

УДК 343.9-053.6:004.056.55:351.746(477)

DOI <https://doi.org/10.32782/1813-3401.2025.1.12>

Н. О. Малько

аспірантка кафедри права, національної безпеки та європейської інтеграції
Навчально-наукового інституту «Інститут державного управління»
Харківського національного університету імені В.Н. Каразіна

ВИКЛИКИ ТА НАПРЯМИ ВДОСКОНАЛЕННЯ ПУБЛІЧНОЇ ПОЛІТИКИ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ НЕПОВНОЛІТНІХ

Досліджено проблему кіберзлочинності серед неповнолітніх як одну з найактуальніших загроз цифрового суспільства. Встановлено, що поширення інформаційних технологій сприяє залученню дітей до протиправної онлайн-діяльності, що вимагає посилення превентивних заходів та вдосконалення механізмів правового регулювання. Виявлено недостатню ефективність чинних державних ініціатив у сфері протидії кіберзлочинам серед дітей, що зумовлено обмеженими можливостями правоохоронних органів, низьким рівнем цифрової грамотності населення та відсутністю комплексного підходу до запобігання таким діям.

Метою дослідження є аналіз актуальних викликів у сфері запобігання кіберзлочинності серед неповнолітніх та розроблення пропозицій щодо вдосконалення публічної політики з урахуванням психологічних, соціальних і правових аспектів поведінки дітей у цифровому середовищі. Для досягнення поставленої мети використано методи системного аналізу для оцінювання тенденцій кіберзлочинності, порівняльно-правовий метод – для визначення розбіжностей між національним і міжнародним законодавством, а також структурно-функціональний підхід – для надання оцінки ефективності заходів державної політики.

Результати дослідження свідчать про необхідність перегляду чинної системи правового регулювання та запровадження більш ефективних механізмів запобігання кіберзлочинності серед неповнолітніх. Доведено, що чинні освітні ініціативи з цифрової безпеки є недостатньо розвиненими, а державна політика потребує комплексного підходу, що включає міжвідомчу взаємодію, залучення приватного сектору та адаптацію найкращих міжнародних практик. Запропоновано створення національної програми з кібербезпеки для дітей, яка передбачатиме посилення правових механізмів захисту, впровадження обов'язкових навчальних курсів із цифрової грамотності та розширення повноважень правоохоронних органів у сфері онлайн-моніторингу загроз.

Перспективи подальших досліджень охоплюють створення моделей оцінювання ризиків кіберзлочинності серед дітей, аналіз ефективності міжнародних програм у сфері цифрової безпеки та розроблення алгоритмів моніторингу і раннього виявлення онлайн-загроз.

Ключові слова: цифрова безпека, правове регулювання, онлайн-ризик, профілактика правопорушень, державне управління, цифрова грамотність, кіберзлочинність неповнолітніх.

Постановка проблеми. Стрімка диджиталізація всіх сфер суспільного життя призводить до появи нових форм злочинної діяльності в кіберпросторі, що становить серйозну загрозу для суспільства. Особливу тривогу викликає втягнення в кіберзлочинну діяльність неповнолітніх, які є однією з найбільш уразливих категорій інтернет-користувачів. Неповнолітні стають як об'єктами, так і суб'єктами таких злочинів, що зумовлює потребу в розробленні дієвих механізмів протидії та профілактики.

Кіберзлочинність неповнолітніх охоплює широкий спектр протиправних дій, включаючи кібербулінг, шахрайство, розповсюдження шкідливого програмного забезпечення, несанкціонований доступ до інформації, розповсюдження дитячої порнографії тощо.

Хоча пряма статистика щодо участі неповнолітніх у кіберзлочинах обмежена, непрямі дані та аналітичні звіти вказують на загрозливі тенденції. Зокрема, збільшення кількості онлайн-ризиків для дітей, як-от кібербулінг, шахрайство та

сексуальна експлуатація, свідчить про зростання потенціалу криміналізації поведінки підлітків у цифровому середовищі.

Актуальність дослідження зумовлена тим, що кіберзлочинність неповнолітніх може мати далекосяжні наслідки як для самих дітей (руйнування здорових соціальних зв'язків, правова відповідальність, перешкоди в майбутній самореалізації), так і для суспільства загалом (формування негативних ціннісних орієнтирів, заповднення шкоди інформаційній безпеці держави, посилення напруження між владою та громадянськістю).

На особливу увагу заслуговує необхідність формування ефективної публічної політики, яка б узгоджувала інтереси держави, суспільства та сім'ї з урахуванням потреб і психологічних особливостей дітей.

Аналіз останніх досліджень і публікацій. Аналіз останніх досліджень демонструє зростання інтересу науковців та міжнародних організацій до проблеми кіберзлочинності, в тому числі до злочинності серед неповнолітніх у кіберсфері. ЮНІСЕФ у звіті «Діти в цифровому світі» (2022) акцентує увагу на ризиках цифрової соціалізації підлітків, зокрема кібербулінгу, сексуальній експлуатації та шкідливому контенті [17].

Рада Європи у своєму дослідженні (2023) підкреслює, що поширення цифрових технологій створює нові загрози, зокрема онлайн-грумінг і розповсюдження матеріалів сексуального характеру за участю дітей [16].

Дослідження українських науковців підкреслюють необхідність гармонізації законодавства з міжнародними стандартами [10].

Дослідження А. С. Діденко (2024) аналізує недоліки державної політики у сфері кібербезпеки та пропонує шляхи її вдосконалення [1]. Авторка зазначає, що українське законодавство значно відстає від міжнародних стандартів: у Кримінальному кодексі України відсутнє визначення грумінгу як злочину, механізми блокування небезпечного контенту не відповідають європейським нормам, а відповідальність онлайн-платформ за безпеку дітей не регламентовано. Це створює серйозні правові прогалини, які ускладнюють боротьбу з кіберзлочинністю серед неповнолітніх.

Українські дослідники значною мірою концентруються на аналізі нормативно-правових аспектів запобігання кіберзлочинності неповнолітніх. Зокрема, Н. А. Сперкач та В. С. Ковбасюк

(2024) обґрунтували необхідність розроблення Стратегії інформаційної безпеки дітей у кіберпросторі, акцентуючи на загрозах кібербулінгу та грумінгу [11].

Міжнародні дослідження демонструють мультидисциплінарний підхід. Проєкт CC Driver Європолу (2022) виявив, що 58% британських підлітків вчиняють кіберзлочини через недостатню усвідомленість правових наслідків [18]. Китайський дослідник Ю. Чжао (Zhao, 2023) наголошує на впливі віртуального середовища на формування девіантної поведінки, пропонує впроваджувати програми кібербезпеки в шкільну освіту [20].

Незважаючи на актуальність проблеми кіберзлочинності серед неповнолітніх, вітчизняна державна політика поки що не відповідає міжнародним стандартам, що ускладнює боротьбу з кіберзагрозами. Важливим завданням є гармонізація законодавства, посилення цифрової грамотності та розширення міжнародного співробітництва. Необхідно здійснити комплексний аналіз державної політики, що враховує нормативне регулювання, міжнародний досвід та інституційні механізми профілактики кіберзлочинності серед дітей і підлітків. Це дозволить адаптувати найкращі практики до українських реалій та створити ефективну систему захисту неповнолітніх у цифровому середовищі.

Виділення не вирішених раніше частин загальної проблеми. Незважаючи на зростання уваги до проблеми кіберзлочинності серед неповнолітніх, залишаються нерозв'язаними питання впливу соціально-психологічних факторів на залучення дітей до протиправної онлайн-діяльності, ефективності превентивних заходів та гармонізації українського законодавства з міжнародними стандартами. Недостатня емпірична база ускладнює оцінювання дієвості освітніх і правоохоронних ініціатив, а також упровадження ефективних механізмів державного контролю й захисту дітей у цифровому середовищі.

Дослідження заповнює ці прогалини шляхом аналізу основних видів кіберзлочинів, до яких залучені неповнолітні, й надання оцінки сучасному стану правового регулювання та ефективності заходів державної політики. Запропоновані рекомендації базуються на міжнародному досвіді та спрямовані на вдосконалення нормативного регулювання, розвиток міжвідомчої співпраці й впровадження сучасних методів превенції, що сприятиме формуванню

ефективної стратегії запобігання кіберзлочинності серед дітей.

Мета статті – аналіз сучасних викликів у сфері запобігання кіберзлочинності неповнолітніх і розроблення пропозицій щодо вдосконалення публічної політики, яка враховуватиме психологічні, соціальні та правові особливості поведінки дітей у цифровому середовищі.

Завдання статті:

1) проаналізувати основні види кіберзлочинів, до яких залучені неповнолітні, та дослідити їх соціальні, психологічні й технологічні передумови;

2) оцінити стан правового регулювання кіберзлочинності неповнолітніх в Україні в порівнянні з міжнародними стандартами та визначити ключові виклики публічної політики в цій сфері;

3) розробити рекомендації щодо вдосконалення заходів запобігання кіберзлочинності серед неповнолітніх, ураховуючи міжнародний досвід, освітні ініціативи та правоохоронні механізми.

Виклад основного матеріалу. Кіберзлочинність є складним явищем, що формується на перетині технологічного розвитку та все більших загроз у цифровому просторі. Відповідно до Конвенції Ради Європи про кіберзлочинність (2001), кіберзлочинами називають «сукупність протиправних дій, вчинених з використанням електронно-обчислювальних систем, мереж електрозв'язку або проти них» [4]. В Україні правове регулювання цієї сфери здійснюється через Закон «Про основні засади забезпечення кібербезпеки України», який визначає основні механізми запобігання, зокрема через протидію несанкціонованому доступу, модифікації або знищенню інформаційних ресурсів [8].

Українське законодавство класифікує кіберзлочини як окрему категорію правопорушень, що охоплюють широкий спектр протиправних дій – від втручання в роботу комп'ютерних систем до фінансових махінацій. Однак правові рамки продовжують еволюціонувати, адаптуючись до нових загроз. Наприклад, кібербулінг, який не має чіткої правової кваліфікації, розглядається через призму психологічного насильства та несанкціонованого доступу до даних, тоді як фішингові атаки підпадають під шахрайство та несанкціоноване втручання в інформаційні системи [13].

Дослідники наголошують, що через динамічний розвиток цифрових технологій коло

кіберзлочинів розширюється, включаючи такі злочини, як онлайн-шахрайство, незаконне поширення контенту, а також маніпуляції з фінансовими активами. Відсутність контролю з боку дорослих, низький рівень цифрової грамотності, недостатня правова обізнаність є ключовими чинниками, що сприяють залученню підлітків до правопорушень у кіберпросторі. Крім того, психологічні аспекти, як-от соціальна ізоляція, емоційна нестабільність чи прагнення статусу в онлайн-середовищі, можуть спричиняти девіантну поведінку і сприяти участі молоді в протиправній діяльності.

У таблиці 1 відображено основні види кіберзлочинів, які можуть бути скоєні неповнолітніми, з відповідними правовими кваліфікаціями згідно з українським законодавством.

Зростання рівня залученості підлітків до кіберзлочинності є наслідком поєднання технологічних, соціальних та психологічних факторів. Як показує аналіз, у багатьох випадках неповнолітні можуть одночасно виступати і жертвами, і виконавцями кіберзлочинів. Особливо небезпечними є кібербулінг та фінансові махінації, оскільки вони часто супроводжуються тривалими психологічними наслідками та правовими ризиками для підлітків.

Відсутність жорсткої відповідальності онлайн-платформ за модерацію контенту, а також недостатня цифрова грамотність серед батьків і педагогів призводять до того, що підлітки залишаються вразливими до негативного впливу кіберпростору. Це свідчить про необхідність удосконалення законодавчих механізмів захисту, а також про важливість впровадження комплексних освітніх програм, спрямованих на підвищення обізнаності щодо кіберзлочинності та її наслідків.

Соціальна ізоляція, булінг, проблеми в сім'ї або брак підтримки змушують підлітків шукати прихисток у віртуальному середовищі. Анонімність інтернету дозволяє експериментувати із соціальними ролями, знижуючи страх покарання. Це збільшує ризик потрапляння в деструктивні онлайн-спільноти, що пропагують злочинну діяльність. Відсутність емоційного контролю та бажання привернути увагу також можуть підштовхнути до правопорушень.

Кіберзлочинність серед неповнолітніх в Україні протягом 2020–2024 років демонструвала тривожну тенденцію до зростання.

Дослідження, проведене UNICEF у 2020 році, показало, що 64% українських дітей стикалися

Таблиця 1

Основні види кіберзлочинів та їх правове регулювання в Україні

Види кіберзлочинів	Опис порушення	Правове регулювання
Несанкціоноване втручання в роботу комп'ютерних систем	Використання шкідливого програмного забезпечення, злом баз даних, отримання доступу до конфіденційної інформації без дозволу	Закон «Про основні засади забезпечення кібербезпеки України»; кримінальне правопорушення згідно із законодавством
Кібербулінг	Переслідування, цькування, поширення компромату в онлайн-просторі	Кваліфікується як психологічне насильство та несанкціоноване використання персональних даних
Фінансові кіберзлочини	Шахрайство в інтернеті, використання фішингових схем для отримання банківських даних, незаконні фінансові операції	Відноситься до злочинів, пов'язаних із шахрайством, підробленням фінансових документів та незаконним доступом до платіжних систем
Незаконне поширення контенту	Поширення шкідливого програмного забезпечення, заборонених матеріалів, незаконного відеоконтенту, порнографії	Включає правопорушення, пов'язані з порушенням прав інтелектуальної власності та незаконним контентом
Кібершпигунство	Збір або викрадення конфіденційної інформації, що містить державну чи комерційну таємницю	Розглядається в контексті злочинів, спрямованих на порушення інформаційної безпеки
Використання комп'ютерних мереж для незаконного обігу наркотичних речовин	Поширення наркотичних речовин через соціальні мережі, месенджери або даркнет	Відноситься до злочинів, що порушують закони щодо обігу заборонених речовин
Порушення конфіденційності особистого листування і телефонних розмов	Несанкціоноване отримання та розголошення приватних повідомлень, електронної пошти	Розглядається як порушення права на конфіденційність та інформаційну безпеку

Джерело: сформовано автором на підставі [3; 8; 13]

з кібернасильством, включаючи погрози, приниження та шантаж [9]. Згідно з іншими даними, 23% підлітків стали жертвами кібербулінгу, що на 9% більше, ніж у попередні роки.

Треба зазначити, що хоч кібербулінг не завжди кваліфікується як кримінальний злочин, його ескалація часто стає передумовою для більш серйозних правопорушень, зокрема шахрайства або розповсюдження незаконного контенту. Кривдниками в цьому випадку переважно є саме однолітки, тобто неповнолітні.

Психологічні фактори впливають як на жертв, так і на агресорів. Дослідження показують, що підлітки, які займаються кібербулінгом, нерідко самі є жертвами насильства в сім'ї або відчувають емоційну нестабільність. Використання онлайн-цькування може бути способом компенсувати відчуття безсилля, отримати статус або привернути увагу однолітків. Особливо непокоїть, що третина випадків кібербулінгу пов'язана зі шкільними конфліктами, а майже половина – з гендерною дискримінацією, що свідчить про необхідність посилення освітніх програм із цифрової грамотності та етики онлайн-спілкування [7].

Незаконний контент, що поширюється підлітками в інтернеті, також є серйозною проблемою. Це можуть бути порнографічні матеріали, що містять зображення неповнолітніх, контент, що

пропагує насильство, тероризм або екстремізм, заклики до участі в небезпечних інтернет-челенджах, що загрожують життю та здоров'ю дітей, продаж наркотичних речовин через месенджери та даркнет.

У 2021 році кіберполіція затримала двох неповнолітніх, які керували так званими «групами смерті» в соціальних мережах [5]. Ці групи займалися психологічним маніпулюванням і спонуканням до самопошкодження.

Часто підлітки не усвідомлюють серйозність таких дій і сприймають це як гру або спосіб самовираження. Проте відповідно до статті 301 Кримінального кодексу України, поширення забороненого контенту карається позбавленням волі на строк від 3 до 10 років [13].

Інтернет створює умови для фінансових махінацій, в яких підлітки можуть бути як жертвами, так і співучасниками. Фішинг, підроблення банківських даних, шахрайські онлайн-продажі та мультиакаунтинг набирають обертів серед неповнолітніх. Підлітки часто не розуміють наслідки і можуть стати «дропами» – посередниками в переведенні коштів для злочинних схем.

Психологічні механізми впливу включають бажання швидкого заробітку, потребу у визнанні та статусі, а також недостатнє критичне мислення. Участь у фінансових махінаціях може

призвести до блокування банківських рахунків та кримінальної відповідальності. Судова практика показує, що 62% засуджених неповнолітніх були причетні до фінансових махінацій, що свідчить про поширеність цієї проблеми.

Зростання проявів кіберзлочинності неповнолітніх можна також пояснити впливом воєнного стану: соціологічні дослідження вказують на кореляцію між війною, що триває, і зростанням кіберзлочинності серед молоді. Неповнолітні, які перебувають у зоні бойових дій або постраждали від міграції, частіше залучаються до кібератак, зокрема до поширення дезінформації та шпигунства [12].

Несформована критичність мислення та недосконала правова обізнаність підлітків сприяють виникненню ризиків вчинення або потрапляння в ситуації, пов'язані з кіберзлочинами. Легкість доступу до інструментів кіберзлочинності (наприклад, вірусів або фішингових ботів) також робить їх привабливими для підлітків з обмеженими можливостями легального заробітку.

Кіберзлочини мають складний характер – підлітки часто одночасно є і жертвами, і виконавцями. Низький рівень цифрової грамотності та правової обізнаності робить молодь уразливою до маніпуляцій у цифровому середовищі. Це вимагає комплексного підходу, що включає посилення законодавчої бази, впровадження профілактичних освітніх програм та міжнародну співпрацю у сфері кібербезпеки [2].

Ефективна державна політика та профілактичні програми відіграють ключову роль у запобіганні кіберзлочинності серед неповнолітніх. В Україні реалізовано низку стратегічних ініціатив, серед яких – Національна стратегія захисту дітей у цифровому середовищі (2021), що передбачає цифрову освіту, розвиток законодавства та створення безпечних онлайн-просторів [6]. Проте її реалізація відбувається повільно. Відсутність координації між державними органами спричиняє дублювання заходів та низьку ефективність ініціатив. Обов'язкове включення теми кібербезпеки в шкільні програми досі перебуває на стадії пілотних проєктів, а превентивні заходи обмежуються інформаційними кампаніями. Крім того, бракує механізмів оцінювання ефективності цієї стратегії, що ускладнює розуміння її реального впливу на запобігання кіберзлочинності неповнолітніх.

Публічна політика у сфері запобігання кіберзлочинності неповнолітніх стикається

з низкою викликів, що значною мірою ускладнюють ефективність превентивних заходів. З одного боку, стрімкий розвиток цифрових технологій створює нові загрози, до яких законодавча база та механізми державного реагування не завжди встигають адаптуватися. З іншого боку, низька обізнаність як дорослих, так і самих дітей щодо потенційних кіберризиків сприяє поширенню правопорушень у цифровому просторі.

Ключові виклики публічної політики щодо запобігання кіберзлочинності серед неповнолітніх узагальнено в таблиці 2.

З огляду на поточну ситуацію в Україні особливу увагу слід приділити захисту дітей від дезінформації та кібератак, пов'язаних із воєнними подіями. Це може включати розроблення спеціальних програм для виявлення та протидії ворожій пропаганді, спрямованій на дітей та підлітків.

Якщо розглянути міжнародний досвід публічної політики у сфері запобігання кіберзлочинності неповнолітніх, то він демонструє комплексний підхід до розв'язання цієї проблеми. Європейський Союз впровадив програму «Better Internet for Kids» (BIK+), яка спрямована на створення безпечного та сприятливого онлайн-середовища для дітей та молоді. Ця стратегія, прийнята у 2022 році, базується на трьох основних принципах: гарантування безпечного онлайн-досвіду, цифрове розширення можливостей та активна участь дітей у цифровому середовищі. BIK+ передбачає співпрацю між державними органами, освітніми установами, IT-індустрією та громадянським суспільством для досягнення поставлених цілей [19].

Велика Британія пішла шляхом посилення відповідальності технологічних компаній за безпеку дітей в інтернеті. Закон про онлайн-безпеку (Online Safety Act) передбачає кримінальну відповідальність для керівників IT-компаній, які свідомо ігнорують вимоги щодо захисту дітей від шкідливого контенту. Це створює потужний стимул для платформ активно боротися із загрозами для неповнолітніх користувачів [14].

Адаптація цих міжнародних практик в Україні може відбуватися через розширення державних програм цифрової безпеки. Зокрема, можливе створення національної стратегії, подібної до BIK+, яка б об'єднала зусилля різних секторів суспільства для захисту дітей онлайн. Важливим кроком може стати посилення відповідальності онлайн-платформ за безпеку неповнолітніх користувачів, ураховуючи досвід Великої Британії.

Таблиця 2

Основні виклики публічної політики у сфері запобігання кіберзлочинності неповнолітніх

Виклик	Опис проблеми	Наслідки для системи запобігання кіберзлочинності
Швидкі темпи розвитку технологій	Нові цифрові платформи та комунікаційні технології з'являються швидше, ніж встигає реагувати законодавство. Діти активно використовують анонімні месенджери, VPN-сервіси й темний веб, що ускладнює моніторинг їх діяльності	Неефективність застарілих механізмів контролю; відсутність правових норм для регулювання новітніх технологій
Недосконалість законодавства	Відсутність спеціальних норм щодо запобігання залученню неповнолітніх до кіберзлочинної діяльності. Недостатня відповідальність онлайн-платформ за безпеку дітей, відсутність механізмів блокування незаконного контенту	Онлайн-ресурси, які містять небезпечний контент, не підлягають швидкому видаленню, а цифрові шахраї можуть залишатися безкарними
Недостатня координація між суб'єктами профілактики	Нацполіція, Держспецзв'язку, МОН та інші органи працюють у розрізнених напрямках, що призводить до дублювання заходів і низької ефективності профілактичних програм	Відсутність єдиної державної стратегії; розпорошення ресурсів; недостатня співпраця з міжнародними організаціями
Низький рівень цифрової грамотності дорослих	Батьки та вчителі не мають достатніх знань про інтернет-загрози, методи захисту та цифрові ризики, з якими зіштовхуються діти	Неспроможність вчасно виявляти підозрілу поведінку дитини онлайн; недостатній рівень контролю над діяльністю неповнолітніх у цифровому просторі
Низький рівень цифрової грамотності дорослих	Батьки та вчителі не мають достатніх знань про інтернет-загрози, методи захисту та цифрові ризики, з якими стикаються діти	Неспроможність вчасно виявляти підозрілу поведінку дитини онлайн; недостатній рівень контролю над діяльністю неповнолітніх у цифровому просторі

Джерело: власна розробка автора

Вважаємо за доцільне посилити міжнародне співробітництво у сфері запобігання кіберзлочинності, у тому числі з боку неповнолітніх. Україна має активніше співпрацювати з такими міжнародними організаціями, як Europol, UNICEF та ITU, а також переймати досвід країн ЄС, США та Канади щодо технологічних рішень для моніторингу цифрових загроз. Це може включати спільні освітні проекти, фінансування від міжнародних фондів та імплементацію кращих практик у вітчизняну систему захисту дітей онлайн.

З огляду на наявні виклики необхідно вдосконалити законодавство у сфері запобігання кіберзлочинності шляхом внесення змін до Кримінального кодексу України, Кримінального процесуального кодексу України, Закону України «Про захист персональних даних» та інших нормативно-правових актів з метою посилення відповідальності за кіберзлочини, скоєні неповнолітніми або стосовно них. Водночас доцільно розглянути питання створення медіаційних центрів для розв'язання проблеми правопорушень без криміналізації.

Необхідне посилення координації між суб'єктами, що здійснюють попередження кіберзлочинності, через створення міжвідомчої робочої групи з питань попередження кіберзлочинності

неповнолітніх за участю представників правоохоронних органів, органів освіти, соціальних служб, організацій громадянського суспільства та інших зацікавлених сторін, розроблення та впровадження єдиних стандартів та протоколів взаємодії між цими суб'єктами.

Розвиток державно-приватного партнерства у сфері запобігання кіберзлочинності неповнолітніх та кіберзахисту є ще одним перспективним напрямом. Співпраця між урядом, освітніми установами та технологічними компаніями може сприяти створенню ефективних освітніх програм та інструментів для підвищення цифрової грамотності дітей та їхніх батьків. Прикладом такої співпраці може слугувати канадська ініціатива «Be Web Aware» [15]. Ця ініціатива, розроблена Media Awareness Network у співпраці з приватним сектором, надає батькам актуальну інформацію про онлайн-активність дітей та поради щодо забезпечення їх безпеки в цифровому просторі.

Актуальною є підготовка та підвищення кваліфікації фахівців з питань попередження кіберзлочинності неповнолітніх – педагогів, працівників правоохоронних органів, служб у справах дітей, соціальних служб тощо, також необхідна організація просвітницьких кампаній, інформаційних заходів для батьків і місцевих

громад, що дозволить підвищити рівень знань про кіберризик та правомірні способи реагування на них.

Висновки з дослідження і перспективи подальших досліджень. Аналіз наукових джерел свідчить про наявність активної дослідницької діяльності в цій галузі, проте складність проблеми вимагає комплексного підходу з боку держави, освітніх установ, громадських організацій та сім'ї. Для зменшення ризиків учинення дітьми кіберзлочинів та їх потрапляння в криміногенне середовище необхідна цілісна та системна публічна політика, орієнтована на формування безпечного цифрового простору і захист прав дітей.

Порівняння міжнародного досвіду та українських реалій вказує на суттєві відмінності. У країнах ЄС та США активно впроваджуються державні програми цифрової грамотності, що охоплюють дітей, батьків і вчителів, тоді як в Україні подібні ініціативи залишаються необов'язковими. Крім того, міжнародний досвід підтверджує ефективність державно-приватного партнерства у сфері кібербезпеки, що дозволяє державним органам співпрацювати з технологічними компаніями для моніторингу цифрових загроз та модерації контенту. В Україні ця взаємодія залишається слабкою, що ускладнює боротьбу з грумінгом і кібербулінгом. Також українське законодавство потребує оновлення відповідно до міжнародних стандартів, оскільки чинні нормативно-правові акти не забезпечують належного попередження кіберзлочинності неповнолітніх.

Таким чином, подолання кіберзлочинності неповнолітніх потребує комплексного підходу: вдосконалення нормативно-правової бази, розширення програм цифрової грамотності та створення ефективних механізмів взаємодії держави, освітнього сектору та приватних компаній.

Оскільки проблема кіберзлочинності серед дітей є багатовимірною та динамічною, подальші дослідження мають бути спрямовані на вдосконалення механізмів захисту неповнолітніх у цифровому просторі та розроблення інноваційних підходів до боротьби з кіберзагрозами. Зокрема, варто приділити увагу:

1) аналізу впливу освітніх програм із цифрової грамотності на реальний рівень обізнаності та поведінку дітей в інтернеті;

2) оцінюванню ефективності національних ініціатив щодо боротьби з кіберзлочинністю серед неповнолітніх;

3) розробленню й тестуванню алгоритмів раннього виявлення груп ризику серед дітей, які можуть бути втягнуті в злочинну діяльність у кіберсфері.

Таким чином, подальший розвиток публічної політики щодо запобігання кіберзлочинності серед неповнолітніх потребує комплексного підходу, що охоплює правові, освітні та технологічні рішення, а також міжсекторальну співпрацю для забезпечення ефективного захисту прав дітей у цифровому суспільстві.

Список використаної літератури:

1. Діденко А. С. Державна політика у сфері протидії кіберзлочинності як об'єкт адміністративно-правового регулювання. *Харківський національний університет внутрішніх справ: 25 років досвіду та погляд у майбутнє (1994-2019 рр.)*. Харків: ХНУВС. 2019. С. 154. URL: <https://app-journal.in.ua/wp-content/uploads/2024/12/133.pdf> (дата звернення: 25.02.2025).
2. *Дослідження цифрової грамотності*. Міністерство цифрової трансформації України. 2023. 70 с. URL: https://osvita.diia.gov.ua/uploads/1/8800-ua_cifrova_gramotnist_naselenna_ukraini_2023.pdf (дата звернення: 25.02.2025).
3. Ковальчук А. Ю., Гавловський В. Д. Кіберзлочини, як загроза державній безпеці: кримінологічні та організаційні особливості обліку. *Інформація і право*. 2023. Вип. 4, № 47. С. 187-196. URL: <http://il.ippi.org.ua/article/view/291662> (дата звернення: 25.02.2025).
4. *Конвенція про кіберзлочинність: Конвенція Ради Європи від 23.11.2001 р.* URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 29.01.2025).
5. *На примусовому лікуванні: кіберполіція повідомила про затримання кураторів "груп смерті"*. RBC.ua: веб-сайт. 2025. URL: <https://www.rbc.ua/ukr/news/prinuditelnom-lechenii-kiberpolitsiya-soobshchila-1615498792.html> (дата звернення: 25.02.2025).
6. *Національна стратегія захисту дітей у цифровому середовищі на період до 2025 року*. Міністерство цифрової трансформації України. 2025. URL: <https://surl.li/qreqrv> (дата звернення: 25.02.2025).
7. *Попередження та протидія кібербулінгу в дитячому середовищі України: аналітичний огляд*. ГО «Докудейз». 2020. 98 с. URL: https://cyber.bullyingstop.org.ua/storage/media-archives/cyberbuling_preview_5-10.pdf (дата звернення: 25.02.2025).
8. *Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 5*

- жовтня 2017 року. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 25.02.2025).
9. *Протидія булінгу. Міністерство освіти і науки України: веб-сайт*. URL: <https://mon.gov.ua/tag/protidiya-bulingu?&type=all&tag=protidiya-bulingu> (дата звернення: 25.02.2025).
 10. Саєнко М. І., Савела Є. А., Тополянський Ю. Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського національного університету. Серія ПРАВО*. 2021. Вип. 64. С. 386-391. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2021/08/74.pdf> (дата звернення: 25.02.2025).
 11. Сперкач Н. А., Ковбасюк В. С. Напрями запобігання кіберзлочинності та вдосконалення правового регулювання захисту прав людини у кіберпросторі. *Аналітично-порівняльне правознавство*. 2024. Вип. 6. С. 785-790. URL: <https://doi.org/10.24144/2788-6018.2024.06.131> (дата звернення: 25.02.2025).
 12. Чаплинська Ю. Кіберкультура та кібербезпека в умовах війни: психологічний практикум. Київ: *Національна академія педагогічних наук України*. 2023. 80 с. URL: https://ispp.org.ua/wp-content/uploads/2023/09/posib_chaplinska_2023.pdf (дата звернення: 25.02.2025).
 13. Шипілова Ю. Правова база української кібербезпеки: загальний огляд і аналіз. Київ: *Міжнародна фундація виборчих систем*. 2019. 40 с. URL: <https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf> (дата звернення: 25.02.2025).
 14. *Criminal Liability for Senior Managers. RPC Legal: website*. 2025. URL: <https://www.rpclegal.com/thinking/tech/criminal-liability-for-senior-managers-under-the-online-safety-act/> (date of access: 25.02.2025).
 15. *Media Awareness Network. Newswire.ca: website*. 2025. URL: <https://www.newswire.ca/news-releases/media-awareness-network-launches-enhanced-web-site-to-help-parents-be-webaware-539457251.html> (date of access: 25.02.2025).
 16. *Newsroom cyberviolence against children. Council of Europe: website*. URL: <https://www.coe.int/en/web/cyberviolence/-/the-council-of-europe-works-to-create-a-safer-digital-environment-for-children-worldwide-1> (date of access: 25.02.2025).
 17. *The state of the world's children 2017: Children in a digital world*. New York: UNICEF, 2017. 215 p. URL: https://www.unicef.org/media/48581/file/SOWC_2017_ENG.pdf (date of access: 25.02.2025).
 18. *Two thirds of European youth involved in cybercrime. University of East London: website*. 2025. URL: <https://www.uel.ac.uk/about-uel/news/2022/december/two-thirds-european-youth-involved-some-form-cybercrime-online-risk-taking> (date of access: 25.02.2025).
 19. *What is Better Internet for Kids (BIK)? European Schoolnet: website*. 2025. URL: <http://www.eun.org/news/detail?articleId=11811959> (date of access: 25.02.2025).
 20. Zhao Y. Research on Juvenile Cybercrime. *International Journal of Mathematics and Systems Science*. 2019. Vol. 6. № 2. P. 187-191. URL: <https://systems.enpress-publisher.com/index.php/IJMSS/article/viewFile/2439/1617> (date of access: 25.02.2025).

Malko N. O. Challenges and directions for improving the public policy of preventing juvenile cybercrime

The article examines the problem of cybercrime among minors as one of the most pressing threats to the digital society. It is established that the proliferation of information technologies contributes to the involvement of children in illegal online activities, which requires strengthening preventive measures and improving legal regulation mechanisms. The author reveals the insufficient effectiveness of the current government initiatives in combating cybercrime among children, which is due to the limited capacity of law enforcement agencies, the low level of digital literacy of the population and the lack of a comprehensive approach to preventing such actions.

The purpose of the study is to analyse the current challenges in preventing cybercrime among minors and develop proposals for improving public policy, taking into account the psychological, social and legal aspects of children's behaviour in the digital environment. To achieve this goal, the author uses system analysis methods to assess cybercrime trends, the comparative legal method to identify differences between national and international legislation, and the structural and functional approach to assess the effectiveness of public policy measures.

The study results indicate the need to revise the current system of legal regulation and introduce more effective mechanisms for preventing cybercrime among minors. It is proved that existing educational initiatives on digital security are underdeveloped, and public policy requires a comprehensive approach that includes interagency cooperation, involvement of the private sector and adaptation of international best practices. The author proposes to create a national programme on

cybersecurity for children, which would include strengthening legal mechanisms of protection, introducing mandatory digital literacy courses and expanding the powers of law enforcement agencies in the field of online threat monitoring.

Prospects for further research include creating models for assessing the risks of cybercrime among children, analysing the effectiveness of international programmes in digital security, and developing algorithms for monitoring and early detection of online threats.

Key words: digital security, legal regulation, online risks, crime prevention, public administration, digital literacy, cybercrime by minors.