УДК 343.85:004.77-053.6(477)
DOI https://doi.org/10.32782/2524-0374/2025-10/94

БЕЗПЕКА МАЛОЛІТНІХ ТА НЕПОВНОЛІТНІХ ОСІБ В СОЦІАЛЬНИХ ІНТЕРНЕТ-МЕРЕЖАХ: СУЧАСНІ ПІДХОДИ ДО ЗАПОБІГАННЯ ПРАВОПОРУШЕННЯМ

SAFETY OF MINORS AND MINORS IN SOCIAL INTERNET NETWORKS: MODERN APPROACHES TO PREVENTING OFFENSES

Бабенко А.М., д.ю.н., професор,
завідувач кафедри кримінально-правових дисциплін
Одеський державний університет внутрішніх справ
orcid.org/0000-0002-9498-2484

Резніченко Г.С., к.ю.н., доцент,
доцент кафедри кримінально-правових дисциплін
Одеський державний університет внутрішніх справ
orcid.org/0000-0001-6386-4154

Теслюк І.О., к.ю.н.,
начальник відділу аспірантури (ад'юнктури) і докторантури
Одеський державний університет внутрішніх справ
orcid.org/0000-0001-8081-2743

Для сучасного покоління молоді соціальні інтернет-платформи трансформувалися з факультативних інструментів комунікації у фундаментальний простір соціалізації, що охоплює широкий спектр активності: від освітньої діяльності до реалізації рекреаційних потреб. Утім, інтенсифікація мережевої взаємодії неминуче супроводжується генеруванням значних масивів персоналізованих даних та формуванням чіткого «цифрового сліду».

В умовах глобальної цифровізації спостерігається чітка тенденція до віртуалізації злочинності, де кримінальні елементи та організовані угруповання інтегруються у цифрову інфраструктуру. Це призводить до перетворення звичних соціальних медіа на джерело підвищених ризиків, де детермінантами протиправної поведінки стають анонімність, транскордонність та доступність конфіденційної інформації користувачів. Таким чином, сучасний кіберпростір вимагає розробки нових превентивних стратегій, спрямованих на нівелювання загроз, що виникають у процесі повсякденної онлайн-активності молоді.

Аналіз міжнародної практики свідчить, що потенціал сучасних інформаційно-комунікаційних технологій та глобальної мережі Інтернет виступає стратегічним ресурсом для суб'єктів вітчизняної системи запобігання злочинності, що потребує імплементації у практичну правоохоронну діяльність. Особливої актуальності набуває розвиток методології використання соціальних інтернет-мереж як інструментарію багаторівневої превенції.

Зокрема, видається перспективним впровадження інтерактивних механізмів на наступних ієрархічних рівнях запобіжної діяльності. На загальносоціальному рівні: використання цифрових платформ для формування правосвідомості громадян, поширення антикримінальних цінностей та зміцнення соціального контролю через широке охоплення аудиторії. На спеціально-кримінологічному рівні: застосування алгоритмів моніторингу та аналізу контенту (Big Data) з метою виявлення детермінант окремих видів злочинів, прогнозування криміногенної обстановки та проведення цільових інформаційних операцій серед груп ризику. На індивідуальному рівні: здійснення спрямованого виховного та психологічного впливу на осіб з ознаками девіантної поведінки, а також проведення заходів віртуального патронажу для запобігання рецидивам.

Ключові слова: неповнолітні, мережа Інтернет, соціальні Інтернет-мережі, інформаційні технології, злочинність, запобігання.

For the contemporary younger generation, social media platforms have evolved from optional communication tools into a fundamental space for socialization, encompassing a broad spectrum of activities ranging from educational endeavors to the fulfillment of recreational needs. However, the intensification of network interaction is inevitably accompanied by the generation of vast arrays of personalized data and the formation of a distinct 'digital footprint.'

In the context of global digitalization, there is a clear trend toward the virtualization of crime, as criminal elements and organized groups integrate themselves into the digital infrastructure. This shift transforms conventional social media into a source of heightened risk, where the determinants of illicit behavior include anonymity, cross-border accessibility, and the availability of sensitive user information. Consequently, modern cyberspace necessitates the development of novel preventive strategies aimed at mitigating the threats arising from the everyday online activities of youth.

An analysis of international practice demonstrates that the potential of modern information and communication technologies and the global Internet serves as a strategic resource for entities within the national crime prevention system, requiring implementation into practical law enforcement activities. The development of a methodology for utilizing social networking sites as a toolkit for multi-level prevention is becoming particularly relevant.

Specifically, the implementation of interactive mechanisms appears promising at the following hierarchical levels of preventive activity: At the general social level: leveraging digital platforms to shape the legal consciousness of citizens, disseminate anti-criminal values, and strengthen social control through extensive audience outreach. At the special criminological level: employing monitoring algorithms and content analysis (Big Data) to identify the determinants of specific types of crimes, forecast the criminogenic environment, and conduct targeted information operations among at-risk groups. At the individual level: exercising directed educational and psychological influence on individuals exhibiting signs of deviant behavior, as well as implementing virtual patronage measures to prevent recidivism.

Key words: minors, Internet, social Internet networks, information technologies, crime, prevention.

Забезпечення цифрової безпеки неповнолітніх у сучасному інформаційному суспільстві перестає бути суто технічним питанням, трансформуючись у фундаментальний пріоритет сучасних кримінологічних студій. Актуальність цієї проблеми зумовлена стрімкою віртуалізацією соціальних зв'язків, де дитина постає як найбільш вразливий суб'єкт віктимізації. Попри активне впровадження освітніх програм, спрямованих на формування медіаграмотності, критичного сприйняття контенту та навичок безпечної комунікації з анонімними користувачами, емпіричні дослідження все частіше фіксують обмежену результативність таких превентивних стратегій. Це пояснюється психологічними особливостями підліткового віку, схильністю до ризикованої поведінки та високим рівнем довіри до цифрового середовища, що часто нівелює теоретичні знання про безпеку.

Ситуація значно ускладнюється феноменом високої латентності правопорушень у кіберпросторі. Значна частина злочинних посягань, таких як грумінг, кібербулінг або фінансове шахрайство, залишається поза межами офіційної статистики через страх потерпілих, відсутність дієвих механізмів психологічної підтримки або нерозуміння батьками суті загрози. На правозастосовчому рівні спостерігається гострий дефіцит правосуддя: специфічні характеристики мережі - транскордонність, анонімність за допомогою VPN та шифрування, а також можливість миттєвого знищення цифрових доказів — створюють інституційні бар'єри для ідентифікації зловмисників. Це унеможливлює реалізацію засадничого принципу кримінального права — невідворотності покарання, що, своєю чергою, стимулює подальшу криміналізацію віртуального простору та вимагає докорінного перегляду методології захисту прав дитини в онлайн-середовищі.

Питання інтеграції інструментарію соціальних інтернет-мереж у систему протидії злочинності та методику розслідування злочинів перебувають у центрі уваги таких дослідників, як: А.М. Бабенко, Л.В Сапейко, С. П. Єгорченко, О. Ф. Гіда, А. І. Марущак, Д. М. Цехан, В. П. Шеломенцев та інші.

Зосередження на вивченні змістовної сутності соціальних мереж як інструментарію превентивного впливу на злочинність, а також на розробці прикладного інструментарію для підвищення ефективності такої діяльності.

Глобальні соціальні платформи інтегрувалися у структуру суспільних відносин як критично важливий елемент комунікації. Завдяки функціональним можливостям щодо оперативного збору та поширення даних, мережі мінімізували трансакційні витрати у процесі людської взаємодії, значно прискоривши інформаційні потоки та спростивши доступ до знань для кожного учасника соціальної мережі [1].

Емпіричне дослідження яке було проведено Юхно О. О. та Загуменним О. О., сформоване на основі соціологічного опитування активної аудиторії соціальної мережі «Facebook», дозволило виявити низку закономірностей, що мають суттєве значення для визначення рівня віктимності користувачів та потенційних криміногенних ризиків. Зокрема, встановлено такі показники:

Рівень активності та залученості: Переважна більшість респондентів (70 %) демонструють високу інтенсивність використання платформи, відвідуючи персональні профілі щоденно.

Ступінь приватності та відкритості даних: Викликає занепокоєння той факт, що 80 % опитаних ігнорують інструменти обмеження доступу, залишаючи свої персональні дані відкритими для загального огляду. При цьому 74 % користувачів розміщують автентичну особисту інформацію, що значно спрощує можливість її використання у протиправних цілях (соціальна інженерія, сталкінг тощо).

Мета та характер мережевої взаємодії: Основним вектором експлуатації мережі для 60 % осіб залишається підтримання міжособистісних зв'язків, а 70 % респондентів при формуванні списку контактів керуються критерієм попереднього реального знайомства.

Схильність до девіантної комунікації: Найбільш репрезентативним у контексті превенції злочинності є показник готовності до обміну інформацією про протиправну діяльність. З'ясовано, що лише третина опитаних (30 %) категорично відкидає можливість використання приватних повідомлень для обговорення або вчинення неправомірних діянь. Водночас 70 % респондентів не виключають ймовірності залучення до такої взаємодії, що свідчить про високий латентний потенціал правопорушень у віртуальному середовищі [2, с. 58].

Проблематика забезпечення кібербезпеки неповнолітніх виходить за межі класичної віктимологічної парадигми, де дитина розглядається виключно як пасивний об'єкт злочинного посягання. Сучасний стан криміногенної ситуації в цифровому середовищі вказує на стійку тенденцію до трансформації неповнолітніх у самостійних суб'єктів протиправної діяльності.

Даний феномен характеризується детермінованою двоїстістю, що в науковій літературі часто описується як конвергенція ролей «жертва-агресор». Ключовим каталізатором такої трансформації виступає кібербулінг, який функціонує як механізм реципрокної (зворотної) агресії. У цьому контексті віртуальний простір стає платформою, де попередня віктимізація індивіда стає психологічним підґрунтям для вчинення ним власних деліктів, що вимагає розробки комплексних превентивних заходів, орієнтованих як на захист, так і на корекцію поведінки активних користувачів-підлітків.

О. М. Лисенко до найбільш релевантних загроз правам та інтересам неповнолітніх у цифровому середовищі відносить мультимодальний спектр правопорушень. Зокрема, автором виокремлюються такі деструктивні явища, як кібербулінг, поширення порнографічного контенту та пропаганда насильства. Окрему увагу приділено специфічним формам онлайн-експлуатації, зокрема грумінгу та кібершахрайству, а також ризикам некримінального характеру, що мають негативні психосоціальні наслідки, як-от формування адиктивної поведінки (ігрової залежності) та ретрансляція ідеологій расової нетерпимості [3, с. 28].

Вагомими детермінантами деструктивної онлайн-поведінки виступають суб'єктивне відчуття безкарності та технічно зумовлена анонімність цифрового середовища. Феномен опосередкованої взаємодії (відсутність безпосереднього фізичного контакту) у поєднанні з можливістю верифікаційної інкогніто-комунікації спричиняє девальвацію етико-правових обмежень та суттєву редукцію психологічних бар'єрів щодо вчинення агресивних актів.

Даний стан характеризується ефектом онлайн-розгальмування, за якого в індивіда - зокрема, у дитини з несформованою системою самоконтролю - спостерігається нівелювання моральних імперативів та соціальних гальм. Це призводить до реалізації таких поведінкових патернів, які є нетиповими для особистості у фізичному соціумі та на які вона не наважилася б в умовах безпосередньої соціальної взаємодії.

Окремим аспектом деструктивного впливу соціальних інтернет-мереж є функціонування суїцидальних віртуальних спільнот (так званих «груп смерті»), діяльність яких спрямована на схиляння неповнолітніх до суїцидальної поведінки. Незважаючи на варіативність номінацій («Синій кит», «Тихий дім», «Розбуди мене о 04:20», «Червона сова», «Момо» тощо), зазначені мережеві структури мають ідентичну цільову спрямованість — доведення до самогубства дитини шляхом застосування методів психологічного тиску та маніпулятивних технологій у процесі поетапного залучення до деструктивної взаємодії.

Надзвичайно високий ступінь суспільної небезпеки цього явища зумовлений специфікою об'єкта посягання: у переважній більшості випадків потенційними та реальними жертвами стають особи дитячого та підліткового віку. Таке вибіркове фокусування на вказаній віковій категорії пояснюється психологічною лабільністю неповнолітніх та їхньою особливою чутливістю до зовнішнього маніпулятивного впливу, що вимагає розробки спеціалізованих кримінологічних заходів протидії та моніторингу контенту соціальних медіа [4, с. 218].

Водночас соціальні інтернет-мережі виступають стратегічним ресурсом для превенції та розслідування злочинів, виконуючи роль джерела релевантної криміналістичної інформації. Під такою інформацією слід розуміти сукупність верифікованих даних про механізм формування матеріальних та ідеальних (цифрових) слідів злочинного діяння, отриманих за допомогою спеціалізованого інструментарію.

Методологія криміналістичного аналізу мережевого контенту базується на чотириетапному алгоритмі: пошук, виявлення, фіксація (зняття) та дослідження інформації. До основних способів акумуляції доказової бази належать: системний інформаційно-аналітичний моніторинг; направлення процесуальних запитів; застосування спеціалізованого програмного забезпечення (OSINT-інструментів); методи оперативної імітації [5, с. 143–144].

Перспективним напрямом є впровадження системного правоохоронного моніторингу соціальних платформ, спрямованого не лише на детекцію ознак кримінальних та адміністративних правопорушень, а й на ідентифікацію деструктивних соціальних процесів. Мова йде про верифікацію загроз національній безпеці, зокрема проявів екстремізму, сепаратизму та інспірування міжетнічної чи релігійної ворожнечі.

Така діяльність дозволяє здійснювати предиктивний аналіз ризиків для суспільної злагоди та реалізовувати комплекс упереджувальних заходів, спрямованих на нейтралізацію криміногенних чинників у віртуальному середовищі ще до моменту їх трансформації у реальні протиправні акти [6, с. 21].

Враховуючи специфіку контенту та методику вилучення мережевих даних, імплементація міжнародного досвіду дозволяє оптимізувати використання потенціалу соціальних платформ у практичній діяльності правоохоронних органів за такими стратегічними напрямами: Інформаційно-аналітичне забезпечення: збір релевантних відомостей про учасників кримінального провадження (підозрюваних, свідків, потерпілих) та верифікація їхніх персональних даних. Оперативна та слідча діяльність: встановлення структури соціальних зв'язків правопорушників, ідентифікація прихованих комунікаційних каналів, локація об'єктів та перевірка достовірності алібі. Комунікаційна стратегія: реалізація заходів із підвищення рівня суспільної довіри до правоохоронної системи через прозору взаємодію у цифровому середовищі [7, с. 95].

Резюмуючи, слід зазначити, що диференціація та ускладнення механізмів злочинності в умовах інтенсивного розвитку інформаційно-комунікаційних технологій актуалізують потребу в системних наукових розвідках та фундаментальному переосмисленні існуючих кримінологічних парадигм. Модернізація теоретико-методологічних підходів має бути спрямована на розробку ефективних стратегій протидії новітнім викликам, зокрема кіберзлочинності, кібербулінгу, виготовленню та дифузії дитячої порнографії, а також іншим формам деліктної поведінки у віртуальному просторі.

Узагальнюючи результати дослідження, можна констатувати, що основними векторами реалізації потенціалу соціальних інтернет-мереж у сфері запобігання злочинності є:

1. Прогностично-аналітичний напрям, що передбачає системний моніторинг кримінологічно значущого контенту для прогнозування динаміки злочинності та ідентифікації латентних загроз у цифровому середовищі;
2. Багаторівневий превентивний підхід, який полягає у впровадженні спеціалізованих заходів впливу на загальносоціальному, спеціально-кримінологічному та індивідуальному ієрархічних рівнях;
3. Комунікативно-інституційний аспект, спрямований на інтенсифікацію взаємодії між органами правопорядку та суспільством, а також стимулювання громадської активності, зокрема через підтримку цифрових форм «сусідського нагляду» та інших інструментів колективної безпеки;
4. Оперативно-дифузійний вектор, що полягає у використанні мережевого інструментарію для розшуку осіб, оперативного сповіщення про вчинені кримінальні правопорушення та локалізації потенційних небезпек для територіальних громад.

Окремої уваги заслуговує розробка та впровадження спеціалізованих інтерактивних платформ превентивного спрямування. Це дозволить оптимізувати комунікаційну взаємодію між дільничними офіцерами поліції та територіальними громадами, забезпечуючи ефективний інструментарій для оперативного вирішення безпекових питань на локальному рівні та сприяючи інклюзивному підходу до запобігання злочинності.

ЛІТЕРАТУРА

1. Битяк Ю. П., Калиновський Ю. Ю. Деструктивний вплив соціальних мереж на інформаційну безпеку людини й суспільства : матеріали наук. семінару ХНУ ПС ім. І. Кожедуба, 21 жовт. 2020 р. URL: http://www.hups.mil.gov.ua/assets/doc/science/stud-conf/suchasna-vijna-gumanitarnij-aspekt-21-10-2020/3.pdf (дата звернення: 09.11.2025).
2. Юхно О. О., Загуменний О. О. Використання сучасних інформаційних технологій працівниками поліції при проведенні негласних слідчих (розшукових) дій : навч. посіб. 2-ге вид., допов. і перероб. Харків : Колегіум, 2020. 116 с.
3. Лисенко О. М. Міжнародно-правове регулювання прав дитини в кіберпросторі. *Соціологія права*. 2016. № 3 (18). URL: http://soclaw.idpnan.kyiv.ua/archive/2016/3/8.pdf (дата звернення: 10.11.2025).
4. Павленко С. Тактика запобігання доведенню неповнолітніх до самогубств через соціальні мережі (інтернет-спільноти): сучасні вітчизняні реалії та зарубіжний досвід. *Підприємництво, господарство і право*. 2018. № 11. С. 217–225.
5. Шевчук В. М. Використання інформації із соціальних інтернет-мереж при розслідувані кіберзлочинів: криміналістичні проблеми. *Кримінальні загрози в секторі безпеки: практики ефективного реагування* : матеріали панельної дискусії III Харків. міжнар. юридичного форуму «Право» (м. Харків, 26 верес. 2019 р.) / редкол.: В. Я. Тацій та ін. Харків : Право, 2019. С. 142–146. URL: https://dspace.nlu.edu.ua/bitstream/123456789/17042/1/Shevchuk_142-146.pdf (дата звернення: 09.01.2026).
6. Гавловський В. Д. Правоохоронний моніторинг соціальних мереж. *Правова інформатика*. 2014. № 3 (43). С. 19–25.
7. Косолап О. В. Використання соціальних мереж у виявленні та розслідуванні злочинів: зарубіжний досвід та перспективні напрямки. *Young Scientist*. 2016. № 8 (35). С. 93–96.

Дата першого надходження рукопису до видання: 20.10.2025
Дата прийнятого до друку рукопису після рецензування: 14.11.2025
Дата публікації: 28.11.2025