DOI: 10.33663/1563-3349-2022-33-584-592
УДК 343 (477)+ 343.9:659.3

О. М. КОСТЮК,
*аспірант Інституту держави і права імені В. М. Корецького НАН України**
ORCID: 0000-0001-9380-8663

РОЛЬ СОЦІАЛЬНИХ МЕРЕЖ У ПРОТИДІЇ ЗЛОЧИНАМ ПРОТИ ОСНОВ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

У статті аналізується роль соціальних мереж у протидії злочинам у сфері національної безпеки. Враховуючи істотне значення соціальних мереж, саме на них, а не на традиційних засобах масової інформації має фокусуватись увага у питаннях прогнозування та протидії злочинам загалом та злочинам проти національної безпеки зокрема. При цьому відповідні дії мають вчинятись не лише правоохоронними органами, а й громадянським суспільством, до якого належать не лише користувачі соціальних мереж, а й їх власники. Окремим сучасним напрямом протидії злочинності з використанням соціальних мереж є аналіз даних, які в них містяться. Для цього необхідним є створення, коригування та вдосконалення алгоритмів аналізу активності користувачів.

Ключові слова: *національна безпека, засоби масової інформації, соціальні мережі, протидія злочинам, прогнозування злочинів.*

Kostyuk O. **The role of social networks in combating crimes against the fundamentals of national security**

The article analyzes the role of social networks in combating crimes in the field of national security. Given the importance of social networks, it is on them, and not on the traditional media, that attention should be focused on predicting and combating crimes in general and crimes against national security in particular. At the same time, appropriate actions should be taken not only by law enforcement agencies, but also by civil society, which includes not only users of social networks, but also their owners. A separate modern direction of combating crime with the use of social networks is the analysis of data contained in them. This requires the creation, adjustment and improvement of algorithms for analyzing user activity.

Key words: *national security, mass media, social networks, crime prevention, crime forecasting.*

Вступ. Визначення ролі засобів масової інформації у протидії злочинам загалом і злочинам проти основ національної безпеки України зокрема на сьогодні є надзвичайно актуальним. Водночас у цьому контексті не менш важливим є вивчення кримінологічного потенціалу соціальних мереж.

* ***Kostyuk O.,*** *Postgraduate Student of Koretsky Institute of State and Law of the NAS of Ukraine*

Аналіз наукових джерел свідчить про існування на сьогодні доволі спрощеного описання співвідношення ЗМІ та мережі Інтернет. Автори здебільшого визначають класифікацію ЗМІ як друкованих ЗМІ, телебачення та Інтернет, під яким зазвичай розуміють електронні ЗМІ, максимум авторські блоги. Водночас є й більш розширені класифікації Інтернет ЗМІ, які, проте, все ж залишаються спрощеними і не відображають усієї повноти існуючих на сьогодні інструментів.

Так, О. Коцарєв пропонує власну типологію мережевих ЗМІ. Дослідник виділяє п'ять основних типів інтернет-ЗМІ: інтернет-телебачення, інтернет-радіо, інтернет-газети, інтернет-журнали та новинні сайти[1].

Спрощеність такої типологізації, на нашу думку, полягає в тому, що у ній не виділяється такий істотний інтернет-феномен як соціальні мережі. І гадаємо, що в контексті протидії злочинності та криміногенності саме соціальні мережі мають на сьогодні привертати основну увагу кримінологів. Незаперечним на сьогодні є факт безпрецедентного психологічного впливу соціальних мереж на свідомість громадян, на зміну або утвердження їх поглядів, на підсилення їх агресивності.

Стан дослідження. Дослідженню проблеми створення ефективної системи протидії злочинам проти основ національної безпеки свої праці присвятили Г. В. Андрусів, В. Ф. Антипенко, О. Ф. Бантишев, С. Б. Гавриш, В. О. Глушков, І. В. Діордіца, В. П. Ємельянов, О. О. Кияшко, О. М. Костенко, В. А. Ліпкан, П. С. Матишевський, М. І. Мельник, Л. В. Мошняга, В. О. Навроцький, А. В. Савченко, О. С. Сотула, В. В. Сташис, Є. Л. Стрельцов, В. Я. Тацій, М. І. Хавронюк, О. А. Чуваков, О. В. Шамара, С. С. Яценко, А. М. Ященко та ін. У цьому контексті слід зауважити, що загалом в Україні увага до впливу засобів масової інформації (далі − ЗМІ) як з боку науковців, так і практиків здійснюється переважно на рівні ювенальної юстиції (О. І. Бугера, О. І. Напиральська, В. І. Галаган) та ін. Вплив ЗМІ на стан злочинності в Україні та запобіжна роль у протидії їй досліджено у працях М. О. Д'ячкової, В. М. Дрьоміна, Н. С. Юзікової та ін. Проте на сьогодні недостатня увага приділяється аспектам використання соціальних мереж у протидії злочинам проти основ національної безпеки, а отже, розкриття відповідних аспектів і є **метою цієї статті.**

Виклад основного матеріалу. Технології таргетування, які на сьогодні активно розвиваються, значно посилюють ефект соціальних мереж, спрощують пошук однодумців, фокусування на тому описанні реальності, що узгоджується із внутрішнім переконанням особи. Вочевидь ці технології можуть мати подвійне значення та використовуватись як з добрими, так і, без сумніву, з негативними намірами. Зокрема, це стосується і вчинення злочинів у сфері національної безпеки. За певними параметрами, вподобаннями особи, за тими новинами, які привертають її увагу, соціальні мережі диференціюють користувачів за численними фокус-групами, відповідно до яких формують «рекламний» контент. Слово «рекламний» узяте у лапки,

адже під такою рекламою на сьогодні в соціальних мережах здійснюється на лише продаж матеріальних благ і послуг, а досягаються політичні цілі, здійснюється пропаганда / нав'язування будь-яких ідей, починаючи від екологічних прагнень та соціальної допомоги хворим, завершуючи президентськими виборами.

Загальновідомо, що вплив ЗМІ може бути прямий (умисний), може бути опосередкований, а може взагалі бути невидимим, тліючим. Останній є найбільш небезпечним, адже його складно виявити, а отже, і йому протидіяти. Зокрема, чи може вважатись таким тліючим впливом діяльність певних ЗМІ, яка полягає у тому, що новинний контент формується лише із негативних новин? На нашу думку, так, може вважатись.

Фактор прихованості такого впливу значною мірою ускладнює протидію йому. Адже не можна звинувачувати відповідні ЗМІ у неправдивості інформації, оскільки новини, хоча й негативні, але вони правдиві, а отже, такими ЗМІ в дійсності подаються достовірні відомості. Відтак, в умовах права на свободу вираження поглядів ані держава, ані суспільство не можуть порушувати питання стосовно припинення діяльності таких ЗМІ, оскільки це суперечитиме усім можливим демократичним стандартам.

Водночас, враховуючи те, що така діяльність є цілеспрямованою та може мати різні цілі, зокрема, й цілі щодо загроз національній безпеці, не можливо такій діяльності не протидіяти.

Ми вважаємо, що можливими шляхами протидії таким випадкам є два: по-перше, необхідним є створення чи заохочення щодо створення засобів масової інформації, які відображатимуть об'єктивну реальність, що включатиме висвітлення не лише негативних, а й позитивних новин. По-друге, необхідним є підвищення культури «споживання» інформації у ЗМІ та соціальних мережах. На системному рівні до громадян має доноситись інформація про те, що вони стають жертвами «накачування» негативною інформацією, що здійснюється з метою маніпулювання ними, та подальшого підсвідомого їх використання. Це має стати невід'ємною частиною освітніх процесів, як у школах, а особливо – у вищих навчальних закладах.

О. І. Бугера за результатами проведеного дослідження констатує, що для зниження рівня криміналізації мережі Інтернет та ефективного запобігання злочинності (у т. ч. кіберзлочинності) необхідним є: по-перше, забезпечення зміни загальної парадигми ставлення до такого інформаційно-комунікаційного феномену, як Інтернет – від акцентування зусиль правоохоронних органів тільки на боротьбі з кіберзлочинністю, що є наслідком процесу криміналізації Інтернету, до комплексного використання можливостей мережі Інтернет для підвищення рівня ефективності запобігання злочинності; по-друге, правоохоронні органи повинні мати належний рівень технологічного оснащення на основі сучасних Інтернет-технологій для запобігання злочинності[2].

На нашу думку, окрім справедливо наведених заходів, потрібно активно в аналізованому контексті використовувати потенціал громадянського

суспільства, а саме активних користувачів соціальних мереж. На сьогодні можна спостерігати істотне посилення ролі таких мереж, як у питаннях, які сприяють злочинності, так і у питаннях, які їй запобігають. Суспільний резонанс, який на сьогодні продукується, як штучним, так і органічним способом через соціальні мережі в рази перевищує той, який міг бути створений традиційними засобами масової інформації до появи соціальних мереж.

На сьогодні можемо спостерігати, що традиційні ЗМІ часто починають відігравати роль «другого номера» і лише підхоплюють інформацію щодо подій, які висвітлюються у соціальних мережах. Тож існує теоретична необхідність у перегляді класичних уявлень щодо ролі громадянського суспільства у протидії злочинності, адже така роль набула нових значень з розвитком соціальних мереж і надала громадянському суспільство у нові ефективні інструменти, які зробили з пасивного спостерігача активного діяча.

У цьому контексті Т. Крайнікова обґрунтовано зазначає, що сучасний медіаспоживач опанував на власній практиці співвідношення «ціна – якість», навчився орієнтуватися у великому колі пропозицій; він не сприймає на віру кожне твердження в газеті, розуміє, що його свідомістю намагаються маніпулювати, апелює до редакцій із різноманітними пропозиціями, скаргами, оцінками, повідомленнями тощо. Зрештою, він сам стає медіа: послуговуючись сучасною цифровою технікою, генерує та оперативно оприлюднює інформацію в Інтернеті, при цьому не раз випереджаючи професійних журналістів[3].

Окремого значення в аналізованому контексті набувають як користувачі соціальних мереж, так і їх власники, які, усвідомлюючи вагомий вплив створеного ними продукту, вживають заходів контролю за використанням соціальних мереж, використовуючи ті чи ті інструменти для мінімізації негативного впливу. Найбільш яскравою ілюстрацією наведеного є події, які відбулись в Сполучених Штатах Америки в січні 2021 р., а саме спроба захоплення Капітолію озброєними громадянами.

У цей день Конгрес повинен був остаточно затвердити підсумки президентських виборів, перемогу на яких здобув кандидат від демократів Джозеф Байден молодший. Після мітингу і виступу на ньому іншого кандидата – Дональда Трампа, його прихильники на його ж заклик вирушили «висловлювати незгоду» під стінами Капітолію. Протест вийшов з-під контролю, мітингувальники увірвалися до будівлі Конгресу – під час штурму загинуло чотири прихильники Трампа і один поліцейський, який охороняв будівлю. Через кілька годин результати виборів усе ж затвердили. Трамп опублікував через Twitter відеозвернення, у якому закликав прихильників покинути Конгрес, проте вкотре назвав вибори вкраденими. Через це соцмережа позначила пост як такий, що містить помилкові твердження і заборонила його репости[4].

Відтак, одним із наслідків цих подій стало блокування акаунту в соціальній мережі Twitter, а згодом і Facebook тодішнього президента США Дональда Трампа. Мотивація такого блокування полягала саме у тому, що

цей акаунт використовувався Трампом для підбурювання громадськості для вчинення насильницьких дій та нападу на урядові установи. Власники відповідних соціальних мереж констатували, що таке обмеження у доступі було продиктовано саме метою протидії загрозам громадській безпеці[5].

Відтак констатуємо, що на сьогодні питання протидії використання ЗМІ, а особливо – соціальних мереж, у вчиненні злочинів має охоплювати не лише діяльність правоохоронних органів, а й громадянського суспільства, яке, своєю чергою, в аналізованому контексті має дві складові: власники соціальних мереж та користувачі соціальних мереж.

Одним із наслідків блокування облікового запису президента США Дональда Трампа в соціальних мережах стала дискусія про те, чи не є таке блокування недопустимою цензурою та нападом на свободу слова і свободу вираження поглядів. Думки учасників дискусії майже розділились, адже сам факт відповідної цензури сприймався як небезпечний прецедент, що в подальшому могло призвести до використання цього ж механізму, а відтак певною мірою поставити під контроль погляди певних людей, тим самим допустивши можливість зловживання та придушування свободи слова.

У цьому випадку, на нашу думку, відповідне обмеження мало легітимну мету, адже був очевидним причинно-наслідковий зв'язок між певними публікаціями власника облікового запису та нападом на урядові будівлі, що, з-поміж іншого, призводило до заподіяння смерті кільком особам, а відтак, очевидною була й необхідність активної протидії відповідним вчинкам. Інакше демократичний інструмент щодо свободи вираження поглядів використовувався б на зло самій демократії.

Соціальні мережі створюють додаткові можливості користувачам для висловлювання своїх думок, що формують величезну базу даних. Якщо створені кожним окремим користувачем дані не можуть забезпечити необхідної інформації, у випадку їх поєднання, вони включають приховані змінні, які можуть відображати важливі фактори. Також в аналізованому контексті розглядається питання про те, чи може контекст соціальних мереж надавати соціально-поведінкові «сигнали» для прогнозування злочинів. Припущення полягає в тому, що загальнодоступні дані натовпу в соціальних мережах, зокрема Twitter, можуть включати прогностичні змінні, які можуть вказувати на зміни рівня злочинності[6].

Як зазначають дослідники Центру демократії та верховенства права, Facebook з 2017 р. використовує автоматичні алгоритми для пошуку терористичного контенту. Цей механізм передбачає: виявлення збігів із зображеннями, вже позначеними як екстремістські матеріали; багатомовність та встановлення лінгвістичних індикаторів протиправного контенту; видалення мереж терористичних комунікацій (алгоритм аналогічний до реакції на координовану неавтентичну поведінку – масове блокування або видалення акаунтів, які залучені у заборонену діяльність чи підтримують її поширеннями, реакціями, коментарями тощо); швидке видалення нових фейкових акаунтів.

При цьому зазначимо, що Facebook не розкриває алгоритм для виявлення зв'язку новоствореного акаунту з нещодавно видаленим, що потенційно створює загрозу для приватності користувачів[7].

Щодо можливості прогностичного визначення місць та часу вчинення злочинів, то в цьому контексті аналіз наявних джерел дає підстави засвідчити, що ці спроби не є надто вдалими. У цьому контексті аналізується щонайменше два кейси: програми прогнозування злочинності, які запроваджувались у департаменті поліції Лос-Анджелеса, а також програми щодо прогнозування терористичних актів. І той, і той підхід здебільшого формується за принципом: якщо в попередні роки певна подія мала місце в певній локації, то вона з великою ймовірністю в цій же локації повториться. Зрештою, після певного часу випробування алгоритмів прогнозування злочинності в Лос-Анджелесі від цієї ідеї поліція відмовилась[8].

Водночас у наукових джерелах наводяться й успішні приклади реалізації відповідних алгоритмів. Як зазначає М. І. Демура, схожі проєкти були втілені у Сполученому Королівстві в рамках пілотного проєкту з прогнозування можливих місць крадіжок зі зломом, розкрадання і нападу за допомогою штучного інтелекту. Вони показали, що використані програмні проєкції, які називаються PREDPOL, були точними в 78% випадків, порівняно з 51% прогнозів, складених з використанням традиційних методів[9].

Аналогічно, недоліки та критику викликав концепт прогнозування терактів. Учені розробили структуру для прогнозування терактів по всьому світу, попередньо вивчивши випадки терористичних атак, які сталися в період із 2002 по 2016 рр. (тобто протягом 795 тижнів) у 13 регіонах, включаючи всі субконтинентальні регіони, що відповідають умовам Глобальної бази даних про тероризм (GTD), і Західну Африку. Для кожного регіону побудували прогностичні моделі, які дають змогу виявляти, оцінювати та порівнювати роль основних рушійних терористичних сил. Як зазначають вчені, машинні алгоритми ефективно пророкують події на територіях, які багаторазово піддавалися атакам, однак їм складно будувати прогнози для регіонів, де терактів не було вже тривалий час[10].

Також в аналізованому контексті цікавим є американський стартап Voyager Labs – система, яка працює над встановленням «вини через асоціацію»: алгоритм оцінює пости, коментарі, зв'язки і навіть смайли для перехресних посилань з непублічною інформацією. Ця «персональна топографія» оцінює людей, які найбільше взаємодіють з людиною, і публікації для встановлення інших можливих злочинців, створюючи систему «вини за асоціацією»[11].

З аналізом подібних даних працює програмне забезпечення Palantir Technologies, механізм дії якого полягає в аналізі персональних даних та виявленні транзакцій, які завжди йдуть у тісній зв'язці з патернами, які супроводжують ті чи інші злочини. Іншими словами, у спецслужб є значні масиви даних, серед яких відомості про фінансові операції, відбитки пальців

і зразки ДНК, плани будівель і топографічні карти, дані радіоперехоплення, «гарячі» новини зі ЗМІ, повідомлення інформаторів, інформація з соцмереж і ін. Програмне забезпечення Palantir вже допомогло розкрити злочинну мережу, яка готує теракти в декількох країнах світу. Його також використовували в Афганістані для прогнозування атак моджахедів. Крім того, програмне забезпечення Palantir дало змогу виявити членів мексиканського наркокартелю, які вбили співробітника митної служби США, а також розкрити багато не таких гучних, але не менш важливих випадків, у тому числі знайти педофіла в Нью-Йорку вже через годину після нападу на дитину, виявивши його на відеозаписах з камер поліцейського управління[11].

Загалом, у сучасній правоохоронній практиці 'predictive policing' (політика прогнозування) аналіз використовується за чотирма основними напрямами: прогнозування кримінальних правопорушень; прогнозування осіб, що вчиняють кримінальні правопорушення, осіб, що схильні до вчинення (або повторного вчинення) кримінальних правопорушень; здійснення передбачень щодо особистості злочинця або створення профілів таких осіб з врахуванням характеристик вже виявлених правопорушників; прогнозування майбутніх жертв кримінальних правопорушень (груп осіб, які з високою вірогідністю можуть стати жертвою кримінальних правопорушень)[12].

Як обґрунтовано зазначають М. О. Яцина та О. Ю. Петечел, багато неурядових організацій займаються збором та аналізом інформації, яка входить до сфери їх діяльності. Як відомо, масив інформації, який необхідно зібрати та обробити, щоб використання технологій штучного інтелекту було справді дієвим та мало позитивний ефект, зокрема і для протидії злочинності, є вкрай великим. Результати такої інформаційної роботи неурядових організацій, своєю чергою, можуть бути корисними для держави в цілому, так і кримінально-правової системи. Наприклад, міжнародна неурядова дослідницько-викривальна мережа Bellingcat, яка розслідує поточні події з цілого світу, використовує метод OSINT: аналіз інформації з відкритих джерел, таких як відео, карти та фотографії. Таким чином, членами цієї неурядової організації ведеться розслідування широкого кола злочинної діяльності – від мексиканських наркокартелів і злочинів проти людства до відстеження використання хімічної зброї та конфліктів у всьому світі[17].

Висновки і перспективи подальших розвідок. Підсумовуючи, вважаємо за доцільне наголосити на тому, що, враховуючи істотне значення соціальних мереж, саме на них, а не на традиційних засобах масової інформації, має фокусуватись увага у питаннях прогнозування та протидії злочинам загалом і злочинам проти основ національної безпеки України зокрема. При цьому відповідні дії мають вчинятись не лише правоохоронними органами, а й громадянським суспільством, до якого належать не лише користувачі соціальних мереж, а й їх власники. Окремим сучасним напрямом протидії злочинності з використанням соціальних мереж є аналіз даних, які в них містяться. Для

цього необхідним є створення, коригування та вдосконалення алгоритмів аналізу активності користувачів.

1. Коцарев О. О. Типология Интернет-СМИ. *Ученые записки Таврического национального университета им. В. И. Вернадского*. Сер. Филология. Т. 19. № 5. С. 323–324. **2.** Бугера О. І. Кримінологічні засади використання мережі Інтернет для запобігання злочинності: автореф. дис. … д. ю. н. 12.00.08. Київ, 2020. С. 12. **3.** Крайнікова Т. ЗМІ в умовах глобальної трансформації медіаспоживання. *Вісник Книжкової палати.* 2012. № 6. С. 1–4. С. 1. **4.** Як Трампа заблокували в Твітері. Цензура чи внутрішні правила? URL: https://rubryka.com/article/trump-twitter/. **5.** Глава Твітеру Джек Дорсі вважає, що блокування облікового запису президента США Дональда Трампа було правильним рішенням. URL: https://www.ukrinform.ua/rubric-world/3170693-glava-twitter-vvazae-blokuvanna-akaunta-trampa-pravilnim-risennam.html. **6.** Mining Social Media Content for Crime Prediction. URL: https://ieeexplore.ieee.org/abstract/document/7817106 **7.** Вибуховий контент онлайн. Частина 3. URL: https://cedem.org.ua/analytics/vybuhovyj-kontent-onlajn-3/. **8.** LAPD ended predictive policing programs amid public outcry. A new effort shares many of their flaws. URL: https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform. **9.** Демура М. І. Використання технологій штучного інтелекту у протидії злочинності: матеріали наук.-практ. онлайн-семінару (Харків, 5 листоп.2020 р.). Харків: Право, 2020. С. 24–28. **10.** Комп'ютер проти тероризму: вчені навчили ШІ передбачати теракти по всьому світу. URL: https://focus.ua/uk/digital/489637-kompyuter-protiv-terrorizma-uchenye-nauchili-ii-predskazyvat-terakty-po-vsemu-miru. **11.** Programa de vigilância quer estudar perfis do Facebook para prever quem vai cometer crimes. URL: https://olhardigital.com.br/2021/11/17/seguranca/facebook-prever-crimes/ **12.** Струков В. М., Узлов Д. Ю. Використання штучного інтелекту у правоохоронній сфері зарубіжних країн. *Досвід США. Використання технологій штучного інтелекту у протидії злочинності:* матеріали наук.-практ. онлайн-семінару (Харків, 5 листоп. 2020 р.). Харків: Право, 2020. 112 с. С. 76. **13.** González Fuster G. Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights. The European Parliament's Committee on Civil Liberties, Justice and Home Affairs. European Parliament. Brussels. July 2020. 87 p, p. 22 **14.** Яцина М. О., Петечел О. Ю. Роль неурядових організацій у впровадженні технологій штучного інтелекту у протидії злочинності. *Використання технологій штучного інтелекту у протидії злочинності:* матеріали наук.-практ. онлайн-семінару (Харків, 5 листоп. 2020 р.). Харків: Право, 2020. С. 108–111.

References

1. Kotsarev O. O. Typolohyia Ynternet-SMY. *Uchenыe zapysky Tavrycheskoho natsyonalnoho unyversyteta ym. V. Y. Vernadskoho.* Ser. Fylolohyia. T. 19. № 5. S. 323–324. **2.** Buhera O. I. Kryminolohichni zasady vykorystannia merezhi Internet dlia zapobihannia zlochynnosti. avtoreferat. dys. d.iu.n. 12.00.08. Kyiv, 2020. S. 12. **3.** Krainikova T. ZMI v umovakh hlobalnoi transformatsii mediaspozhyvannia. *Visnyk Knyzhkovoi palaty.* 2012. № 6. S. 1–4. S. 1. **4.** Yak Trampa zablokuvaly v Tvitteri. Tsenzura chy vnutrishni pravyla? URL: https://rubryka.com/article/trump-twitter/ **5.** Hlava Tviteru Dzhek Dorsi vvazhaie, shcho blokuvannia oblikovoho zapysu prezydenta SShA Donalda Trampa bulo pravylnym rishenniam. URL: https://www.ukrinform.ua/rubric-world/3170693-glava-twitter-vvazae-blokuvanna-akaunta-trampa-pravilnim-risennam.html **6.** Mining Social Media Content for Crime Prediction. URL: https://ieeexplore.ieee.org/abstract/document/7817106 **7.** Vybukhovyi kontent onlain. Chastyna 3. URL: https://cedem.org.ua/analytics/vybuhovyj-

kontent-onlajn-3/ **8.** LAPD ended predictive policing programs amid public outcry. A new effort shares many of their flaws. URL: https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform. **9.** Demura M. I. Vykorystannia tekhnolohii shtuchnoho intelektu u protydii zlochynnosti: materialy nauk.-prakt. onlain-seminaru (m. Kharkiv, 5 lystop. 2020 r.). Kharkiv: Pravo, 2020. S. 24–28. **10.** Kompiuter proty teroryzmu: vcheni navchyly ShI peredbachaty terakty po vsomu svitu. URL: https://focus.ua/uk/digital/489637-kompyuter-protiv-terrorizma-uchenye-nauchili-ii-predskazyvat-terakty-po-vsemu-miru. **11.** Programa de vigilância quer estudar perfis do Facebook para prever quem vai cometer crimes. URL: https://olhardigital.com.br/2021/11/17/seguranca/facebook-prever-crimes/ **12.** Strukov V. M., Uzlov D. Iu. Vykorystannia shtuchnoho intelektu u pravookhoronnii sferi zarubizhnykh krain. *Dosvid SShA. Vykorystannia tekhnolohii shtuchnoho intelektu u protydii zlochynnosti:* materialy nauk.-prakt. onlain-seminaru (m. Kharkiv, 5 lystop. 2020 r.). Kharkiv: Pravo, 2020. 112 s. C. 76. **13.** González Fuster G. Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights. The European Parliaments Committee on Civil Liberties, Justice and Home Affairs. European Parliament. Brussels. July 2020. 87 p, p. 22. **14.** Yatsyna M. O., Petechel O. Iu. Rol neuriadovykh orhanizatsii u vprovadzhenni tekhnolohii shtuchnoho intelektu u protydii zlochynnosti. *Vykorystannia tekhnolohii shtuchnoho intelektu u protydii zlochynnosti:* materialy nauk.-prakt. onlain-seminaru (m. Kharkiv, 5 lystop.2020 r.). Kharkiv: Pravo, 2020. S. 108–111.

Kostyuk O. **The role of social networks in combating crimes against the fundamentals of national security**

Introduction. *Defining the role of the media in combating crimes in general and crimes against national security in particular is extremely relevant today. In this context, it is equally important to study the criminological potential of social networks. An analysis of scientific sources shows that there is currently a somewhat simplified description of the relationship between the media and the Internet. Authors mostly define the classification of media as print media, television and the Internet, which is usually understood as electronic media, at most author's blogs. There are also more extensive classifications of online media, which, however, remain simplified and do not reflect the full range of tools available today.*

The aim of the article. Disclosure of aspects of the use of social networks in combating crimes against the foundations of national security.

Results. *Given the importance of social networks, it is on them, and not on the traditional media, that attention should be focused on the issues of forecasting and combating crimes in general and crimes against the foundations of national security of Ukraine, in particular. At the same time, appropriate actions should be taken not only by law enforcement agencies, but also by civil society, which includes not only users of social networks, but also their owners..*

Conclusions. *A separate modern direction of combating crime with the use of social networks is the analysis of data contained in them. This requires the creation, adjustment and improvement of algorithms for analyzing user activity.*

Key words: *national security, mass media, social networks, crime prevention, crime forecasting.*