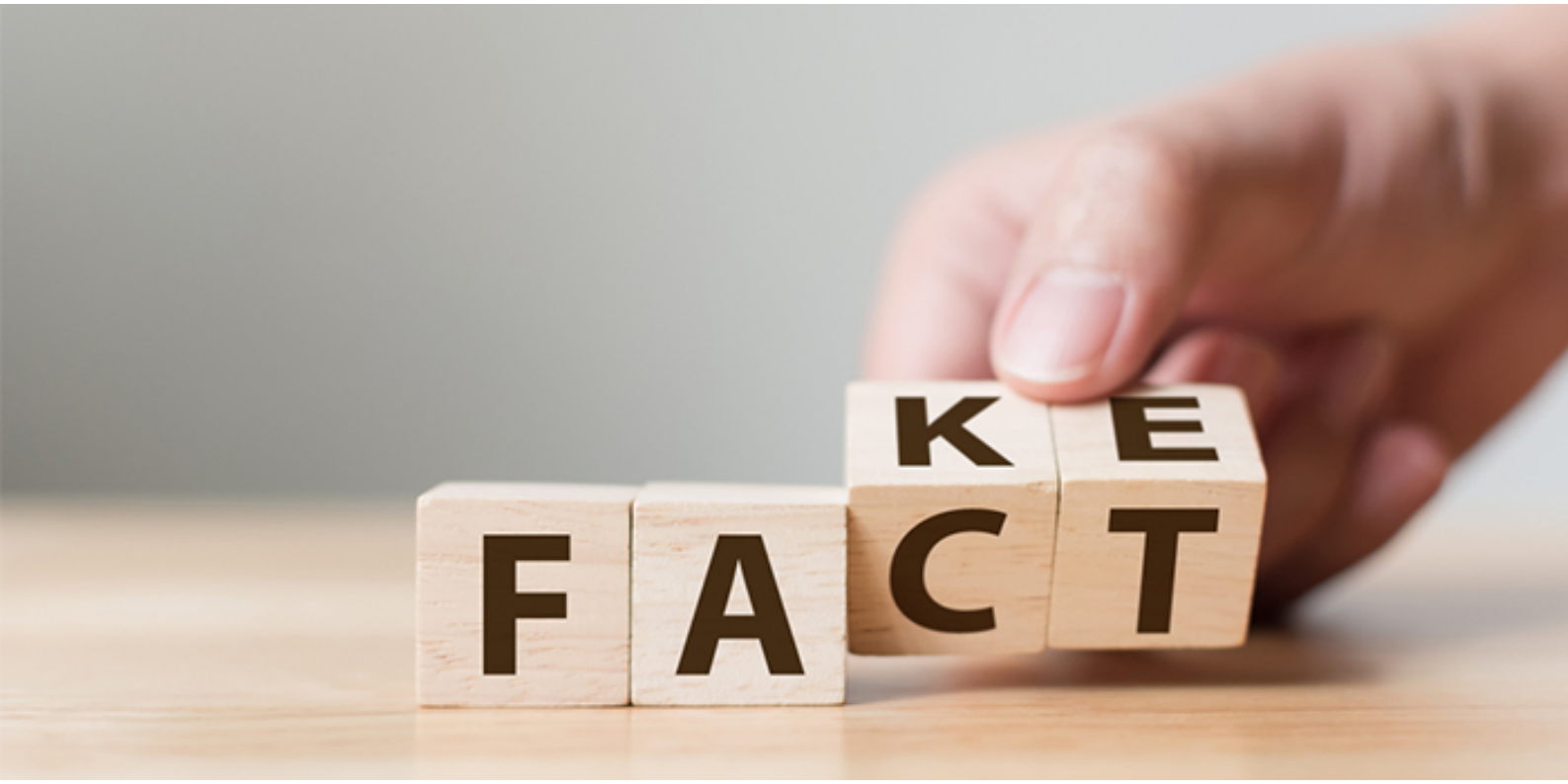
Цифрова безпека
в галузі вищої освіти:

аналітичні матеріали



Дослідження проводиться за підтримки Української асоціації дослідників освіти в рамках Конкурсу малих грантів на великі проєкти членів УАДО.

Термін реалізації проєкту: **01.02.2022-01.04.2022**

УДК 378:004.56
Ц 75

Цифрова безпека в галузі вищої освіти: аналітичні матеріали / Прокоф'єва М.О., Султанова Л.Ю. – Кропивницький: Імекс-ЛТД, 2022. – 38 с.

ISBN978-966-189-641-2

Аналітичні матеріали є результатом виконання проєкту «Fake-free-освіта» за підтримки ГО «Українська асоціація дослідників освіти». Аналітичні матеріали можна використовувати як методичну розробку для здобувачів вищих навчальних закладів в рамках викладання курсів з медіаграмотності, академічної доброчесності та цифрової безпеки. Крім того, укладені «Аналітичні матеріали» сприяють популяризації сучасних досліджень в галузі цифрової безпеки, можуть бути корисними при написанні дипломних або магістерських робіт, стати інтелектуальним підґрунтям для подальших наукових проєктів.

УДК 378:004.56

ISBN 978-966-189-641-2

ЗМІСТ

РОЗДІЛ І.
ЦИФРОВА БЕЗПЕКА
В ГАЛУЗІ ВИЩОЇ ОСВІТИ

Актуальність дослідження

Однією із галузей, яка вносить вагомий вклад не лише у формування суспільної свідомості, але й в економічний розвиток кожної держави, є освіта. Однак, в епоху цифрових технологій, освіту необхідно переосмислити. У дослідженні «Rethinking Education in the Digital Age», проведеному на замовлення Європарламенту у 2020 р., зазначається, що це питання є центральним в сучасній політиці. Адже лише освіта може сформувати кваліфікованих спеціалістів в умовах появи нових професій та трансформацій на ринку праці, а також створити передумови соціальної інтеграції та рівної участі громадян в умовах цифрової демократії (Rethinking Education in the Digital Age, 2020).

Варто зазначити, що освіта є вагомою складовою суспільного життя, безпеки та стабільності країни, які все більше набувають цифрового формату. Інформаційний контент часто є засобом маніпулювання свідомістю, причиною конфліктів та негативних проявів. Питання свідомого споживання інформації, особливо в освіті, критичного аналізу та якості інформації стали стратегічними для розвитку країн на національному та наднаціональному рівнях. Отже, розвиток цифрових технологій стимулює створення цифрової безпеки в галузі вищої освіти. Оскільки сучасна освіта з березня 2020 року функціонує переважно у дистанційному та/або online форматі, то питання цифрової безпеки в галузі вищої освіти посідає пріоритетне місце (Sultanova, L., Milto, L. and Zheludenko, M., 2021). Саме ці фактори зумовили дослідження обраної тематики.

Аналіз досліджень і публікацій з обраної проблеми

У звіті 2019 року Організації економічного співробітництва та розвитку (Organisation for Economic Co-operation and Development) цифровізацію розглядається як один з мегатрендів, що має вплив на майбутнє освіти (Trends Shaping Education, 2019). Однак, як зазначено у проекті Стратегії розвитку вищої освіти в Україні на 2021-2031 роки, освіта наразі відстає від цифровізації. Необхідно докласти більше зусиль, щоб скористатися інструментами та потенціалом нових технологій, одночасно вирішуючи проблеми щодо можливих

зловживань, наприклад, кібервторгнення та проблеми конфіденційності (Стратегія розвитку вищої освіти в Україні на 2021-2031 роки, 2020).

Проблема цифровізації та цифрової безпеки в галузі вищої освіти висвітлена у низці національних та європейських документів. 3 лютого 2021 року у доповіді міністра освіти і науки С. Шкарлета на засіданні Комітету Верховної Ради з питань освіти, науки та інновацій йшлося про те, що впровадження цифрової трансформації освіти і науки є одним з пріоритетних напрямів роботи Міністерства освіти і науки (Звіт Міністерства освіти і науки України з виконання оперативного плану Міністерства освіти і науки України на 2020 рік та основні цілі на 2021 рік, 2020). На необхідності цифровізації освітньої сфери акцентовано увагу в низці нормативно-правових документів. Зокрема, у Законі України «Про освіту» серед ключових компетентностей визначено й інформаційно-комунікаційну (Закон України «Про освіту», 2017). У проекті Концепції Цифрової адженди України – 2020 зазначено, що цифровізація має стати об'єктом фокусного та комплексного державного управління (Проект Концепції Цифрової адженди України – 2020, 2020).

Міністерство освіти і науки України підготувало та пропонує для громадського обговорення проєкт Концепції цифрової трансформації освіти і науки на період до 2026 року, яка представляє комплексне системне стратегічне бачення цифрової трансформації цих сфер та відповідає засадам реалізації органами виконавчої влади принципів державної політики цифрового розвитку, що затверджено постановою Кабінету Міністрів України від 30 січня 2019 р. № 56, а також пріоритетним напрямам та завданням (проєктам) цифрової трансформації на період до 2023 року, схваленим розпорядженням Кабінету Міністрів України від 17 лютого 2021 року № 365-р (Проєкт Концепції цифрової трансформації освіти і науки на період до 2026 року, 2019).

Про потребу у розвитку «електронного навчання і формування цифрової компетентності учасників

освітнього процесу» зазначається й у наказі Міністерства освіти і науки України «Про затвердження Положення про Національну освітню електронну платформу» (Наказ Міністерства освіти і науки України № 523 від 22.05.2018, 2018).

Серед європейських документів варто відмітити Цифровий порядок денний прийнятий Європейською Комісією, який є однією із семи флагманських ініціатив стратегії Європа 2020 (Digital Agenda for Europe, 2022).

Його метою було визначення ключової ролі використання інформаційно-комунікаційних технологій для досягнення Європою своїх амбітних цілей на 2020 рік. Щоб забезпечити справедливе, відкрите та безпечне цифрове середовище, Комісія запропонувала стратегію єдиного цифрового ринку, яка базувалась на трьох стовпах:

- забезпечення кращого доступу споживачів і бізнесу до цифрових товарів і послуг по всій Європі;
- створення належних умов для цифрових мереж і послуг;
- розвиток та посилення потенціалу цифрової економіки.

Окремі аспекти підготовки фахівців в умовах цифровізації суспільства розкрито у працях вітчизняних та зарубіжних науковців. Інформатизація освіти, а також інтеграція інформаційно-комунікаційних технологій в освітній процес представлена у дослідженнях: В. Бикова, К. Власенко, І. Герасименко, А. Гуржій, М. Жалдак, Ю. Запорожченко, С. Семеряков, О. Співаковський, О. Спірін, та ін.

Питання формування загальних компетентностей ІТ-фахівців досліджували: П. Беспалов, В. Биков, В. Вембер, А. Гуржій, О. Елізаров, М. Жалдак, А. Кочарян та ін.

Особливості формування фахових компетентностей ІТ-фахівців, використовуючи хмаро орієнтоване навчальне середовище

досліджували Т. Вакалюк, Г. Дацiв, І. Герасименко, Л. Зубик, В. Круглик, Т. Морозова та ін.

Аналіз досліджень з цифрової безпеки в галузі вищої освіти є підґрунтям для вивчення та розвитку теорії і практики підготовки майбутнього викладача закладу вищої педагогічної освіти до безпечної професійної діяльності у цифровому середовищі (Прокоф'єва, М., Султанова, Л., 2022а).

Мета проекту

Підвищення рівня цифрової обізнаності для посилення якісної складової вищої освіти через вміння розпізнавати фейкові цифрові ресурси.

Цифрова компетентність як основа безпеки

Цифрова безпека базується на цифровій компетентності. Цифрова компетентність є однією з 8 ключових компетенцій для повноцінного життя та діяльності, визначених Європейським Союзом. У 2021 році Міністерством цифрової трансформації України було розроблено Рамку цифрової компетентності для громадян України (Опис Рамки цифрової компетентності для громадян України, 2021). За основу було взято європейську концептуально-еталонну модель цифрових компетентностей для громадян DigComp 2.1: The Digital Competence Framework for Citizens та рекомендації у сфері цифрових компетентностей від європейських та міжнародних інституцій. Враховуючи виклики сьогодення, цей опис Рамки було адаптовано до національних, культурних, освітніх та економічних особливостей України. Наразі ця Рамка містить 4 виміри, 6 сфер, 30 компетентностей та 6 рівнів володіння цифровими компетентностями.

Безпека у цифровому середовищі є однією з шести сфер компетентностей, визначених у першому Вимірі. До цієї сфери віднесено наступні компетентності:

- захист пристроїв та безпечне підключення до мережі Інтернет;
- захист персональних даних та приватності, безпека в Інтернеті;
- захист особистих прав споживача від шахрайства і зловживань;

- захист здоров’я та благополуччя;
- захист навколишнього середовища.

Захист пристроїв та безпечне підключення до мережі Інтернет передбачає наявність умінь захищати пристрої та цифровий контент, розуміння ризиків та загроз у цифровому середовищі; знань про заходи безпеки та захисту, враховуючи при цьому питання надійності й приватності.

Захист персональних даних та безпека в Інтернеті передбачають дотримання таких правил: приватність у цифровому просторі; розуміння того, як користуватися та обмінюватися інформацією, яка дозволяє встановити особу, зі збереженням можливості захистити себе та інших від небезпеки; усвідомлення того, що цифрові служби користуються «Політикою конфіденційності» для інформування про те, як використовуються персональні дані.

Захист особистих прав споживача від шахрайства і зловживань передбачає знання найважливіших правових положень щодо захисту мережевого споживача; вміння виявляти сумнівні інтернет-магазини та порівнювати ціни; застосування заходів захисту прав споживачів.

Захист здоров’я та благополуччя передбачає уміння уникати ризиків і загроз для фізичного та психологічного здоров’я при користуванні цифровими технологіями; уміння захистити себе та інших від можливих небезпек у цифрових середовищах (наприклад, кіберзалякування, булінг, фішинг); знання про цифрові технології для забезпечення соціального благополуччя та соціальної інтеграції.

Захист навколишнього середовища передбачає усвідомлення впливу цифрових технологій та користування ними на навколишнє середовище.

Автори документу виокремлюють три рівня володіння цифровими компетентностями (базовий, середній та високий). Рівні володіння цифровими компетентностями вказують на певний мінімально

необхідний набір знань, умінь і навичок громадян, яким вони повинні володіти для виконання функцій залежно від посади чи поставленої задачі. Реальний рівень володіння певними компетентностями визначається тестуванням громадян за відповідними змістовними навчальними модулями. Такі модулі містять деталізовану інформацію щодо компетентностей згідно з їх дескрипторами.

Предметом нашого дослідження є інформаційна безпека в освіті. Враховуючи масштаби та рівень проблеми, варто звернути особливу увагу на формування медіакомпетентності, критичного мислення, цифрової обізнаності та доброчесності в процесі здобуття вищої освіти. Йдеться про так звану «fake-free-освіту», тобто сучасну цифрову освіту, яка базується на принципах визнання знань найвищою цінністю суспільства, доброчесності та критичного мислення (Прокоф'єва, М., Султанова, Л., 2022b).

Основою такої освіти є вміння розпізнавати фейкові освітні ресурси. Однак, це стає майже неможливим для пересічного користувача Інтернету чи здобувача вищої освіти. Фейкова інформація – це наслідок, а причина – низький рівень ерудиції, критичного мислення та медіакомпетентності. Отже, метою fake-free-освіти є протидія поширенню фейкової інформації на макрорівні та розвитку вмінь критичного відбору інформації на мікрорівні, а також у формуванні світогляду з орієнтацією на цінність достовірної інформації в процесі здобуття вищої освіти.

Нами було розроблено опитувальник з метою визначення рівня медіаграмотності та академічної доброчесності здобувачів вищої освіти та викладачів закладів вищої освіти у сфері цифрової безпеки. Опитування здійснюється в рамках реалізації проєкту «Fake-free-освіта» Громадської організації Українська асоціація дослідників освіти.

Опитувальник складався з трьох розділів, кожен з яких містив 6 запитань.

Розділ I. Інформація про респондента.

Розділ II. Медіаграмотність.

Розділ III. Академічна доброчесність.

В опитуванні взяли участь 361 респондент. З них 59% – студенти закладів вищої освіти, 41% – викладачі. Опитуванням було охоплено респондентів з міста Києва (37,7%), Івано-Франківської області (23,5%), Дніпропетровської області (10,5%), Хмельницької області (7,2%), Запорізької області (6,1%), а також інших (18) областей України (Рисунок 1).

Половину респондентів (51,5%) становить вікова категорія від 18 до 30 років. Переважна більшість респондентів (89,5%) – це жінки.

Більша частина респондентів (66,9%) за своєю спеціальність належить до галузі освіти, зокрема гуманітарних наук.

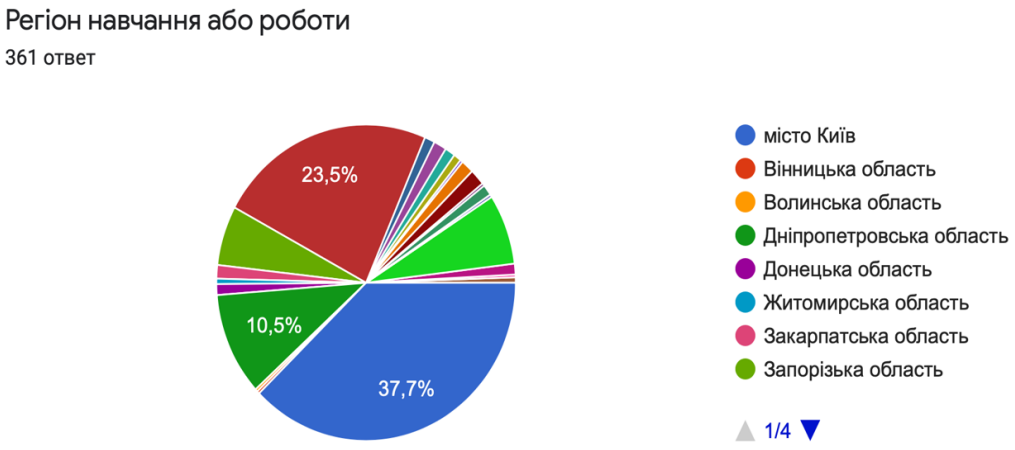


Рис. 1. Регіон навчання або роботи

Із запропонованих запитань найбільш складним виявилось запитання про те, у якій ситуації потрібно використовувати резервні способи підтвердження під час подвійної автентифікації? На це запитання більшість респондентів (біля 60%) дали неправильну відповідь.

Практична більшість респондентів знає, як діяти у ситуації погроз у соціальних мережах (96,7%); який пароль є надійним для власного акаунту (92,8%); що таке фішинг (82%). Однак, значна частина респондентів не розуміє, де і як краще зберігати паролі (51,2%), а також плутається у

поняттях «фішинг», «спамінг» та «тролінг» (біля 27%) (Рисунок 2).

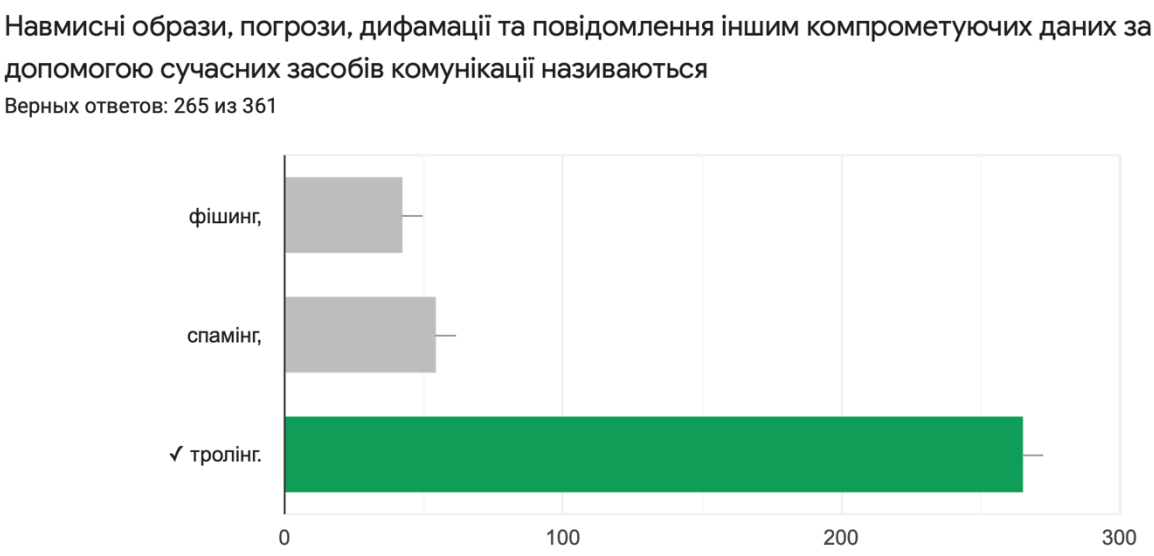


Рис. 2. Диференціація понять «фішинг», «спамінг» та «тролінг»

Щодо питань пов'язаних з академічною доброчесністю, респонденти є досить обізнаними. Переважна більшість респондентів (91,1%) розуміє різницю між авторським правом, академічною доброчесністю і інтелектуальною власністю. А також знає, що надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації не є різновидом академічного плагіату (85,3% правильних відповідей). Практично всі респонденти (95,6%) знають, що дотриманння академічної доброчесності учасниками освітнього процесу передбачає самостійне виконання навчальних завдань поточного та підсумкового контролю.

Дещо складною виявилася диференціація понять «плагіат», «фабрикація» та «фальсифікація». Розрізняють ці поняття лише 57,1% респондентів (Рисунок 3). Також, біля 40% респондентів не знають, які наслідки має порушення академічної доброчесності.

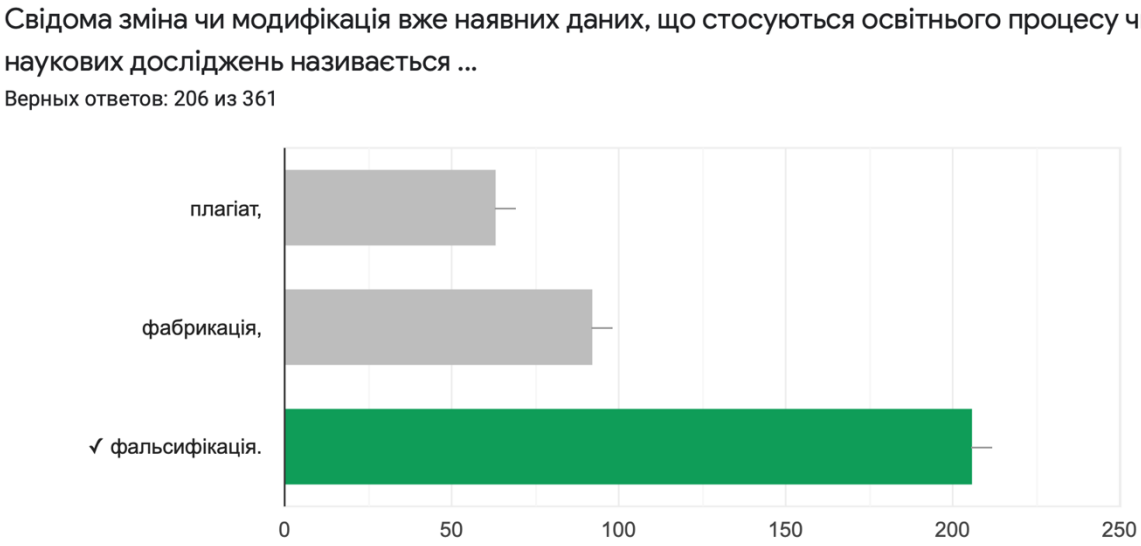


Рис. 3. Диференціація понять «плагіат», «фабрикація» та «фальсифікація»

Проведене опитування дозволило з'ясувати, що викладачі і студенти потребують вдосконалення цифрової компетентності. Наразі освітній процес у закладах вищої освіти більшою мірою зорієнтований на фундаментальну фахову підготовку. Однак сучасні виклики вимагають від здобувачів комплексного підходу та інформаційно-технологічну готовність: знання засобів інформаційних і цифрових технологій та вміння їх використовувати; вміння збирати, оцінювати і використовувати інформацію; адаптивність у здатності пристосовуватися до нових умов праці; усвідомлення самоосвіти і потреба в регулярному підвищенні кваліфікації, тощо). Для цього доречними є посилення цифрової складової освіти (спецкурси з медіаграмотності, фактчекінгу, розвитку критичного мислення, консультації ІТ-фахівців, створення міждисциплінарних курсів на основі цифрових навчальних платформ) тощо. Освітній процес необхідно спланувати таким чином, щоб у результаті здобувачі вищої освіти могли захистити свої пристрої та безпечно підключатися до мережі Інтернет. Ця компетентність на низькому рівні передбачає можливість визначити прості способи захисту своїх пристроїв та цифрового контенту; диференціювати прості ризики та загрози в цифрових середовищах; вибрати прості заходи безпеки та гарантії; визначити

прості способи належного врахування надійності та конфіденційності; обрати прості способи захисту своїх приладів та цифрового контенту; дотримуватися простих заходів безпеки; визначити прості способи належного врахування надійності та конфіденційності.

На середньому рівні – передбачає можливість самостійно вказати чітко визначені і рутинні способи захисту своїх пристроїв та цифрового контенту; диференціювати чітко визначені і рутинні ризики та загрози в цифрових середовищах; обрати чітко визначені і рутинні заходи безпеки та гарантії; вказати чітко визначені і рутинні способи належного врахування надійності та конфіденційності; вирішити чітко визначені і нестандартні проблеми, організувати способи захисту своїх пристроїв та цифрового контенту.

На високому рівні – передбачає можливість, окрім допомоги іншим, застосовувати різні способи захисту своїх пристроїв та цифрового контенту; диференціювати низку ризиків та загроз у цифрових середовищах; застосовувати заходи безпеки та гарантії; використовувати різні способи належного врахування надійності та конфіденційності. А також, у складних контекстах, відповідно до власних потреб та потреб інших людей, можливість вибрати найбільш відповідний захист пристроїв та цифрового контенту; дискримінувати ризики та загрози в цифрових середовищах; вибрати найбільш відповідні заходи безпеки та гарантії; оцінити найбільш оптимальні способи належного врахування надійності та конфіденційності.

Висновки і перспективи подальших досліджень

Отже, розвиток інформаційного суспільства, яке характеризується розвиненими інфраструктурами, високим рівнем інформаційних технологій, наявністю інформаційних ресурсів і можливостей доступу до інформації, зумовлює зміну парадигми освіти. Завдяки інформаційним технологіям уможливлюється створення освітніх спільнот, до яких долучаються як студенти так і викладачі, а також фахівці обраної сфери діяльності. Така співпраця забезпечує доступ до освітніх

матеріалів і необхідних ресурсів. Зважаючи на вищевикладене постає потреба у розробці та впровадженні методик нового покоління у процес підготовки майбутніх фахівців.

Аналіз досліджень з цифрової безпеки в галузі вищої освіти є підґрунтям для вивчення та розвитку теорії і практики підготовки майбутнього викладача закладу вищої педагогічної освіти до безпечної професійної діяльності у цифровому середовищі.

Список використаних джерел

Sultanova L., Milto L. and Zheludenko M. (2021). «The Impact of the Covid-19 Pandemic on the Development of Higher Education», *Acta Paedagogica Vilnensia*, 2021. 46, pp. 132-147. doi: 10.15388/ActPaed.46.2021.9. URL: https://doi.org/10.15388/ActPaed.46.2021.9

Rethinking Education in the Digital Age (2020). EPRS. European Parliamentary Research Service Scientific Foresight Unit (STOA), p. 641.528 – March 2020 URL:https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641528/EPRS_STU(2020)641528(ANN1)_EN.pdf

Trends Shaping Education (2019). OECD (2019), Trends Shaping Education 2019, OECD Publishing, Paris. URL: https://doi.org/10.1787/trends_edu-2019-en

Стратегія розвитку вищої освіти в Україні на 2021-2031 роки (2020). МОН України. URL: https://mon.gov.ua/storage/app/media/rizne/2020/09/25/rozvitku-vishchoi-osviti-v-ukraini-02-10-2020.pdf

Звіт Міністерства освіти і науки України з виконання оперативного плану Міністерства освіти і науки України на 2020 рік та основні цілі на 2021 рік (2020). URL: https://mon.gov.ua/ua/news/ministr-sergij-shkarlet-prezentuvav-zvit-mon-za-2020-rik-i-plani-na-2021-rik

Закон України «Про освіту». URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text

Проект Концепції Цифрової адженди України – 2020 (2020). URL: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf

Проєкт Концепції цифрової трансформації освіти і науки на період до 2026 року (2019). URL: https://mon.gov.ua/ua/news/koncepciya-cifrovoyi-transformaciyi-osviti-i-nauki-mon-zaproshuye-do-gromadskogo-obgovorennya

Наказ Міністерства освіти і науки України № 523 від 22.05.2018 «Про затвердження Положення про Національну освітню електронну платформу» (2018). URL: https://zakon.rada.gov.ua/laws/show/z0702-18#Text

Digital Agenda for Europe (2022). URL: https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe

Опис Рамки цифрової компетентності для громадян України (2021). URL:

https://thedigital.gov.ua/storage/uploads/files/news_post/2021/3/mintsifra-oprilyudnyue-ramku-tsifrovoi-kompetentnosti-dlya-gromadyan/OP%20ЦК.pdf

Прокоф'єва, М., Султанова, Л. (2022a). Аналіз досліджень з цифрової безпеки в галузі вищої освіти. II Всеукраїнська науково-практична конференція «Розвиток педагогічної майстерності майбутнього педагога в умовах освітніх трансформацій», 01 квітня 2022 року, Глухів. С. 260-262.

Прокоф'єва, М., Султанова, Л. (2022b). Fake-free-освіта як інструмент інформаційного захисту. IX International Scientific and Practical Conference «Modern Scientific Research: Achievements, Innovations and Development Prospects» (20-22 February 2022, Berlin), С. 252-258. URL: https://sci-conf.com.ua/ix-mezhdunarodnaya-nauchno-prakticheskaya-konferentsiya-modern-scientific-research-achievements-innovations-and-development-prospects-20-22-fevralya-2022-goda-berlin-germaniya/

РОЗДІЛ ІІ.
ОПИТУВАЛЬНИК FAKE-FREE-ОСВІТА

Опитувальник спрямований на визначення рівня медіаграмотності та академічної доброчесності здобувачів вищої освіти та викладачів закладів вищої освіти у сфері цифрової безпеки.

Опитувальник складається з трьох розділів, кожен з яких містить 6 запитань:

Розділ I. Інформація про респондента.
Розділ II. Медіаграмотність.
Розділ III. Академічна доброчесність.

Даючи відповіді на запитання опитувальника, Ви погоджуєтесь на обробку наданих Вами персональних даних відповідно до Закону України "Про захист персональних даних".

Результати опитування будуть використані виключно в рамках дослідження.

РОЗДІЛ I: Інформація про респондента

Відповідаючи на запитання цього розділу Вам потрібно обрати один з наведених варіантів відповідей або (якщо це передбачено у питанні) надати свою відповідь.

Вік:
до 17 років
18-30 років
31-60 років
60+ років

Стать:
Жінка
Чоловік
Інше

Регіон навчання або роботи:
місто Київ
Вінницька область
Волинська область
Дніпропетровська область
Донецька область
Житомирська область
Закарпатська область
Запорізька область
Івано-Франківська область

Київська область
Кіровоградська область
Луганська область
Львівська область
Миколаївська область
Одеська область
Полтавська область
Рівненська область
Сумська область
Тернопільська область
Харківська область
Херсонська область
Хмельницька область
Черкаська область
Чернівецька область
Чернігівська область
місто Севастополь
АР Крим

Рід діяльності:
Працюю
Навчаюсь

Повна офіційна назва закладу (без абревіатур), в якому Ви працюєте або навчаєтесь:

Галузь знань, за якою здійснюється підготовка здобувачів вищої освіти (якщо Ви викладач) або навчання (якщо Ви студент). Якщо Ваша діяльність передбачає кілька спеціальностей - оберіть основну
01 Освіта
02 Культура і мистецтво
03 Гуманітарні науки
04 Богослов'я
05 Спеціальні поведінкові науки
06 Журналістика
07 Управління адміністрування
08 Право
09 Біологія
10 Природничі науки
11 Математична статистика
12 Інформаційні технології

13 Мехонічна інженерія
14 Електрична інженерія
15 Автоматизація приладободування
16 Хімічна біоінженерія
17 Електроніка телекомунікації
18 Виробництво технології
19 Архітектура будівництво
20 Аграрні науки продовольство
21 Ветеринарна медицина
22 Охорона здоров'я
23 Соціальна робота
24 Сфера обслуговування
25 Воєнні науки, національна безпека, безпека державного кордону
26 Цивільна безпека
27 Транспорт
Не знаю

РОЗДІЛ ІІ. Медіаграмотність

Відповідаючи на запитання цього розділу, Вам потрібно обрати один із наведених варіантів відповідей.

У якій ситуації потрібно використовувати резервні способи підтвердження під час подвійної автентифікації?
Відновити доступ до акаунту, якщо ви придбали телефон.
Відновити доступ до акаунту, якщо ви загубили телефон.
Увійти в свій обліковий запис на надійному пристрої.

У соціальній мережі ви отримали погрози від якогось користувача. Якими будуть ваші дії у відповідь?
Видалити свою сторінку в соціальній мережі.
Запросити друзів написати цьому користувачу погрози.
Подати скаргу на користувача адміністрації мережі.

Який із наведених паролів є надійнішим для власного акаунту.
Olena2022
18091971
B&h28Pz#

Ви зареєструвалися на порталі освітніх послуг. Пароль краще зберегти ...
В блокноті
В голові
Скористатися спеціальною програмою

Найпоширеніша атака на цифровий запис називається ... .
Фішінг
Двофакторна автентифікація
Булінг

Навмисні образи, погрози, дифамації та повідомлення іншим компрометуючих даних за допомогою сучасних засобів комунікації називаються:
Фішинг
Спамінг
Тролінг

РОЗДІЛ ІІІ. Академічна доброчесність

Відповідаючи на запитання цього розділу, Вам потрібно обрати один з наведених варіантів відповідей.

Сукупність етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень називається
Авторське право
Академічна доброчесність
Інтелектуальна власність

Що НЕ є різновидом академічного плагіату?
Дослівне запозичення текстових фрагментів без оформлення їх як цитат з посиланням на джерело.
Використання інформації з джерела без посилання на це джерело.
Надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Дотримання академічної доброчесності здобувачами вищої освіти передбачає:
Самостійне виконання навчальних завдань поточного та підсумкового контролю.
Відсутність посилань на джерела інформації.
Фабрикацію фактів.

Свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень називається ...
Плагіат
Фабрикація
Фальсифікація

За порушення академічної доброчесності здобувачі вищої освіти НЕ можуть бути притягнені до такої академічної відповідальності:
Повторне проходження відповідного освітнього компонента освітньої програми.
Заборона відвідування занять.
Позбавлення академічної стипендії.

На які випадки НЕ поширюється авторське право?
Для захисту абстрактних ідей.
Для захисту зовнішньої форми вираження об’єкта (твір, малюнок, збірник, фотографія тощо).
Для копіювання наукової публікації.

РОЗДІЛ ІІІ.
СЛОВНИК ТЕРМІНІВ З МЕДІАГРАМОТНОСТІ ТА ОНЛАЙН-БЕЗПЕКИ

Академічна доброчесність	Сукупність етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.
Академічна свобода	самостійність і незалежність учасників освітнього процесу під час провадження педагогічної, науково-педагогічної, наукової та/або інноваційної діяльності, що здійснюється на принципах свободи слова, думки і творчості, поширення знань та інформації, вільного оприлюднення і використання результатів наукових досліджень з урахуванням обмежень, установлених законом.
Асиметрія комунікаційних ресурсів	поняття зі сфери міжнародної медіакомунікації, що означає однобічність руху інформаційних потоків, фільтрацію їх утримання в інтересах інформаційних монополій і пов'язаних із ними фінансових груп. Асиметрія комунікаційних ресурсів призводить до обмеження національних інтересів менш розвинених в інформаційному відношенні країн, створює дисбаланс у поширенні новин та інформації в світовому медіапросторі.
Бот	автоматизована програма, яка «пише» замість реальних людей замовні коментарі. Або ж людина, яка заробляє на життя написанням таких коментарів із спеціально створених для цього акаунтів. Найчастіше ботів можна «виловити» на сайтах із відгуками про товари і послуги, або в соціальних мережах.
Булінг	діяння (дії або бездіяльність) учасників освітнього процесу, які полягають у психологічному, фізичному, економічному, сексуальному насильстві, у тому числі із застосуванням засобів електронних комунікацій, що вчиняються стосовно малолітньої чи неповнолітньої особи та (або) такою особою стосовно інших учасників освітнього процесу, внаслідок чого могла бути чи була заподіяна шкода психічному або фізичному здоров'ю потерпілого.

Верифікація	технологія перевірки на справжність чого-небудь з наявністю доказів або аргументів. Це широке поняття, яке використовують у різних галузях життєдіяльності людини, зокрема перевірці підлягають документи, інформація, акаунти, карти, підписи, особи тощо.
Дипфейк	(англ. deepfake) – технологія підробки та імітації відеозображення, що заснована на штучному інтелекті та використовується для виробництва або зміни відеоконтенту. Цілком правдоподібно зображує те, чого насправді не було.
Електронна культура	(е-культура) - це форма культури, яка передбачає стимулювання та мотивування поширення здобутків у сфері культури за допомогою інформаційно-комунікаційних технологій (Головко О.М.).
Ельфи	бот-акаунти, які за допомогою коментарів підтримують автора поста, використовуючи позитивну емоційно-забарвлену лексику. Підтримка позицій відбувається на таких платформах, як форуми, блоги, групи в соціальних мережах, щоденниках.
Зомбіфейк	повідомлення, стилістично створене як справжня новина, але повністю чи частково неправдиве, яке спливає через рік, два, а то й більше, та отримує змінене тлумачення. Швидко поширюється за допомогою активного перепостингу користувачів, що продовжує час існування зомбіфейку.
Інтернет-шлюзи	це програмне забезпечення, призначене організувати передачу трафіку між різними мережами.
Інформаційний булінг	особливий різновид морального насильства, який полягає в цькуванні людини за допомогою інформаційних, часто неправдивих повідомлень негативного, образливого й обурливого змісту з метою її залякати, принизити, знецінити чи перекрутити її позицію, знешкодити як опонента, переводячи дискусію із раціональної площини в емоційну.

Інформаційна бідність	стан інформаційно відсталих країн в світовому інформаційному просторі і одна з характеристик рівня їх соціального розвитку, а також якості життя в цих країнах (Девтеров І.В.).
Інформаційна бульбашка	система алгоритмів соціальних мереж та пошукових систем, запрограмована на те, щоб «підкидати» вам тільки ті думки/людей/пости, які подобаються. З часом може спотворювати об’єктивну картину реальності, створивши віртуальний світ, в якому немає альтернативних чи опозиційних думок.
Інформаційний менталітет	цілісна система соціально-духовних, емоційно-психічних, комунікативних, геополітичних, етнічних та інших способів зв'язку особистості зі своїм народом, яка надає їй можливість зрозуміти багатоаспектність глобальних інформаційних процесів.
Кібербулінг	цькування онлайн. Навмисна та неодноразова ворожа поведінка в онлайні з метою соціальної, психологічної чи фізичної шкоди. Зазвичай термін використовується для визначення жорстокої поведінки з дітьми та підлітками в інтернеті.
Кілоґер	(з англ. keylogger той, що веде журнал клавіш) - це або апаратний пристрій, встановлений на клавіатурі, або шпигунське програмне забезпечення для запису кожного натискання (або послідовності натискань) на клавіатурі. Кілоґґер записує все, що користувач вводить, включаючи електронну пошту, імена користувачів, паролі, номери кредитних карт і/або банківських рахунків, з метою крадіжки інформації.
Комунікація	взаємодія осіб з метою передавання інформації, узгодження дій, спільної діяльності.
Медіагігієна	система знань, що вивчає закономірності впливу інформаційно-комунікаційних технологій на людину та розробляє заходи профілактики негативних ефектів медійного впливу на здоров'я окремої людини, соціальних груп і населення в цілому.

Медіаграмотність — складова медіакультури, яка стосується вміння користуватися інформаційно-комунікативною технікою, виражати себе і спілкуватися за допомогою медіазасобів, успішно здобувати необхідну інформацію, свідомо сприймати і критично тлумачити інформацію, отриману з різних медіа, відділяти реальність від її віртуальної симуляції, тобто розуміти реальність, сконструйовану медіаджерелами, осмислювати владні стосунки, міфи і типи контролю, які вони культивують.

Медіа-імунітет — (від лат. immunitas – звільнення від чогось) – здатність особистості до опору впливу з боку медіа, звільнення від спрямованого на неї небажаного психологічного тиску. Самозахист від навіювання, маніпулювання, психологічного тиску з боку ЗМІ.

Медіа-компетентність — рівень медіакультури, що забезпечує розуміння особистістю соціокультурного, економічного і політичного контексту функціонування медіа, засвідчує її здатність бути носієм і передавачем медіакультурних цінностей, смаків і стандартів, ефективно взаємодіяти з медіапростором, створювати нові елементи медіакультури сучасного суспільства, реалізувати активну громадянську позицію.

Медіакультура — культура сприймання і виробництва соціальними групами та соціумом у цілому сукупності інформаційно-комунікаційних засобів, що функціонують у суспільстві, знакових систем, технологій комунікації, пошуку, збирання, виробництва і передавання інформації. На особистісному рівні медіакультура означає здатність людини ефективно взаємодіяти з мас-медіа, адекватно поводитися в інформаційному середовищі, здійснювати ціннісно-вольову рефлексивну регуляцію інформаційної поведінки.

Медіаобізнаність — складова медіакультури, яка передбачає засвоєння особистістю системи знань про засоби масової комунікації, їх історію та особливості функціонування, користь і шкоду для людини, уміння убезпечити себе від деструктивних

	медіаінформаційних впливів і вільно орієнтуватись у світі інформації.
Медіаосвіта	частина освітнього процесу, спрямована на формування в суспільстві медіакультури, підготовку особистості до безпечної та ефективної взаємодії із сучасною системою мас-медіа, включаючи як традиційні, так і новітні медіа з урахуванням розвитку інформаційно-комунікаційних технологій.
Мем	(англ. meme) – втілення ідеї, символ, який не вимагає роз'яснень, який може мати форму слів, дій, звуків, малюнків, що передають певну ідею й активно поширюються. Меми виникають і функціонують у будь-якій сфері соціальної культури: в економіці, мистецтві, літературі, науці, релігії, маркетингу.
Ментальний вірус	штучно створена впорядкована інформаційна структура, яка через передачу інформаційного повідомлення підкорює увагу та свідомість непідготовленого суб'єкта та робить його вразливим до зовнішнього керування.
Містифікація	це неправдива інформація, яка поширюється в Інтернеті.
Національна рамка кваліфікацій	Системний і структурований за компетентностями опис кваліфікаційних рівнів.
Онлайн-відчуження	(ostracism) - видалення з груп у соціальних мережах, чатів однокласників, які умисно ігнорують повідомлення від конкретної особи. Це також є проявом кібербулінгу.
Освітня кваліфікація	визнана закладом освіти чи іншим уповноваженим суб'єктом освітньої діяльності та засвідчена відповідним документом про освіту сукупність встановлених стандартом освіти та здобутих особою результатів навчання та компетентностей.

Персональні дані	за статтею 2 Закону України «Про захист персональних даних», це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Правники тлумачать «персональні дані» як інформацію про особу, що наявна в її паспорті або в іншому документі, який посвідчує особу, у трудовій книжці, документах про освіту, стан здоров'я тощо.
Першоджерело	особа, що володіє безпосередньою інформацією про конкретну подію/ ситуацію; учасник/учасниця події/ ситуації. Першоджерелом також вважають документ, який містить первинну або основоположну інформацію.
Підміна фактів	маніпулятивний прийом, засіб дезінформації, що полягає в висуванні на перший план в інформаційному повідомленні не фактів, а емоцій, пов'язаних із конкретними подіями та ситуаціями, а також інтерпретацій цих подій і ситуацій.
Плагін	це фрагмент програмного забезпечення, який додає функції до повноцінних програм, наприклад, аудіоплагін, який дозволяє веб-браузеру відтворювати музику.
Професійна кваліфікація	визнана кваліфікаційним центром, суб'єктом освітньої діяльності, іншим уповноваженим суб'єктом та засвідчена відповідним документом стандартизована сукупність здобутих особою результатів навчання та компетентностей, що дають змогу виконувати певний вид роботи або провадити професійну діяльність.
Рерайтинг	переписування чужого тексту своїми словами. Використовується для того, щоб уникнути звинувачень у порушенні авторського права.
Самоплагіат	оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів.

Серфінг в Інтернеті	(web surfing) - це перехід від веб-сторінки до веб-сторінки подібно до перемикання каналів на телебаченні.
Спамінг	масове несакціоноване розсилання електронних повідомлень рекламного або іншого характеру або захаращення електронної поштової адреси безліччю повідомлень.
Фабінг	від англ. phone ≈ телефон та snubbing ≈ зневажливе ставлення. Це психологічний термін, що означає звичку постійно відволікатися на свій телефон під час розмови зі співрозмовником.
Фабрикація	вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях.
Фальсифікація	свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень.
Фішинг	це метод соціальної інженерії, що дозволяє шахрайським шляхом отримувати інформацію, яку потім можна використовувати для доступу до пристроїв або мереж.
Фрейм	структурна одиниця медійного поля, певна система уявлень, збережених у пам'яті (людини / соціуму), стереотипна одиниця (універсум), що спирається на фонові знання реципієнта та не підлягає додатковому тлумаченню. Напр., фрейм «політика», «культура», «мистецтво» та ін.
Хедлайн-ньюз	(англ. Headline news) – екстрені новини, сенсаційне повідомлення. Зазвичай, виходять поза основним часом виходу програми новин, а тому мають позначку «спеціальний випуск».
Хештег	це слово або фраза, яка починається з символу #. За допомогою хештегу легко ідентифікувати повідомлення на певну тему в соціальних мережах, зокрема в Твіттері. Хештеги дозволяють людям легко знаходити і відстежувати цікаві для них теми.

Цифрова ідентичність	(або ідентичність онлайн) – це сукупність інформації, дані, які унікально описують особу, організацію або електронне обладнання, що існує в Інтернеті (імена користувачів і паролі, операції пошуку в Інтернеті, дата народження, соціальне забезпечення та історія покупок).
Цифрова ідеологія	ідеологія, яка базується на пріоритеті цифрових технологій та їх можливостей у всіх сфер життя людини з метою забезпечення соціальної захищеності, а також максимальне сприяння цифрових технологій сталому розвитку економіки держави та досягненню високих економічних та соціальних стандартів життя (Прокоф'єва М.О., Султанова Л.Ю.).
Цифрова нерівність	дистанції у розвитку та використанні комунікаційних технологій між розвинутими країнами та рештою світу, між різними верствами населення всередині країни – багатими і бідними, молоддю та людьми похилого віку, здоровими порівняно з інвалідами тощо. Виникає внаслідок неоднакового технічного, економічного, соціального й ін. розвитку країн чи забезпечення населення.
Цифровий розрив	(цифрова нерівність) – нерівність у доступі до можливостей в економічній, соціальній, культурній, освітній галузях, які існують або поглиблюються в результаті неповного, нерівномірного або недостатнього доступу до комп'ютерних, телекомунікаційних та цифрових технологій.
Цифровізація	одна з визначальних тенденцій розвитку людської цивілізації, яка формує більш інклюзивне суспільство та кращі механізми управління, розширює доступ до охорони здоров'я, освіти та банківської справи, підвищує якість та охоплення державних послуг, розширює спосіб співпраці людей, а також дає змогу скористатися більшим розмаїттям товарів за нижчими цінами.
Цільовий фішинг	це фішинг, спрямований на конкретну особу або компанію. Подібні атаки, як правило, застосовують наступні методи та технології: клонування сторінки

входу в корпоративні інтернет-мережі, використання особистої інформації, зібраної заздалегідь для збільшення ймовірності успіху, та інші.

ADSL	(асиметрична цифрова абонентська лінія) - спосіб доступу до інтернету, який дозволяє обмінюватися більшою кількістю даних порівняно зі стандартом DSL (цифрова абонентська лінія). Перевага технології полягає в різних швидкостях прийому та передачі даних. Для користувача це зручно тому, що зазвичай обсяг інформації, яка отримується з інтернету, набагато вища за ту, що надсилається до нього.
Fake-free-освіта	сучасна цифрова освіта, яка базується на принципах визнання знань найвищою цінністю суспільства, доброчесності та критичного мислення та метою якої є протидія поширенню фейкової інформації, розвитку вмінь критичного відбору інформації, формуванні світогляду з орієнтацією на цінність достовірної інформації в процесі навчання (Султанова Л.Ю., Прокоф'єва М.О.).
URL	(англ. Uniform resource locator) – універсальний локатор (покажчик) ресурсів, адреса Web-сторінки, що визначає документ у мережі Інтернет. В URL входять: ім'я домену, назви файлу та каталогу, мережева адреса машини та метод доступу до файлу.
VPN	(«віртуальна приватна мережа») – це послуга, яка дозволяє мати приватне з'єднання під час використання загальнодоступної мережі. VPN часто використовується для приховування вашого місцезнаходження, надаючи приватний шлях між комп'ютером та вуцйеб-сайтами, які ви відвідуєте в Інтернеті. Це означає, що ваше місцезнаходження не буде видно під час перегляду в Інтернеті.

Список використаних джерел

Адаменко М. Цифровізація. Термінологія. URL: https://oth.nlu.org.ua/?p=5614

Головко О.М. Цифрова культура та інформаційна культура: права людини в епоху цифрових трансформацій. URL: http://ippi.org.ua/sites/default/files/6_13.pdf

Девтеров І.В. Роль і місце кіберкультури в інформаційному суспільстві. URL: https://ela.kpi.ua/bitstream/123456789/34001/1/s_6_Cyberculture.docx

Закон України про освіту. URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text

Концепція впровадження медіаосвіти в Україні. URL: https://ms.detector.media/mediaprosvita/mediaosvita/kontseptsiya_vprovadzhennya_mediaosviti_v_ukraini_nova_redaktsiya/

Медіакультура особистості: соціально-психологічний підхід. URL: https://drive.google.com/file/d/0B0VbC0WlJ54oZWVWb2ZZakg2MDA/view?pref=2&pli=1&resourcekey=0-ONbKerLltf_TMD1LUn8pOQ

Національна рамка кваліфікацій. URL: https://zakon.rada.gov.ua/laws/show/1341-2011-%D0%BF#n12

Словник корисних термінів для користувача. URL: https://software.net.ua/blog/post/slovnik-korisnih-terminiv.html

Словник медіаграмотності. https://www.pro100ua.com/slovnyk-mediahramotnosti/

Словниковий запас. Саморозвиток. URL: https://t.me/zapas_slv

Словник термінів з онлайн-безпеки. URL: https://drive.google.com/file/d/10iCbwK00IdXXOSQCM6PBey5hXPf56APL/view

Словник Media IQ. URL: http://media-iq.tilda.ws/glossary

Фактчекінг і медіаграмотність: словник термінів. URL: https://without-lie.info/laboratory/posibnyky/faktchekinh-i-mediahramotnist-slovnyk-terminiv/

Фішинг та цільовий фішинг: поради по захисту. URL: https://www.imena.ua/blog/phishing-and-target-phishing/

Шевченко Л.І. Медіалінгвістика : словник термінів і понять / Л.І. Шевченко, Д.В. Дергач, Д.Ю. Сизонов / за ред. Л.І. Шевченко. – Вид. 2-ге, випр. і доп. – К. : ВПЦ "Київський університет", 2014. – 380. URL: http://medialing.spbu.ru/upload/files/file_1452013437_9323.pdf

РОЗДІЛ IV.
СПИСОК КОРИСНИХ ПОСИЛАНЬ

Список публікацій авторів проекту

Султанова Л.Ю., Прокоф'єва М.О. Цифрова безпека у галузі вищої освіти // Освіта дорослих: теорія, досвід, перспективи: зб. наук. пр. / [редкол. Л.Б. Лук'янова (голова), Аніщенко О.В. (заступник голови) та ін.]; Ін-т пед. освіти і освіти дорослих імені Івана Зязюна НАПН України. Київ, 2022. Вип. 1 (21).

Прокоф'єва М.О., Султанова Л.Ю. Fake-free-освіта як інструмент інформаційного захисту // The 9 th International scientific and practical conference "Modern scientific research: achievements, innovations and development prospects", February 20-22, MDPC Publishing, Berlin, Germany. 2022. P. 252-257.

Султанова Л.Ю., Прокоф'єва М.О. Аналіз досліджень з цифрової безпеки в галузі вищої освіти // ІІ Всеукраїнська науково-практична конференція «Розвиток педагогічної майстерності майбутнього педагога в умовах освітніх трансформацій», 01 квітня 2022 року, Глухів. С. 260-262.

Прокоф'єва М.О., Султанова Л.Ю. Медіаграмотність як інструмент освоєння соціального та комунікаційного середовища // IV Всеукраїнська науково-практична конференція «Іноземна мова у полікультурному просторі: досвід, перспективи», 19-20 квітня 2022, Кам'янець-Подільський. С. 145-148.

Прокоф'єва М.О., Ярошенко Ю.І. Академічна доброчесність під час дистанційного навчання // Роль іноземних мов у соціокультурному становленні особистості (в умовах війни): збірник наукових праць / за заг. ред. О.В. Ковтун. Київ: НАУ, 2022. С. 127-132.

Перелік курсів підвищення кваліфікації

Султанова Л.Ю. Курс «Інформаційна безпека».
Освітня онлайн-платформа Prometheus.com.ua
https://courses.prometheus.org.ua:18090/cert/61296368c0c144f49d9d023183e9f864

Прокоф'єва М.О. Курс ««Академічна доброчесність: онлайн-курс для викладачів» (60 год.)»
Освітня онлайн-платформа Prometheus.com.ua
https://www.facebook.com/fililogiaNAU/posts/1925565314313089

Прокоф'єва М.О. Курс «Медіаграмотність для освітян» (60 год.)
Освітня онлайн-платформа Prometheus.com.ua
https://www.facebook.com/fililogiaNAU/posts/481565117100297

Список інтернет-посилань на інформацію пов'язану з проектом

Проведення студентського гуртка німецькою мовою. Тема дискусії «Факт чи фейк?»
https://www.facebook.com/fililogiaNAU/posts/470408491549293

Онлайн-опитувальник «Fake-free-освіта»
https://docs.google.com/forms/d/1m50_b4c9qnJ-N8SGVb7rTjSUrYqt2BlB9nGQK7ri-M/edit

Research Gate
https://www.researchgate.net/project/Fake-free-osvita

Telegram
https://t.me/+AGjij_WSy4UxMTNi

Facebook:
https://www.facebook.com/fililogiaNAU/posts/1911201355749485
https://www.facebook.com/fililogiaNAU/posts/470408491549293
https://www.facebook.com/fililogiaNAU/posts/494129419177200

YouTube
https://www.youtube.com/channel/UCamqHuchFGfHwQhrukQW0NQ

Прокоф'єва Марина Олександрівна *– керівник проєкту, кандидат педагогічних наук, доцент, доцент кафедри іноземної філології факультету лінгвістики та соціальних комунікацій Національного авіаційного університету*
ORCID ID 0000-0003-2992-9481
E-mail: maryna.zheludenko@ukr.net

Султанова Лейла Юріївна *– виконавець проєкту, доктор педагогічних наук, професор, завідувач відділу теорії і практики педагогічної освіти Інституту педагогічної освіти і освіти дорослих імені Івана Зязюна НАПН України*
ORCID ID 0000-0002-3324-6926
E-mail: leilasultanova22.07@gmail.com

Прокоф'єва Марина Олександрівна
Султанова Лейла Юріївна

Цифрова безпека в галузі вищої освіти:
аналітичні матеріали

Обл.вид.арк. 1,15.Замовлення № 0000096
Поліграфічно-видавничий центр ТОВ «Імекс-ЛТД»
Свідоцтво про реєстраціюсерія ДК № 196 від 21.09.2000.
25006, м. Кропивницький, вул. В. Панченка, 29
тел./факс (0522) 32-08-32, 32-17-05
E-mail: design@imex.kr.ua