

УДК 37.01/09:510

DOI <https://doi.org/10.32782/1992-5786.2025.101.4>

**М. В. Гончаренко**

здобувач третього освітньо-наукового рівня вищої освіти,  
кафедри освітології та інноваційної педагогіки  
Харківського національного педагогічного університету  
імені Г.С. Сковороди

**Т. М. Собченко**

доктор педагогічних наук, професор,  
професор кафедри освітології та інноваційної педагогіки  
Харківського національного педагогічного університету  
імені Г.С. Сковороди

## ІНФОРМАЦІЙНА І ЦИФРОВА БЕЗПЕКА ПІД ЧАС РЕАЛІЗАЦІЇ НАВЧАЛЬНИХ ПРОЄКТІВ З МАТЕМАТИЧНОЇ ОСВІТНЬОЇ ГАЛУЗІ У БАЗОВІЙ СЕРЕДНІЙ ШКОЛІ З ВИКОРИСТАННЯМ ЦИФРОВИХ ТЕХНОЛОГІЙ

**Актуальність** вивчення проблеми інформаційної і цифрової безпеки під час реалізації навчальних проєктів з математичної освітньої галузі у базовій середній школі з використанням цифрових технологій визначена чинниками: стрімкий розвиток цифрових технологій, доступність цифрових сервісів, трансформації і розвиток штучного інтелекту, організаційна і методична особливості навчальних проєктів. **Мета статті** полягала у розкритті ключових векторів забезпечення інформаційної і цифрової безпеки здобувачів під час реалізації навчальних проєктів з математичної освітньої галузі у базовій середній школі. **Методологія дослідження**: компетентнісний, ризик-орієнтований, комплексний підходи. У ході вивчення і критичного аналізу наявних матеріалів отримано **наступні результати**. Установлено, що активне використання цифрових сервісів і застосунків, у тому числі – із системами штучного інтелекту, зафіксовано результатами аналітичних досліджень на рівні близько 25% (учнями і вчителями). Це обумовлює доцільність широкого інформування цільових аудиторій (учнів базової середньої школи, їхніх батьків і вчителів) про корисні цифрові сервіси, формування гайдів цифрових застосунків, які оптимізують навчальний процес. У статті відмічено, що кількість користувачів цифровими сервісами і застосунками постійно зростає, однак є ризик нецільового використання. Зазначений аспект забезпечення інформаційної і цифрової безпеки передбачає посилення ролі вчителя – гіда у світі розумного використання цифрових технологій. Другий аспект інформаційної і цифрової безпеки визначено через наявні ризики появи залежностей у користувачів цифровими застосунками, втрати контролю над обсягом навчального навантаження, що може зумовити виснаження і психологічного дискомфорту, зниження якості освіти. Автором запропоновано супроводжувати програмами чи карт реалізації навчальних проєктів, з використанням міжпредметних зв'язків. У таких програмах чи картах проєкту за участю учнів визнають способи забезпечення фізичної, психологічної безпеки, маркери емоційного благополуччя учасників проєктної роботи, фіксують алгоритм звернень у випадку будь-якої загрози чи порушенню прав. У цьому аспекті посилюється роль вчителя консультанта, тьютора. Третім аспектом інформаційної і цифрової безпеки під час реалізації навчальних проєктів з математичної освітньої галузі у базовій середній школі з використанням цифрових технологій визначено соціальну спрямованість. Така соціальна спрямованість передбачає, що у структуруванні завдань і процедур реалізації навчальних проєктів учні базової ланки загальної школи набувають досвід конструктивної взаємодії в спільнотах, утворених на цифрових сервісах, реалізації особливих освітніх потреб чи забезпечення інклюзивного супроводу. У цьому аспекті роль вчителя визначається так: координатор навчальних і творчих ініціатив, експерт з дотримання прав дитини, ментор для досягнення навчального прогресу часниками проєкту. Перспективним напрямом подальшого вивчення заявленої проблеми є створення кейсів успішних реалізованих навчальних проєктів, формування відповідних інформаційних хабів.

**Ключові слова**: безпечне освітнє середовище, формування компетентності, навчальний проєкт, дослідницька діяльність, здобувач освіти, базова середня освіта, математична освітня галузь, цифрові технології.

**Постановка проблеми.** Стрімкий розвиток цифрових технологій, загальна доступність сервісів і застосунків, трансформації, обумовлені роз-

витком штучного інтелекту – це та інші чинники актуалізують систематичного оновлення і детального розроблення проблематики інформаційної

і цифрової безпеки під час освітнього процесу. Беручи до уваги той факт, що навчальні проекти передбачають високу самостійність здобувачів базової середньої освіти, самодіяльність на всіх етапах від задуму до презентування результатів, питання інформаційної і цифрової безпеки затребувані для усієї освітянської спільноти.

#### **Аналіз останніх досліджень і публікацій.**

Вивчення матеріалів з означеної теми свідчить про динаміку і теми, і способів її висвітлення в наукових, прикладних виданнях. Актуальні, важливі аспекти створення безпечного інформаційного простору і навчальних комунікацій презентовано у навчальному посібнику авторів С. Доценко, В. Ворожбіт-Горбатюк, Т. Собченко [8]. Прикладний аспект розвитку безпечного інформаційного середовища викладено у посібнику авторів: О. Овчарук, О. Гриценчук, І. Іванюк [13]. У наукових розвідках Т. Собченко, О. Кін, В. Ворожбіт-Горбатюк [14] розкрито актуальні питання створення освітнього середовища в закладах загальної середньої освіти в умовах воєнного стану. Порівняльно-педагогічне дослідження теми представлено у публікації О. Дорош, В. Василенко [4]. Цінні дороговкази задекларовано у рекомендаціях та інструкціях на ресурсі Міністерства освіти і науки України [2; 3], Нової української школи [1; 7], у застосунку «Дія. Освіта» [9]. Доволі чіткі рекомендації щодо створення безпечного освітнього середовища розроблено Державною службою якості освіти спільно із експертами ініціативи «Система забезпечення якості освіти» у рамках проекту «Супровід урядових реформ в Україні» (SURGe) [3].

Разом з тим, динамічний характер понять інформаційної і цифрової безпеки, поява нових технологічних рішень, сервісів, застосунків, виклики, пов'язані із проблемами фізичної і психологічної безпеки учасників освітнього процесу, – усе це актуалізує проведення окремого дослідження.

**Мета статті.** розкрити ключові вектори забезпечення інформаційної і цифрової безпеки здобувачів під час реалізації навчальних проектів з математичної освітньої галузі у базовій середній школі. Метою обумовлено опору в методології дослідження на компетентнісний, ризик-орієнтований, комплексний підходи.

Зокрема, компетентнісний підхід визначає перелік фахових компетентностей у межах предметно-методичної, інформаційно-цифрової, емоційно-етичної, педагогічного партнерства та здоров'язбережувальної компетентностей, визначених у професійному стандарті на групу професій «Вчитель закладу загальної середньої освіти» [10]. Ризик-орієнтований підхід в методології цього дослідження обумовлений стрімкою цифровізацією освітнього процесу, проникненням систем штучного інтелекту у навчальні взаємодії. Він передбачає під час розроблення і реалізації

навчальних проектів ідентифікацію, оцінку і управління ризиками для досягнення мети навчального проекту під час опанування математичної освітньої галузі у базовій школі. Цей підхід сприяє зменшенню негативних впливів цифровізації на суб'єкт-суб'єктні відносини учасників освітнього процесу. Комплексний підхід у межах теми, що досліджується, основну увагу спрямовує на використання навчального проектування під час опанування математичної освітньої галузі на формування у підлітків цілісної картини світу. Це вимагає вдумливого інтегрування математичної з іншими освітніми галузями. Креативне бачення, ідея будь-якого навчального проекту, передусім, має слугувати вирішенню освітніх цілей, передбачених програмних забезпеченням математичної галузі, використання потенціалу математичних наук для осмислення інших галузей знань.

**Виклад основного матеріалу.** Навчальне проектування у цільових і процедурних моментах продукують у модельній навчальній програмі для 5–6 класів «STEM: дослідження та проектування» [6]. З огляду на тему цієї статті розкриємо ключові аспекти забезпечення інформаційної і цифрової безпеки у пропонованій авторами канві навчального проектування.

Наголосимо, що сьогодення розвитку цифрових технологій пріоритезує стрімке поширення систем штучного інтелекту. Водночас, доволі цікаві аналітичні дані презентовано у спеціальному дослідженні «Освіта як інструмент формування особистої стійкості, соціального капіталу країни та культури миру», результати якого представлено на П'ятому саміті перрших леді і дженгельменів, ініційованому О. Зеленською у вересні 2025 р. [10] (рис. 1).

Як бачимо, активне використання учнями і вчителями цифрових сервісів і застосунків із системами штучного інтелекту зафіксовано результатами аналітичних досліджень на рівні близько 25%. Це, на наш погляд, є спонукою для більш широкого інформування цільових аудиторій, зокрема, учителів, учнів базової середньої школи, їхніх батьків, про корисні цифрові сервіси, які угруповано за освітніми галузями. Поінформованість, звісно, передбачає комплексний підхід. У межах методології цього дослідження комплексний підхід передбачає не тільки обізнаність із переліком і ресурсністю цифрових сервісів, застосунків, систем штучного інтелекту у вирішенні завдань математичної освітньої галузі у базовій середній школі, але й алгоритми розумного та відповідального використання таких сервісів і застосунків, узгоджуваності практики їх використання з політиками академічної доброчесності і попередження поширення недостовірної інформації.

Саме такий комплексний підхід використано у побудові навчального посібника видавництва

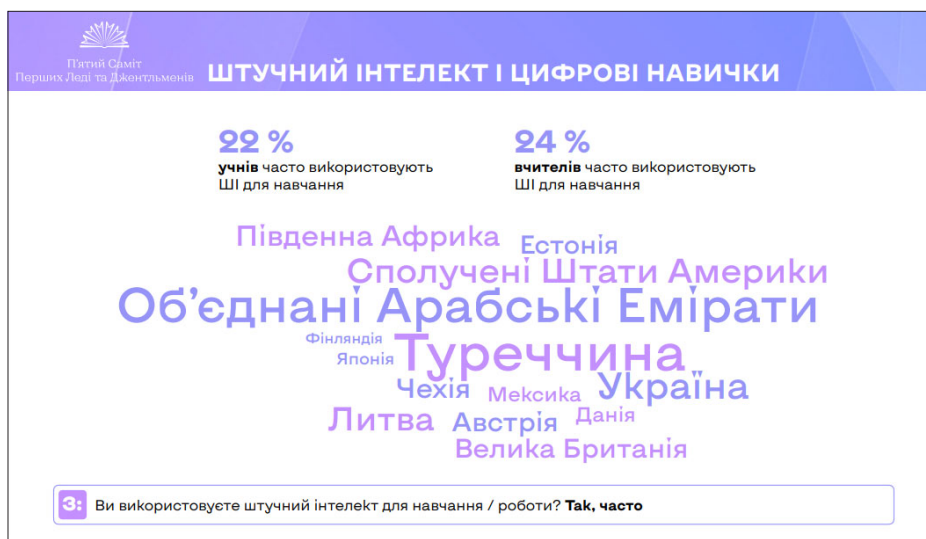


Рис. 1. Скріншот візуалізації результатів спеціального дослідження [10]

«Ранок» «Штучний інтелект асистент сучасного учителя» [15]. Звісно, палітра цифрових застосунків із системами штучного інтелекту постійно розширюється, і відповідно збільшується кількість користувачів. Навіть програми мобільних меседжерів, налаштування Zoom віднедавна містять структуровані елементи із штучним інтелектом. Це допомагає оптимізувати комунікації, роботу з документами, використовувати сервіси для стислого огляду, аналітики, конспектування та інших видів у навчальному проектуванні і дослідницькій роботі.

У цьому ключі на етапах, визначених в структурі навчальних проєктів у названій вище модельній програмі (організаційно-підготовчий, конструкторський, технологічний, заключний) доречно створити і регулярно оновлювати гайди цифрових застосунків, які оптимізують підготовку, планування, перебіг і презентування результатів навчальних проєктів STEM. Варто звернути увагу, що автори модельної програми запропонували визначати конкретну послідовність дослідження і проектування. Ми стоїмо на позиції про те, що цільове використання того чи іншого застосунку, сервісу чи великої мовної моделі передбачає синтезування дослідження і проектування з орієнтацією на формування певної компетентності. Основним критерієм безпечності відповідно до компетентнісного підходу виступає ретельне вивчення умов використання конкретного застосунку чи сервісу, визначення доцільності застосування для вирішення конкретного завдання у переліку навчального проєкту чи теми з модельної програми, міра відповідальності за порушення умов для користувача.

Для реалізації комплексного і компетентнісного підходу учитель у роботі активує роль гіда у світі розумного використання цифрових технологій. Для досягнення успіху в цій ролі важливо забезпе-

чити баланс між технологічним прогресом і апіорністю цінностей дитинства, права дитини на приватність і конфіденційність, адже використання будь-якого сервісу містить відповідні ризики. Крім того, важлива узгоджуваність науковості змісту і доступністю для розуміння складних наукових понять, явищ, процесів з наявним рівнем загальної цифрової грамотності не лише безпосередніх учасників навчального проєкту, а й їхніх батьків. Роль вчителя-гіда під час організації навчальних проєктів поширюється і на взаємодію з батьками учнів, оскільки є потреба постійного підвищення рівня обізнаності про цифрові права, процедури і приписи використання програм «Батьківського контролю». Про ефективні програми і налаштування «Батьківського контролю» предметно висвітлено матеріали у навчальному посібнику «Онлайн-безпека учасників освітнього процесу в умовах дистанційного і змішаного навчання» [8].

Водночас слід звернути увагу, розширення ідей педагогічного партнерства, збільшення практик використання форм і методів самостійної навчально-пізнавальної і дослідницької діяльності учнів у 5–6 класах під час розроблення і реалізації навчальних проєктів вимагає розширення практики реалізації ризик-орієнтованого підходу. Це передбачає завчасне вивчення цифрового сервісу чи застосунку з позицій ризиків і викликів щодо інформаційної і цифрової безпеки. Наприклад, уже понад п'ять років усі учасники освітнього процесу активно використовують Zoom для навчальних комунікацій, хоча на рівні міжнародного комунікативного досвіду цей сервіс не визнано безпечним. Важливо брати до уваги питання, які впливають на реалізацію ризик-орієнтованого підходу під час організації навчального проектування з використанням названого сервісу. Зокрема: політика конфіденційності не виключає поширення аналітичних даних про використання

сервісу для конференцій у соціальній мережі Фейсбук; можливі ризики, пов'язані із наскрізним шифруванням відео та аудіоконференцій; ризик витоку облікових даних користувачів; ризик використання функції відстеження користувачів; ризик порушення приватності зустрічі [12].

На теперішній час відносна більшість користувачів цим сервісом уже навчилася прийомів убезпечення від фішингових посилань, небажаних відвідувачів і поширення аналітики в соцмережі, однак у використанні цього сервісу до цього часу помітна формалізація, звуження до проведення синхронних зустрічей. Тоді як учні інтуїтивний інтерфейс цього сервісу опановують поза цілями освітнього процесу набагато швидше, що часто є причиною порушення дисципліни чи безпекових правил взаємодії нецільовим використанням розширеного функціоналу сервісу (онлайн-дошка, робота спільноти з документами, створення відеоматеріалів, багатокомпонентне структурування, агентські можливості делегування наступних зустрічей, синхронізація з іншими комунікаторами тощо).

Тож учитель гід не просто пропонує певний сервіс чи застосунок, а на рівні партнерства пропонує учням самостійно дослідити сильні сторони і ризики для інформаційної та цифрової безпеки, і на основі їх дати пропозиції для вирішення навчальних завдань на різних етапах навчального проєкту. Таким чином учитель створює простір відповідального, розумного використання конкретного сервісу. Так само функціонально слабко використовується і потенціал комунікування в мобільних меседжерах. Поза увагою лишається їх потенціал для когнітивного і розвитку емпатії, конструктивної рефлексії учасників комунікування. Злободенними питаннями безпечного використання мобільних меседжерів є попередження проникнення електронної комерції (поширення чи створення рекламних дописів, інше), продукування спаму (реакції окремим дописом чи позначкою, вільне комунікування, яке відволікає увагу інших учасників, оскільки меседжер зазвичай пов'язаний з номером мобільного телефону), порушення приватності і вразливості даних акаунту користувачів. Для забезпечення цифрової безпеки на прикладі мобільних меседжерів, доречним видається визначення повноважень адміністратора каналів комунікацій спільноти навчального проєкту, модерування синхронних і асинхронних взаємодій, наприклад, за напрямками «Цифрова етика спілкування», «Доречний таймінг взаємодій у чаті», «Стоп засміченню ефіру!».

Широке проникнення цифрових застосунків в усі етапи навчання, звісно, автономізує учнів ще більше, робить їх менш залежними від учителя, інших здобувачів. Поряд з позитивними момен-

тами, віртуальні математичні тренажери, дистанційне опанування будь-яким когнітивним компонентом навчального проєкту, чат-бот в образі друга актуалізує другий аспект інформаційної і цифрової безпеки: робота з попередження появи залежностей у користувачів цифровими застосунками, втрати контролю над обсягом навчального навантаження, що може зумовити виснаження і психологічний дискомфорт, що врешті-решт приведе до зниження якості освіти. Для цього вбачається доречним розроблення будь-якого навчального проєкту STEM супроводжувати програмами або картами реалізації проєкту. В такій карті можна візуалізувати міжпредметні зв'язки, синтезувати навчальні дії з формування певної компетентності, ціннісних ставлень тощо. Об'єктивно, навчальне проєктування і дослідження це додаткове навантаження і на учнів, і на вчителя. Тож оптимальна інтеграція, чіткі міжпредметні лінії на рівні узгодженого змістк освітніх компонент у базовій середній школі дадуть змогу реалізувати програму STEM без перенавантаження і виснаження. У таких картах корисно за участю учнів визначати межі чи правила фізичної безпеки, психологічного комфорту та емоційного благополуччя учасників не через використання застережень чи обмежень, а формулювань-спонук. Усі учасники навчального проєктування мають чітко відпрацювати алгоритм звернення до відповідальної особи у випадках порушення правил роботи, дисципліни, що можуть посилити безпекову ситуацію. Останній важливий момент вимагає від учителя включеності у ролі консультанта і тьютора.

Третім аспектом інформаційної і цифрової безпеки під час реалізації навчальних проєктів з математичної освітньої галузі у базовій середній школі з використанням цифрових технологій визначимо соціальну спрямованість, коли у структуруванні завдань і процедур реалізації навчальних проєктів учні базової ланки загальної школи набувають досвіду конструктивної взаємодії в спільнотах, реалізації особливих освітніх потреб чи забезпечення інклюзивного супроводу. Цей аспект обумовлений особливістю соціалізації учнів 5-6 класів у реаліях воєнного стану в Україні. Зокрема, вразливість підлітків внаслідок реальних загроз через відкриту збройну агресію проти України, деструкції у родинних відносинах, труднощі змішаного і дистанційного навчання, обумовлені самим форматом (дистанціювання, автономізація, формальний підхід до викладу навчального матеріалу, перевантаженість креативними, дослідницькими завданнями без чіткого визначення реального таймінгу на виконання таких завдань за межами організації синхронних занять не менше 6–7 год. на день). На основі вивчення верифікованих результатів дослідження проблеми захисту дітей у відкритому мережевому

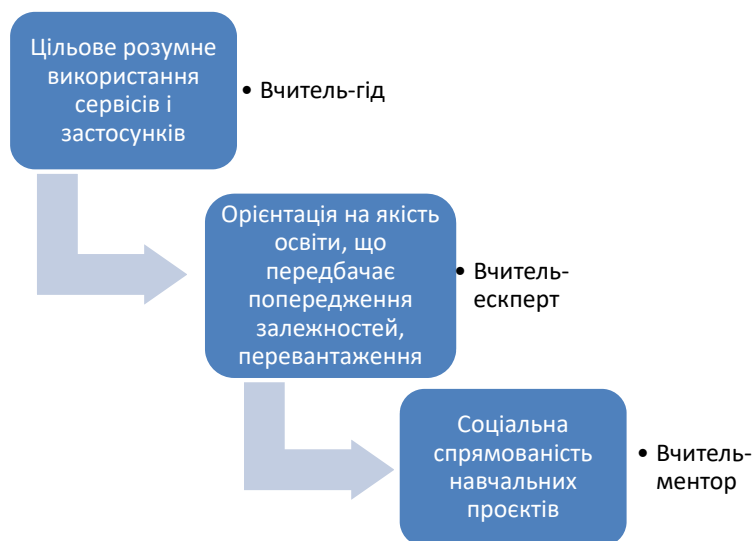


Рис. 2. Ключові аспекти інформаційної і цифрової безпеки під час навчального проєктування з математичної освітньої галузі у 5–6 класах

просторі зазначимо, що «частка дітей, які проводять понад 2 години на день у соціальних мережах: 71%» [5]. Крім того, на наш погляд, доволі системно виділено «п'ять основних факторів стресу в Інтернеті, з якими стикаються діти (думка дітей): Натрапив (-ла) на дезінформацію або «фейкові новини», Натрапив (-ла) на мову ворожнечі, Натрапив (-ла) на матеріали, що пропагують насильство й жорстокість, Зазнав (-ла) цькування в Інтернеті, Натрапив (-ла) на матеріали для дорослих або порнографію» [5]. Такі результати свідчать про неефективність безпекових заходів у викликах інформаційної розпорошеності простору, системного таргетування соціальних мереж. Тож оптимізувати питання інформаційної і цифрової безпеки під час навчального проєктування може допомогти роль вчителя як координатора навчальних і творчих ініціатив, ментора досягнення навчального та особистісного прогресу часниками проєкту. Соціальна значущість ідеї навчального проєкту має стати критеріальною ознакою STEM-освіти. У цьому, на наш погляд, потужний мотиваційний посил, перспектива використання елементів навчального проєктування навіть на етапі актуалізації опорних знань учнів. Нове бачення проблеми через соціальне значення це можливість інтеграції на рівні побудови аналогій (прямих предметних, особистісних рефлексій та емпатії, символічних образних), опанування математичної освітньої галузі в органічній єдності з іншими, і на цій основі сприяння формуванню цілісної картини світу. Розроблення рішень у навчальному проєктуванні, безсумнівно, має включати критеріальні ознаки участі чи охоплення учнів з особливими освітніми потребами, осіб з інклюзією. Хороша практика проживання одного дня чужим життям повертає учнів до усві-

домленої готовності прийняти тих, хто постійно чи періодично потребує допомоги.

**Висновки і пропозиції.** Отже, розгляд проблеми інформаційної і цифрової безпеки під час реалізації навчальних проєктів з математичної освітньої галузі у базовій середній школі з використанням цифрових технологій через призму компетентнісного, ризик-орієнтованого, комплексного підходів дав змогу виділити три важливих (але не вичерпних) аспекти забезпечення безпеки в динаміці (рис. 2).

Перспективним напрямом подальшого вивчення заявленої проблеми є створення кейсів успішних реалізованих навчальних проєктів, формування відповідних інформаційних хабів, які синтезують інформаційні, дорадчі матеріали, світовий і національний досвід навчальних проєктів відповідно до визначених аспектів.

#### Список використаної літератури:

1. Базові правила цифрової безпеки для освітан. URL: <https://ua.hive-mind.community/blog/375,bazovi-pravila-cifrovoyi-bezpeki-dlya-osvityan> (дата звернення: 12.09.2025)
2. Безпека дітей в Інтернеті. URL: <https://mon.gov.ua/osvita-2/pozashkilna-osvita/vikhovna-robotata-zakhist-prav-ditini/bezpeka-ditey-v-interneti> (дата звернення: 12.09.2025)
3. Безпечне освітнє середовище: нові виміри безпеки. 2022. URL: [https://sqe.gov.ua/wp-content/uploads/2022/08/Bezpechne-osvitnie-seredovysche\\_2022\\_SQE-SURGe.pdf](https://sqe.gov.ua/wp-content/uploads/2022/08/Bezpechne-osvitnie-seredovysche_2022_SQE-SURGe.pdf)
4. Дорош О.В., Василенко В.Ю. Цифрова безпека в освіті: досвід зарубіжних країн. *Прикладні аспекти сучасних міждисциплінарних досліджень*. Січень. 2024). С. 22-24. URL: <https://jpasmd.donnu.edu.ua/article/view/14750>

5. Захист дитинства: виміри безпеки для молодого покоління. 10.09.2024. URL: <https://summitflg.org/study/zahyst-dytynstva-vymirybezpeky-dlya-molodogo-pokolinnya/>
6. Модельна навчальна програма «STEM: дослідження та проектування» 5-6 класи. Автори: Ольга Коршунова, Оксана Абрамова, Оксана де Конінг, Інна Дьоміна. 2025. URL: <https://mon.gov.ua/static-objects/mon/sites/1/zagalna%20serednya/Navchalni.prohramy/2025/modelni-navchalni-prohramy-pilotni-haluzi-2025-26-nr-5-6-klas/mnp-stem-1-1.pdf>
7. Обачність. Пильність. Захист. Ввічливість. Сміливість. Посібник із цифрового громадянства й безпеки. Розробники: Google у співробітництві з Альянсом із захисту безпеки користувачів в інтернеті (Internet Keep Safe Coalition, iKeepSafe.org), 2017. 42 с. URL: <https://nus.org.ua/wp-content/uploads/2018/08/PRESS.pdf>
8. Онлайн-безпека учасників освітнього процесу в умовах дистанційного і змішаного навчання навч.-метод. посіб. С. О. Доценко, В. В. Ворожбіт-Горбатюк, Т. М. Собченко. Харків Вид-во «Ранок», 2021. 192 с. URL: <https://surl.li/xhnsoi>
9. Онлайн-безпека. Дія. Освіта. URL: <https://osvita.diia.gov.ua/catalog/topic/online-security> (дата звернення: 12.09.2025)
10. Освіта як інструмент формування особистості, соціального капіталу країни та культури миру. Україна. Спеціальне дослідження. 26.08.2025 р. URL: <https://summitflg.org/study/osvita-yak-instrument-formuvannya-osobistosti-stijkosti-socialnogo-kapitalu-krayini-ta-kulturi-miru/>
11. Про затвердження професійного стандарту «Вчитель закладу загальної середньої освіти». Наказ Міністерства освіти і науки України №1225 від 29.08.2024. URL: <https://mon.gov.ua/npa/pro-zatverdzhennia-profesiinoho-standartu-vchitel-zakladu-zahalnoi-serednoi-osvity>
12. Проблеми безпеки в Zoom: як захистити власну конфіденційність? 2020. URL: <https://surl.li/rukpmo>
13. Розвиток інформаційно-цифрового навчального середовища закладу загальної середньої освіти методичний посібник. О.В.Овчарук, О.О.Гриценчук, І.В.Іванюк, Л.А.Карташова, О.Є.Кравчина, М.П.Лещенко, І.Д.Малицька. Київ: НАПН України. 2022. 223 с. URL: <https://surl.li/awnzsw>
14. Собченко Т.М., Кін О.М., Ворожбіт-Горбатюк В.В. Створення освітнього середовища у закладах освіти в умовах воєнного стану. *Новий колегіум*. Вип.№3 (111). 2023. С. 39–42. DOI:10.30837/nc.2023.3.39
15. Штучний інтелект – асистент сучасного вчителя. Доценко С., Ворожбіт-Горбатюк В., Собченко Т., Корнієнко М. Харків: Ранок, 2025. 176 с.

**Honcharenko M., Sobchenko T. Information and digital security during the implementation of educational projects in the mathematical educational field in basic secondary school using digital technologies**

*The relevance of studying the problem of information and digital security during the implementation of educational projects in the mathematical educational field in a basic secondary school using digital technologies is determined by the following factors: the rapid development of digital technologies, the availability of digital services, the transformation and development of artificial intelligence, the organizational and methodological features of educational projects. The purpose of the article was to reveal the key vectors of ensuring the information and digital security of applicants during the implementation of educational projects in the mathematical educational field in a basic secondary school. Research methodology: competency-based, risk-oriented, comprehensive approaches. In the course of studying and critically analyzing the available materials, the following results were obtained. It was established that the active use of digital services and applications, including those with artificial intelligence systems, was recorded by the results of analytical research at the level of about 25% (by students and teachers). This makes it advisable to widely inform target audiences (secondary school students, their parents and teachers) about useful digital services, to form guides for digital applications that optimize the educational process. The article notes that the number of users of digital services and applications is constantly growing, but there is a risk of inappropriate use. This aspect of ensuring information and digital security involves strengthening the role of the teacher a guide in the world of intelligent use of digital technologies. The second aspect of information and digital security is determined due to the existing risks of users becoming addicted to digital applications, losing control over the volume of educational workload, which can lead to exhaustion and psychological discomfort, and a decrease in the quality of education. The author proposes to accompany the implementation of educational projects with programs or maps using interdisciplinary connections. In such programs or project maps with the participation of students, methods of ensuring physical and psychological safety, markers of emotional well-being of project participants are recognized, and an algorithm of appeals is fixed in the event of any threat or violation of rights. In this aspect, the role of the teacher-consultant, tutor is strengthened. The third aspect of information and digital security during the implementation of educational projects in the mathematical educational field in a basic secondary school using digital technologies is defined as social orientation. Such social orientation*

*assumes that in structuring tasks and procedures for implementing educational projects, students of the basic level of general school gain experience in constructive interaction in communities formed on digital services, implementing special educational needs or providing inclusive support. In this aspect, the role of the teacher is defined as follows: coordinator of educational and creative initiatives, expert in observing the rights of the child, mentor for achieving educational progress by project participants. A promising direction for further study of the stated problem is the creation of cases of successful implemented educational projects and the formation of relevant information hubs.*

**Key words:** *safe educational environment, competence development, educational project, research activity, student, basic secondary education, mathematical educational branch, digital technologies.*

Дата першого надходження рукопису до видання: 24.09.2025

Дата прийнятого до друку рукопису після рецензування: 23.10.2025

Дата публікації: 27.11.2025