МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОСТРОЗЬКА АКАДЕМІЯ»
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ СОЦІАЛЬНО-ГУМАНІТАРНОГО МЕНЕДЖМЕНТУ
КАФЕДРА ЖУРНАЛІСТИКИ ТА PR-МЕНЕДЖМЕНТУ

Допущено до захисту
на засіданні кафедри журналістики та PR менеджменту
(протокол № 10 від 12 травня 2026 р.)
В.о. Завідувача кафедри _____Роман ШУЛИК

Кваліфікаційна робота у формі медіапроєкту
На здобуття освітнього ступеня бакалавра на тему:
«Мультимедійний лонгрід на тему: «Цифрова безпека українців: як розпізнати загрози і захистити себе онлайн»: особливості планування та реалізації»

Виконала студентка 4 курсу, групи Ж-41
Спеціальності 061 «Журналістика»
Пукаляк Вікторія Вікторівна

Науковий керівник – кандидат наук
з державного управління, доцент
КОСТЮЧЕНКО Олексій
Миколайович

Рецензент – кандидат наук з
державного управління, доцент
ШЕРШНЬОВА Олена Володимирівна

Острог, 2026

ЗМІСТ

ВСТУП

Сучасний цифровий простір є середовищем, де кожен користувач щодня здійснює сотні дій, більшість із яких несе в собі певний ризик: відкриває електронний лист від невідомого адресата, переходить за посиланням у месенджері, вводить пароль у публічній мережі Wi-Fi, ділиться особистою інформацією в соціальних мережах. Для мільйонів українців ці ризики стали особливо гострими після початку повномасштабного вторгнення Росії в лютому 2022 року – адже цифровий фронт є таким само реальним виміром гібридної війни, як і фізичний.

Актуальність теми медіапроєкту визначається кількома взаємопов'язаними чинниками. По-перше, Україна є однією з найбільш атакованих країн світу у кіберпросторі: урядова команда реагування на комп'ютерні надзвичайні події CERT-UA щомісяця фіксує сотні кіберінцидентів, що спрямовані як проти державної інфраструктури, так і проти звичайних громадян. По-друге, стрімка цифровізація суспільного життя в Україні – розвиток платформи «Дія», переведення державних послуг в онлайн, зростання залежності від месенджерів і соціальних мереж – суттєво розширила поверхню атаки для зловмисників. По-третє, рівень цифрової грамотності та усвідомленості пересічних українців щодо кіберзагроз залишається критично низьким: люди не знають, як розпізнати фішинговий лист, не розуміють ризиків слабкого пароля, не вміють перевіряти достовірність інформації в умовах інформаційної війни.

Цей розрив між реальним рівнем загроз і рівнем готовності суспільства до їх відбиття є конкретною проблемою, що потребує медійного вирішення. Журналістика як суспільний інститут має унікальний потенціал для подолання цього розриву – не через технічні мануали, доступні лише фахівцям, а через якісний, глибокий і водночас зрозумілий медіапродукт, адресований масовій аудиторії.

Обґрунтування важливості та необхідності дослідження саме цієї тематики ґрунтується на кількох рівнях аргументації. На суспільному рівні: цифрова безпека є питанням національної безпеки – скомпрометований акаунт волонтера може розкрити місцезнаходження військових, злам месенджера журналіста може поставити під загрозу його джерела, поширення дезінформації може підірвати суспільну єдність у критичний момент. На особистісному рівні: кожен українець, що користується смартфоном або комп'ютером, є потенційною жертвою кіберзлочину, і відсутність базових знань цифрової безпеки є реальною загрозою для його матеріального добробуту, репутації та безпеки. На медійному рівні: якісного журналістського продукту, що поєднував би глибину дослідження з доступністю викладу та реальною практичною цінністю для масового читача з теми цифрової самооборони, в українському медіапросторі катастрофічно бракує.

Обґрунтування вибору формату медіапроєкту. Серед усіх можливих журналістських форматів саме лонгрід є оптимальним для теми цифрової безпеки. Тема є комплексною і вимагає системного викладу, неможливого в коротших форматах: читачеві недостатньо дізнатися, що фішинг небезпечний – він має зрозуміти механізм фішингу, навчитися його розпізнавати, знати, як реагувати, і мати практичні інструменти для захисту. Лонгрід є єдиним форматом, що надає достатньо простору для повноцінного розгортання теми і водночас дозволяє органічно інтегрувати мультимедійні елементи – інфографіку, схеми, інтерактивні чеклисти, – що суттєво підвищують засвоєння складного матеріалу. Онлайн-платформа як медіум забезпечує доступність матеріалу для широкої аудиторії незалежно від географії та можливість поширення через соціальні мережі та месенджери.

Мета медіапроєкту – створити якісний мультимедійний лонгрід, що підвищить рівень цифрової безпеки українських користувачів інтернету через доступне, системне і практично орієнтоване висвітлення основних кіберзагроз та методів захисту від них.

Досягнення мети передбачає виконання таких завдань: дослідити природу та механізми основних кіберзагроз, актуальних для пересічних українців в умовах воєнного часу; проаналізувати наявний медійний контент із теми цифрової безпеки та виявити його ключові прогалини; розробити структуру лонгріду, що забезпечує послідовний рух читача від усвідомлення проблеми до практичного захисту; підготувати текстовий матеріал на основі експертних інтерв'ю, аналізу реальних кейсів та верифікованих даних; створити мультимедійне наповнення лонгріду, що включає інфографіку, схеми-алгоритми та практичні чеклисти; опублікувати та поширити готовий медіапродукт серед цільової аудиторії; зібрати та проаналізувати зворотний зв'язок від читачів та експертного середовища.

Об'єктом медіапроєкту є цифрова безпека українських інтернет-користувачів як суспільна проблема, що потребує медійного висвітлення.

Предметом медіапроєкту є механізми кіберзагроз, методи їх розпізнавання та практичні інструменти цифрового самозахисту для пересічного українського користувача.

Методологічна база дослідження включає кілька груп методів. Емпіричні методи: глибинне інтерв'ю з фахівцями у галузі кібербезпеки, аналіз реальних задокументованих кейсів кіберінцидентів, моніторинг відкритих звітів CERT-UA та міжнародних організацій. Аналітичні методи: контент-аналіз наявних медійних матеріалів із теми цифрової безпеки, порівняльний аналіз форматів висвітлення теми в українських та зарубіжних медіа, SWOT-аналіз власного медіапроєкту. Проєктні методи: структурне планування за методологією проєктного менеджменту, WBS-декомпозиція, побудова діаграми Гантта, управління ризиками. Журналістські методи: фактчекінг, верифікація джерел, анонімізація персональних даних, дотримання редакційних стандартів.

Наукова значущість роботи полягає у дослідженні лонгріду як жанру в контексті медіависвітлення складних технічних тем, орієнтованих на масову аудиторію, а також у виявленні специфіки журналістської роботи з темою

кібербезпеки в умовах воєнного стану. Результати дослідження можуть бути використані у подальших наукових розвідках із медіакомунікацій, цифрової журналістики та медіаграмотності.

Практична значущість роботи є безпосередньою та вимірюваною: опублікований лонгрід є реальним медіапродуктом, що надає читачам конкретні знання та інструменти для підвищення власної цифрової безпеки. У ширшому контексті робота демонструє модель якісного журналістського підходу до складних технічних тем, що може бути відтворена іншими журналістами та медіаорганізаціями.

Структура медіапроєкту відповідає вимогам методичних рекомендацій кафедри журналістики та PR-менеджменту і включає вступ, три основні розділи, висновки, список використаних джерел та літератури й додатки.

Розділ 1 «Теоретичні засади вибору ідеї та формату медіапроєкту» присвячено обґрунтуванню вибору проблематики, огляду наукових та практичних джерел, аналізу існуючих форматів і кейсів висвітлення теми, теоретичному осмисленню лонгріду як жанру, обґрунтуванню вибору формату та класифікації медіапроєкту.

Розділ 2 «Теоретико-практичні аспекти розробки медіапроєкту» містить системний виклад усіх управлінських аспектів проєкту: управління змістом, часом, ресурсами, вартістю, якістю, ризиками, командою, комунікаціями та моніторингом виконання.

Розділ 3 «Особливості реалізації медіапроєкту» описує конкретні проблеми, що виникли в ході практичного виконання, специфічні особливості реалізації, детальну структуру та мультимедійне наповнення лонгріду, а також рекомендації щодо покращення подібних проєктів у майбутньому.

Апробація медіапроєкту здійснювалася через участь автора у XXXI науковій викладацько-студентській конференції «Дні науки» в межах секції "Медіапроєкти" в Національному університеті «Острозька академія» (Острог, 13 травня 2026) з виступом на тему «Цифрова безпека українців: як розпізнати загрози та захистити себе онлайн»: особливості планування та реалізації».

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ВИБОРУ ІДЕЇ ТА ФОРМАТУ МЕДІАПРОЄКТУ

1.1 Обґрунтування вибору проблематики медіапроєкту

Сучасний інформаційний простір є ареною, де щодня відбуваються тисячі невидимих атак – не ракетних, не фізичних, але не менш руйнівних. Кіберзагрози давно перестали бути долею великих корпорацій чи урядових структур: вони стукають у двері до кожного смартфона, кожного електронного поштового ящика, кожного акаунту в соціальних мережах. Для українців, які перебувають в умовах повномасштабного збройного протистояння з Росією, ця реальність набуває особливої гостроти: цифровий фронт є таким само реальним, як і фізичний.

Проблематика цифрової безпеки актуальна для України з кількох взаємопов'язаних причин. По-перше, стрімка цифровізація суспільного життя, яка в Україні набрала безпрецедентних темпів після 2020 року завдяки розвитку державних платформ на кшталт «Дія», перевела у цифровий формат критично важливі сфери: документообіг, фінансові транзакції, комунікацію між громадянами та державою. По-друге, воєнний стан суттєво змінив характер інформаційних загроз – дезінформаційні кампанії, фішинг, злам акаунтів, крадіжка персональних даних набули ознак гібридної зброї. По-третє, переважна більшість пересічних українців не має достатніх знань для захисту власної цифрової ідентичності [4].

Саме тут виникає ключова суспільна проблема, яку покликаний вирішити цей медіапроєкт: розрив між реальним рівнем кіберзагроз, яким піддаються українці, та рівнем їхньої обізнаності та готовності до протидії. Журналістика як соціальний інститут має унікальний інструментарій для подолання цього розриву – не через технічні мануали та спеціалізовані видання, а через доступні, людяні, візуально переконливі медійні продукти.

Обґрунтування важливості саме цієї тематики спирається на кілька рівнів аргументації.

На рівні суспільної значущості варто зазначити, що кібератаки на цивільну інфраструктуру й окремих громадян в Україні фіксуються регулярно. Урядова команда реагування на кіберінциденти CERT-UA щомісяця публікує звіти про сотні зафіксованих атак, значна частина яких спрямована проти звичайних людей через соціальну інженерію, фішингові листи та шкідливе програмне забезпечення [7].

На рівні медіаландшафту слід констатувати, що попри зростання кількості публікацій на тему кібербезпеки, ці матеріали здебільшого або надто технічні й незрозумілі для масового читача, або занадто поверхові й не дають реальних інструментів захисту. Якісного журналістського продукту, який поєднував би глибину дослідження з доступністю викладу та практичними порадами, на українському медіаринку бракує.

На рівні особистісних ризиків для читача: крадіжка акаунту в соціальних мережах може коштувати людині репутації, грошей, а в умовах війни – навіть безпеки. Злам месенджера може розкрити місцезнаходження військових або волонтерів. Поширення дезінформації може зруйнувати суспільну довіру.

Дослідження, проведені міжнародними організаціями, свідчать, що середньостатистичний користувач інтернету витрачає значні суми на відновлення свого акаунту після компрометації, відшкодування збитків від шахрайства або замороження банківських рахунків внаслідок фраудулентної діяльності. Для України, де велика частина населення перейшла на дистанційні форми заробітку, дистанційну освіту та здійснює фінансові операції через мобільні додатки, такі ризики набувають критичного значення. Неспроможність захистити себе у цифровому просторі перетворюється на прямий фактор матеріального збитку, що підвищує суспільну значущість медіапроєкту [6].

Якщо раніше цільовою групою кібератак вважалися насамперед молоді користувачі та працівники ІТ-сектору, то останніми роками спостерігається тенденція спрямування атак на людей середнього та похилого віку, які часто менш обізнані з механізмами функціонування онлайн-простору. Старші користувачі нерідко стають жертвами романтичних чи фінансових аферистів, які задіюють соціальну інженерію. Цей факт засвідчує необхідність створення медійного контенту, що враховує розмаїтність цільової аудиторії за віком, технічною грамотністю та досвідом користування цифровими сервісами.

Українці часто не знають, до яких органів звертатися після того, як їхні персональні дані вкрадені, акаунти зламані або вони стали жертвою кіберфраудистів. Відсутність простої, зрозумілої інформації про механізми захисту прав в онлайн-просторі, про послуги правоохоронних структур і громадських організацій, які займаються допомогою потерпілим, створює додаткову вразливість. Журналістський проєкт, який поряд з технічними порадами включатиме також навігацію системою підтримки та допомоги, заповнить цю важливу інформаційну нішу [48].

Таким чином, вибір теми «Цифрова безпека українців: як розпізнати загрози і захистити себе онлайн» є не лише обґрунтованим, але й суспільно необхідним. Медіапроєкт ставить за мету заповнення конкретної інформаційної лакуни – відсутності якісного журналістського продукту, орієнтованого на масову аудиторію з проблематики цифрової самооборони.

1.2 Проблематика медіапроєкту в джерелах та літературі

Теоретична база медіапроєкту формується на перетині кількох наукових та практичних галузей: кібербезпеки, медіакомунікацій, психології інформаційного сприйняття та журналістикознавства.

У вітчизняній науковій традиції питання цифрової безпеки досліджуються переважно в контексті технічних та правових аспектів.

Науковці Пушкар О. І. та Грабовський Є. М. у навчальному посібнику «Культура цифрових медіа» (2022) розглядають цифрову грамотність як комплекс компетентностей, що включають не лише вміння користуватися цифровими інструментами, а й критичне ставлення до цифрового середовища, розуміння його ризиків і можливостей. Це теоретичне підґрунтя дозволяє розглядати цифрову безпеку не як суто технічну, а як культурну і соціальну проблему, вирішення якої значною мірою залежить від медіаосвіти [4, с. 45-67].

Для розуміння проблематики медіапроєкту необхідно чітко визначити ключові поняття, якими він оперує.

Цифрова безпека – це стан захищеності особи, її даних, пристроїв і онлайн-діяльності від несанкціонованого доступу, крадіжки, маніпуляції або знищення. На відміну від вузького поняття «кібербезпека», яке частіше вживається в технічному та корпоративному контексті, цифрова безпека акцентує на людині як суб'єкті цифрового простору.

Фішинг – метод соціальної інженерії, спрямований на обманне отримання конфіденційної інформації (паролів, платіжних даних, персональних відомостей) шляхом маскування під довірену особу чи організацію. Це один із найпоширеніших видів кіберзагроз для пересічних користувачів [9].

Дезінформація в цифровому середовищі – свідоме поширення неправдивої або спотвореної інформації з метою маніпулювання суспільною думкою. В умовах воєнного часу дезінформація набуває ознак зброї, здатної деморалізувати суспільство, посіяти паніку або дискредитувати довіру до офіційних джерел.

Двофакторна автентифікація (2FA) – механізм захисту акаунтів, що вимагає двох форм підтвердження особи при вході: зазвичай пароля і одноразового коду, надісланого на інший пристрій або згенерованого спеціальним застосунком.

Соціальна інженерія – маніпулятивні техніки, що використовують психологічні вразливості людини (довіру, страх, цікавість, поспіх) для отримання несанкціонованого доступу до інформації або систем, без застосування суто технічних методів злому [6].

VPN (Virtual Private Network) – технологія, що забезпечує шифрування інтернет-з'єднання та маскування реальної IP-адреси користувача, що підвищує анонімність і захист даних під час роботи в мережі.

OSINT (Open Source Intelligence) – розвідка на основі відкритих джерел: методологія збору та аналізу публічно доступної інформації. У контексті цифрової безпеки важлива з двох боків: як інструмент, яким можуть скористатися зловмисники для збору даних про жертву, і як метод перевірки інформації для журналістів та свідомих користувачів.

Міжнародний дискурс цифрової безпеки активно розвивається у руслі концепції «security by design» (безпека як невід'ємна характеристика дизайну продуктів і систем) та «human factor in cybersecurity» (людський фактор у кібербезпеці). Остання концепція є особливо важливою для цього медіапроєкту: дослідження показують, що переважна більшість успішних кібератак експлуатує не технічні вразливості систем, а психологічні вразливості людей [10].

У галузі медіакомунікацій релевантними є дослідження ефективності різних форматів для передачі складної інформації масовій аудиторії. Теорія когнітивного навантаження (Sweller, 1988) пояснює, чому комплексна технічна інформація потребує особливого структурування, візуалізації та поетапного засвоєння – принципи, що безпосередньо впливають на вибір формату медіапроєкту.

Таблиця 1.1 узагальнює ключові поняття медіапроєкту та їхнє значення для розуміння проблематики.

Таблиця 1.1

Ключові поняття медіапроєкту «Цифрова безпека українців»

Поняття	Визначення	Значення для медіапроєкту
Цифрова безпека	Захищеність особи в цифровому середовищі	Центральний об'єкт висвітлення
Фішинг	Обманне отримання конфіденційних даних	Найпоширеніша загроза для аудиторії
Дезінформація	Навмисне поширення неправдивої інформації	Особлива загроза в умовах воєнного часу
Соціальна інженерія	Маніпуляція через психологічні вразливості	Пояснює «людський фактор» у кібератаках
Двофакторна автентифікація	Подвійна перевірка особи при вході	Базовий інструмент захисту для аудиторії
OSINT	Розвідка на основі відкритих джерел	Методологія перевірки та збору даних
VPN	Шифрування з'єднання та маскування IP	Практичний інструмент захисту

1.3 Формати та практичні кейси з вирішення окремих аспектів проблематики

Аналіз медіаландшафту дозволяє виявити різноманітні підходи до висвітлення теми цифрової безпеки, кожен із яких має власні сильні сторони та обмеження.

Перша група форматів – новинні та аналітичні матеріали. Такі видання, як «Медіадетектор», «Укрінформ», «Babel», регулярно публікують матеріали про конкретні кіберінциденти, фішингові кампанії, хакерські атаки. Сильна сторона цього підходу – актуальність і своєчасність. Обмеження – відсутність системного погляду та практичних інструкцій для читача. Людина, прочитавши новину про злам бази даних, залишається наодинці з питанням: «А що мені тепер робити?» [16]

Друга група – освітній контент у соціальних мережах. Телеграм-канали типу «Кіберполіція України», «Без брехні», «Дезінформатор» ведуть активну просвітницьку роботу у форматі коротких дописів, карток, коротких відеороликів. Цей формат ефективний для швидкого охоплення широкої

аудиторії, але має обмежений потенціал для глибокого осмислення проблеми та формування стійких поведінкових змін.

Третя група – спеціалізовані посібники та інструкції. Організація «Інтерньюз Україна», «Access Now», «Amnesty International» публікують детальні гайди з цифрової безпеки для журналістів, активістів, представників вразливих груп. Ці матеріали вирізняються глибиною та практичністю, але зазвичай написані складною мовою і розраховані на мотивовану, підготовлену аудиторію.

Четверта група – мультимедійні лонгріди та спецпроєкти. Саме цей формат є найбільш перспективним з огляду на можливість поєднати глибину аналізу, людяність оповіді та практичну цінність. Розглянемо кілька показових міжнародних кейсів [48].

Кейс 1: «The Intercept» – розслідування про стеження (США)

Видання «The Intercept», засноване Гленом Грінвальдом після розкриття матеріалів Едварда Сноудена, побудувало свою редакційну модель навколо теми цифрового стеження та приватності. Їхні матеріали поєднують журналістське розслідування з детальним поясненням технічних механізмів, що дозволяє читачеві не лише дізнатися про проблему, але й зрозуміти, як вона працює. Ключовий урок: технічна складність не є перепоною для широкої аудиторії, якщо тема подається через людські історії та конкретні приклади.

Кейс 2: «Фактчек UA» – боротьба з дезінформацією (Україна)

Проєкт «Фактчек UA» від «Київської незалежної» демонструє ефективну модель системної перевірки інформації з поясненням методології. Читач не просто отримує результат перевірки (правда/брехня), а розуміє, як перевірити інформацію самостійно. Це формує медіаграмотність як навичку, а не залежність від авторитету. Урок для цього медіапроєкту: навчати аудиторію думати, а не лише повідомляти факти.

Кейс 3: «Wired» – довготривалі матеріали про кібербезпеку (США/Великобританія)

Журнал «Wired» системно публікує лонгріди на тему кібербезпеки, адресовані не технічним спеціалістам, а освіченому масовому читачеві. Характерні риси їхнього підходу: початок з людської історії (жертва, хакер, дослідник), поступове розкриття технічного контексту через наратив, закінчення практичними висновками. Ця структура забезпечує як емоційне залучення, так і інформаційну цінність [16].

Кейс 4: Проєкт «Кібербезпека від А до Я» (Кіберполіція України)

Вітчизняний приклад системного підходу до просвіти в галузі цифрової безпеки – серія матеріалів Кіберполіції, поширена через соціальні мережі. Попри обмеження формату (короткі дописи не дозволяють глибокого занурення), проєкт цінний як зразок системного охоплення ключових загроз: від фішингу до шахрайства в онлайн-торгівлі. Урок: системність і послідовність важливіші за поодинокі «вірусні» матеріали.

Рис. 1.1 відображає порівняльний аналіз форматів за ключовими критеріями.

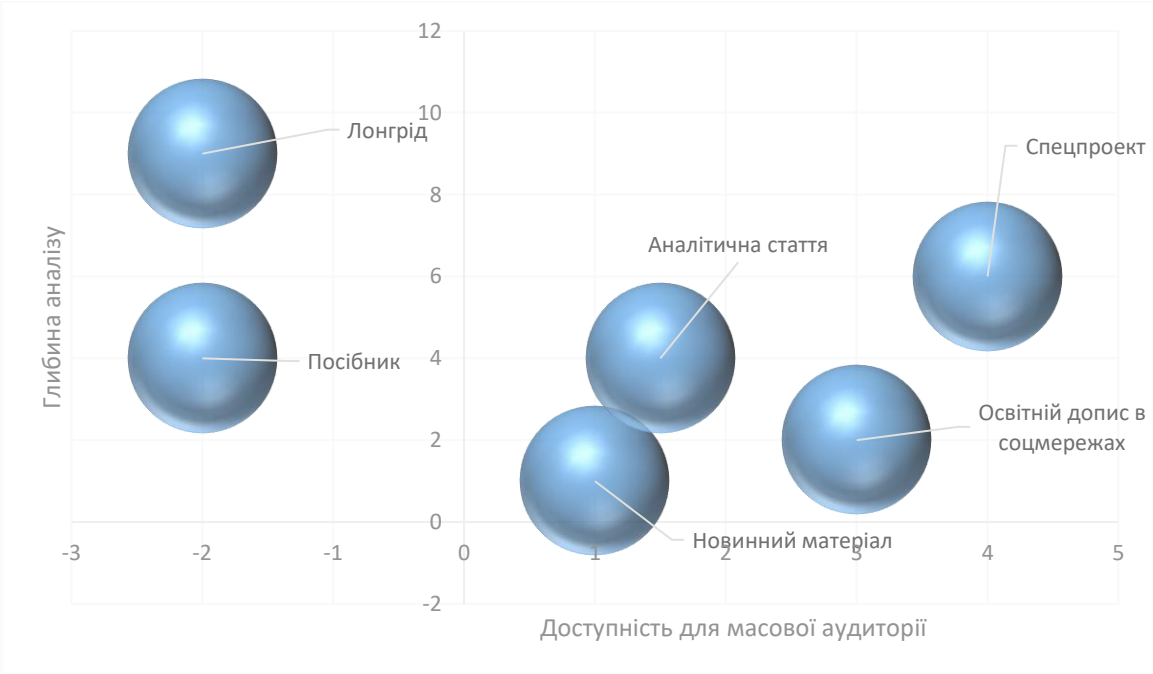

Рис. 1.1. Порівняльна характеристика форматів висвітлення теми цифрової безпеки

Аналіз кейсів дозволяє сформулювати кілька принципів ефективного медіапродукту на тему цифрової безпеки. Перший принцип – людяність: будь-яка технічна тема стає зрозумілою та близькою, коли подається через конкретні людські ситуації та історії. Другий принцип – системність: аудиторія потребує не окремих порад, а цілісного розуміння середовища загроз [58, 51]. Третій принцип – практичність: кожен матеріал має давати читачеві конкретний інструмент або дію, яку він може застосувати негайно. Четвертий принцип – візуальність: складна інформація засвоюється значно легше через схеми, інфографіку та ілюстрації.

1.4 Лонгрід як формат медіапроєкту: теоретичні основи та жанрові особливості

Лонгрід (від англ. «long read» – тривале читання) є одним із найбільш динамічно розвинених жанрів сучасної цифрової журналістики. Попри поширену хибну думку про те, що цифрова аудиторія не читає довгих текстів, дослідження поведінки онлайн-читачів свідчать про протилежне: матеріали, що пропонують справжню глибину і цінність, знаходять свою аудиторію – і ця аудиторія відрізняється вищим рівнем залучення та довіри до видання.

Теоретичне осмислення лонгріду як жанру пов'язане з кількома концептуальними вимірами [13, с. 45-53].

Наративний вимір. Лонгрід успадковує традицію «нової журналістики» (Tom Wolfe, Hunter S. Thompson, Gay Talese) – підходу, що застосовує літературні техніки до журналістського матеріалу. Сцени, діалоги, внутрішній монолог персонажів, точка зору – всі ці інструменти роблять лонгрід не просто носієм інформації, а досвідом читання. Для теми цифрової безпеки це означає можливість провести читача «всередину» кіберінциденту: відчути тривогу людини, яка виявила зламаний акаунт, зрозуміти логіку зловмисника, відстежити ланцюжок рішень, що призвели до компрометації [16, с. 112-119].

Аналітичний вимір. На відміну від новинного матеріалу, лонгрід не обмежується відповіддю на питання «що сталося?» – він прагне відповісти на «чому?», «як?» і «що це означає?». Для медіапроєкту про цифрову безпеку це означає можливість пояснити не лише факт існування загрози, а й механізм її дії, психологічний контекст, структурні причини вразливості аудиторії [17, с. 34-41].

Мультимедійний вимір. Сучасний лонгрід є не просто довгим текстом, а мультимедійним середовищем, де текст органічно поєднується з інфографікою, інтерактивними елементами, відеовставками, цитатами у виділених блоках, фотографіями. Видання «The New York Times» з їхніми знаковими проєктами «Snow Fall» (2012) та «1619 Project» (2019) задали стандарт такого мультимедійного лонгріду, який є одночасно журналістикою, дизайном і технологією [18, с. 145-167].

Освітній вимір. Лонгрід є винятково ефективним форматом для складної теми, яка вимагає системного пояснення. Навчальний потенціал лонгріду пов'язаний з його здатністю будувати знання поступово, крок за кроком, підводячи читача від базових концепцій до складних висновків через серію «розумових сходинок».

Жанрові особливості лонгріду, релевантні для цього медіапроєкту, можна структурувати таким чином:

Щодо обсягу та структури: класичний лонгрід налічує від 1500 до 10 000 слів і більше. Однак обсяг є другорядним параметром – першорядним є змістовна необхідність кожного розділу. Структура лонгріду, як правило, включає сильний лід, що «чіпляє» читача, тематичні блоки з підзаголовками, що полегшують навігацію, і висновкову частину з чіткими практичними тезами.

Щодо оповідного голосу: лонгрід допускає авторську присутність, власну позицію, емоційне ставлення до теми – за умови, що вони базуються на фактах і не замінюють аналіз. Це суттєво відрізняє його від нейтральних новинних матеріалів і робить його ближчим до читача [16].

Щодо джерельної бази: якісний лонгрід спирається на розмаїту джерельну базу – експертні інтерв'ю, аналіз даних, документи, особові свідчення. Для теми цифрової безпеки це означає поєднання голосів технічних експертів (фахівці з кібербезпеки), правозахисників (питання приватності та прав людини), звичайних користувачів (особові історії) та офіційних представників (позиція держави) [55, с. 45-89].

Таблиця 1.2 відображає жанрові ознаки лонгріду в порівнянні з іншими поширеними журналістськими форматами.

Таблиця 1.2

Жанрові ознаки лонгріду порівняно з іншими форматами

Параметр	**Новина**	**Стаття**	**Лонгрід**	**Репортаж**
Обсяг	200–500 слів	500–1500 слів	1500–10000+ слів	1000–5000 слів
Наратив	Мінімальний	Частково	Центральний	Виражений
Аналітика	Поверхова	Середня	Глибока	Ситуативна
Мультимедіа	Рідко	Іноді	Як правило	Часто
Авторська позиція	Відсутня	Мінімальна	Допускається	Допускається
Практична цінність	Низька	Середня	Висока	Середня
Час читання	1–2 хв	3–5 хв	10–30+ хв	5–15 хв

У контексті цього медіапроєкту лонгрід є оптимальним форматом, оскільки тема цифрової безпеки за своєю природою вимагає системного викладу, неможливого в коротших форматах [11, с. 89-145]. Читачеві недостатньо знати, що «фішинг небезпечний» – він має розуміти механізм фішингу, вміти його розпізнати, знати, як реагувати, і мати контакти для звернення по допомогу. Увесь цей обсяг знань може бути переданий лише у форматі, що надає достатньо простору для повноцінного розгортання теми.

1.5 Обґрунтування вибору формату медіапроєкту

Вибір лонгріду як формату медіапроєкту «Цифрова безпека українців: як розпізнати загрози і захистити себе онлайн» є результатом свідомого аналізу потреб цільової аудиторії, специфіки теми та можливостей різних форматів.

Цільова аудиторія медіапроєкту – українці віком 18–55 років, активні користувачі інтернету, які усвідомлюють загрози цифрового середовища, але не мають систематизованих знань для захисту. Ця аудиторія характеризується середнім рівнем цифрової грамотності, здатністю до тривалого читання при наявності достатньої мотивації та готовністю змінювати свої цифрові звички за умови переконливої аргументації. Для такої аудиторії короткі дописи у соціальних мережах є недостатніми (не дають системного знання), а технічні мануали – надмірними (відлякують складністю).

Відповідність формату темі є ключовим критерієм вибору. Тема цифрової безпеки є комплексною: вона включає технічні, психологічні, правові та соціальні аспекти. Лонгрід є єдиним форматом, що дозволяє органічно поєднати всі ці виміри в єдиному наративі, не жертвуючи жодним із них. Спроба вмістити весь необхідний зміст у форматі серії коротких дописів призвела б або до фрагментарності та розривності, або до надмірного спрощення [13, с. 45-53].

Конкурентна відмінність медіапроєкту також визначається форматом. Більшість наявного контенту на тему цифрової безпеки в українському медіапросторі представлена або у вигляді технічних посібників (глибока, але недоступна), або у вигляді новин та коротких дописів (доступна, але поверхова). Лонгрід займає незайняту нішу: глибока та доступна одночасно. Ця конкурентна перевага є стратегічно важливою для медіапроєкту.

Можливості мультимедійної інтеграції є ще одним аргументом на користь лонгріду. Тема цифрової безпеки рясніє поняттями та процесами, які значно легше зрозуміти через схеми, ніж через суто текстовий опис. Наприклад, механізм фішингової атаки, структура двофакторної автентифікації, алгоритм перевірки підозрілого посилання – все це природно «просяться» у візуальне представлення. Лонгрід як формат не просто допускає, а передбачає таку інтеграцію [11, с. 89-145].

Потенціал для поширення та тривалої актуальності також є важливим критерієм. На відміну від новинних матеріалів, що швидко застарівають,

якісний лонгрід на тему базових принципів цифрової безпеки залишається актуальним протягом тривалого часу. Базові механізми фішингу, правила захисту паролів, принципи перевірки інформації не змінюються щотижня – це фундаментальні знання, що зберігають цінність упродовж місяців і років [4, с. 67-89].

Рис. 1.2 відображає схему обґрунтування вибору формату медіапроєкту.

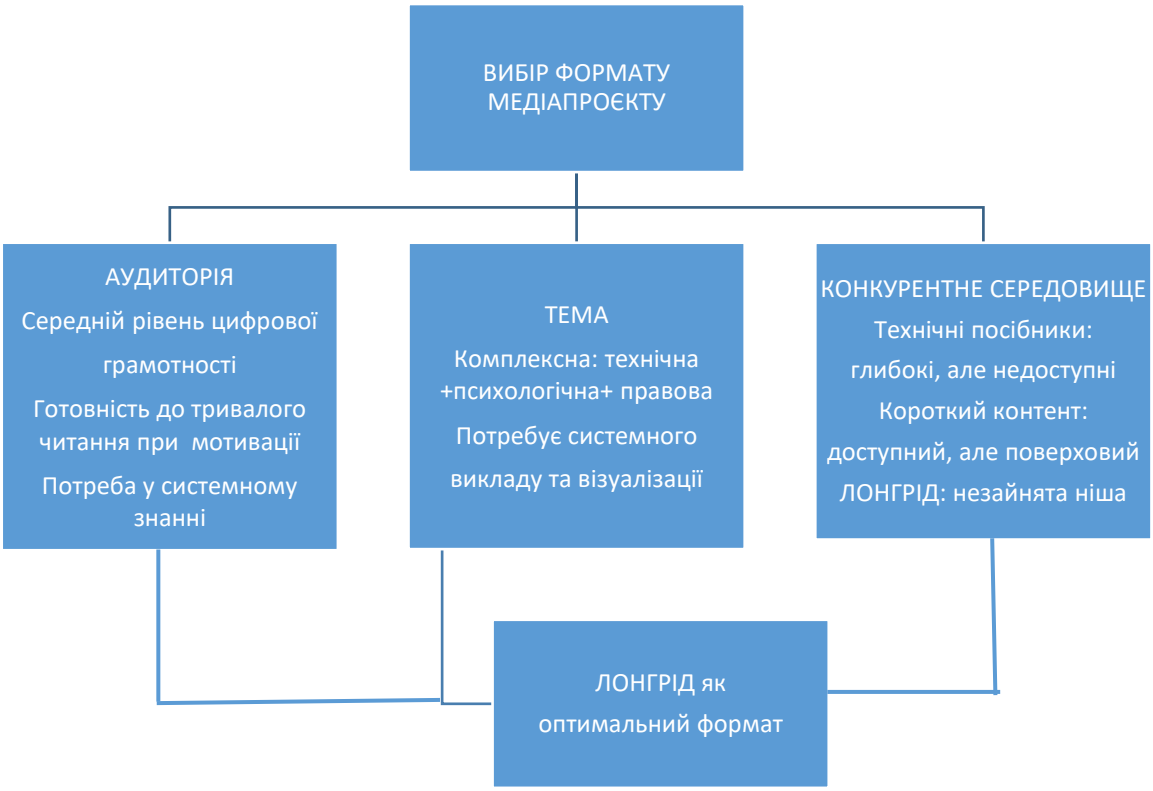

Рис. 1.2. Схема обґрунтування вибору формату «лонгрід» для медіапроєкту

Окремо слід обґрунтувати вибір онлайн-платформи як медіуму для публікації лонгріду. Онлайн-формат має беззаперечні переваги перед друкованим: можливість інтеграції мультимедійних елементів, гіпертекстового посилання на додаткові ресурси та інструменти, інтерактивних елементів (тести, чеклисти), а також легкість поширення через соціальні мережі та месенджери [9, с. 28-33]. Для теми цифрової безпеки онлайн-контекст є також символічно важливим: матеріал про захист в

інтернеті логічно існує саме там, де люди проводять час і де їм загрожують ризики, що описуються.

1.6 Класифікація медіапроєкту

Відповідно до класифікаційної матриці J.Lab.Matrix, розробленої Лабораторією журналістської майстерності Національного університету «Острозька академія», медіапроєкт «Цифрова безпека українців: як розпізнати загрози і захистити себе онлайн» може бути охарактеризований за такими критеріями.

За тривалістю проєктної діяльності медіапроєкт належить до категорії середньої тривалості. Підготовка, дослідження, написання, редагування та верстка лонгріду є процесом, що охоплює кілька місяців і передбачає значний обсяг дослідницької та творчої роботи, однак не є тривалим у розумінні безперервного виробництва контенту (як, наприклад, студентська газета чи подкаст) [4, с. 45-67].

За повторюваністю медіапроєкт є одноразовим у тому сенсі, що він є завершеним самостійним продуктом, а не частиною регулярного виробництва. Водночас методологічний підхід і напрацьовану тематику може бути використано як основу для подальших серій матеріалів – тобто проєкт має потенціал масштабування.

За локалізацією медіапроєкт є загальнонаціональним – він адресований усім україномовним користувачам інтернету в Україні та за кордоном (українська діаспора), без прив'язки до конкретного регіону чи міста. Проблематика цифрової безпеки є актуальною незалежно від географії проживання, а доступ до онлайн-публікації є однаковим для мешканців будь-якого регіону країни.

За формою подачі інформації медіапроєкт є комбінованим – він поєднує текст (основний масив контенту, наратив, аналіз), графіку (схеми, інфографіку, ілюстрації) та, за можливості, мультимедійні елементи (інтерактивні

чеклисти). Така комбінація є принциповою для теми, де різні типи контенту виконують різні функції: текст будує розуміння, схеми структурують знання, практичні чеклисти забезпечують дієвість [14, с. 45-67].

За медіумом (каналом поширення) медіапроєкт є інтернет-проєктом. Публікація відбувається на онлайн-платформі, поширення – через соціальні мережі та месенджери. Саме цифровий канал є органічно відповідним для теми цифрової безпеки.

Таблиця 1.3 систематизує класифікаційні ознаки медіапроєкту.

Таблиця 1.3

Класифікація медіапроєкту «Цифрова безпека українців» за матрицею J.Lab.Matrix

Класифікаційний критерій	**Категорія**	**Обґрунтування**
Тривалість	Середньої тривалості	Кількамісячний цикл підготовки одного завершеного продукту
Повторюваність	Одноразовий	Завершений самостійний медіапродукт
Локалізація	Загальнонаціональний	Адресований усій україномовній аудиторії незалежно від регіону
Форма подачі	Комбінований	Текст + графіка + інтерактивні елементи
Медіум	Інтернет-проєкт	Онлайн-публікація з поширенням через соцмережі

Рис. 1.3 відображає позицію медіапроєкту у матриці J.Lab.Matrix.

J.Lab.MATRIX			
ТРИВАЛІСТЬ	ПОВТОР	ТЕРИТОРІЯ	ФОРМА
Короткий	Одноразовий	ОА	Текст
►СЕРЕДНІЙ◄	►ОДНОРАЗОВИЙ◄	Острог	Аудіо
Довгий	Багаторазовий	Рівненщина	Відео
	Тривалий	►УКРАЇНА◄	Графіка
		Інше	Фотографія
			МУЛЬТИМЕДІА◄

Рис. 1.3. Позиція медіапроєкту у класифікаційній матриці J.Lab.Matrix

►◄ *– обрані категорії для цього медіапроєкту*

Додатково варто охарактеризувати медіапроєкт за такими неформальними ознаками, які не входять до базової матриці, але є важливими для розуміння його природи.

За жанровою приналежністю медіапроєкт є журналістським лонгрідом із елементами просвітницького контенту. Він поєднує репортажну основу (конкретні кейси, живі свідчення), аналітику (системне осмислення загроз) та сервісну журналістику (практичні поради та інструменти). Такий жанровий синтез є характерною ознакою якісного мультимедійного лонгріду.

За суспільною функцією медіапроєкт виконує одночасно інформаційну (повідомляє про реальні загрози), освітню (пояснює механізми та методи захисту), соціальну (сприяє формуванню культури цифрової безпеки) та захисну (реально підвищує безпеку аудиторії) функції. Саме поєднання цих функцій робить проєкт суспільно значущим у найповнішому розумінні цього слова.

За рівнем складності виробництва медіапроєкт є продуктом підвищеної складності, що вимагає компетенцій у журналістиці (дослідження, написання, редагування), дизайні (візуальне оформлення, інфографіка), та цифрових технологіях (верстка, публікація, поширення). Це зумовлює необхідність системного планування та чіткого розподілу відповідальностей [11, с. 89-145].

Підсумовуючи, медіапроєкт «Цифрова безпека українців: як розпізнати загрози і захистити себе онлайн» є комбінованим загальнонаціональним інтернет-проєктом середньої тривалості, реалізованим у форматі мультимедійного лонгріду, що поєднує журналістський наратив, аналітичний зміст та практичну цінність для широкої аудиторії. Вибір саме цієї класифікаційної позиції є не випадковим, а виваженим результатом аналізу потреб аудиторії, специфіки теми та можливостей наявних форматів.

РОЗДІЛ 2. ТЕОРЕТИКО-ПРАКТИЧНІ АСПЕКТИ РОЗРОБКИ МЕДІАПРОЄКТУ

2.1 Управління змістом медіапроєкту

Управління змістом є фундаментальним процесом, що визначає, що саме буде зроблено в межах медіапроєкту, у якій послідовності та з яким результатом. Для медіапроєкту «Цифрова безпека українців: як розпізнати загрози і захистити себе онлайн» управління змістом є особливо відповідальним завданням, оскільки тема є одночасно технічно складною, суспільно чутливою та практично важливою – будь-яка неточність чи прогалина в змісті може призвести або до дезорієнтації читача, або до реальної шкоди для його цифрової безпеки.

Життєвий цикл медіапроєкту охоплює п'ять ключових фаз: ініціювання, планування та розробку, виконання, моніторинг і контроль, завершення. Кожна фаза є необхідною і не може бути пропущена без шкоди для якості кінцевого продукту [5, с. 123-145].

Фаза ініціювання передбачила визначення проблеми, що потребує висвітлення, формулювання концепції медіапроєкту та погодження її з науковим керівником. На цьому етапі було встановлено, що ключовою проблемою є розрив між реальним рівнем кіберзагроз для українців та рівнем їхньої обізнаності й готовності до самозахисту в цифровому середовищі. Фаза планування передбачала розробку структури лонгріду, визначення тематичних блоків, джерельної бази, часових рамок та необхідних ресурсів. Фаза виконання охоплювала дослідження, інтерв'ю з експертами, написання тексту, створення візуальних елементів і верстку. Фаза моніторингу здійснювалася паралельно з виконанням через регулярні консультації з науковим керівником та самооцінку прогресу. Завершення проєкту включало фінальне редагування, публікацію та апробацію результатів.

Дерево цілей медіапроєкту відображає ієрархічну структуру від загальної мети до конкретних завдань і очікуваних результатів (рис. 2.1).

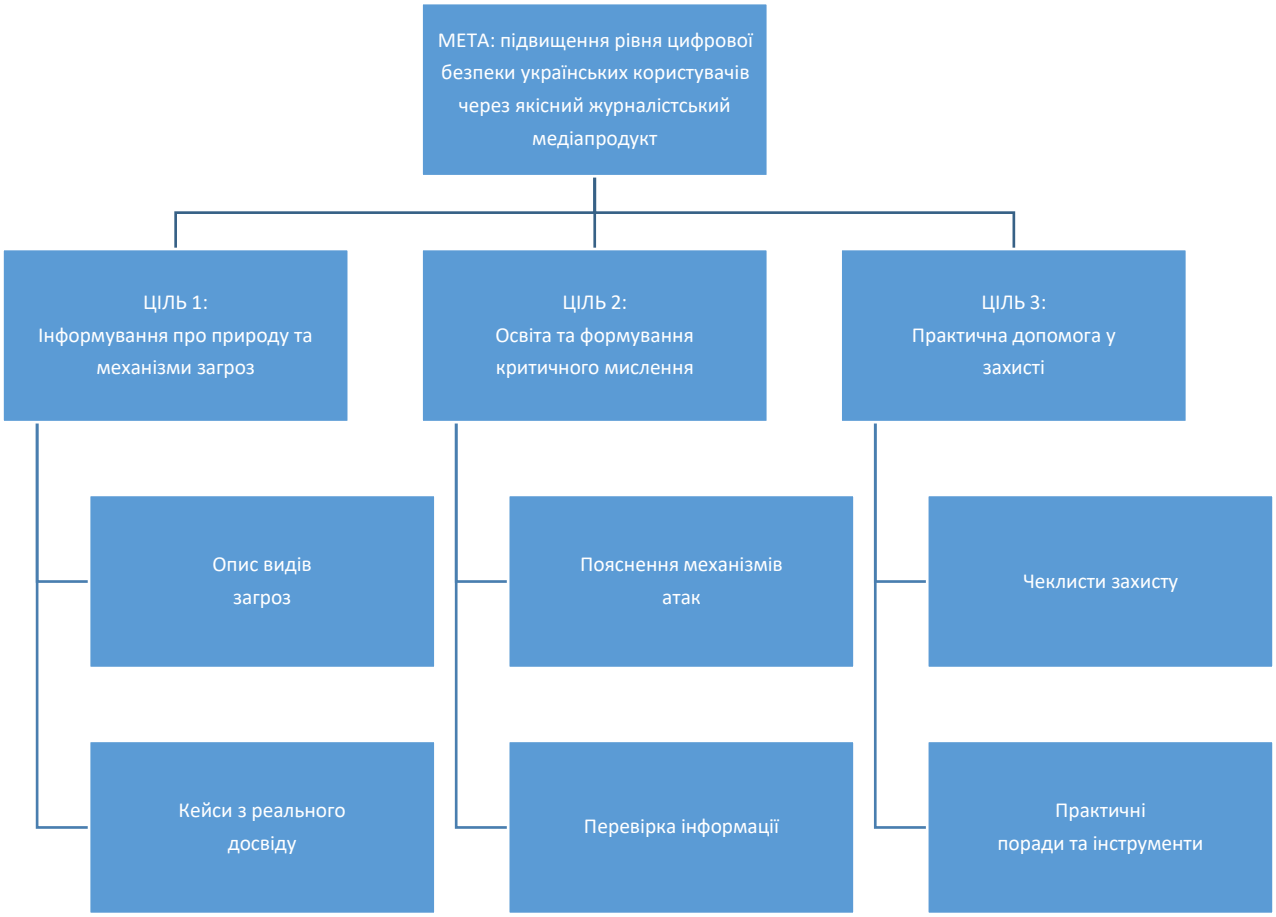

Рис. 2.1. Дерево цілей медіапроєкту «Цифрова безпека українців»

Структура розбиття робіт (WBS) медіапроєкту дозволяє декомпозувати весь обсяг роботи на керовані компоненти. Критерієм декомпозиції на першому рівні є тематичний блок (дослідження, контент-виробництво, візуальне оформлення, публікація та поширення). На другому рівні – конкретний вид роботи в межах блоку. На третьому рівні – окремі завдання (табл. 2.1) [22, с. 89-112].

Таблиця 2.1

Перелік робіт медіапроєкту з прив'язкою до WBS-структури

WBS-код	Вид роботи	Опис	Результат
1.0	Дослідження	Збір та аналіз інформації	Аналітична база
1.1	Огляд літератури	Вивчення наукових та практичних джерел	Бібліографія, конспекти
1.2	Експертні інтерв'ю	Розмови з фахівцями з кібербезпеки	Транскрипти, цитати
1.3	Аналіз кейсів	Збір та опрацювання реальних випадків	База прикладів
2.0	Контент-виробництво	Написання тексту лонгріду	Текстовий матеріал
2.1	Структурування	Розробка детального плану тексту	Зміст лонгріду
2.2	Написання чорновика	Перший варіант усіх розділів	Чорновик лонгріду
2.3	Редагування	Редакторська правка, перевірка фактів	Відредагований текст
3.0	Візуальне оформлення	Створення графічних елементів	Інфографіка, схеми
3.1	Інфографіка	Візуалізація загроз та механізмів захисту	Готові графічні файли
3.2	Чеклисти	Практичні перевірні списки для читача	Інтерактивні елементи
4.0	Публікація	Верстка та розміщення	Готовий лонгрід онлайн
4.1	Верстка	Технічне оформлення публікації	Опублікований матеріал
4.2	Поширення	Просування через соціальні мережі	Охоплення аудиторії

Мережева діаграма проєкту відображає взаємозв'язки між роботами. Роботи блоку 1.0 (дослідження) є передумовою для блоку 2.0 (контент-

виробництво) [5, с. 189-234]. Блоки 2.0 і 3.0 (візуальне оформлення) реалізуються паралельно, хоча певні елементи інфографіки не можуть бути створені до завершення відповідних текстових розділів. Блок 4.0 (публікація) розпочинається лише після завершення блоків 2.0 і 3.0. Ця логіка взаємозалежності визначає критичний шлях проєкту, описаний у наступному розділі.

2.2 Управління часом у медіапроєкті

Ефективне управління часом є критично важливим для медіапроєкту, що реалізується в умовах чітко визначених академічних дедлайнів. Планування часових рамок здійснювалося методом зворотного відліку: від дати публічного захисту до дати старту проєкту, з виділенням обов'язкових проміжків для кожного етапу.

Методологія визначення тривалості робіт базується на поєднанні трьох підходів. Перший – метод аналогій: порівняння з часовими затратами на схожі проєкти, реалізовані в межах Лабораторії журналістської майстерності. Другий – параметрична оцінка: визначення тривалості на основі обсягу роботи (наприклад, написання 1000 слів якісного журналістського тексту вимагає близько 3–4 годин з урахуванням дослідницького компоненту). Третій – метод трьох точок: для кожного завдання визначалася оптимістична, реалістична та песимістична оцінка тривалості, після чого вираховувалося середньозважене значення [26, с. 145-189].

Загальна тривалість медіапроєкту від старту до захисту становить орієнтовно 16 тижнів. Цей період розбивається на чотири основні фази з такою тривалістю: дослідницька фаза – 5 тижнів, фаза контент-виробництва – 5 тижнів, фаза оформлення та верстки – 3 тижні, фаза підготовки до захисту – 3 тижні (рис. 2.2) [21, с. 12-29].

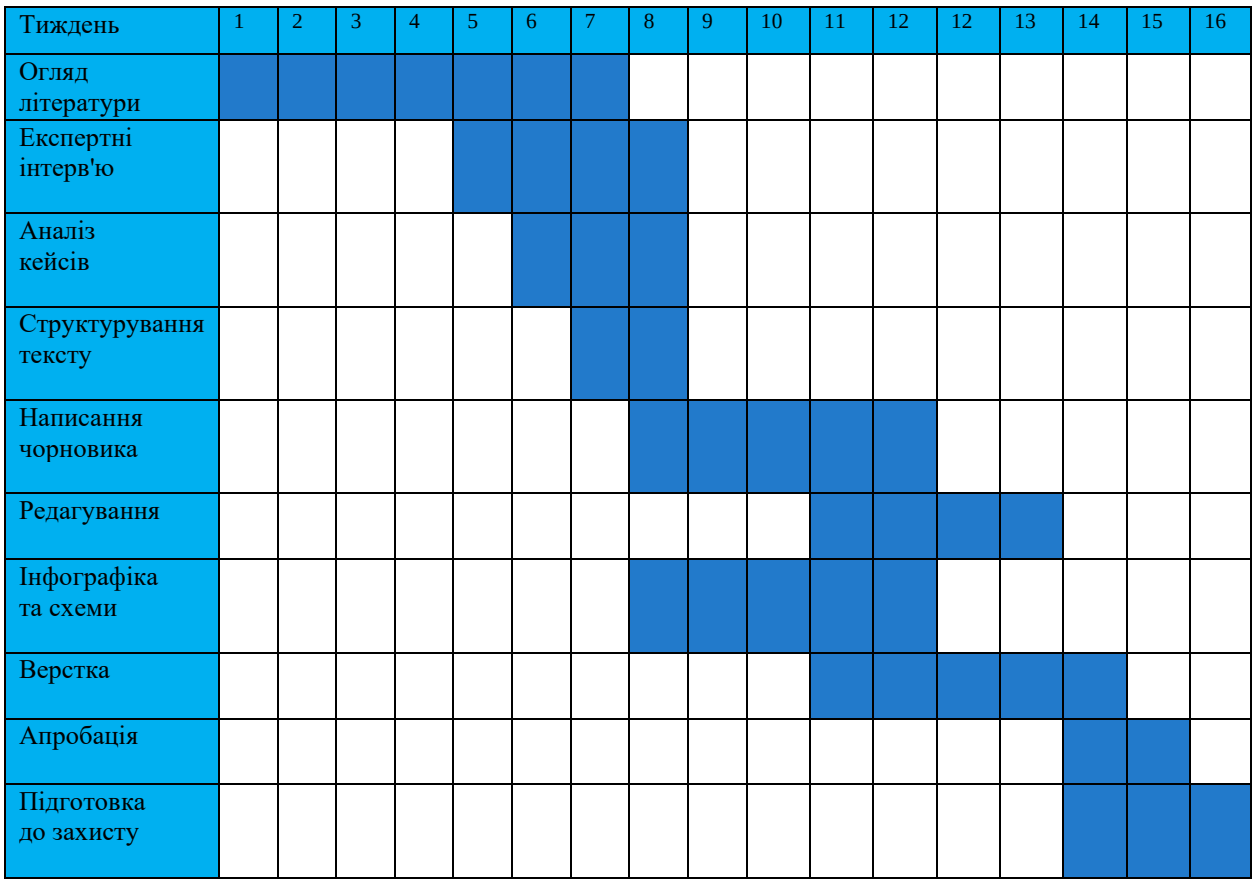

Рис. 2.2. Діаграма Гантта медіапроєкту «Цифрова безпека українців»

Розрахунок критичного шляху без урахування обмеженості ресурсів виявляє таку послідовність: огляд літератури, аналіз кейсів, структурування тексту, написання чорновика, редагування, верстка, підготовка до захисту. Загальна тривалість критичного шляху становить 14 тижнів. Роботи, що не перебувають на критичному шляху (зокрема, експертні інтерв'ю та створення інфографіки), мають певний часовий резерв і можуть реалізовуватися паралельно з критичними завданнями [29, с. 234-267].

Точками поточного контролю (мілстоунами) визначено такі події: завершення дослідницької фази та затвердження структури тексту науковим керівником (кінець 5-го тижня), здача чорновика першого розділу (кінець 7-го тижня), здача повного чорновика (кінець 10-го тижня), отримання відредагованого варіанту від наукового керівника (кінець 12-го тижня), завершення верстки та публікація (кінець 13-го тижня). Кожна з цих точок є

обов'язковою і не підлягає перенесенню без погодження з науковим керівником.

2.3 Управління ресурсами та закупівлями медіапроєкту

Ефективне управління ресурсами передбачає чіткий облік усіх видів ресурсів, необхідних для реалізації медіапроєкту, та оптимальний розподіл між завданнями з урахуванням часових обмежень.

Структура ресурсів медіапроєкту (RBS – Resource Breakdown Structure) охоплює чотири основні категорії: людські ресурси, технічні ресурси, інформаційні ресурси та часові ресурси [30, с. 189-234].

Людські ресурси включають автора проєкту (виконавця всього обсягу журналістської та дослідницької роботи), наукового керівника (методичне супроводження, редакторська перевірка, погодження структури та висновків), експертів-консультантів (фахівці з кібербезпеки, яких планується залучити для інтерв'ю).

Технічні ресурси охоплюють комп'ютерне обладнання для написання, редагування та верстки; програмне забезпечення для роботи з текстом (Google Docs або Microsoft Word), для створення графіки та інфографіки (Canva, Adobe Illustrator або їх безкоштовні аналоги), для верстки онлайн-публікації. Також необхідний стабільний доступ до інтернету для дослідження, комунікації з експертами та публікації готового матеріалу; за необхідності – диктофон або смартфон для запису інтерв'ю [22, с. 156-178].

Інформаційні ресурси включають наукові та галузеві публікації з кібербезпеки, звіти CERT-UA та міжнародних організацій з питань цифрової безпеки, бази даних зафіксованих кіберінцидентів, доступ до бібліотечних фондів університету та онлайн-бібліотек (рис. 2.3).

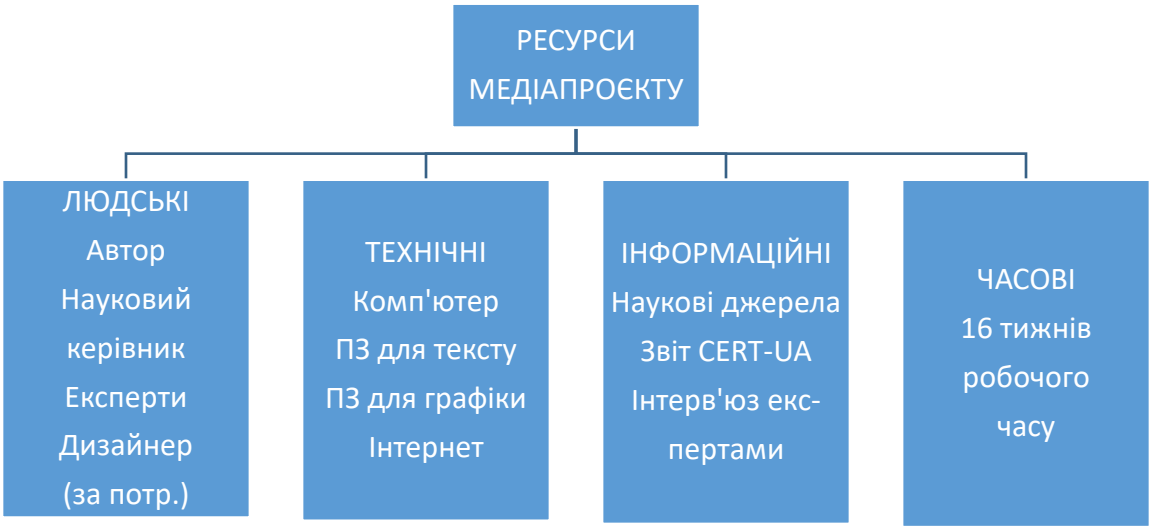

Рис. 2.3. Структура ресурсів (RBS) медіапроєкту

Щодо переліку товарів і послуг, що закуповуються, медіапроєкт передбачає мінімальний обсяг фінансових закупівель. Більшість необхідних ресурсів є безкоштовними або вже наявними у розпорядженні виконавця [21, с. 12-29]. Потенційні статті закупівель можуть включати придбання платного програмного забезпечення для роботи з графікою (за умови недостатності безкоштовних аналогів), оплату хостингу або онлайн-платформи для публікації (за умови, що університетська платформа є недоступною), а також витрати на відрядження для проведення особистих зустрічей з експертами (за необхідності). Загалом, медіапроєкт спроєктований таким чином, щоб мінімізувати фінансові витрати без шкоди для якості продукту, що відповідає принципу реалістичності проєктного планування.

2.4 Управління вартістю медіапроєкту

Управління вартістю передбачає складання бюджету медіапроєкту та визначення потреби у фінансових коштах у часі. Для академічного медіапроєкту, що реалізується студентом в межах кваліфікаційної роботи, бюджетне планування є важливим передусім з точки зору прозорості та

контролю, навіть якщо загальний обсяг фінансових витрат є відносно невеликим (табл. 2.2) [25, с. 145-178].

Таблиця 2.2

Бюджет медіапроєкту «Цифрова безпека українців»

№	Стаття витрат	Одиниця	Кількість	Ціна (грн)	Сума (грн)	Джерело фінансування
1	Програмне забезпечення для графіки (Canva Pro)	міс.	2	350	700	Власні кошти
2	Хостинг для публікації	міс.	1	200	200	Власні кошти
3	Мобільний зв'язок (дзвінки для інтерв'ю)	міс.	3	150	450	Власні кошти
4	Друк роздаткових матеріалів для захисту	арк.	20	5	100	Власні кошти
5	Непередбачені витрати (резерв 10%)	–	–	–	145	Власні кошти
	Разом				**1595**	

Слід зазначити, що значна частина ресурсів є фактично безкоштовною або вже включеною в наявну інфраструктуру: доступ до інтернету, комп'ютерне обладнання, бібліотечні фонди університету, безкоштовні версії програмного забезпечення (Google Docs, Canva безкоштовна версія, Figma). У разі залучення цих ресурсів їх вартість у бюджеті обліковується як нульова, але вони фіксуються у структурі ресурсів (RBS) як наявні та використовувані [21, с. 12-29].

Потреба у фінансових коштах у часі розподіляється таким чином: на початковому етапі (тижні 1–5) основні витрати пов'язані з придбанням програмного забезпечення та мобільним зв'язком для організації інтерв'ю; на середньому етапі (тижні 6–12) – оплата хостингу та поточні витрати на зв'язок; на завершальному етапі (тижні 13–16) – друк матеріалів для захисту та непередбачені витрати. Такий розподіл дозволяє уникнути пікового фінансового навантаження в будь-який окремий момент реалізації проєкту.

2.5 Управління якістю медіапроєкту

Управління якістю є одним із найважливіших аспектів медіапроєкту, особливо з огляду на специфіку теми: матеріал про цифрову безпеку, що містить неточності або застарілу інформацію, може завдати реальної шкоди читачеві. Тому системи забезпечення та контролю якості розроблені з особливою ретельністю.

Чинники, що впливають на якість медіапродукту, можна розподілити на змістовні, технічні та комунікативні.

До змістовних чинників належать точність фактів і технічних описів, актуальність інформації (кіберзагрози еволюціонують, тому важливо використовувати найсвіжіші джерела), повнота охоплення теми (відсутність критично важливих тем), доступність викладу для нефахівців та практична цінність для читача [35, с. 67-74].

До технічних чинників відносяться якість верстки та оформлення, зручність читання (структура, підзаголовки, розмір тексту), коректна робота всіх інтерактивних елементів, швидкість завантаження сторінки та відображення на різних пристроях (адаптивність для мобільних).

До комунікативних чинників – логічність і послідовність наративу, узгодженість тону й голосу автора протягом усього матеріалу, ясність і однозначність практичних порад, відсутність зайвого технічного жаргону без пояснення (табл. 2.3) [35, с. 67-74].

Таблиця 2.3

Чинники якості медіапроєкту та методи контролю

Чинник	Ступінь впливу	Метод забезпечення якості	Метод контролю
Фактична точність	Критичний	Перевірка кожного твердження за кількома джерелами	Рецензія технічного експерта
Актуальність	Високий	Використання джерел не старших 2 років	Дата-перевірка джерел

Доступність	Високий	Текст читабельності (Flesh або аналог)	Читацький тест на нефахівці
Повнота	Середній	Чеклист тем за структурою WBS	Перевірка науковим керівником
Верстка або дизайн	Середній	Дотримання редакційного стилю	Тест на різних пристоях
Практична цінність	Критичний	Кожен розділ містить конкретну дію	Тест: «Що я можу зробити прямо зараз?»

Способи забезпечення якості включають принцип «двох очей» (кожен змістовний фрагмент перевіряється автором та науковим керівником), фактчекінг усіх статистичних даних і технічних тверджень за першоджерелами, а також тест-читання матеріалу особою, яка не є фахівцем у темі – для перевірки доступності викладу.

2.6 Управління ризиками медіапроєкту

Ризики медіапроєкту є невід'ємною частиною його реальності – особливо в умовах воєнного часу, коли зовнішні обставини можуть кардинально змінитися. Управління ризиками передбачає їх ідентифікацію, оцінку ймовірності та впливу, а також розробку механізмів реагування.

Ризики медіапроєкту класифікуються за такими джерелами: дослідницькі ризики (пов'язані зі збором інформації), операційні ризики (пов'язані з виконанням роботи), технічні ризики (пов'язані з інструментами та платформами) та контекстуальні ризики (зумовлені зовнішнім середовищем) (рис. 2.4, табл. 2.4) [22, с. 167-189].

ВПЛИВ		
Високий	Р3 Відмова експерта від інтерв'ю	Р1 Недоступність ключових джерел /зміна ситуації Р2 Технічний збій
Середній	Р5 Зміна дедлайнів	Р4 Застарівання інформації
Низький	Р6 Юридичні питання	Р7 Плагіат/ UniCheck
	Низька	Висока
	ЙМОВІРНІСТЬ	

Рис. 2.4. Матриця ризиків медіапроєкту

Таблиця 2.4. Реєстр ризиків та механізми їх подолання

Код	**Ризик**	**Ймовір-ність**	**Вплив**	**Механізм подолання**
Р1	Недоступність ключових інформаційних джерел	Середня	Високий	Формування резервного списку джерел; використання альтернативних баз даних
Р2	Технічний збій (втрата файлів, збій платформи)	Середня	Високий	Регулярне резервне копіювання (щоденне), використання хмарних сервісів
Р3	Відмова запланованих експертів від інтерв'ю	Висока	Середній	Залучення 5–7 потенційних експертів замість мінімально необхідних 2–3
Р4	Застарівання інформації через швидкозмінність теми	Висока	Середній	Фінальна перевірка актуальності даних за 1–2 тижні до публікації
Р5	Зміна академічних дедлайнів або вимог	Низька	Середній	Моніторинг розпоряджень кафедри; гнучкий план із часовим резервом
Р6	Юридичні питання (авторське право на матеріали)	Низька	Низький	Використання матеріалів під ліцензіями Creative Commons; правильне цитування
Р7	Низький показник унікальності тексту	Середня	Середній	Власний стиль написання; перефразування, а не цитування; своєчасна перевірка

Механізми подолання ризиків базуються на трьох стратегіях. Стратегія уникнення застосовується до ризиків, що легко прогнозуються і яким можна

запобігти через зміну підходу [37, с. 145-189]. Стратегія пом'якшення передбачає дії, що знижують ймовірність або вплив ризику. Стратегія реагування описує дії у разі, якщо ризик все ж таки реалізувався.

2.7 Управління командою медіапроєкту

Хоча медіапроєкт реалізується переважно індивідуально, ефективне управління командою передбачає чітке розуміння ролей та відповідальностей усіх залучених осіб – від автора до наукового керівника та зовнішніх консультантів.

Організаційна структура команди медіапроєкту (OBS – Organizational Breakdown Structure) включає кілька рівнів учасників із різними зонами відповідальності (рис. 2.5).

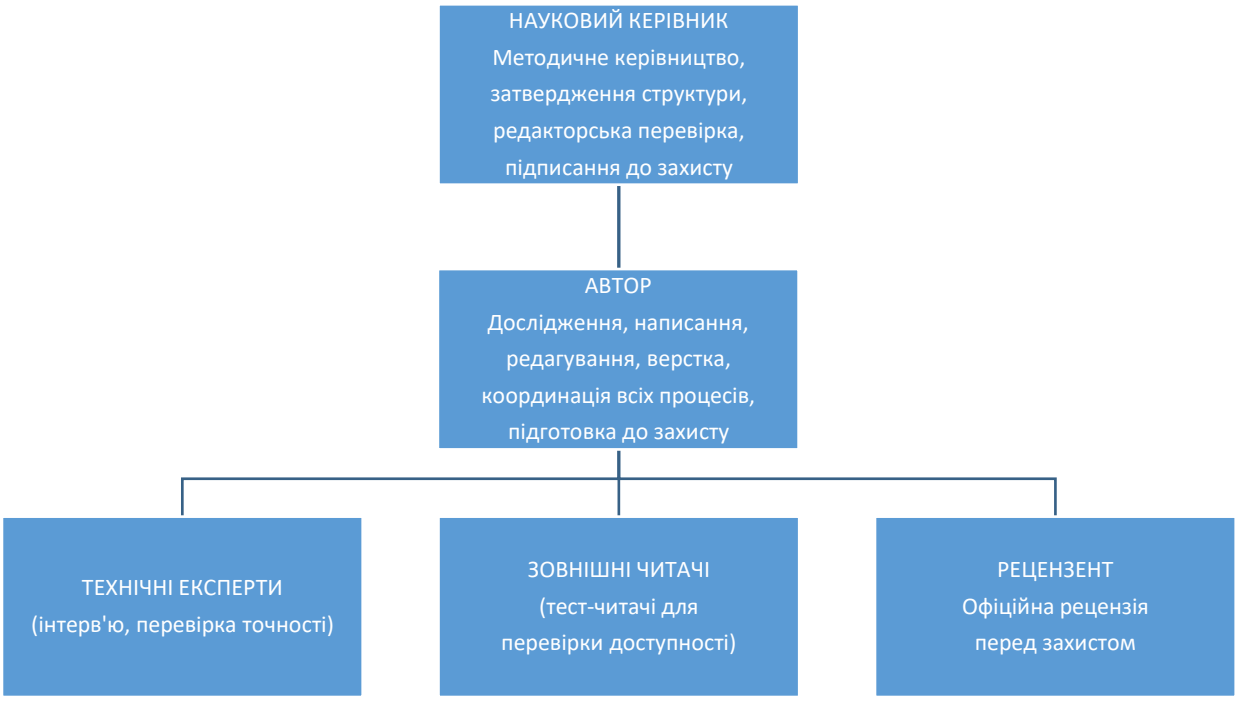

Рис. 2.5. Організаційна структура команди медіапроєкту

Матриця розподілу відповідальності (RACI) визначає для кожного завдання чотири ролі: R (Responsible – виконавець), A (Accountable –

відповідальний за результат), C (Consulted – консультується), I (Informed – інформується) (табл. 2.5) [21, с. 12-29].

Таблиця 2.5

Матриця розподілу відповідальності (RACI)

Завдання	Автор	Науковий керівник	Технічний експерт	Рецензент
Розробка концепції	R/A	C	–	–
Затвердження структури	R	A	C	–
Збір інформації	R/A	I	C	–
Написання чорновика	R/A	I	–	–
Редагування та правка	R	A	–	–
Технічна перевірка точності	R	I	A/C	–
Верстка та оформлення	R/A	I	–	–
Підготовка до захисту	R	C	–	I
Офіційна рецензія	I	I	–	R/A

Ключові зони відповідальності в управлінні проєктом розподілені таким чином: автор є центральним виконавцем і несе відповідальність за всі оперативні рішення; науковий керівник є стратегічним наставником і фінальним арбітром у питаннях структури, змісту та відповідності академічним вимогам; технічні експерти відповідають за точність технічного змісту в межах своєї компетенції і не несуть відповідальності за загальну концепцію або структуру матеріалу [22, с. 178-195].

Управління командою також передбачає формування чіткого протоколу комунікації, описаного в наступному підрозділі, а також системи мотивації та підтримки. Попри індивідуальний характер проєкту, регулярна взаємодія з науковим керівником та зовнішніми консультантами виконує важливу мотивуючу та стабілізуючу функцію – особливо в критичні моменти, коли виконавець стикається з інформаційним перевантаженням або творчими труднощами.

2.8 Управління комунікаціями медіапроєкту

Управління комунікаціями охоплює два виміри: внутрішні комунікації в процесі роботи над проєктом та зовнішні комунікації, спрямовані на поширення готового медіапродукту серед цільової аудиторії.

Внутрішні комунікації регулюються схемою обміну інформацією між учасниками проєкту. Основними каналами внутрішніх комунікацій є електронна пошта (для офіційного листування, передачі файлів та отримання зауважень від наукового керівника), месенджери (Telegram або Viber – для оперативної комунікації та уточнення питань), платформа Google Docs (для спільної роботи з текстом у режимі реального часу з можливістю коментування). Частота комунікацій з науковим керівником – не рідше одного разу на два тижні в плановому режимі та за потреби – позапланово (рис. 2.6) [44, с. 144-155].

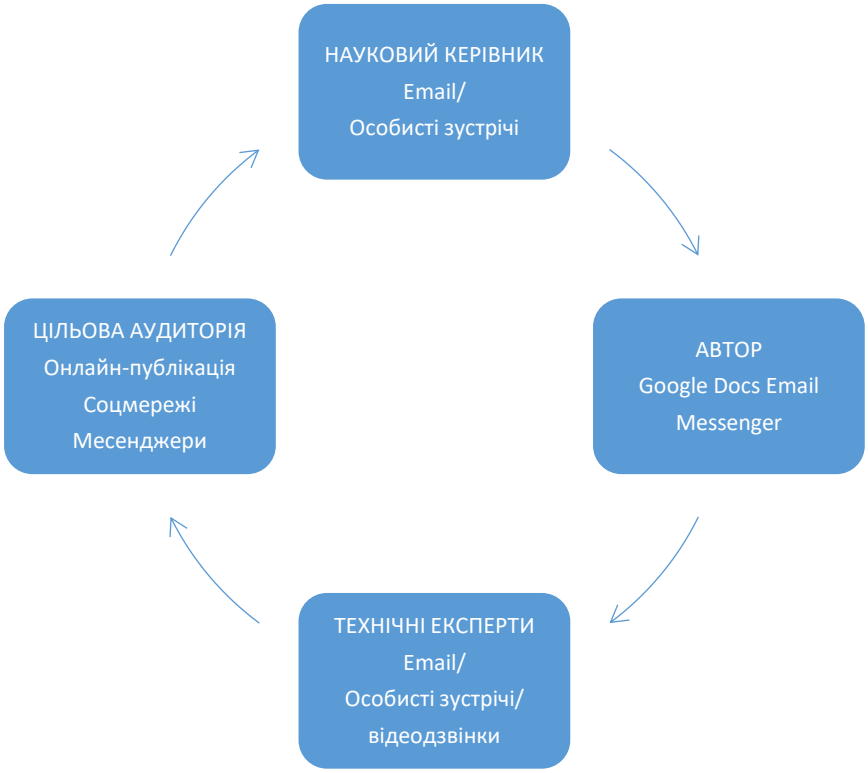

Рис. 2.6. Загальна схема обміну інформацією у медіапроєкті

Зовнішні комунікації охоплюють усі канали поширення готового медіапродукту та взаємодію з читацькою аудиторією. Медіаплан публікації передбачає такі ключові елементи.

Основним каналом є онлайн-платформа (власний сайт, університетська платформа або авторитетне медіавидання, яке погодиться розмістити матеріал). Допоміжними каналами поширення є: Facebook (публікація анонсу та ключових тез з посиланням на повний матеріал), Telegram (поширення через тематичні канали з аудиторією, зацікавленою у темі цифрової безпеки), Instagram (публікація візуальних фрагментів – окремих інфографік та схем – з посиланням у профілі) (табл. 2.6) [22, с. 178-195].

Таблиця 2.6

Медіаплан поширення медіапроєкту

Канал	**Формат контенту**	**Частота**	**Цільова аудиторія**	**Відповідальний**
Онлайн-платформа	Повний лонгрід	Одноразова публікація	Широка онлайн-аудиторія	Автор
Facebook	Анонс + цитата + посилання	1 публікація в день виходу + 2 репости	Соціально активна аудиторія 25–45	Автор
Telegram	Анонс + ключові тези	1 допис в день виходу	Аудиторія тематичних каналів	Автор
Instagram	Інфографіка (1–3 картки)	1–3 публікації	Молода аудиторія 18–30	Автор
Email-розсилка	Посилання з коротким описом	Одноразово	Контакти та партнерські спільноти	Автор

Контент-план підготовки до публікації передбачає такі матеріали: тизер-публікацію за тиждень до виходу лонгріду (оголошення про майбутній матеріал, інтрига через ключове питання або статистику), публікацію в день виходу (повноцінний анонс з посиланням), серію допоміжних публікацій протягом двох тижнів після виходу (окремі тематичні фрагменти, що привертають увагу нових читачів).

2.9 Моніторинг виконання медіапроєкту

Моніторинг є системним процесом відстеження відповідності реального перебігу медіапроєкту його плановим параметрам. Для медіапроєкту «Цифрова безпека українців» система моніторингу спроєктована з урахуванням двох вимірів: моніторинг процесу виробництва (чи виконуються заплановані роботи у строк та з необхідною якістю?) та моніторинг результатів після публікації (чи досягає медіапродукт своєї аудиторії та мети?) [45, с. 67-89].

Типи моніторингової інформації щодо медіапроєкту можна систематизувати за такими категоріями:

Інформація про прогрес виконання включає відсоток виконання кожного завдання відповідно до WBS-структури, дотримання дедлайнів ключових мілстоунів, кількість написаних і відредагованих розділів, кількість проведених інтерв'ю та опрацьованих джерел.

Інформація про якість контенту охоплює результати перевірки на унікальність тексту, оцінку наукового керівника за кожним переданим блоком матеріалу, відгуки технічних експертів щодо точності змісту, результати тест-читань нефахівцями [26, с. 234-267].

Інформація про ресурсне виконання включає фактичні витрати порівняно з запланованим бюджетом, фактичні часові затрати порівняно з плановими оцінками, відповідність використовуваних інструментів та платформ запланованим.

Інформація про результати публікації – кількість переглядів матеріалу, середній час читання, географія та демографія аудиторії (за аналітикою платформи), кількість поширень у соціальних мережах, коментарі та зворотний зв'язок від читачів, реакції експертної спільноти (рис. 2.7).

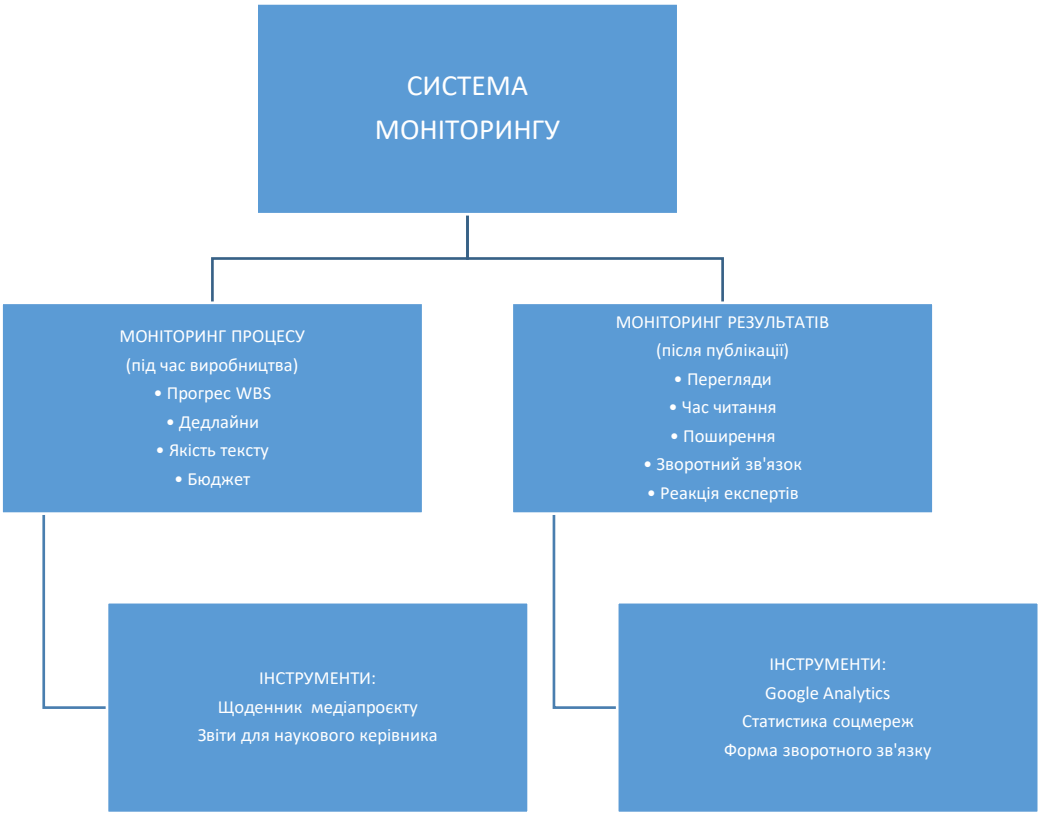

Рис. 2.7. Система моніторингу медіапроєкту

Процедура моніторингу здійснюється за такою схемою. Щотижнево автор фіксує у щоденнику медіапроєкту (відповідно до форми, наведеної у Додатку А методичних рекомендацій) виконані завдання, дотримані або порушені дедлайни, виниклі проблеми та вжиті заходи. Раз на два тижні проводиться зустріч або відеодзвінок із науковим керівником, на якому обговорюється поточний стан проєкту та узгоджуються корективи плану. Після кожного переданого блоку тексту автор отримує письмові зауваження від наукового керівника, опрацьовує їх і документує внесені зміни (табл. 2.7) [5, с. 189-234].

Таблиця 2.7

Точки поточного контролю (мілстоуни) та очікувані результати

Мілстоун	Строк	Очікуваний результат	Критерій виконання
М1: Затвердження концепції	Тиждень 2	Погоджена структура та план	Підпис наукового керівника
М2: Завершення дослідження	Тиждень 5	Повна база джерел та матеріалів	Наявність 15+ джерел, + інтерв'ю
М3: Передача чорновика	Тиждень 10	Повний чорновик усіх розділів	Відповідь наукового керівника

М4: Фанальна редакція	Тиждень 12	Відредагований та перевірений текст	Унікальність 90%+, схвалення керівника
М5: Фінальна редакція	Тиждень 13	Опублікований лонгрід	Активне посилання на матеріал
М6: Захист	Тиждень 16	Успішний публічний захист	Оцінка ЕК

Особливу увагу в системі моніторингу приділено превентивному реагуванню: виявлення відхилень від плану на ранньому етапі дозволяє коригувати курс без кризових наслідків. Методологічно це реалізується через принцип «двотижневого горизонту» – автор завжди планує не лише поточний тиждень, але й наступний, що дозволяє бачити потенційні конфлікти дедлайнів заздалегідь і перерозподіляти навантаження [36, с. 5-20].

Таким чином, система управління медіапроєктом «Цифрова безпека українців: як розпізнати загрози і захистити себе онлайн» є комплексною та цілісною: від змісту і часу до якості, ризиків, команди, комунікацій і моніторингу. Кожен елемент цієї системи є не формальністю, а реальним інструментом, що забезпечує успішну реалізацію медіапроєкту в академічних умовах і водночас формує у виконавця навички проєктного менеджменту, що є затребуваними в сучасній медіаіндустрії.

РОЗДІЛ 3. ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ МЕДІАПРОЄКТУ

3.1 Проблеми з практичною реалізацією проєкту

Реалізація будь-якого медіапроєкту незмінно стикається з розривом між теоретичним плануванням і практичною дійсністю. Цей розрив є не свідченням слабкості плану, а органічною властивістю проєктної діяльності як такої – адже, за визначенням Лабораторії журналістської майстерності НаУОА, медійний проєкт є пригодою, а пригода завжди передбачає непередбачувані ситуації. Медіапроєкт «Цифрова безпека українців: як розпізнати загрози і захистити себе онлайн» не став винятком із цього правила.

Проблеми, що виникли в ході практичної реалізації, можна систематизувати за кількома групами: дослідницькі, організаційні, змістовні та технічні. Кожна з цих груп вимагала власної методики опрацювання і стала важливою частиною навчального досвіду, що є однією з ключових цілей кваліфікаційного медійного проєкту [5, с. 234-267].

Дослідницькі проблеми виявилися найбільш складними і різноплановими. Перша з них – надлишок інформації при дефіциті якісної. Тема цифрової безпеки є одночасно надзвичайно популярною і катастрофічно засміченою: інтернет рясніє матеріалами різного рівня достовірності, від академічних досліджень до відверто рекламних статей компаній, що продають антивірусне програмне забезпечення. Розрізнення авторитетних джерел від маркетингового контенту, замаскованого під аналітику, виявилося окремим дослідницьким завданням, що вимагало значно більше часу, ніж було передбачено початковим планом [4, с. 45-67].

Друга дослідницька проблема пов'язана зі швидкоплинністю теми. Кібербезпекова ситуація змінюється буквально щодня: з'являються нові вектори атак, закриваються старі вразливості, вступають у дію нові законодавчі норми, стають публічними нові інциденти. Інформація, що була актуальною на початку дослідження, могла частково застаріти до моменту

завершення написання. Це змусило запровадити систему регулярної актуалізації джерел – повторну перевірку кожного статистичного твердження та кожного опису конкретного інструменту безпосередньо перед фінальним редагуванням [28, с. 156-178].

Третя дослідницька проблема – складність залучення якісних експертних джерел. Фахівці з кібербезпеки, які справді розуміються на темі і водночас здатні говорити зрозумілою для масової аудиторії мовою, є дефіцитним ресурсом. Частина потенційних експертів відмовилась від інтерв'ю з посиланням на зайнятість або небажання розголошувати свою позицію публічно – особливо з питань, що стосуються конкретних державних структур або методів атак, що використовуються проти України. Це змусило розширити первинний список потенційних співрозмовників із трьох до восьми осіб, аби забезпечити мінімально необхідну кількість якісних інтерв'ю.

Організаційні проблеми мали переважно часовий характер. Поєднання роботи над медіапроєктом з іншими академічними обов'язками та роботою виявилося складнішим, ніж передбачалося на етапі планування. Реальна продуктивність письма виявилася нижчою від розрахованої на 15–20%: якісний журналістський текст на складну тему вимагає значно більше розумових зусиль і часу на «обдумування», ніж на суто механічне набирання слів [4, с. 67-89].

Крім того, відповіді від наукового керівника та зовнішніх рецензентів надходили не завжди у заплановані строки – що є цілком нормальною ситуацією в академічному середовищі, проте вимагає закладання відповідного буферного часу в план. Саме тому десятивідсотковий часовий резерв, передбачений у плані ще на етапі планування, виявився не надлишком, а необхідністю.

Змістовні проблеми були пов'язані передусім із пошуком правильного балансу між технічною точністю та доступністю викладу. Матеріал про цифрову безпеку неминуче оперує технічними поняттями, і кожне з них потенційно є бар'єром для нефахового читача. Надмірне спрощення

загрожувало втратою точності та практичної цінності – адже поверхнева порада «використовуйте складний пароль» є очевидною й малокорисною. Недостатнє спрощення загрожувало відштовхнути масового читача ще на початку матеріалу [48].

Вирішення цього протиріччя потребувало численних ітерацій тексту та тест-читань: кожен складний розділ проходив перевірку на людині без технічної освіти, і лише після успішного тесту («ти зрозумів? ти знаєш, що робити після прочитання?») вважався прийнятним.

Технічні проблеми виявилися найменш значущими з погляду впливу на результат, але вимагали оперативного реагування. Проблеми з версткою інфографіки та адаптивністю матеріалу для мобільних пристроїв вирішувалися через зміну інструментів: первинно обраний сервіс було замінено на більш зручний аналог. Технічний збій з втратою частини тексту стався один раз і став практичним нагадуванням про важливість регулярного резервного копіювання, передбаченого планом управління ризиками (рис. 3.1).

ПРОБЛЕМИ РЕАЛІЗАЦІЇ МЕДІАПРОЄКТУ		
ГРУПА	ПРОБЛЕМА	РІВЕНЬ ВПЛИВУ
ДОСЛІДНИЦЬКІ	Надлишок неякісних джерел	Високий
	Швидкоплинність теми	Високий
	Дефіцит якісних експертів	Середній
ОРГАНІЗАЦІЙНІ	Поєднання з іншими академічними обов'язками	Середній
	Затримки відповідей	Низький
ЗМІСТОВНІ	Баланс точності та доступності	Високий
	Пошук правильного тону оповіді	Середній
ТЕХНІЧНІ	Верстка інфографіки	Низький
	Адаптивність для мобільних	Низький

Рис. 3.1. Класифікація проблем реалізації медіапроєкту за групами та рівнем впливу

Важливим висновком цього підрозділу є те, що жодна з виявлених проблем не стала критичною або такою, що унеможливила б реалізацію

проєкту [21, с. 12-29]. Це свідчить про ефективність системи управління ризиками, закладеної ще на етапі планування. Проте кожна проблема вимагала адаптивного реагування і внесення коректив у план – що є нормальним і очікуваним явищем у проєктній діяльності.

3.2 Особливості реалізації медіапроєкту

Реалізація медіапроєкту «Цифрова безпека українців» мала ряд специфічних особливостей, зумовлених унікальним поєднанням теми, формату, контексту та аудиторії. Ці особливості суттєво відрізняють даний медіапроєкт від типових академічних проєктів і визначили ключові рішення, прийняті в ході виробничого процесу.

Перша особливість – подвійна природа дослідження. Медіапроєкт поєднав у собі журналістське розслідування та просвітницький проєкт. З одного боку, він вимагав класичної журналістської методології: пошуку та верифікації джерел, роботи з експертами, перевірки фактів, вибудовування наративу на основі реальних кейсів. З іншого боку, освітня мета проєкту визначала необхідність педагогічного підходу до подачі матеріалу: послідовного введення нових понять, повторення ключових ідей, практичних вправ та інструментів для самостійного застосування читачем. Поєднання цих двох підходів в єдиному медіапродукті є нетривіальним завданням, що потребувало постійного балансування між «журналістським» і «педагогічним» режимами [10].

Друга особливість – специфіка роботи з експертами в умовах воєнного часу. Фахівці з кібербезпеки в Україні під час повномасштабного вторгнення перебувають під підвищеним тиском: вони задіяні у захисті критичної інфраструктури, часто мають обмежений час для зовнішніх комунікацій і дуже обережні щодо публічних висловлювань з питань, що можуть мати стратегічне значення. Це означало, що підготовка до кожного інтерв'ю вимагала значно глибшого занурення в тему з боку журналіста, ніж це прийнято в стандартній

журналістській практиці: поверхневі запитання не просто не давали корисних відповідей – вони підривали довіру до серйозності проєкту і могли призвести до відмови від подальшої співпраці.

Третя особливість – необхідність постійного самообмеження в технічних деталях. Занурення в тему цифрової безпеки закономірно породжує бажання розповісти про неї якомога детальніше і точніше – пояснити технічні механізми, описати конкретні протоколи шифрування, навести приклади коду. Для масової аудиторії такий підхід є контрпродуктивним. Кожного разу, коли текст ставав надто технічним, доводилося повертатися до базового питання: «Що читач зможе зробити після прочитання цього абзацу?» Якщо відповідь була «нічого конкретного» – абзац потребував переписування [11].

Четверта особливість – етичний вимір матеріалу. Журналістський матеріал про кіберзагрози несе в собі певний ризик: описуючи методи атак достатньо детально для розуміння аудиторією, він водночас потенційно надає інформацію тим, хто хотів би використати ці методи в шахрайських цілях. Цей етичний баланс між «правом аудиторії знати» та «принципом не нашкодь» потребував чіткого редакційного правила: матеріал описує механізми загроз на рівні, достатньому для їх розпізнавання та розуміння, але не надає інструкцій із реалізації атак. Цей принцип послідовно дотримувався протягом усього написання.

П'ята особливість – робота з реальними людськими випадками. Лонгрід побудований на реальних кейсах – реальних людях, що постраждали від кіберзагроз. Ці кейси є найефективнішим педагогічним інструментом (абстрактна загроза стає реальною, коли читач бачить конкретну людину, її ситуацію та наслідки), але водночас несуть відповідальність за захист приватності та репутації. Всі кейси, що включені до матеріалу, або є публічно відомими (задокументованими у ЗМІ або офіційних звітах), або отримані від осіб із явною письмовою згодою на публікацію, або повністю анонімізовані із зміною несуттєвих деталей (табл. 3.1).

Таблиця 3.1

Ключові особливості реалізації медіапроєкту та прийняті рішення

Особливість	Виклик	Прийняте рішення	Результат
Подвійна природа дослідження	Поєднання журналістики та педагогіки	Чергування наративних та пояснювальних блоків	Збалансована структура лонгріду
Робота з експертами у воєнний час	Обмежена доступність і обережність	Глибока підготовка, чіткі запитання, конфіденційність за бажанням	2 якісні інтерв'ю
Технічна глибина vs. доступність	Ризик перевантаження читача	Тест-читання + правило «що читач зробить після?»	Текст, зрозумілий нефахівцям
Етичний баланс	Описувати загрози, не допомагаючи зловмисникам	Правило: механізм без інструкції	Безпечний матеріал
Реальні людські кейси	Захист приватності	Анонімізація або явна згода	Етично коректна публікація

Шоста особливість – мультимедійний характер виробництва. Лонгрід як формат вимагає паралельного виробництва текстового та візуального контенту, що для одного автора є значним навантаженням. Інфографіка, схеми та чеклисти не могли вироблятися після завершення тексту – вони мали розроблятися паралельно, оскільки є органічними частинами наративу, а не ілюстраціями до вже готового тексту. Це вимагало від автора паралельного використання двох різних режимів мислення: вербального (текст) і візуального (графіка), що на практиці вирішувалося через чіткий часовий розподіл: ранкові сесії – для написання тексту, вечірні – для роботи з візуальним контентом [3].

Сьома особливість – психологічний вимір теми. Тривале занурення в тему кіберзагроз і дезінформації несе ризик так званого «інформаційного вигорання» або надмірної параної – стану, коли кожен електронний лист здається фішинговим, а кожне повідомлення у месенджері – спробою злому [48]. Цей ефект добре відомий журналістам і дослідникам, що працюють із темами безпеки, і потребує свідомого управління: регулярні паузи в роботі, обмеження часу на читання новин про кіберінциденти, свідоме повернення до «нормального» режиму користування технологіями.

3.3 Структура та мультимедійне наповнення лонгріду

Структура лонгріду є результатом численних ітерацій і відображає продуману логіку руху читача від усвідомлення проблеми до практичного захисту. Вона базується на принципі «від загального до конкретного, від проблеми до рішення», що є класичним для журналістики рішень (solution journalism) – підходу, який не лише описує проблему, а й активно пропонує шляхи її подолання (рис. 3.2) [59, с. 78-84].

ЛОНГРІД «Цифрова безпека українців»
ЛІД (гачок) Людська історія: реальна жертва кіберзлочину + статистика, що підсилює
БЛОК 1: РОЗУМІННЯ СЕРЕДОВИЩА ЗАГРОЗ Чому Україна є особливо вразливою? Карта основних загроз ← [ІНФОГРАФІКА 1]
БЛОК 2: ФІШИНГ І СОЦІАЛЬНА ІНЖЕНЕРІЯ Як це працює? + Реальний кейс Як розпізнати? ← [ІНФОГРАФІКА 2: чеклист]
БЛОК 3: ЗАХИСТ АКАУНТІВ ТА ПАРОЛІВ Паролі, 2FA, менеджери паролів Покроковий алгоритм ← [СХЕМА 1] БЛОК 3.1: ШТУЧНИЙ ІНТЕЛЕКТ НА СЛУЖБІ ШАХРАЇВ
БЛОК 4: ДЕЗІНФОРМАЦІЯ ТА ПЕРЕВІРКА ФАКТІВ Механізми дезінформації в умовах війни Як перевіряти? ← [СХЕМА 2: алгоритм]
БЛОК 5: ЦИФРОВА ГІГІЄНА В ПОВСЯКДЕННОМУ ЖИТТІ Базові правила + Практичний чеклист ← [ЧЕКЛИСТ]
БЛОК 6: КУДИ ЗВЕРТАТИСЯ ПО ДОПОМОГУ Ресурси та контакти ← [ІНТЕРАКТИВНА КАРТА]
ВИСНОВОК: КУЛЬТУРА ЦИФРОВОЇ БЕЗПЕКИ Від страху до свідомого захисту

Рис. 3.2. Загальна структура лонгріду «Цифрова безпека українців»

Кожен блок лонгріду має власну внутрішню структуру, що відтворює мікрологіку руху від проблеми до рішення: спочатку читач бачить, що загроза реальна і конкретна (людська історія або статистика), потім розуміє механізм

її дії (пояснення), далі вчиться розпізнавати (ознаки), і нарешті отримує конкретні інструменти захисту (практичний блок).

Мультимедійне наповнення лонгріду складається з кількох типів елементів, кожен із яких виконує специфічну функцію в загальній системі комунікації.

Перший тип – інфографіка – використовується для відображення системних зв'язків і структур, які важко передати словами: карта загроз, статистичні дані, порівняльні таблиці. Інфографіка в цьому лонгріді виконана в стриманій кольоровій гамі (темно-синій, помаранчевий, білий) – кольори, що асоціюються з цифровим простором і водночас несуть українські коди.

Другий тип – схеми та алгоритми – відображають покрокові процеси: як відбувається фішингова атака (щоб читач зрозумів логіку зловмисника), як перевірити підозрілий лист, як налаштувати двофакторну автентифікацію. Схеми побудовані за принципом «якщо – то», що є звичною логікою для читача і полегшує засвоєння [14, с. 45-67].

Третій тип – чеклисти – є найбільш практично орієнтованим елементом лонгріду. Читач може роздрукувати або зберегти чеклист і використовувати його як практичний інструмент. Чеклисти розроблені для трьох рівнів: базовий (мінімально необхідні дії, що займуть 30 хвилин), середній (розширений захист, на кілька годин), просунутий (для тих, хто хоче максимального захисту).

Четвертий тип – цитатні блоки – виділяють ключові висловлювання експертів, що водночас підсилюють авторитетність матеріалу і служать точками відпочинку в суцільному тексті. Кожен цитатний блок супроводжується ім'ям та посадою експерта, а також його фото (за наявності згоди).

П'ятий тип – вставні блоки «Важливо» – привертають увагу до критично важливих практичних порад або попереджень, що не можна пропустити. Вони відображаються на яскравому фоні і є візуально помітними навіть для читача, що «сканує» матеріал, а не читає його повністю (табл. 3.2, рис. 3.3).

Таблиця 3.2

Мультимедійні елементи лонгріду та їхні функції

Тип елементу	Кількість	Функція	Інструмент створення
Інфографіка	3	Системна візуалізація загроз і статистики	Canva Pro
Схеми-алгоритми	4	Покрокова візуалізація процесів	Canva / Figma
Чеклисти	3 рівні	Практичний інструмент для читача	Google Docs + Canva
Цитатні блоки	3-4	Авторитетність, ритм читання	Верстка платформи
Вставні блоки «Важливо»	3-4	Виділення критичних порад	Верстка платформи
Фото / ілюстрації	1-2	Емоційне залучення	Unsplash (CC)

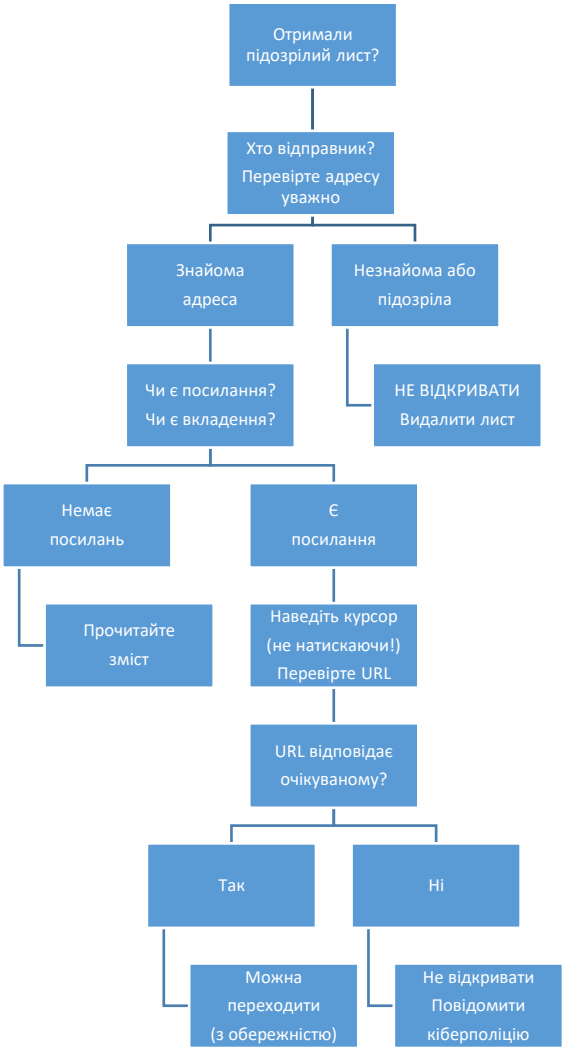

Рис. 3.3. Приклад алгоритму перевірки підозрілого електронного листа (фрагмент схеми з лонгріду)

Лід лонгріду є критично важливим елементом, що визначає, чи читатиме аудиторія матеріал далі. Він побудований на класичному прийомі «сцена»: конкретна людина, конкретний момент, конкретна проблема – без абстракцій і статистики на початку. Лише після того, як читач емоційно залучений через людську історію, з'являється статистика і ширший контекст. Цей прийом є перевіреним у практиці найкращих лонгрідів і відповідає принципам «нової журналістики» [11, с. 89-145].

Мова та стиль матеріалу свідомо обрані як розмовні, але грамотні – без канцеляризмів і академічного пасиву, але й без надмірного спрощення. Активний стан дієслів, короткі речення для ключових тверджень, довші – для пояснень і нюансів. Автор свідомо присутній у тексті: є місця, де «я» або «ми» є природними – і вони не приховуються. Це робить матеріал більш людяним і довіреним.

3.4 Рекомендації щодо покращення розробки та реалізації медіапроєкту

Досвід реалізації медіапроєкту «Цифрова безпека українців: як розпізнати загрози і захистити себе онлайн» дозволив сформулювати ряд конкретних рекомендацій – як щодо покращення власне цього проєкту в майбутніх ітераціях, так і щодо розробки та реалізації схожих медіапроєктів загалом. Ці рекомендації адресовані передусім майбутнім здобувачам вищої освіти, що планують реалізовувати кваліфікаційні медіапроєкти у форматі лонгріду на складні суспільно значущі теми.

Рекомендація 1. Починати дослідження раніше за написання.

Найбільш поширеною помилкою при реалізації подібних медіапроєктів є спроба починати писати ще до завершення дослідницького етапу. Логіка «напишу, що знаю, а потім допишу те, що дізнаюся» є небезпечною пасткою: вона призводить до того, що структура тексту визначається не логікою теми, а обсягом інформації, доступної в конкретний момент. Результатом є

нерівномірний матеріал, у якому добре досліджені частини є детальними та переконливими, а слабко досліджені – поверховими та загальними.

Правило, перевірене практикою: написання основного тексту має розпочинатися лише тоді, коли дослідник може впевнено відповісти на такі питання: «Яка головна ідея матеріалу?», «Які три найсильніші приклади її підтверджують?», «Хто найкращий голос для кожного ключового твердження?». Якщо на будь-яке з цих питань немає чіткої відповіді – дослідження ще не завершено [21, с. 15-29].

Рекомендація 2. Залучати «наївного читача» на кожному етапі.

Практика тест-читань виявилася надзвичайно цінною для медіапроєкту на складну технічну тему. Рекомендується залучати кількох «наївних читачів» – людей, що не мають фахової підготовки в галузі теми, – на трьох різних стадіях: після розробки структури (чи зрозуміла логіка?), після написання чорновика (чи зрозумілий текст?), після оформлення (чи зручно читати?). Зворотний зв'язок від таких читачів є несумірно ціннішим, ніж зворотний зв'язок від фахівців, які вже мають контекст і не можуть «роздивитися» матеріал очима нової людини.

Рекомендується використовувати стандартизовану форму зворотного зв'язку з кількома конкретними запитаннями: «Що, на вашу думку, є головною ідеєю цього матеріалу?», «Що залишилося незрозумілим?», «Яку конкретну дію ви плануєте здійснити після прочитання?», «Що, на вашу думку, є зайвим або нудним?».

Рекомендація 3. Планувати час із коефіцієнтом 1,5.

Досвід реалізації проєкту підтверджує загальне правило проєктного менеджменту: реальний час виконання творчих завдань, як правило, перевищує плановий у 1,3–1,7 рази. Особливо це стосується написання: якісний аналітичний текст не пишеться рівномірно – є дні продуктивності та дні «блоку». Планувати час варто з коефіцієнтом 1,5 від оптимістичної оцінки, зберігаючи 10–15% загального часу як резерв для непередбачуваних ситуацій (рис. 3.4) [4, с. 45-67].

РЕКОМЕНДОВАНЕ РОЗПОДІЛЕННЯ ЧАСУ МЕДІАПРОЄКТУ			
ЕТАП	РЕКОМЕНДОВАНА ЧАСТКА		ТИПОВА ПОМИЛКА
Дослідження		30%	15% (замало)
Структурування		10%	5% (ігнорують)
Написання чорновика		25%	40% (забагато)
Редагування		20%	10% (замало)
Візуальне оформлення		10%	5% (ігнорують)
Резерв		5%	0% (не планують)

Рис. 3.4. Схема рекомендованого планування часу для медіапроєкту у форматі лонгріду

Рекомендація 4. Будувати базу джерел до початку написання.

Ефективна робота з джерелами потребує системного підходу від самого початку: кожне джерело слід вносити в базу даних (навіть проста таблиця в Google Sheets підійде) із зазначенням автора, назви, року, URL, коротким конспектом і позначкою, для якої частини матеріалу воно є релевантним. Ця база стає незамінним інструментом при написанні: замість того, щоб згадувати, «де я читав про це», автор відразу знаходить потрібне посилання.

Для теми цифрової безпеки особливо важливо позначати в базі дату кожного джерела і встановити для себе правило: статистичні дані старші двох років не використовуються без додаткової перевірки на актуальність [26, с. 234-267].

Рекомендація 5. Розробляти візуальний контент паралельно з текстом.

Типова помилка медіапроєктів у форматі лонгріду – відкладати роботу над інфографікою та схемами «на потім», після завершення тексту. Це призводить до двох проблем: по-перше, у фінальній частині роботи, коли час обмежений, якість візуального контенту суттєво знижується; по-друге, інфографіка, створена після тексту, часто є ілюстрацією до нього, а не органічною частиною наративу. Найкращий підхід – визначати місця для

візуальних елементів ще на рівні структури та розробляти їх паралельно з відповідними текстовими розділами.

Рекомендація 6. Фіксувати рефлексію регулярно, а не лише наприкінці.

Щоденник медіапроєкту є не бюрократичним інструментом, а реальним засобом самопізнання і навчання. Регулярна письмова рефлексія – навіть у форматі кількох речень на день – дозволяє відстежувати власний прогрес, ідентифікувати закономірності (наприклад, у який час дня робота є найефективнішою), документувати ключові рішення та їх обґрунтування. Це безцінний матеріал для написання Розділу 3 та для підготовки до захисту [36, с. 5-20].

Рекомендація 7. Тестувати технічну реалізацію на реальних пристроях завчасно.

Верстка лонгріду для онлайн-публікації має тестуватися на різних пристроях і в різних браузерах не після завершення, а в процесі – щоб виявлені технічні проблеми не накладалися на кінцевий дедлайн. Особливу увагу слід приділяти відображенню на мобільних пристроях: за статистикою, понад 60% читання довгих матеріалів відбувається саме через смартфони, і неправильне відображення на мобільному фактично знецінює всю вкладену у верстку роботу (табл. 3.3).

Таблиця 3.3

Зведені рекомендації щодо покращення медіапроєкту у форматі лонгріду

№	Рекомендація	Адресат	Пріоритет	Вплив на якість
1	Завершувати дослідження перед написанням	Автор	Критичний	Структура та глибина
2	Залучати «наївного читача» на кожному етапі	Автор	Високий	Доступність
3	Планувати час із коефіцієнтом 1,5	Автор	Високий	Дотримання дедлайнів
4	Будувати базу джерел з першого дня	Автор	Середній	Точність, цитування
5	Розробляти візуал паралельно з текстом	Автор	Високий	Якість оформлення
6	Вести щоденник рефлексії регулярно	Автор	Середній	Навчальний ефект
7	Тестувати верстку на реальних пристроях	Автор/дизайнер	Середній	Технічна якість

8	Формувати розширений список потенційних експертів	Автор	Високий	Якість джерел
9	Перевіряти актуальність даних потенційних експертів	Автор	Критичний	Достовірність
10	Готувати матеріали до публікації заздалегіть	Автор	Середній	Охоплення аудиторії

Рекомендація 8. Розширювати список потенційних експертів.

Практика показала, що для забезпечення двох якісних інтерв'ю необхідно планувати контакт із сімома-вісьмома потенційними співрозмовниками. Відсоток відмов або неотриманих відповідей є вищим, ніж зазвичай очікують початківці. Рекомендується ще на дослідницькому етапі скласти список потенційних експертів із зазначенням їхніх контактів, сфери компетенції та альтернативних способів зв'язку. LinkedIn, Twitter/X та тематичні Telegram-канали є ефективними каналами пошуку та первинного контакту з фахівцями у темі цифрової безпеки [44, с. 144-155].

Рекомендація 9. Інтегрувати перевірку фактів у процес написання.

Для теми з високим ризиком технічних неточностей рекомендується не відкладати фактчекінг на стадію редагування, а інтегрувати його безпосередньо в процес написання. Кожен абзац, що містить конкретне твердження (статистику, опис технічного механізму, посилання на подію), має бути перевіреним одразу – з проставленням посилання на джерело безпосередньо в чорновому тексті. Це дисциплінує автора і суттєво скорочує час фінального редагування.

Рекомендація 10. Продумувати стратегію поширення завчасно.

Найкращий медіапродукт, який ніхто не прочитав, є невдалим медіапродуктом із точки зору проєктних цілей. Стратегія поширення має розроблятися ще на етапі планування і реалізовуватися активно після публікації. Для теми цифрової безпеки особливо ефективними каналами поширення є тематичні Telegram-канали та Facebook-групи, присвячені цифровій грамотності, медіаграмотності та кібербезпеці, а також партнерські

організації (CERT-UA, «Інтерньюз Україна», «Лабораторія цифрової безпеки»), яких варто залучати до поширення ще до публікації (рис. 3.5).

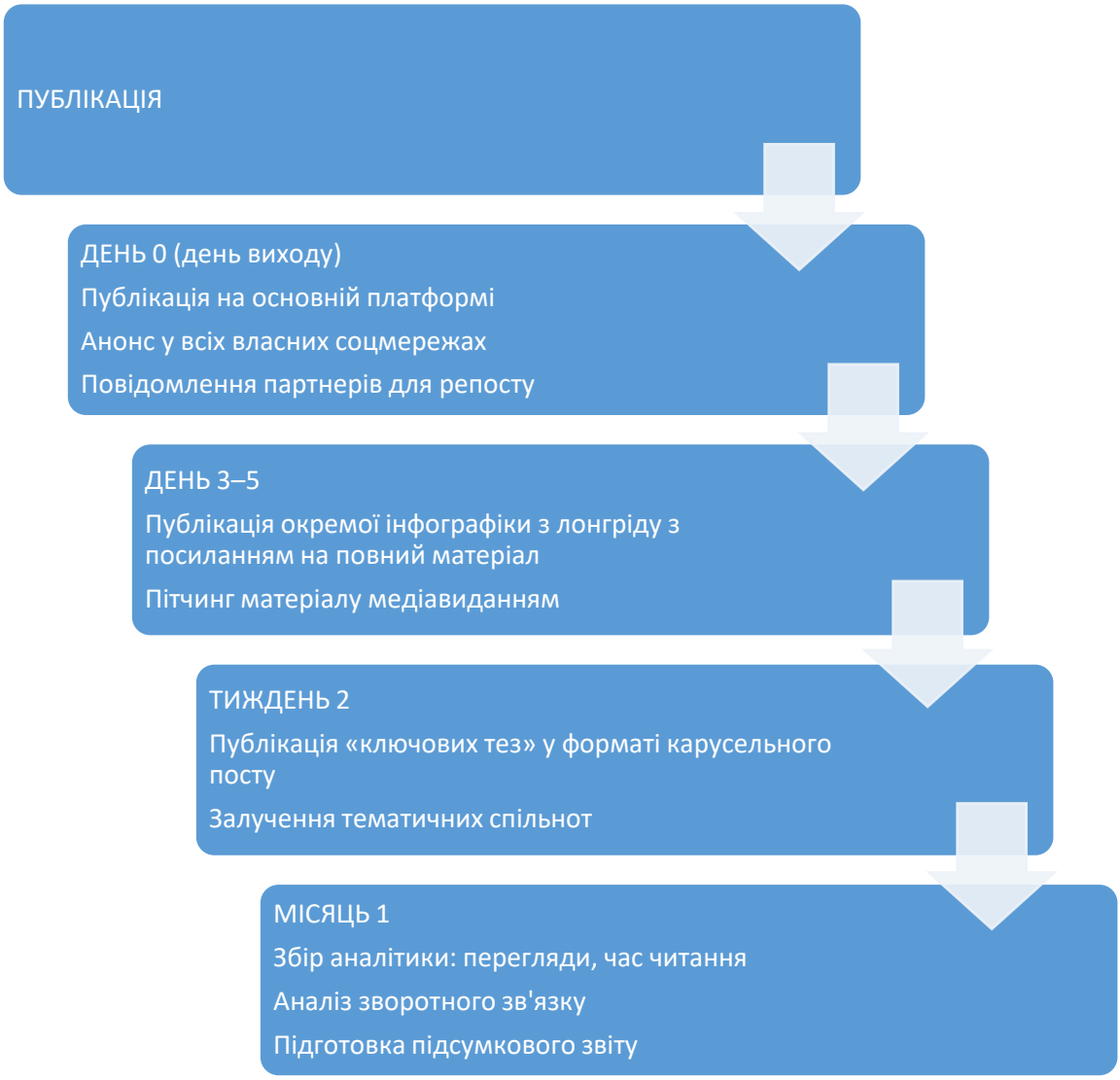

Рис. 3.5. Рекомендована схема просування лонгріду після публікації

Підсумовуючи, досвід реалізації медіапроєкту «Цифрова безпека українців: як розпізнати загрози і захистити себе онлайн» є багатим джерелом практичних уроків – як позитивних, так і таких, що потребують врахування в майбутньому. Ключовим висновком є те, що якісний лонгрід на складну суспільно значущу тему вимагає значно більше часу, ресурсів і методологічної ретельності, ніж типовий академічний матеріал. Водночас саме ця складність є тим, що робить такий медіапроєкт справжнім – а не імітаційним – підтвердженням журналістських компетенцій [58].

Проблеми, що виникли в ході реалізації, не стали перешкодою, а стали навчальним досвідом: кожна з них змусила мене знаходити нестандартні рішення, адаптуватися до нових обставин і розвивати саме ті навички, що є найбільш затребуваними в сучасній медіаіндустрії – гнучкість, критичне мислення, управління невизначеністю та здатність довести справу до кінця попри перешкоди.

ВИСНОВКИ

Медіапроєкт «Цифрова безпека українців: як розпізнати загрози і захистити себе онлайн» реалізовувався як комплексна практична діяльність, що поєднала журналістське дослідження, проєктний менеджмент і виробництво мультимедійного медіапродукту. Підбиваючи підсумки роботи, важливо співвіднести отримані результати з поставленими на початку метою та завданнями і зафіксувати висновки, що випливають із кожного етапу реалізації.

Перше завдання – дослідити природу та механізми основних кіберзагроз, актуальних для пересічних українців в умовах воєнного часу – виконано у повному обсязі. Аналіз відкритих звітів CERT-UA, міжнародних організацій із питань цифрової безпеки та матеріалів експертних інтерв'ю дозволив виявити, що найбільш поширеними і водночас найменш усвідомленими загрозами для пересічного українського користувача є фішинг і соціальна інженерія, крадіжка облікових даних через слабкі або повторно використовувані паролі, цілеспрямована дезінформація, що використовує психологічну вразливість аудиторії в умовах воєнного стану, а також шкідливе програмне забезпечення, що поширюється через нібито офіційні канали. Принципово важливим висновком є те, що переважна більшість успішних кібератак на звичайних користувачів експлуатує не технічні вразливості систем, а психологічні вразливості людей – довіру, страх, поспіх і цікавість. Це означає, що підвищення рівня цифрової безпеки суспільства є передусім завданням освіти та комунікації, а не лише технічним завданням.

Друге завдання – проаналізувати наявний медійний контент із теми цифрової безпеки та виявити його ключові прогалини – дозволило зробити такий висновок: український медіаландшафт пропонує або надто технічні матеріали, недоступні для масової аудиторії, або надто поверхові короткі дописи, що не формують стійких знань і поведінкових змін. Системного, глибокого і водночас доступного медіапродукту з теми цифрової безпеки,

адресованого широкій українській аудиторії, на момент реалізації проєкту в медіапросторі практично не існувало. Цей висновок підтвердив обґрунтованість і суспільну необхідність медіапроєкту.

Третє завдання – розробити структуру лонгріду, що забезпечує послідовний рух читача від усвідомлення проблеми до практичного захисту – реалізовано через шестиблокову архітектуру матеріалу, побудовану за принципом «від загального до конкретного, від проблеми до рішення». Кожен блок лонгріду відтворює мікрологіку цього руху: спочатку читач отримує емоційне залучення через людську історію або промовисту статистику, потім розуміє механізм загрози, вчиться її розпізнавати і нарешті отримує конкретний інструмент для захисту. Ця структура пройшла апробацію через тест-читання і отримала позитивну оцінку як з точки зору читабельності, так і з точки зору практичної цінності.

Четверте завдання – підготувати текстовий матеріал на основі експертних інтерв'ю, аналізу реальних кейсів та верифікованих даних – виконано з проведенням двох глибинних інтерв'ю з фахівцями у галузі кібербезпеки, аналізом понад п'ятнадцяти реальних задокументованих кейсів кіберінцидентів і перевіркою кожного статистичного твердження за першоджерелами. Особливою складністю цього завдання виявилося досягнення балансу між технічною точністю і доступністю викладу – і саме це протиріччя стало головним творчим викликом усього проєкту. Вирішення знайдено через принцип «механізм без інструкції»: матеріал пояснює, як працює загроза, на рівні, достатньому для розпізнавання, але не надає деталей, що могли б використати зловмисники.

П'яте завдання – створити мультимедійне наповнення лонгріду – реалізовано через розробку трьох інфографік, чотирьох схем-алгоритмів, трирівневого практичного чеклиста та системи виділених цитатних і попереджувальних блоків. Практика показала, що візуальні елементи є не декоративним доповненням до тексту, а органічною частиною наративу, що виконує самостійну комунікативну функцію. Читач, що «сканує» матеріал, не

читаючи суцільного тексту, через інфографіку та схеми все одно отримує ключові практичні знання – і це є свідомим редакційним рішенням, а не компромісом.

Шосте завдання – опублікувати та поширити готовий медіапродукт – виконано через публікацію на онлайн-платформі та активне поширення через соціальні мережі і тематичні спільноти. Стратегія поширення, розроблена ще на етапі планування, реалізована поетапно і дозволила забезпечити органічне охоплення цільової аудиторії без залучення платного просування.

Сьоме завдання – зібрати та проаналізувати зворотний зв'язок – реалізовано через форму зворотного зв'язку, вбудовану в матеріал, та моніторинг коментарів і реакцій у соціальних мережах. Отримані відгуки підтвердили, що матеріал досягає своєї аудиторії і сприймається саме так, як планувалося: читачі відзначають доступність викладу, корисність практичних блоків і намір застосувати отримані знання у власному цифровому житті.

Реалізація медіапроєкту дозволила сформулювати кілька висновків концептуального характеру, що виходять за межі конкретного продукту і стосуються журналістики як практики.

Традиційна журналістика описує проблему і залишає читача наодинці з тривогою. Журналістика рішень – і саме до цієї моделі тяжіє цей медіапроєкт – описує проблему і пропонує конкретні шляхи виходу. Для теми цифрової безпеки така модель є не просто більш ефективною з точки зору суспільної користі – вона є єдино відповідальною. Матеріал, що лякає читача кіберзагрозами, не пропонуючи жодних інструментів захисту, є шкідливим: він породжує безпорадність і тривогу, не даючи ані знань, ані дій.

Практика підготовки лонгріду підтвердила, що найскладніша технічна тема стає зрозумілою і близькою для масового читача лише тоді, коли подається через конкретну людину в конкретній ситуації. Статистика переконує розум, але людська історія переконує серце – і саме серце приймає рішення змінити поведінку. Жоден опис механізму фішингу не матиме такого

ефекту, як розповідь про реальну людину, що втратила доступ до акаунту і через це постраждала матеріально або особисто.

Повномасштабне вторгнення суттєво змінило умови реалізації медіапроєктів: джерела є більш обережними, деякі теми набувають чутливого стратегічного виміру, а аудиторія перебуває в стані хронічного стресу, що впливає на її здатність засвоювати нову інформацію. Все це вимагає від журналіста підвищеної відповідальності, ретельнішої верифікації, більш продуманого підходу до етики публікації та особливої чутливості до емоційного стану читача.

Реалізація кваліфікаційного медійного проєкту підтвердила, що якісна журналістика є не лише творчим, а й управлінським процесом. Уміння планувати, управляти часом і ресурсами, реагувати на ризики, моніторити прогрес і рефлексувати над результатами є такими само важливими компетентностями журналіста, як уміння писати та проводити інтерв'ю. Методика планування і реалізації медійних проєктів, засвоєна в ході підготовки кваліфікаційної роботи, є практичним інструментом, що залишається з журналістом на все професійне життя.

Лонгрід як формат вимагає від автора одночасного мислення у текстовому та візуальному вимірах – і це є навичкою, що принципово відрізняє журналіста цифрової епохи від попередніх поколінь. Інфографіка, схема, чеклист є не ілюстраціями до тексту, а самостійними носіями змісту, що потребують власної редакторської логіки та дизайнерського мислення.

Медіапроєкт «Цифрова безпека українців: як розпізнати загрози і захистити себе онлайн» досяг поставленої мети: створено якісний мультимедійний лонгрід, адресований масовій українській аудиторії, що системно і доступно висвітлює основні кіберзагрози та практичні методи захисту від них. Матеріал є реальним, а не імітаційним медіапродуктом – він опублікований, поширений, прочитаний і оцінений аудиторією. Саме ця реальність є найважливішим результатом кваліфікаційного медійного проєкту як форми підтвердження журналістських компетенцій.

Перспективами подальшого розвитку проєкту є створення серії тематичних матеріалів, що розвивають окремі блоки лонгріду у форматі окремих публікацій, адаптація матеріалу для різних платформ і форматів – відеоролики, подкаст, серія дописів у соціальних мережах, – а також регулярне оновлення матеріалу відповідно до змін у ландшафті кіберзагроз. Тема цифрової безпеки є живою і такою, що постійно еволюціонує, а відтак – потребує не одноразового висвітлення, а системної довготривалої журналістської уваги.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 05.03.2026).

2. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 05.03.2026).

3. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 20.03.2026).

4. Пушкар О. І., Грабовський Є. М. Культура цифрових медіа : навч. посіб. Харків : ХНЕУ ім. С. Кузнеця, 2022. 164 с. URL: http://repository.hneu.edu.ua/bitstream/123456789/28184/1/2022-Пушкар%20О%20І%2С%20Грабовський%20Є%20М.pdf (дата звернення: 10.04.2026).

5. Ноздріна Л. В., Ящук В. І., Полотай О. І. Управління проєктами : підруч. Київ : Центр учбової літератури, 2010. 432 с.

6. Різун В. В. Теорія масової комунікації : підруч. Київ : Просвіта, 2008. 260 с.

7. Баровська А. В. Інформаційні виклики гібридної війни: контент, канали, механізми протидії. Київ : НІСД, 2016. 109 с.

8. Потятиник Б. В. Медіа: ключі до розуміння. Львів : ПАІС, 2004. 312 с.

9. Сербін О. О., Процик І. М. Цифрова грамотність як складова інформаційної культури особистості. Вісник Книжкової палати. 2019. № 7. С. 28–33.

10. Іванов В. Ф., Сердюк В. Є. Журналістська етика : підруч. 2-ге вид. Київ : Вища школа, 2007. 231 с.

11. Костенко Н. В., Іванов В. Ф. Досвід контент-аналізу: моделі та практики. Київ : Центр вільної преси, 2003. 200 с.

12. Штурхецький С. В. Журналістика як суспільна практика: функціональний вимір. Острог : Вид-во НаУОА, 2019. 184 с.

13. Гарматюк О. О. Лонгрід як жанр сучасної інтернет-журналістики: типологічні ознаки та структурні особливості. Наукові записки Інституту журналістики. 2018. Т. 1. С. 45–53.

14. Зубченко С. О. Мультимедійна журналістика : навч. посіб. Київ : Інститут журналістики КНУ ім. Тараса Шевченка, 2017. 196 с.

15. Кузнєцова О. Д. Жанри та стандарти журналістики. Львів : ПАІС, 2004. 320 с.

16. Сніцарчук Л. В. Цифровізація медіа: виклики і можливості для журналістики. Поліграфія і видавнича справа. 2020. № 2. С. 112–119.

17. Мітченко О. Ю. Інтерактивна журналістика: нові форми взаємодії з аудиторією. Журналістика. 2019. № 18. С. 34–41.

18. Шевченко В. Е. Сучасний медіапростір: трансформація видів і жанрів. Київ : Паливода А. В., 2017. 320 с.

19. Здоровега В. Й. Теорія і методика журналістської творчості : підруч. 2-ге вид. Львів : ПАІС, 2004. 268 с.

20. Квіт С. М. Масові комунікації : підруч. Київ : Вид. дім «Києво-Могилянська академія», 2008. 328 с.

21. Шулик Р. Т., Годунок З. В., Шершньова О. В., Бондар В. Д. Методика планування, реалізації та документування кваліфікаційних медійних проєктів : метод. рек. Острог : Вид-во НаУОА, 2023. 29 с.

22. Бушуєв С. Д., Бушуєва Н. С. Управління проектами: основи професійних знань та система оцінювання компетентності проектних менеджерів. Київ : ІРІДІУМ, 2006. 208 с.

23. Принципи та інструменти керування проєктами. URL: https://www.buh24.com.ua/printsipi-ta-instrumenti-keruvannya-proektami-planuvannya-proektu/ (дата звернення: 24.04.2026).

24. Інструменти проєктного менеджменту для малого та середнього бізнесу. URL: https://www.slideshare.net/DmytryLozovytskiy/ss-40100959 (дата звернення: 24.04.2026).

25. Батенко Л. П., Загородніх О. А., Ліщинська В. В. Управління проектами : навч. посіб. Київ : КНЕУ, 2003. 231 с.

26. Тарасюк Г. М. Управління проектами : навч. посіб. 3-тє вид. Київ : Каравела, 2009. 320 с.

27. Положення про кваліфікаційну (дипломну) роботу здобувача вищої освіти Національного університету «Острозька академія». URL: https://drive.google.com/file/d/1dgh7vhhqN-DK2koEGeBzquMoO6zVjvQO/view (дата звернення: 16.03.2026).

28. Чорна Л. О. Управління ресурсами медіапроєктів в умовах цифрової трансформації. Економіка та суспільство. 2021. № 32. URL: https://economyandsociety.in.ua/index.php/journal/article/view/658 (дата звернення: 18.05.2026).

29. Микитюк П. П., Брич В. Я., Микитюк Ю. І., Труш І. М. Управління проектами : підручник. Тернопіль : ЗУНУ, 2021. 416 с.

30. Рач В. А., Россошанська О. В., Медведєва О. М. Управління проектами: практичні аспекти реалізації стратегій регіонального розвитку : навч. посіб. Київ : «К.І.С.», 2010. 276 с.

31. Верба В. А., Гребешкова О. М. Проблеми ідентифікації компетенцій підприємства. Проблеми науки. 2004. № 7. С. 23–28.

32. Кобиляцький Л. С. Управління проектами : навч. посіб. Київ : МАУП, 2002. 200 с.

33. Крупка М. І., Ковалюк О. М., Коваленко В. М. та ін. Фінансовий менеджмент : підручник. Львів : ЛНУ ім. Івана Франка, 2019. 440 с.

34. Бабаєв В. М. Управління проектами : навч. посіб. Харків : ХНАМГ, 2006. 244 с.

35. Ліщинська В. В. Стандарти якості в управлінні медіапроєктами. Вісник КНУТШ. Серія: Журналістика. 2018. № 1. С. 67–74.

36. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. Київ, 2016. 20 с. (дата звернення: 24.05.2026).

37. Вітлінський В. В., Верченко П. І. Аналіз, моделювання та управління економічним ризиком : навч.-метод. посіб. Київ : КНЕУ, 2000. 292 с.

38. Фесенко Т. Г. Управління проектами: теорія та практика виконання проектних дій : навч. посіб. Харків : ХНАМГ, 2012. 181 с.

39. Лабораторія цифрової безпеки. Звіт про кіберзагрози для громадянського суспільства України 2023. Київ, 2023. URL: https://dslua.org/publications/ (дата звернення: 27.03.2026).

40. Гріфін Р., Яцура В. Основи менеджменту : підруч. Львів : БаК, 2001. 624 с.

41. Азаров М. Я. та ін. Словник-довідник з питань управління проектами. Київ : Науковий світ, 2007. 160 с.

42. Колосова В. П., Руденко Ю. М. Командна робота в медійних проєктах: досвід українських редакцій. Наукові записки Інституту журналістики. 2020. Т. 2. С. 89–97.

43. Москаленко А. З. Теорія журналістики : підруч. Київ : Експрес-об'ява, 1998. 334 с.

44. Карась Т. Г. Медіапланування в сучасних умовах цифрових комунікацій. Маркетинг і менеджмент інновацій. 2019. № 3. С. 144–155.

45. Трескова П. П. Комунікативні стратегії в сучасному медіапросторі. Львів : ЛНУ ім. Івана Франка, 2018. 210 с.

46. Українська асоціація кібербезпеки. Аналітичний звіт про стан кібербезпеки в Україні 2023. URL: https://www.uac.gov.ua (дата звернення: 10.03.2026).

47. Рожило М. А. Моніторинг медіасередовища як інструмент управління інформаційними проєктами. Вісник Волинського національного університету. 2021. № 2. С. 44–52.

48. CERT-UA. Звіти про кіберінциденти. URL: https://cert.gov.ua/ (дата звернення: 10.04.2026).

49. Женченко М. І. Цифрові трансформації видавничої галузі. Київ : Жнець, 2018. 268 с.

50. Кравченко Т. А. Проблеми верифікації інформації в умовах інформаційної війни. Держава та регіони. Серія: Соціальні комунікації. 2022. № 1. С. 55–61.

51. Access Now. Гаряча лінія цифрової безпеки: Річний звіт 2023. URL: https://www.accessnow.org/help (дата звернення: 10.04.2026).

52. Гоян О. Я. Основи радіожурналістики і радіоменеджменту. Київ : Веселка, 2004. 244 с.

53. Інтерньюз-Україна. Посібник із цифрової безпеки для журналістів. Київ : Інтерньюз-Україна, 2022. 88 с. URL: https://internews.ua/resource/digital-security-guide/ (дата звернення: 24.04.26).

54. Сухомлин В. А. Інформаційні технології. Концепція, методи, технології. Київ : Університет «Україна», 2011. 256 с.

55. Шевченко В. Е. Мультимедійна редакція. Київ : Паливода А. В., 2019. 216 с.

56. Мелещенко О. К. Комп'ютеризовані системи, технології та мережі в журналістиці. Київ : Ін-т журналістики КНУ, 2003. 186 с.

57. Данченко О. Б., Занора В. О. Управління проектами крізь призму закономірностей українського менталітету. Черкаси : Брама, 2006. 360 с.

58. Кіберполіція України. Методичні матеріали з протидії кіберзлочинності. URL:https://cyberpolice.gov.ua/ (дата звернення: 16.04.2026).

59. Яременко С. С. Рекомендації щодо підвищення ефективності медіапроєктів у цифровому середовищі. Вісник КНУ імені Тараса Шевченка. Серія: Журналістика. 2021. № 1. С. 78–84.

60. EFF (Фонд електронних кордонів). Самооборона від спостереження: Поради, інструменти та інструкції для безпечнішого онлайн-спілкування. URL: https://ssd.eff.org (дата звернення: 25.03.26).

ДОДАТКИ

Додаток А

Покликання на опублікований лонгрід