

УДК 37:[316.658:004.9-049.5(477)]

DOI: <https://doi.org/10.31470/2786-6246-2023-3-14-21>

Валентина ГУБЕНКО,

*викладачка кафедри публічного управління та адміністрування
Університету Григорія Сковороди в Переяславі*

Valentina GUBENKO,

*A lecturer of the Department of Public management
of Hryhorii Skovoroda University in Pereiaslav*

ORCID: <https://orcid.org/0000-0003-4099-6933>

gubenko080570@ukr.net

ОСВІТА В УКРАЇНІ І ОСНОВИ ПРАВОВОГО АСПЕКТУ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ

EDUCATION IN UKRAINE AND FUNDAMENTALS OF THE LEGAL ASPECT OF COUNTERING INFORMATION THREATS

***Анотація.** У статті розглянуто проблеми вразливості Української держави в умовах інформаційної війни, правовий аспект протидії інформаційним загрозам, зокрема, що стосується освіти в Україні. Акцентуємо увагу на те, що технічні можливості інформаційно-комп'ютерних систем, нові програми, які знаходять дедалі ширше застосування у освітньому процесі, дозволяють використовувати колосальні обсяги інформації. Але це несе з собою не лише нові можливості, але й нові загрози для молодого покоління. На питання інформаційної безпеки в системі освіти все більше звертають увагу не лише вчені-дослідники, а й державні службовці, освітяни, батьки учнівської та студентської молоді.*

У роботі описано основні загрози, серед них: руйнування єдиного інформаційного простору держави; маніпуляція суспільною думкою, недостатня координація діяльності органів державної влади, слабкість системи освіти та виховання, протиправне застосування спеціальних засобів впливу на суспільну свідомість, загострення міжнародної конкуренції за володіння інформаційними технологіями та ресурсами; діяльність міжнародних терористичних організацій; недостатність нормативної правової бази, що регулює відносини в інформаційній сфері, а також недостатня практика застосування права. В інформаційній війні виділяються три основних мети: контроль інформаційного простору і забезпечення захисту своєї інформації від ворожих дій; використання контролю над інформаційним простором для проведення інформаційних атак на противника; підвищення загальної ефективності збройних інформаційних функцій. Розглянуто складові інформаційних воєн та описано пріоритетні напрями державної інформаційної політики та важливі кроки з боку владних органів України. Формування суспільної свідомості за допомогою суб'єктів інформаційної війни з використанням методів психологічного впливу стає найбільш ефективним способом контролю і маніпуляції як всередині держави, так і за її межами. Все залежить від того, хто фактично визначає інформаційний контент. Таким чином, наше ставлення до проблем і явищ, навіть сам підхід до того, що вважати проблемою або явищем, багато в чому визначені тими, хто контролює світ комунікацій.

***Ключові слова:** інформація, інформаційні загрози, система освіти, державна політика, контроль, маніпуляції.*

***Annotation.** Information security is one of the main problems of modern society. This problem can be solved not only the technical and legal means, but also by means of education. The author considers the distinctive features of information security in the education of students, pupils of elementary, middle and high school. Assessment of pedagogical tools is taking into account the age and social psychology. The author demonstrates the dynamics of threats at each age and offers his vision of the concept of «information security» for each group of children and youth.*

The article describes the main threats: the destruction of the unified information space of the state; manipulation of public opinion, insufficient coordination of the activities of state authorities, weakness of the education and training system, illegal use of special means of influencing public consciousness, intensifying international competition for possession of information technologies and resources; activities of international terrorist organizations; insufficiency of the regulatory legal framework regulating relations in the information sphere, as well as insufficient practice of applying the law. In the information war, three main goals are distinguished: control of the information space and ensuring the protection of one's information from hostile actions; use of control over the information space to carry out information attacks on the enemy; increasing the overall efficiency of armed information functions. The components of information wars are considered and the priority directions of the state information policy and important steps taken by the authorities of Ukraine are described. The formation of public consciousness with the help of subjects of information war using methods of psychological influence becomes the most effective way of control and manipulation both within the state and outside it. It all depends on who actually determines the information content. Thus, our attitude to problems and phenomena, even the very approach to what is considered a problem or phenomenon, is largely determined by those who control the world of communications.

***Key words:** information, information threats, education system, state policy, control, manipulation.*

Глобалізація суспільства, перехід на нову стадію свого розвитку як інформаційного суспільства, ознаменувався не лише появою не бачених до цього можливостей, а й появою нових видів загроз. Особливо небезпечні вони для молодого покоління, яке є інформаційно уразливим. Під впливом медійної інформації формуються світоглядні позиції людини, патріотизм, ціннісні орієнтири, закладаються підвалини правомірної чи неправомірної поведінки. Особливого значення це набуває у зв'язку із запровадженням у середній школі елементів медіа-освіти. Тож є підстави стверджувати, що проблеми інформаційної безпеки мають знаходитися у полі зору не лише фахівців в галузі національної безпеки, правознавців, філософів, соціологів, а й педагогів.

Мета статті – розглянути правовий аспект ряду інформаційних загроз та потреб забезпечення інформаційної безпеки в системі освіти України.

Матеріали та методи. При підготовці статті використано загальнонаукові методи аналізу і синтезу, абстрагування й узагальнення.

Результати розгляду питання. Інформаційний простір, інформація виступають не лише невід'ємною, але й визначальною складовою освітнього процесу. Достовірність інформації, її ґрунтовність, аргументація, опрацювання, дозволяють формувати науково-обґрунтовані уявлення здобувача освіти про державу та її кордони, суспільство, оточуючий світ і самого себе як окремого індивіда в площині сьогодення і майбутнього. Але випадкове чи цілеспрямоване пошкодження інформації, її недостовірність, викривлення, призводить до формування хибних уявлень, переконань, або ж порушує попереднє розуміння матеріалу та вступає у критичну суперечність, що може привести навіть до зникнення бажання продовжувати навчання.

Сьогодення – це час інформаційної ери в усіх галузях. Від народження ми вже в полоні різного виду інформації як про нас, так і для нас. Інформаційний потік неодмінно проходить через освіту, як ту галузь, яка формує майбутнє нашого суспільства. Інформація є невід’ємною складовою освітнього середовища і освітнього процесу.

Джерела інформаційних загроз:

- Оператори ботнет – це хакери, проте, замість отримання доступу до системи заради розваги або виклику, вони беруть під контроль декілька (від десятків до сотень та тисяч) систем для координації атак і для поширення фішингових схем, спаму і DoS-атак.

- Злочинні групи прагнуть атакувати системи заради грошової вигоди. Зокрема, організовані злочинні групи використовують спам, фішинг, шпигунські або шкідливі програми для скоєння крадіжки особистих даних і інтернет-шахрайства. Міжнародні корпоративні шпигуни і організовані злочинні організації становлять загрозу для усіх країн через їх здатність вести промислове шпигунство, провести великомасштабну грошову крадіжку і найняти та розвинути нового талановитого хакера.

- Іноземні спецслужби можуть використовувати кібер-інструменти як частину їх шпигунської діяльності. Крім того, деякі країни активно працюють над розробкою доктрини інформаційної війни та програм. Такі програми дають змогу одному об’єкту мати значний вплив на торгівлю, зв’язок та економічну інфраструктуру, що підтримують військову міць країн.

- Хакери зламують мережі заради гострих відчуттів від «перемоги» або заради підвищення свого статусу у хакерському співтоваристві або заради грошей. У той час як дистанційне отримання доступу до комп’ютера потребує невеликої кількості знань, хакери можуть завантажити сценарії атак і протоколи з мережі Інтернет і запустити їх проти сайту жертви. Таким чином, в той час як шкідливе програмне забезпечення стає більш витонченим, воно також стає простішим у використанні.

- Інсайдер – людина, що незадоволена своєю роботою в організації, чи організацією в цілому. Така людина може стати основним джерелом комп’ютерних злочинів. Інсайдерам не потрібен високий рівень знань щодо злому системи, тому що їх знання про цільову систему дозволяє їм отримувати майже необмежений доступ, щоб викликати пошкодження системи або щоб вкрасти дані системи.

- Терористи прагнуть знищити, знешкодити або використати критичні інфраструктури для того, щоб поставити під загрозу національну безпеку країн, привести до масових жертв, послабити економіку цілих країн або окремих організацій [2].

На рівні держави повинна враховуватись необхідність реалізації інформаційної безпеки в галузі освіти, що набуває особливої гостроти в сучасних умовах війни. Розглянемо предметно.

Саме інформаційна сфера є однією з найбільш важливих, і її захист визначається серед пріоритетів державної політики. Необхідність підтримання безпеки схвалена на державному рівні, що пояснює активну діяльність уповноважених органів влади спрямовану на забезпечення інформаційної безпеки відносин, пов’язаних із збиранням, накопиченням, обробкою та передачею інформації. Проблематику інформаційних загроз в Україні вивчають науковці, але є й загальнодержавні нормативно-правові акти. Указом Президента України від 28 грудня 2021 р. №685/2021 підписано Стратегію інформаційної безпеки, в якій визначено поняття інформаційної загрози як потенційно або реально негативного явища, тенденції і чинника інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні [9]. Це визначення більш сконцентроване на інтересах держави, тоді як інтереси суспільства чи тим більше –

окремої людини, лишаються без уваги. В Стратегії розглядаються навіть такі джерела інформаційних загроз як соціальні мережі, зокрема говориться «збільшення кількості соціальних мереж, їх інтегрованість з іншими соціальними сервісами повсякденного користування, а також специфіка організації всесвітньої мережі Інтернет ставлять під загрозу гарантії права особи на приватність» [9]. Дане формулювання є вкрай важливим саме в контексті освітянського середовища. Відкрита особиста інформаційна політика окремої людини може призвести до надмірного інформування як її близького оточення, так і сторонніх осіб, стосовно подробиць її роботи, стану здоров'я, відпочинку, кола спілкування, стосунків, її думок і переживань.

Також сьогодні існує необхідність запобігання негативним інформаційним впливам, таким як булінг, який набув широкого формату. Закон України «Про освіту» (п. 3.1 ст. 1) визначає булінг (цькування) як «діяння (дії або бездіяльність) учасників освітнього процесу, які полягають у психологічному, фізичному, економічному, сексуальному насильстві, у тому числі із застосуванням засобів електронних комунікацій, що вчиняються стосовно малолітньої чи неповнолітньої особи та (або) такою особою стосовно інших учасників освітнього процесу, внаслідок чого могла бути чи була заподіяна шкода психічному або фізичному здоров'ю потерпілого» [8].

Західні науковці присвячують проблемі виховання у молодого покоління раціональної інформаційної гігієни чимало уваги. В своїх працях Дж. Лукас (G. Loukas) та С. Муругесан (S. Murugesan) наголошують на потребі підтримки користувачів практичними технологічними рішеннями, які варіюють від позначення публікацій у соціальних мережах на основі аналізу вмісту до виявлення дипфейків, які можуть бути неочевидними для людського ока. На нашу думку, дослідники підкреслюють необхідність кращого розуміння проблеми через грамотність, освіту та підвищення обізнаності і практичної підтримки користувачів ефективними технічними рішеннями. А це є перспективним напрямком боротьби з інфодемією дезінформації [11]. Правда наразі не існує єдиного підходу до правильної інформаційної гігієни для закладів освіти. То ж обговорення і дискусії щодо прийнятності інформаційної гігієни в освітньому процесі триватимуть.

Ключові акценти розставлено на захисті прав і свобод здобувачів освіти та інших учасників освітнього процесу. Натомість, законодавство у галузі безпеки, навіть оперуючи дефініціями «національна безпека», «інформаційна безпека» та «національні інтереси», зосереджується, передусім, на інформаційній безпеці в інтересах держави, а не суспільства, чи тим більше – окремої людини. Наразі мало уваги приділяється також культурі інформації, навіть нівелюється це питання.

Небезпечними зі складними наслідками є засоби пропаганди на тимчасово окупованих територіях. У контексті питання відновлення регіонів, тимчасово окупованих росією в ході збройної агресії проти України, проблема соціальної реінтеграції місцевого населення нерідко залишається поза увагою, її розглядають як додатковий політичний фактор, а не окреме явище. Проте саме цей аспект є чи не найважчим викликом, що постане перед нами в процесі відбудови тимчасово окупованих територій. Засоби психологічних маніпуляцій зі смертельною ефективністю переконання, які використовує країна-агресор, майже ідентично відповідають «Вісьмом критеріям реформи мислення», запропонованим Робертом Ліфтоном у його книзі «Реформа мислення і психологія тоталітаризму» [10]. Можна визначити, що першим і найбільш вагомим інструментом, що використовується, є контроль над середовищем. З одного боку, існує технічна ізоляція, яка дозволяє контролювати інформаційне середовище: теле- і радіостанції відключені від українських каналів, заблокований вітчизняний та іноземний сегмент Інтернету. З іншого боку, полегшується доступ населення до російських інформаційних провайдерів.

У своїй праці «Формування людської ідентичності під впливом окупаційного режиму на тимчасово окупованих територіях України» суспільний аналітик Анастасія Коверга

підкреслила, як одна з респонденток розповіла їй, що за часів окупації свого населеного пункту, доводилося ходити на цвинтар, щоб відвідувати онлайн заняття в університеті, адже це було єдине місце, де можна було знайти будь-який сигнал, окрім російського. Якщо пошук альтернативного джерела інформації неможливий або потребує значних зусиль, люди просто починають задовольнятися тим, що мають, а мають вони безперешкодний потік класичної пропаганди. «Кожен факт обговорюється на всіх телеканалах цілий день. Це просто починає відкладатися в голові», – зазначає авторка. Особливо добре це працює з людьми, які не звикли до перевірки фактів чи медіаграмотності. Підсвідомо вибудовується логічний ланцюжок: один канал сказав факт, другий канал погодився, радіо підтвердило – значить, інформація має бути правдивою.

Окрім технічної ізоляції існує ще й фізична. Якщо подолання невеликої відстані у межах області потребувало перетину лінії розмежування, подорож може займати в місцевого населення до кількох діб. Для обмеження пересування між Україною та окупованими територіями створено систему контрольних-пропускних пунктів та офіційних процедур, що стало не лише фізичним, але й психологічним викликом для людей, які там проживають. Бачачи страждання інших, люди, які перетинають кордон, зазнають потужного емоційного стресу, спричиненого метафізичною провинною [1], страхом за власне життя та вторинною травматизацією [7]. Система офіційних процедур створює умови, в яких люди змушені брехати або приховувати факти, і це живить підсвідоме почуття провини. Чому? Навіщо? Перед ким? Фізичні та психологічні труднощі змушують людей на тимчасово окупованих територіях двічі подумати чи варто перетинати кордон, а якщо вони це роблять, то цей процес закарбовується в їхній підсвідомості як щось вкрай негативне.

На окупованих територіях широко використовуються містичні маніпуляції, щоб переконати людей у всемогутності та правоті діючого режиму, виправдати страшні наміри окупантів. Розмовляючи з тимчасово переселеними громадянам, можна помітити, що їм надавали точні дати і прогнози щодо гіпотетичних подій, наприклад, що Україна, нібито, спробує захопити Донецьку і Луганську області на початку весни 2022 р., навіть показували військові плани, а росія, напавши першою, випередила і врятувала Донеччину і Луганщину. Такі заяви поширюються як через офіційні ЗМІ, так і у вигляді «сарафанного радіо» (через «перевірених» осіб). Як наслідок таких маніпуляцій – людина опиняється в оточенні чуток і ілюзорно вірить, що «щось наближається». Так створюється психологічна напруга. Зачасту всі анонсовані події плануються і проводяться тимчасовою владою. І тут окупанти вдаються до лозунгів «ми це передбачили», «ми це попередили». Люди, не маючи змоги оцінити об'єктивно ситуацію, сприймають їх як рятівників, провидців.

До того ж часто пропаганда активно експлуатує навантаження мови, використовуючи специфічні слова або цілі фрази, що функціонують лише в межах пропагандистського лексикону. На прикладі України – це «Українські нацисти», «бандерівці», «ви вісім років бомбили Донбас», «на Україні» замість «в Україні», «українські фейки». Такі жаргони складаються з шаблонних кліше, які слугують для того, щоб змінити мислення громадян відповідно до нав'язливих потреб мислення групи. Багато людей «під впливом» не розуміють, що в Україні йде війна, яка загострилася у 2022 р., а не «спеціальна воєнна операція» [5].

Коли люди живуть під постійними обстрілами, в оточенні постійного відчуття страху і невизначеності, вони травмовані морально, а іноді і фізично – пропагандистська доктрина подається як остаточна істина. У цій війні немає нікого, кого б вона не зачепила особисто: руйнуються будинки, люди гинуть під снарядами, чоловіків примусово забирають до армії. Кожна людина має справу з гострим відчуттям несправедливості без будь-якого чіткого раціонального спрямування, і тут на допомогу приходить пропаганда. Пропаганда чітко, псевдологічно пояснює події, і призначає винних.

Не секрет, що східну Україну будували різні нації, вони вже обжилися на цій землі, а всі трагічні події і пропаганда навколо визначають свою картинку подій і загальний наратив нерідко звучить такий: «Америка (або Захід) все влаштувала, а українська влада продала їм країну», «українська влада маніпульована і русофобна», «ми просто хотіли бути незалежними республіками, а Україна на нас напала» [3].

В силу пропаганди, весь особистий досвід людини і загальні події підпорядковані системі, а все, що випадає за межі цієї системи, маркується як «фейк» або чергове підтвердження підступності та схибленості ворога. «Буча (місто, де відбулося одне з наймасовіших і найжорстокіших масових вбивств мирних жителів, скоєних російською армією) – це фейк, вигаданий українцями, щоб показати, що росіяни погані».

В силу інформації чітко окреслюється контраст між «ми» і «вони». З одного боку, Україна представляється бідною країною, що розвалюється, і бомбардує власні території, а Росія – «старшим братом», який прагне допомогти «республікам». Для підтвердження цього місцева тимчасова новостворена влада використовує класичну тактику популізму: задовольняє базові потреби населення, такі як соціальний захист у вигляді пенсій та інших виплат, низькі ціни на комунальні послуги, гуманітарна допомога тощо. Все це широко висвітлюється в ЗМІ як щедрість і благовоління Росії до свого протекторату. Державні свята також використовуються як ефективний політичний інструмент для цієї мети.

Пропаганда на тимчасово окупованих територіях працює над знищенням зв'язків зі старою ідентичністю. Люди, які змушені були отримати російські паспорти, переконані, що в Україні їх вважають зрадниками, і вони будуть покарані, якщо прийдуть туди. Паспорти, отримані на окупованих територіях, не мають повної юридичної сили в Росії, люди, які емігрували або евакуювалися, є об'єктом інтересу для спецслужб.

Але Україна боронить свою землю для своїх дітей. Щойно провідні країни усвідомили, що Україна не капітулювала й чинитиме опір, голоси на нашу підтримку остаточно переважили волання скептиків.

Для того, щоб користуватися можливостями Інтернет ресурсу, запобігти інформаційним загрозам, молодь має засвоїти основні правила безпечної роботи в Інтернеті:

- Використовуйте лише ліцензійне програмне забезпечення. Установлюйте програми тільки з офіційних джерел. Перед установленням читайте відгуки інших користувачів, якщо вони доступні.

- Установлюйте та оновлюйте антивірусне програмне забезпечення як на стаціонарні, так і на мобільні комп'ютери. Бажано, щоб оновлення антивірусних баз здійснювалося регулярно та автоматично.

- Завжди встановлюйте оновлення операційної системи та іншого програмного забезпечення.

- Використовуйте надійні паролі. Не використовуйте на різних інтернет-ресурсах один і той самий пароль, змінюйте його регулярно.

- Приєднуйтеся лише до перевірених Wi-Fi-мереж. Не відправляйте важливі дані (дані кредитних карток, онлайн-банкінгу тощо) через публічні та незахищені Wi-Fi-мережі.

- Установіть фільтр спливаючих вікон у браузері.

- Перевіряйте сертифікат безпеки сайтів у вигляді замка в адресному рядку браузера.

- Не відкривайте повідомлення електронної пошти від невідомих вам осіб і прикріплені до них файли, яких Ви не очікуєте.

- Подумайте про можливі ризики для вас перед тим, як викласти щось у мережу Інтернет.

- Створюйте резервні копії важливих для вас даних, зберігайте їх на носіях даних, відключених від мережі Інтернет [6].

Список використаних джерел:

1. «Вісім років». Деконструкція найпопулярнішого пропагандистського міфу Росії. URL: <https://rpr.org.ua/news/vosem-let-dekonstruktsiia-naypopuliarnishoho-propahandystskoho-mifu-rosii/>.
2. Джерела загроз. URL: <http://surl.li/flldr>.
3. Про внесення змін до деяких законів України щодо регулювання правового режиму на тимчасово окупованій території України: Закон України № 2217-IX від 21.04.2022 р. URL: <https://zakon.rada.gov.ua/laws/show/2217-20#n173>.
4. Про внесення змін до деяких законодавчих актів України щодо встановлення кримінальної відповідальності за колабораційну діяльність: Закон України № 2108-IX від 03.03.2022 р. URL: <https://zakon.rada.gov.ua/laws/show/2108-IX#Text>.
5. Нам мова болить: як об'єднати українців навколо української мови? URL: <https://osvitoria.media/experience/nam-mova-bolyt-yak-ob-yednaty-ukrayintsiv-navkolo-ukrayinskoji-movy/>.
6. Основні правила. URL: <https://www.miyklas.com.ua/p/informatica/10-klas/informatciini-tekhnologiyi-v-suspilstvi-322205/informatciina-bezpeka-navchannia-v-interneti-321523/re-0cf3c5d6-6a11-458b-b39d-889f102e9e71>.
7. Плетка О.Т. Вторинна травматизація: класифікація медіа травм. *Медіатравма в умовах інформаційної війни: психологічний та педагогічний аспекти. Матеріали Всеукраїнської науково-практичної конференції 20-21 червня 2017 р.* URL: <http://mediaosvita.org.ua/book/pletka-o-t-vtorynnatravmatyzatsiya-klafykatsiya-mediatravm/>.
8. Про освіту: Закон України № 2145-VIII від 05 вересня 2017 р. Офіційний Веб-сайт Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/2145-19#Text>.
9. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 р. «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2021 р. №685/2021. Офіційний веб-сайт Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#n2>.
10. Lifton Robert Jay. Thought Reform and the Psychology of Totalism: A Study of «Brainwashing» in China. 525 p.
11. Loukas G., Murugesan S. and Andriole S. J. «Information Hygiene: The Fight Against the Misinformation «Infodemic», in IT Professional, vol. 24, no. 2, pp. 16-18, 1 March-April 2022, doi: 10.1109/MITP.2022.3163007.

REFERENCES

1. «Visim rokov». Dekonstruktciya najpopulyarnishoho propahandysts'koho mifu Rosiyi [«Eight years». Deconstruction of the most popular propaganda myth of Russia]. *rpr.org.ua*. Retrieved from <https://rpr.org.ua/news/vosem-let-dekonstruktsiia-naypopuliarnishoho-propahandystskoho-mifu-rosii/> [in Ukrainian].
2. Dzherela zahroz [Sources of threats]. Retrieved from <http://surl.li/flldr> [in Ukrainian].
3. Pro vnesennya zmin do deyakykh zakoniv Ukrayiny shchodo rehulyuvannya pravovoho rezhymu na tymchasovo okupovaniy terytoriyi Ukrayiny: Zakon Ukrayiny № 2217-IXh vid 21.04.2022 r. [On the introduction of changes to some laws of Ukraine regarding the regulation of the legal regime in the temporarily occupied territory of Ukraine: Law of Ukraine № 2217-IX from April 21, 2022]. *zakon.rada.gov.ua*. Retrieved from <https://zakon.rada.gov.ua/laws/show/2217-20#n173> [in Ukrainian].
4. Pro vnesennya zmin do deyakykh zakonodavchykh aktiv Ukrayiny shchodo vstanovlennya kryminal'noyi vidpovidal'nosti za kolaboratsiyu diyal'nist': Zakon Ukrayiny № 2108-IXh vid 03.03.2022 r. [On amendments to some legislative acts of Ukraine regarding the establishment of criminal liability for collaborative activity: Law of Ukraine № 2108-IX from

March 3, 2022]. *zakon.rada.gov.ua*. Retrieved from <https://zakon.rada.gov.ua/laws/show/2108-IX#Text> [in Ukrainian].

5. Nam mova bolyt': yak ob'yednaty ukrayintsiv navkolo ukrayins'koyi movy? [Our language hurts: how to unite Ukrainians around the Ukrainian language?]. *osvitoria.media*. Retrieved from <https://osvitoria.media/experience/nam-mova-bolyt-yak-ob-yednaty-ukrayintsiv-navkolo-ukrayinskoyi-movy/> [in Ukrainian].

6. Osnovni pravyla [Basic rules]. *www.miyklas.com.ua*. Retrieved from <https://www.miyklas.com.ua/p/informatica/10-klas/informatciini-tekhnologiyi-v-suspilstvi-322205/informatciina-bezpeka-navchannia-v-interneti-321523/re-0cf3c5d6-6a11-458b-b39d-889f102e9e71> [in Ukrainian].

7. Pletka, O.T. (2017). Vtorynna travmatyzatsiia: klasyfikatsiia mediatravm [Secondary trauma: classification of media injuries]. Proceedings from Vseukrayins'ka naukovo-praktychna konferentsiya «*Mediatravma v umovakh informatsiinoi viiny: psykholohichni ta pedahohichni aspekty*» – AllUkrainian scientific-practical conf. «*Mediatrauma in the conditions of information war: psychological and pedagogical aspects*». Retrieved from <http://mediaosvita.org.ua/book/pletka-o-t-vtorynna-travmatyzatsiya-klasyfikatsiyamediatravm/> [in Ukrainian].

8. Pro osvitu: Zakon Ukrainy № 2145-VIII vid 05 veresnya 2017 r. [On education: Law of Ukraine №2145-VIII from September 5, 2017]. Ofitsiyyny Veb-sayt Verkhovnoyi Rady Ukrainy [Official Website of the Verkhovna Rada of Ukraine]. *zakon.rada.gov.ua*. Retrieved from <https://zakon.rada.gov.ua/laws/show/2145-19#Text> [in Ukrainian].

9. Pro rishennya Rady natsional'noyi bezpeky i oborony Ukrainy vid 15 zhovtnya 2021 r. «Pro Stratehiyu informatsiynoyi bezpeky»: Ukaz Prezydenta Ukrainy vid 28 hrudnya 2021 r. №685/2021 [On the decision of the National Security and Defense Council of Ukraine from October 15, 2021 «On Information Security Strategy»: Decree of the President of Ukraine from December 28, 2021 № 685/2021]. Ofitsiyyny veb-sayt Verkhovnoyi Rady Ukrainy [Official Website of the Verkhovna Rada of Ukraine]. Retrieved from <https://zakon.rada.gov.ua/laws/show/685/2021#n2> [in Ukrainian].

10. Lifton, Robert Jay. Thought Reform and the Psychology of Totalism: A Study of «Brainwashing» in China [in English].

11. Loukas, G., Murugesan, S. & Andriole, S.J. (2022). Information Hygiene: The Fight Against the Misinformation «Infodemic». *In IT Professional*, 24, 2, 16-18. DOI: 10.1109/MITP.2022.3163007 [in English].

*Подано до редакції 12.01.2023 р.
Прийнято до друку 22.02.2023 р.*