КРИМІНАЛЬНЕ ПРАВО; КРИМІНАЛЬНИЙ ПРОЦЕС

Бугера О. І.,
доктор юридичних наук, доцент,
професор кафедри конституційного та адміністративного права
Національного транспортного університету

УДК 343.9
DOI https://doi.org/10.32845/2663-5666.2022.1.12

ЗАПОБІГАННЯ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ РОЗВИТКУ СОЦІАЛЬНИХ ІНТЕРНЕТ-МЕРЕЖ

Постановка проблеми. Соціальні Інтернет-мережі займають значну частину сектора комунікаційних відносин суспільства. Так, з початку 2020-го до початку 2021 року українська аудиторія соціальних мереж збільшилася з 19 до 26 мільйонів користувачів. Найпопулярнішою соцмережею в Україні залишається YouTube з охопленням 96 % користувачів. У середньому на сайті вони проводять майже 40 хвилин на день. Також із 2019 року кількість українців в Instagram зросла на 22 %, а у Facebook – на 7 %. Нині цими соцмережами користуються 14 і 16 мільйонів українців відповідно. За останній рік також нова соціальна мережа TikTok досягла 16 % користувачів (зростання становило 500 %) [1].

Необхідно зазначити, що у сучасних умовах розвитку інформаційних технологій та побудови інформаційного суспільства, взаємодія користувачів соціальних Інтернет-мереж, стає не лише засобом комунікації, а й новою сферою життєдіяльності. Нині соціальні Інтернет-мережі стають все більш масовим, найбільш поширеним засобом комунікації та реалізації конституційних прав окремих громадян. Користувачі активно та всебічно взаємодіють між собою, що призводить до накопичення великої кількості інформації, яка може мати, у тому числі, й неправомірний характер. При цьому поява та широке поширення у вітчизняному інформаційному просторі соціальних Інтернет-мереж призвела до того, що організовані злочинні групи й окремі особи, які вчиняють протиправні діяння, стали активно використовувати широкі можливості всесвітньої мережі. Тому, соціальні мережі сьогодні є важливим джерелом криміналістичної інформації при розслідуванні злочинів, у тому числі й кіберзлочинів [2, с. 142], а також інструментом для запобігання організованій злочинності.

Це питання було і залишається актуальним для України, оскільки у 2020 році поліція знешкодила 353 організованих груп (у 2019 році – 275). До кримінальної відповідальності притягнуто майже півтори тисячі учасників цих груп, які вчинили понад 3,5 тисяч злочинів (500 осіб узято під варту) [3].

Аналіз останніх досліджень і публікацій. Окремі питання використання соціальних Інтернет-мереж для запобігання злочинності, виявлення та розслідування злочинів досліджували такі вчені, як: В. М. Бутузов, В. Д. Гавловський, О. Ф. Гіда, О. В. Косолап, Д. М. Цехан, В. М. Шевчук, В. П. Шеломенцев, О. Ю. Юрченко та ін. Однак, враховуючи процес постійного розширення можливостей соціальних Інтернет-мереж та збільшення кількості їх користувачів, необхідним є проведення наукових досліджень щодо удосконалення шляхів використання вказаних мереж для запобігання організованій злочинності та підвищення рівня її прогнозування.

Метою статті є розгляд шляхів використання соціальних Інтернет-мереж для запобігання організованій злочинності та розроблення відповідних пропозицій щодо удосконалення цієї діяльності.

Виклад основного матеріалу. В Стратегії боротьби з організованою злочинністю [4] вказується, що відсутність системного підходу до ведення боротьби з організованою злочинністю, неналежний рівень взаємодії правоохоронних органів у відповідній сфері, застаріле та розбалансоване нормативно-правове забезпечення з питань боротьби з організованою злочинністю, недосконаліть процедури моніторингу криміногенної ситуації, відсутність консолідованої об'єктивної методології оцінки загроз організованої злочинності, використання застарілих форм і методів боротьби з таким явищем

призводить до загострення проблем, пов'язаних з організованою злочинністю, та низького рівня ефективності боротьби з нею. При цьому запобігання організованій злочинності та боротьба з організованими злочинними угрупованнями у сферах з високим ризиком її прояву повинна здійснюватися, шляхом посилення спроможності державних органів, що беруть участь у боротьбі з організованою злочинністю, щодо протидії кіберзлочинності, реагування на стрімкий розвиток фінансових та інформаційних технологій, поглиблення і розгалуження зв'язків на національному та міжнародному рівні, які сприяють комунікації організованих злочинних угруповань.

Питання запобігання організованій злочинності в умовах розвитку соціальних Інтернет-мереж потребує особливої уваги правоохоронних органів, оскільки має дві складові: по-перше, організовані злочинні угруповання почали все активніше використовувати в своїй злочинній діяльності технологічні досягнення у галузі інформаційно-комунікаційних технологій (в т. ч. з використанням можливостей мережі Інтернет); по-друге, найбільш оптимальним шляхом запобігання організованій злочинності у вказаних умовах є технологічне переоснащення правоохоронних органів та розроблення відповідних методик щодо використання соціальних Інтернет-мереж для здійснення запобіжної діяльності. При цьому важливим є дослідження ризиків використання соціальних Інтернет-мереж зі злочинною метою, і зокрема щодо: координації злочинних дій; підбору нових членів злочинних угрупувань, їх оповіщення для уникнення покарання; моніторингу інформації для виявлення потенційних жертв злочинів та ін. Особливо небезпечною є тенденція щодо використання злочинними угрупуваннями соціальних Інтернет-мереж для пропаганди кримінальної субкультури.

Необхідно зазначити, що соціальні Інтернет-мережі можуть також використовуватись злочинцями для здійснення терористичної діяльності. Зокрема, відповідно до статті 1 Закону України «Про боротьбу з тероризмом» [5] терористична діяльність, це діяльність, яка охоплює: планування, організацію, підготовку та реалізацію терористичних актів; вербування, озброєння, підготовку та використання терористів; пропаганду і поширення ідеології тероризму; фінансування та інше сприяння тероризму.

Відкриття необмеженої кількості нових профілів, публічних сторінок чи спільнот, тематичний пошук будь-якого контенту (аудіо, відео, тексти) – усе це значно полегшує діяльність терористичної організації порівняно зі створенням власного веб-сайту. Соцмережі фактично дозволяють «постукати у двері» цільової аудиторії, тоді як власний онлайн-ресурс потребує довгих днів, а іноді навіть і місяців очікування на читачів [6].

При цьому широка доступність та анонімність Інтернету поруч зі швидким поширенням соціальних мереж використовується терористичними угрупованнями для збору коштів у своїх прихильників по всьому світі. Також терористичні організації широко використовують соціальні мережі та Інтернет для ведення пропаганди тероризму та встановлення контактів з прихильниками.

Часто збір коштів для підтримки тероризму й екстремізму здійснюється під виглядом законної благодійної або гуманітарної діяльності, і навіть створюються благодійні організації з цією метою. Збір грошових коштів може здійснюватися таємно або під прикриттям надання гуманітарної допомоги [7].

Необхідно зазначити, що важливою проблемою соціальних Інтернет-мереж є те, що вони можуть використовуватись для різноманітних маніпуляцій. За оцінками аналітиків, загальний відсоток фейкової активності у соціальних мережах може становити 10 – 30 % від усіх «лайків», репостів та переглядів. Директор Центру стратегічних комунікацій НАТО Яніс Сартс зазначає, що найбільш захищеною від маніпуляцій є соціальна мережа Twitter. Другою за захищеністю є соціальна мережа Facebook. Мережа Instagram, яка передбачає публікацію фотознімків, та популярний відеохостинг YouTube є недостатньо захищеними від маніпуляцій. Найменш захищеною мережею від маніпуляцій серед тих, що досліджувались експертами НАТО, є TikTok, що базується на публікації коротких відеороликів [8].

Необхідно зазначити, що для правоохоронних органів соціальні Інтернет-мережі є цінним джерелом криміналістичної інформації, яка може орієнтувати слідчого для прийняття тактичних рішень при розслідуванні кіберзлочинів. Криміналістична інформація у соціальній Інтернет-мережі являє собою сукупність даних, повідомлень та відомостей, про джерела й механізм виникнення ідеальних та матеріальних слідів, що мають відношення до злочинної події, отримані в мережі Інтернет із застосуванням спеціальних засобів, з метою встановлення обставин

злочинної події у кримінальному провадженні. Криміналістичне дослідження інформації соціальних Інтернет-мереж відбувається у декілька етапів: 1) пошук та виявлення інформації; 2) збір; 3) зняття інформації; 4) дослідження інформації. Способами збору інформації із соціальних мереж є такі: а) інформаційно-аналітична робота; б) запити; в) використання спеціальних програм; г) створення «фейкових» сторінок та ін. Важливого значення набуває інформаційно-аналітична робота по збору інформації про користувачів таких соціальних мереж. Така діяльність надає змогу отримати важливі дані для викриття осіб, які займаються неправомірною діяльністю. Інформаційно-аналітичний аналіз профілів соціальних Інтернет-мереж допомагає скласти соціально-психологічну характеристику особи користувача та з'ясувати його коло друзів та контакти. Вивчення анкет у соціальних Інтернет-мережах надає досить різноманітну інформацію, що може відображати інтереси, вподобання та коло друзів особи. Також власник профілю у соціальній мережі нерідко відмічає плани та події, що бажає відвідати. Така інформація дає можливість оперативним працівникам передбачити поведінку особи правопорушника та місце її знаходження [2, с. 143–145].

Також аналіз інформації, що міститься в соціальних Інтернет-мережах дозволяє завчасно виявляти підготовку до здійснення масових заворушень. Зокрема, дослідники з Університету Кардіффа («Cardiff University» – один із провідних університетів Великої Британії) продемонстрували здатність розробленого програмного забезпечення прогнозувати масові акції та інші події значно швидше, ніж їх виявляла поліція, з випередженням до однієї години. Для цього дослідники вивчили інформацію про заворушення в Лондоні 2011 року та створили програмне забезпечення для автоматичного сканування Twitter і визначення (прогнозування) потенційно небезпечні події. Розроблена система може аналізувати будь-яку інформацію в Twitter і визначати де і коли існує найбільша ймовірність виникнення заворушень та повідомляти в реальному часі інформацію про великі скупчення людей. Для цього було використано низку алгоритмів машинного навчання, щоб проаналізувати 1,6 мільйона повідомлень у Twitter. Система враховувала час і місце публікації повідомлень, а також їхній зміст. Важливо звернути увагу на тенденцію зростання можливостей соціальних мереж щодо збору та трансляції відео-контенту в реальному масштабі часу. Це дозволяє підвищити рівень ефективності розвідки в соціальних мережах – «social media intelligence» або «SOCMINT». При цьому особливістю соціальних мереж є те, що через них негативний інформаційний вплив часто здійснюється приховано і має тривалий характер до моменту свого виявлення та «включення» важелів протидії [9].

Як вказує зарубіжний досвід, соціальні Інтернет-мережі надають поліцейським у всьому світі нові шляхи та інструменти для розкриття злочинів. Зокрема, моніторинг кримінологічно значимої інформації в соціальних мережах та її аналіз дозволяє поліції суттєво підвищити рівень запобіжної діяльності та прогнозної аналітики. Зокрема, за останні роки значно розширилось програмне забезпечення моніторингу соціальних медіа. Наприклад, аналітична платформа Geofeedia, яка використовується поліцією США, аналізує публікації в соціальних мережах пов'язуючи їх з географічним розташуванням [10].

При цьому для ефективного використання можливостей соціальних Інтернет-мереж для запобігання організованій злочинності необхідним є підготовка відповідного рівня фахівців. Перші кроки в цьому напрямі вже зроблені. Так, в Національній академії внутрішніх справ освітній процес доповнено новим курсом – «Інформаційно-аналітична підтримка підрозділів кримінальної поліції». Майбутніх оперативників навчатимуть використовувати можливості сучасних інформаційних технологій у протидії злочинності. Зокрема, користуватися технологіями ILP (Intelligence-led Policing, поліцейська діяльність, керована аналітикою) та OSINT (Open Source Intelligence, розвідка з відкритих джерел інформації); програмним засобом Belkasoft як інструментарієм для збирання, обробки й аналізу електронних (цифрових) доказів з мережі Інтернет, персональних комп'ютерів, мобільних пристроїв; програмним продуктом ArcGIS для геоінформаційного відображення оперативної інформації на електронних картах місцевості. Також навчатимуть пошуку й аналізу оперативної інформації, необхідних документів та зображень у поверхневій (SurfaceWeb), глибинній (DeepWeb) і темній (DarkWeb) частинах мережі Інтернет, у соціальних мережах, державних реєстрах та інформаційних системах, системах електронного банкінгу тощо. Застосування сучасних технологій – це швидка аналітика, компонування

й підготовка інформації, отриманої з різних джерел, наприклад, трафіків і моніторингу телефонних розмов, відеоспостереження, перетину кордону, відомостей з інших баз даних, мережі Інтернет. Це – створення з масиву інформації, отриманої на законних підставах, аналітичного продукту, який можна використовувати як доказову базу під час розкриття злочинів [11].

Таким чином, використання інформації соціальних Інтернет-мереж має не лише важливе практичне значення у протидії кіберзлочинності, а й нині є одним із пріоритетних напрямків діяльності органів правопорядку, спрямованих на оптимізацію кримінального провадження. У реаліях сьогодення соціальні Інтернет-мережі, з одного боку, виступають важливим засобом зв'язку, який дозволяє користувачам таких мереж здійснювати право на свободу думок та їх вільне вираження, а з іншого боку, вони є своєрідною публічною інфраструктурою масиву даних (інформації), яка є цінним джерелом криміналістичної інформації, що має значення при розслідуванні кіберзлочинів. Як свідчить практика, при розслідувані таких злочинів виникає низка проблемних питань, пов'язаних із криміналістичним забезпеченням розслідування, використанням новітніх технологій, залученням спеціалістів, оптимізаціє процесу збору, дослідження та подальшого використання такої інформації тощо. Такий напрям дослідження суттєво впливає на підвищення ефективності слідчої та судової діяльності та безперечно буде забезпечувати її оптимізацію [2, с. 145]. Це також сприятиме побудові ефективної системи запобігання організованій злочинності.

Висновки. Розвиток інформаційно-комунікаційних технологій на основі можливостей мережі Інтернет, з одного боку надає підстави говорити про формування якісно нового комунікаційного рівня суспільства, з іншого вимагає від правоохоронних органів врахування ризиків використання соціальних Інтернет-мереж зі злочинною метою та здійснення відповідних запобіжних заходів. Для цього доцільним є задіяння власне можливостей самих соціальних Інтернет-мереж, як інструменту запобігання злочинності (в т. ч. такому її прояву як організована злочинність), що передбачає, насамперед: моніторинг кримінологічно значимої інформації, її аналіз для подальшого прогнозування злочинності, розроблення відповідних планових запобіжних заходів; забезпечення комунікації між правоохоронними органами і громадськістю з питань запобігання злочинності, і зокрема, щодо оперативного надання громадянами інформації про вчинені злочини, свідками яких вони стали; розміщення інформації для розшуку осіб та ін. Це потребує технологічного переоснащення правоохоронних органів (у тому числі, в частині удосконалення програмного забезпечення моніторингу соціальних Інтернет-мереж), підвищення рівня підготовки кадрів та удосконалення законодавчого забезпечення. Перспективи подальших досліджень з цього питання полягають у формуванні на основі вітчизняного та зарубіжного досвіду новітньої, концептуально цілісної системи наукових знань, спрямованої на формування криміналогічних засад використання мережі Інтернет для запобігання злочинності в умовах постійного оновлення та удосконалення інформаційно-комунікаційних технологій та розвитку процесу цифровізації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кондратенко М. За рік карантину кількість українців у соцмережах зросла на сім мільйонів. URL: https://www.dw.com/uk/za-rik-karantynu-kilkist-ukraintsiv-u-sotsmerezhakh-zrosla-na-sim-milioniv/a-56899697 (дата звернення: 21.01.2022).

2. Шевчук В. М. Використання інформації із соціальних інтернет-мереж при розслідуванні кіберзлочинів: криміналістичні проблеми (с. 142–145). *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. Таційй, Ю. Г. Барабаш, Б. М. Головкін, О. В. Таволжанський. Харків: Право, 2019. 176 с. URL: https://dspace.nlu.edu.ua/bitstream/123456789/17042/1/Shevchuk_142-146.pdf (дата звернення: 21.01.2022).

3. Звіт Національної поліції України про результати роботи у 2020 році. URL: https://www.kmu.gov.ua/storage/app/sites/1/ 17-civik-2018/ zvit2020/npu-zvit 2020.pdf (дата звернення: 21.01.2022).

4. Стратегія боротьби з організованою злочинністю: схвалено розпорядженням Кабінету Міністрів України від 16 вересня 2020 р. № 1126-р. URL: https://zakon.rada.gov.ua/ laws/ show/ 1126-2020-%D1%80#Text (дата звернення: 21.01.2022).

5. Про боротьбу з тероризмом: Закон України від 20 березня 2003 року № 638-IV. *Відомості Верховної Ради України*, 2003, № 25, ст.180. URL: https://zakon.rada.gov.ua/laws/show/638-15#Text (дата звернення: 21.01.2022).

6. Авдєєва Т. Вибуховий контент онлайн. . URL: https://cedem.org.ua/ analtics/ vybuhovyj-kontent-onlajn/ (дата звернення: 21.01.2022).

7. Схеми: Використання збору коштів для фінансування тероризму із застосуванням соціальних мереж. URL: https://finmonitoring.in.ua/vikoristannya-zboru-koshtiv-dlya-finansuvannya-terorizmu-iz-

zastosuvannyam-socialnix-merezh/ (дата звернення: 21.01.2022).

8. Огляд подій у сучасному кіберпросторі за II квартал 2021 року. URL: https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/28072021/Bulltn_NCK_II.pdf (дата звернення: 21.01.2022).

9. Попова Т. Соціальні мережі, кібератаки та гібридні війни. URL: https://www.radiosvoboda.org/a/28598299.html (дата звернення: 21.01.2022).

10. Jaevon George. The Use of Social Media Surveillance for Police Organizations. URL: https://www.linkedin.com/pulse/use-social-media-surveillance-police-organizations-jaevon-george (дата звернення: 21.01.2022).

11. У НАВС навчатимуть «цифрових оперативників». URL: https://www.naiau.kiev.ua /news/ u-navs-navchatimut-cifrovih operativnikiv.html? fbclid=IwAR3hXNUn2serXOM6B3a4UmQdXcFSCfEgzeqIJjVN1bqQmNHAgCoiZcqqZxI (дата звернення: 21.01.2022).

Бугера О.І. ЗАПОБІГАННЯ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ В УМОВАХ РОЗВИТКУ СОЦІАЛЬНИХ ІНТЕРНЕТ-МЕРЕЖ

Метою статті є розгляд шляхів використання соціальних Інтернет-мереж для запобігання організованій злочинності та розроблення відповідних пропозицій для удосконалення цієї діяльності. Зазначено, що в Україні, спостерігається зростання випадків використання соціальних Інтернет-мереж організованими злочинними угрупуваннями для координації злочинних дій; підбору нових членів злочинних угрупувань, їх оповіщення для уникнення покарання; пропаганди кримінальної субкультури та ін. Наголошено, що в Стратегії боротьби з організованою злочинністю вказується, що запобігання організованій злочинності та боротьба з організованими злочинними угрупованнями повинна здійснюватися, шляхом реагування на стрімкий розвиток фінансових та інформаційних технологій. Встановлено, що запобігання організованій злочинності в умовах розвитку соціальних Інтернет-мереж може здійснюватись за такими напрямами, як: моніторинг кримінологічно значимої інформації, її аналіз для подальшого прогнозування злочинності; забезпечення комунікації між правоохоронними органами і громадськістю з питань безпеки; створення умов для оперативного надання громадянами інформації про вчинені злочини, свідками яких вони стали; розміщення інформації для розшуку осіб та ін. Зазначено, що важливою умовою ефективного запобігання організованій злочинності в умовах розвитку соціальних Інтернет мереж є технологічне переоснащення правоохоронних органів, підвищення рівня кваліфікації працівників та удосконалення законодавчого забезпечення. Визначено, що перспективи подальших досліджень з цього питання полягають у формуванні на основі вітчизняного та зарубіжного досвіду новітньої, концептуально цілісної системи наукових знань, спрямованої на формування кримінологічних засад використання мережі Інтернет для запобігання злочинності.

Ключові слова: організована злочинність, запобігання, соціальні Інтернет-мережі, моніторинг кримінологічно значимої інформації, прогнозування злочинності.

Bugera O.I. PREVENTION OF ORGANIZED CRIME IN THE CONDITIONS OF DEVELOPMENT OF SOCIAL INTERNET NETWORKS

The purpose of the article is to consider ways to use social Internet networks to prevent organized crime and to develop appropriate proposals to improve this activity. It is noted that in Ukraine, there is an increase in the use of social Internet networks by organized criminal groups to coordinate criminal activities; selection of new members of criminal groups, their notification to avoid punishment. Particularly dangerous is the tendency for criminal groups to use social Internet networks to promote the criminal subculture. It is emphasized that the Strategy for Combating Organized Crime indicates the lack of a systematic approach to combating organized crime, inadequate level of cooperation between law enforcement agencies in this area, outdated and unbalanced legal framework for combating organized crime, imperfect monitoring procedure the lack of a consolidated objective methodology for assessing the threat of organized crime, the use of outdated forms and methods of combating this phenomenon exacerbates the problems associated with organized crime and the low level of effectiveness in combating it. At the same time, the prevention of organized crime and the fight against organized crime in areas at high risk should be carried out by strengthening the capacity of government agencies involved in the fight against organized crime to combat cybercrime, respond to the rapid development of financial and information technology. and branching out links at the national and international levels that facilitate the communication of organized crime groups. It is established that the prevention of organized crime in the development of social Internet networks can be carried out in such areas as: monitoring of criminologically relevant information, its analysis for further prediction of crime; ensuring communication between law enforcement agencies and the public on security issues; creating conditions for the prompt provision of information by citizens about the crimes they have witnessed; placement of information for search of persons, etc. It is emphasized that the use of information from social Internet networks is not only important in practice in combating cybercrime, but also is now one of the priorities of law enforcement agencies aimed at optimizing criminal proceedings. It is noted that an important condition for effective prevention of organized crime in the development of social Internet networks is technological re-equipment of law enforcement agencies (including the development of software for monitoring social Internet networks), improving the skills of employees and improving legislation. It is determined that the prospects of further research on this issue are to form on the basis of domestic and foreign experience of the latest, conceptually integrated system of scientific knowledge aimed at forming criminological principles of using the Internet to prevent crime, and in particular the possibilities of social Internet networks to monitor criminologically significant information.

Key words: organized crime, prevention, social Internet networks, monitoring of criminologically significant information, crime forecasting.