюється тисячі разів, доки підробка не стане практично, яку не можна відрізнити від оригіналу для людського ока [10]. Завдяки швидкому розвитку обчислювальних технологій та доступності інструментів штучного інтелекту створення подібного контенту стало значно простішим. Існує велика кількість онлайн-сервісів та мобільних додатків, що дозволяють генерувати синтетичні відео та аудіо навіть користувачам без спеціальних технічних знань. Це значно підвищує ризики поширення маніпулятивного контенту в соціальних мережах та ускладнює процес перевірки достовірності інформації [11]. Якщо раніше створення якісного діпфейка потребувало значних потужностей та спеціальних знань, то сьогодні, завдяки мобільним додаткам та хмарним сервісам, синтетичний контент став доступним кожному підлітку. Це перетворює діпфейки з технологічної цікавинки на серйозний інструмент дестабілізації. Основні типи діпфейк-контенту, що найчастіше зустрічаються в цифровому середовищі, подано на рисунку.

Що таке діпфейк (Deepfake)?

Діпфейк – це синтетичний медіа (відео, аудіо або зображення), створений за допомогою штучного інтелекту (ШІ), щоб імітувати зовнішність, голоси або дії реальних людей



1. Діпфейк-відео
Діпфейк-відео дозволяє повністю змінити обличчя людини або навіть створити підроблене відео, де вона говорить або робить те, чого не було в реальності



2. Клонування голосу (voice cloning)
ШІ аналізує голос людини і здатен відтворювати його, копіювати інтонації та манеру мовлення, імітуючи реального мовця



3. Фейкові зображення людей
ШІ може створювати надзвичайно реалістичні підроблені зображення, що виглядають як справжні фото неіснуючих осіб

2. Розширений спектр загроз у молодіжному середовищі

Для учнів НУШ загрози, пов'язані з діпфейками, виходять за межі простого перегляду «смішних відео». Ми виділяємо наступні критичні аспекти:

- Когнітивна деформація та поява діпфейків створює небезпечний побічний ефект. Коли люди знають, що будь-яке відео може бути підробкою, вони починають сумніватися в автентичності реальних доказів. Це підриває саму

концепцію об'єктивної істини, що є особливо небезпечним для несформованого критичного мислення підлітків.

- Синтетичний кібербулінг та деградація репутації. Найбільш болючим аспектом для шкільного середовища є створення «непристойних» або компрометуючих зображень/відео з обличчями однокласників чи вчителів. Навіть якщо факт підробки згодом доводять, психологічна шкода та репутаційні втрати для жертви можуть бути незворотними.

- Соціальна інженерія та витончене шахрайство. Сучасні діпфейки здатні імітувати не лише зовнішність, а й голос (*voice cloning*). Шахраї можуть телефонувати підліткам, імітуючи голос батьків чи друзів, з проханням переказати кошти або розкрити паролі від соціальних мереж.

- Інформаційні операції (ІПСО): в умовах геополітичної нестабільності діпфейки стають зброєю в інформаційних війнах. Поширення фальшивих звернень лідерів думок чи політиків може спричинити паніку або дезорієнтувати молодь, яка є найбільш активним споживачем швидкого контенту в TikTok та Telegram.

Учні часто сприймають цифровий світ як простір гри, не усвідомлюючи, що будь-який цифровий слід — коротке відео в Stories або випадкове селфі — може стати «паливом» для нейромережі. Формування навичок критичного аналізу медіаконтенту є важливою складовою підготовки учнів до життя в сучасному інформаційному суспільстві. Зараз Інформаційна гігієна є складовою цифрової грамотності. Це комплекс навичок, правил і стратегій безпечного споживання, аналізу та поширення інформації в цифровому середовищі. Вона є невід'ємною складовою цифрової грамотності, що дозволяє учням усвідомлено взаємодіяти з інформаційними ресурсами, захищати власні дані та критично оцінювати отриманий контент [6]. Основні принципи інформаційної гігієни для школярів НУШ можна систематизувати наступним чином:

- Перевірка джерела інформації. Учні слід навчити звертати увагу на автора, дату публікації та репутацію ресурсу. Надійне джерело має прозору інформацію про автора та видавця, містить контакти та публікує дані, що можна перевірити через інші незалежні ресурси. Прикладом може бути використання зворотного пошуку для перевірки зображень або відео, що дозволяє визначити їх походження та достовірність.

- Критичний аналіз контенту. Важливо оцінювати логічність, послідовність та достовірність інформації. Учнім рекомендується порівнювати повідомлення у декількох джерелах, звертати увагу на можливі суперечності, маніпулятивні техніки та емоційне навантаження контенту. Це дозволяє формувати навичку «повільного перегляду», коли користувач аналізує кожен елемент повідомлення, а не сприймає його на емоціях.

- Обмеження поширення неперевіреної інформації. Учні повинні усвідомлювати відповідальність за поширення фейкових новин та синтетичного контенту. Перед репостом або коментарем варто перевірити достовірність інформації, оцінити джерело та можливу мету публікації. Це не лише знижує ризик дезінформації, а й формує культуру відповідального цифрового громадянства.

- Захист персональних даних. Публікація особистих фото, адреси проживання, контактів або інших конфіденційних даних у відкритих мережах створює ризик для безпеки підлітка. Вчителі повинні навчати учнів викорис-

товувати налаштування приватності, обмежувати коло підписників і регулярно переглядати власні цифрові сліди. Особлива увага приділяється тому, що навіть короткі відео або селфі можуть бути використані для створення дідфейків або шахрайських схем.

Систематичне впровадження цих принципів на уроках інформатики та інтеграція їх у міжпредметні проекти сприяє формуванню у школярів відповідальної поведінки в цифровому середовищі та підвищує їхню стійкість до інформаційних загроз [7].

3. Методичні підходи до формування навичок кібербезпеки

Узагальнені та представлені у таблиці вправи спрямовані на розвиток у школярів практичних навичок аналізу медіаконтенту, перевірки достовірності інформації та безпечної поведінки в цифровому середовищі. Їх використання під час уроків інформатики дозволяє поєднати теоретичні знання з практичною діяльністю учнів, що сприяє формуванню критичного мислення та відповідального ставлення до інформації.

Практичні вправи для формування інформаційної гігієни та кібербезпеки учнів НУШ

Назва вправи	Мета	Методика проведення	Критерії оцінки
«Знайди фейк»	Розвиток навичок критичного аналізу візуального контенту	Учням демонструють відео або зображення, серед яких є дідфейк. Завдання — визначити підробку та пояснити вибір	Природність кліпання очей; контур обличчя; відповідність аксесуарів; логічність рухів
«Аналіз звуку та мовлення»	Розпізнавання синтетичного аудіоконтенту	Учні слухають аудіозаписи і визначають підроблений контент	Присутність природних пауз та дихання; відсутність «металевого» відлуння; емоційна інтонація
«Алгоритм перевірки інформації»	Формування навичок перевірки достовірності джерел	Кроки: перевірка автора, дати публікації, підтвердження в інших джерелах, зворотний пошук зображень, аналіз мети публікації	Чіткість і послідовність перевірки; аргументованість висновків
«Безпечні соціальні мережі»	Підвищення обізнаності щодо захисту персональних даних	Аналіз власних профілів: налаштування приватності, відкритість даних, коло підписників, потенційні ризики поширення фото/відео	Розуміння та застосування налаштувань приватності; усвідомлення ризиків; рекомендації щодо безпечного використання
«Кейс-аналіз»	Інтеграція теоретичних знань у практику	Учні розглядають реальні або змодельовані випадки кібербулінгу чи поширення дідфейків, пропонують шляхи реагування	Аргументованість рішень; використання алгоритмів перевірки інформації; критичне мислення

4. Роль учителя у формуванні кіберкультури та цифрової стійкості

В освітній парадигмі Нової української школи роль учителя інформатики зазнає суттєвої трансформації. Він перестає бути лише джерелом технічних інструкцій і стає ментором цифрового громадянства. Формування цифрової компетентності вчителя стає ключовим фактором успішного впровадження уроків з медіаграмотності та кібербезпеки [3]. Вчитель, повинен критично мислити, бо його основним завданням є перехід від моделі «запам'ятовування фактів» до моделі «аналізу джерел». Він має стимулювати учнів ставити під сумнів будь-який сумнівний медіний контент. Важливо впроваджувати стратегію «повільного перегляду», коли під час уроку детально розбирається кожна деталь медіаповідомлення. Педагог має власним прикладом демонструвати високий рівень кіберкультури. Це включає:

- Етику використання ШІ: Пояснення учням різниці між креативним використанням нейромереж та створенням шкідливого контенту.
- Культуру поширення: Формування звички «спочатку перевіри — потім репости». Учитель має наголошувати на



юридичній та моральній відповідальності за поширення дезінформації.

Також формування інформаційної гігієни не повинно обмежуватися лише уроками інформатики. Вчитель має виступати ініціатором інтегрованих занять:

- Інформатика + Історія: Аналіз історичних фальсифікацій та порівняння їх із сучасними дідфейками.
- Інформатика + Мистецтво: Вивчення того, як технології ШІ змінюють поняття авторства та візуальної естетики.



• Інформатика + Правознавство: Розгляд кейсів щодо порушення приватності через використання чужого цифрового образу (обличчя чи голосу).

Потрібно не забувати: кіберкультура учня починається в родині, тому вчитель інформатики стає ключовою ланкою у просвіті батьків. Проведення воркшопів для дорослих щодо налаштувань батьківського контролю та розпізнавання шахрайства за допомогою дипфейків допомагає створити цілісне безпечне середовище навколо дитини.

Технології дипфейків розвиваються швидше за навчальні програми. Здатність педагога оперативно освоювати нові детектори ШІ-контенту та адаптувати їх до навчального процесу є запорукою того, що школа залишатиметься актуальною для сучасного покоління учнів, які активно взаємодіють із цифровими технологіями.

Висновок

У сучасному цифровому середовищі проблема поширення дипфейків стає дедалі актуальнішою. Учні НУШ повинні володіти не лише базовими цифровими навичками, а й умінням критично аналізувати інформацію, перевіряти джерела та захищати власні персональні дані. Використання практичних вправ, інтерактивних методів навчання та інтеграції тем інформаційної гігієни у шкільну програму сприятиме формуванню відповідальної поведінки учнів у цифровому просторі.

Подальші дослідження можуть бути спрямовані на розроблення комплексних освітніх програм з медіаграмотності та кібербезпеки для різних вікових груп школярів, що підтверджується сучасними дослідженнями у сфері цифрової освіти [8]. Запропоновані у статті методичні підходи та практичні вправи можуть бути використані під час викладання інфор-

матики, а також у межах міжпредметної інтеграції з курсами громадянської освіти, медіаграмотності та правознавства. Отже, систематичне формування навичок інформаційної гігієни сприятиме підвищенню рівня цифрової культури учнів та їхньої готовності до безпечної взаємодії з інформацією в умовах розвитку технологій штучного інтелекту.

Використані джерела

1. Биков В. Ю. Цифрова трансформація освіти і науки: теорія та практика. Київ: Інститут цифровізації освіти НАПН України, 2021. – С. 312.
2. Морзе Н. В., Кузьмінська О. Г. Цифрова компетентність сучасного вчителя. Інформаційні технології і засоби навчання. 2017. №5. – С. 1–14.
3. Овчарук О. В. Цифрова компетентність вчителя в умовах реформування освіти. Київ: НАПН України, 2019. – С. 45–52.
4. Биков В. Ю., Спірін О. М., Пінчук О. П. Проблеми та перспективи розвитку цифрової освіти. Інформаційні технології і засоби навчання. 2020. №1. – С. 1–15.
5. Дубов Д. В. Кібербезпека: світові тенденції та виклики для України. Київ: НІСД, 2019. – С. 128.
6. Литвинова С. Г. Інформаційна безпека учнів у цифровому освітньому середовищі. Інформаційні технології в освіті. 2020. №4. – С. 78–85.
7. Іванова І. Б. Медіаграмотність та критичне мислення в сучасній школі. Педагогіка і психологія. 2021. №2. – С. 54–60.
8. Hobbs R. Digital and Media Literacy. New York: Routledge, 2017. р. Режим доступу: <https://surl.li/kigvxx> – С. 45–60.
9. Романюк В. Трансформація медіаосвіти для протидії дезінформації: фактчекінг, стратегічні комунікації, ШІ // Образ. – 2025. – № 2. – С. 48.
10. Vaccari C., Chadwick A. Deepfakes and Disinformation. Social Media + Society. 2020. р. Режим доступу: <https://surl.li/djseyr> – С. 1–13.
11. Мудраков В. Феномен безпеки: соціально-гуманітарні виміри 2022. р. Режим доступу: <https://surl.li/kufnib> – С. 58–60.