ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

УДК 354.42/.44 681.142.37

Гавловський Владислав Данилович – старший науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України, кандидат юридичних наук

Щодо використання соціальних мереж для виявлення, розкриття та попередження злочинів

У статті проведено аналіз низки актуальних на сьогодні питань, пов'язаних із створенням державного механізму протидії деструктивному використанню соціальних мереж злочинними елементами. У практичному аспекті розглянуто потенційні можливості використання такого виду інформаційних мереж для виявлення та розкриття злочинів.

Ключові слова: соціальні мережі, протидія злочинності, вчинення злочину, засоби вчинення злочину, правоохоронний моніторинг.

Постановка проблеми. Сьогодні Інтернет-аудиторія постійно збільшується та охоплює значну кількість населення нашої планети. Зокрема, із 7 млрд жителів нашої планети послугами мережі Інтернет користується 2,3 млрд людей, тобто фактично кожний третій житель Землі сьогодні має доступ до цієї мережі, при цьому, за рік кількість Інтернет-юзерів збільшилася на 11 %. Не залишається осторонь таких глобальних процесів і наша держава. Станом на жовтень 2012 року в Україні налічувалось 19,7 млн регулярних користувачів Інтернету серед населення віком старше 15 років. Інакше кажучи, сьогодні доступ до мережі Інтернет має половина мешканців України, з яких майже 50 % є користувачами соціальних мереж [1].

При цьому, поряд із незаперечними позитивними рисами користування, соціальним мережам притаманні також негативні, зокрема: значне марнування часу, в тому числі й робочого; створення передумов

до витоку конфіденційної інформації; виникнення психологічної залежності та шкоди здоров'ю; інтелектуальна деградація, заміна реального міжособистісного спілкування віртуальним, сімейні негаразди, інформаційно-психологічний вплив тощо.

Крім того, удавана анонімність користувачів, фактична відсутність географічних кордонів у мережі Інтернет і її технічні можливості створюють майже ідеальні умови для вчинення злочинів.

Актуальність дослідження. Аналізуючи нові загрози для користувачів соціальних мереж, необхідно констатувати, що, такі мережі вже тривалий час активно використовуються злочинцями як засіб, знаряддя чи місце вчинення як "традиційних" злочинів, так і злочинів у сфері високих технологій. Останнім часом отримали розповсюдження такі злочинні дії як "крадіжка особистості", під якою розуміють діяння, коли протиправно вилучаються та (або) використовуються персональні дані людини з метою незаконного отримання матеріальної вигоди чи інших протиправних діянь [2]. Однією з причин виникнення деструктивних процесів у соціальних мережах є те, що становлення та розвиток суспільних відносин у цьому новому інформаційному середовищі достатньо не врегульовані ні відповідними нормативними актами, ні моральними устоями суспільства. Отже, наразі розробка засад організаційно-правової протидії злочинності у соціальних мережах для нашої держави, де на відміну від низки провідних зарубіжних країн, цей вид правоохоронної державної діяльності практично відсутній, видається безумовно актуальною.

Аналіз останніх публікацій за темою дослідження. Дослідженням окремих аспектів організаційно-правової протидії вчиненню злочинів з використанням специфічних інформаційних можливостей соціальних мереж займались: В. М. Бутузов, В. М. Горовий, А. І. Марущак, В. П. Шеломенцев, О. М. Юрченко та інші, низка наукових праць за вказаною проблематикою належить також і автору представленої статті.

Однак, на сьогодні залишаються остаточно невирішеними теоретичні, практичні та організаційно-правові питання, пов'язані з використанням правоохоронними органами можливостей соціальних мереж безпосередньо для виявлення, розкриття та попередження злочинів.

Отже, **метою представленої праці** є дослідження практичних та організаційно-правових питань, пов'язаних не тільки із використанням злочинцями соціальних мереж для вчинення своїх деструктивних дій, а і в контексті розробки та створення механізмів застосування співробітниками-правоохоронцями соціальних мереж для виявлення, розкриття та попередження злочинів.

Виклад основного матеріалу. Слід зазначити, що інформація стає головним товаром Інтернет-економіки. За прогнозами Boston Consulting, через вісім років частка Інтернет-послуг у ВВП єврозони досягне 8 %,

і більша частина буде припадати на збір і аналіз персональних даних, які сьогодні приносять Інтернет-компаніям понад 300 млрд євро на рік. Європейські компанії наразі заробляють на кожному користувачі близько 1 тис. євро.

Ринок цей росте не тільки бурхливо, але й безконтрольно. Єврокомісія, наприклад, зараз розслідує, як саме Google і Facebook використовують особисті дані відвідувачів [3].

Усе більшого поширення набуває спеціальний вид шахрайства, що характеризується використанням соціальних мереж та Інтернет-магазинів (наприклад, Ebay). При цьому злочинці використовують надзвичайно просту технологію, аналогічну розповсюдженню спаму. Так, викравши дані користувача, або "впровадивши" на його сторінку удаваних друзів, зловмисники заманюють "друзів" користувача, які нічого не підозрюють, на сайти Інтернет-магазинів, які спеціалізуються на обмані клієнтів. Це спрацьовує, так як довіра до "друзів" у соціальних мережах є досить значною.

Варто звернути увагу, що зловмисники із соціальних мереж використовують у своїх цілях найрізноманітнішу інформацію. Наприклад, користувач повідомляє в мережі, що його не буде певний час вдома, цим можуть скористатися зловмисники при вчиненні квартирної крадіжки, угону автотранспорту тощо [1, С. 258].

Соціальні мережі нерідко використовуються також при підготовці та вчиненні особливо тяжких злочинів корисливо-насильницької спрямованості. Прикладом може слугувати злочинна діяльність жительки Московської області Ю. Печеневої, яка в соціальних мережах розшукувала своїх двійників – одиноких жінок, зовні схожих на неї, зближалася з потенційними жертвами, знаходила спільні інтереси і дізнавшись про подробиці життя майбутньої жертви, напрошувалася в гості, а приїхавши, вбивала господинь, за їх паспортами оформляла кредити, а їхні квартири продавала [4].

Також екстремістські та терористичні організації для здійснення своєї деструктивної діяльності активно використовують мережу Інтернет і, зокрема, соціальні мережі, які виступають засобом зв'язку, вербування, координацією при підготовці терактів, центром навчання методам конспірації та терору, джерелом отримання інформації про способи виготовлення сильнодіючих отруйних речовин, виготовлення саморобних вибухових пристроїв і т. ін.

Варто зазначити, що сьогодні практично вся інформаційна діяльність терористичних угруповань перенесена у віртуальний світ. Це пов'язано з тим, що працювати там більш безпечно, ніж у традиційних ЗМІ. Головною причиною успіху застосування терористичними організаціями Інтернет-технологій є складність виявлення і ліквідації мережевих центрів.

У соціальних мережах люди знаходять один одного, знайомляться, спілкуються, беруть участь у обговореннях і об'єднуються в групи по інтересах. Проте інтереси в усіх різні. І один із самих небезпечних "інтере-

сів" – наркотики – не обійшов соціальні мережі. Користувачі соціальних мереж активно створюють групи, які пропагують наркоманію. В таких групах пропонують наркотики, радять, де краще їх придбати, вказують ціни й адреси наркоторговців, виступають за легалізацію наркотиків, усіляко підтримують новачків, друкують статті про наркотики – історію, вплив, властивості, способи виготовлення. До речі, статті написані науковою мовою з посиланням на певні факти і статистичні дані. Тобто, їх готують фахівці, завданням яких є цілеспрямована явна чи завуальована пропаганда наркотиків у соціальних мережах.

Останнім часом усе частіше кіберпростір використовується для цькування опонентів. Особливу занепокоєність викликає кібер-буллінг (кібер-знущання) – це одна із форм залякування, переслідування, насильства, цькування дітей та підлітків з використанням інформаційно-телекомунікаційних технологій – електронної пошти, сервісів миттєвих повідомлень, чатів, соціальних мереж, веб-сайтів, а також мобільного зв'язку.

Кібер-буллінг включає цілий спектр форм поведінки, на мінімальному полюсі якого – жарти, які не сприймаються всерйоз, на радикальному ж – психологічний віртуальний терор, який завдає непоправної шкоди, призводить до суїцидів. Сьогодні навіть з'явилося нове поняття – булліцид – загибель жертви внаслідок буллінгу.

Прикладом буллінгу може бути випадок, що стався на Закарпатті, де школярі зацькували у соціальній мережі свою однокласницю – 14-річну А. Фіцай до самогубства [5].

Особливу занепокоєність викликає те, що за даними фонду Internet Watch Foundation, Україна посідає 7-ме місце у світі за розповсюдженням дитячої порнографії у всесвітній мережі. За даними Інтерполу, український ринок порнографічної продукції оцінюється у 100 млн дол. на рік. У соціальних мережах циркулює близько 12 млн одиниць контенту, що містять дитячу порнографію [6].

Необхідно також констатувати, що кількість злочинів, учинених із використанням інформації, викраденої із соціальних мереж, постійно збільшується. Крім того, аналітики вважають, що однією з причин зростання кількості таких злочинів є збільшення кількості дітей, підлітків і молоді у соціальних мережах. На жаль, вони погано уявляють собі наслідки відкритості та гіперкомунікативності.

Характерною ознакою реальності небезпеки є результати дослідження, проведені Інтернет-провайдером TalkTalk, згідно з яким, кожна двадцята дитина у віці 6–15 років спілкувалася з незнайомцями через веб-камеру, а кожна п'ятдесята зустрічалася з незнайомцем особисто після спілкування з ним у мережі Інтернет [1, С. 259].

Представник компанії "Київстар" зазначила, що згідно з проведеним ними дослідженням, 40 % українських дітей викладають особис-

ту інформацію про себе і свою родину в соціальних мережах, а 60 % дітей знайомляться в реальному світі зі своїми віртуальними друзями без відома батьків [7].

До речі, у червні п. р. Україна ратифікувала "Конвенцію Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства, підписану від імені України 14 листопада 2007 року в м. Страсбурзі.

Отже, Інтернет наповнюється протиправним контентом і використовується з метою протиправної діяльності. Хоча не можна стверджувати, що соціальні мережі здебільшого використовуються в протиправних цілях, однак, тим не менш, очевидно, що зі збільшенням загальної кількості користувачів потенційні можливості правопорушників, а так само їх зацікавленість у протиправному деструктивному використанні соціальних мереж багаторазово зростають. З цим треба боротися. Ми коротко розглянемо досвід окремих країн у протидії цій протиправній діяльності.

Протидія правопорушенням, що вчиняються з використанням соціальних мереж, за кордоном ведеться державними органами, комерційними структурами, громадськими організаціями та громадянами.

Так, у Росії почав працювати сайт з реєстром протизаконних сайтів у Рунеті – www. zapret-info. gov. ru/. До чорного списку тільки після перевірки інформації про те, що на них розміщено протиправну інформацію будуть вноситись сайти, які містять інформацію про наркотики, дитячу порнографію та заклики до суїциду. Вони будуть блокуватися в досудовому порядку, якщо суспільно небезпечна інформація не буде з них вчасно видалена. Крім того, до реєстру потраплять сайти, за якими було винесено судове рішення про порушення.

Створювати і поповнювати цей список сайтів буде Роскомнагляд, приймати рішення про включення до реєстру сайтів зможуть також МВС РФ, Федеральна служба з контролю за обігом наркотиків і Росспоживнагляд.

Якщо власник сайту через добу після звернення провайдера не видалить інформацію, мережеві дані ресурсу потраплять до реєстру, і провайдер повинен буде заблокувати доступ до цього сайту. При цьому блокування за IP-адресою буде крайнім заходом [8].

Показово, що у перші ж дні на сайт надійшло майже 7 тис. звернень, з них уповноваженим органам передано 287: у Федеральній службі РФ з контролю за обігом наркотиків наразі розглядається 199 таких звернень. Росспоживнагляд отримав для експертизи 72 звернення про пропаганду самогубств, а експерти Роскомнагляду вже розглянули і дали позитивні висновки по 17 зверненнях про поширювану в мережі Інтернет дитячу порнографію [9].

У Південній Кореї, де сьогодні найбільша кількість випадків суїциду (щодня близько 40 осіб вчиняють самогубство) влада сформува-

ла спеціальну групу експертів з Інтернет, понад 100 осіб, яким належить шукати суїцидально налаштованих користувачів соціальних мереж і сайти, які спонукають людей до таких актів [10].

В Австралії ще в 2007 році озвучили план установки Інтернет-фільтрів, які повинні були боротися зі сценами жорстокості, детальними інструкціями по вчиненню злочинів або терористичних актів і вживанню наркотиків. Але плани австралійської влади викликали критику з боку правозахисників, які вважали, що Інтернет-фільтри призведуть до появи цензури в країні.

Тому було прийнято рішення, що замість введення обов'язкових Інтернет-фільтрів місцеві провайдери заблокують 1400 сайтів з дитячою порнографією [11].

У той же час, необхідно констатувати, що державними органами окремих країн під приводом боротьби зі злочинами у кіберпросторі робляться спроби законодавчого закріплення засобів, що порушують права людини, а також міжнародне законодавство.

Зокрема, в Нідерландах міністр безпеки та юстиції І. Опстелтен представив у листі парламенту план по створенню законопроекту щодо збору доказів у процесі розслідування кіберзлочинів. А саме, новий закон повинен дати право слідчим встановлювати шпигунське програмне забезпечення на комп'ютери підозрюваних, а також здійснювати "обшук" цих комп'ютерів у дистанційному режимі. Слідчі мають отримати право на знищення шкідливого контенту, такого, наприклад, як дитяча порнографія, якщо знайдуть його під час "обшуку".

Проте, цей закон планує надати слідчим повноваження здійснювати вищевказані дії на комп'ютерах не тільки всередині країни, але й за кордоном – за умови, якщо місце розташування комп'ютера встановити їм не вдалося. Це небезпечне формулювання, оскільки через мережу Інтернет місце розташування будь-якого комп'ютера неможливо встановити із стовідсотковою точністю.

На думку голландських правозахисників, це створить прецедент, а інші країни можуть прийняти аналогічне законодавство, і тоді в мережі Інтернет розпочнеться справжнє свавілля. Хоча експерти вказують, що подібний прецедент уже мав місце з боку США при застосуванні кіберзброї за кордоном [12].

Прикладом участі громадських організацій у пошуку в мережі Інтернет контенту, який може нести загрозу для молоді та підлягає кримінальному переслідуванню, може слугувати німецька організація із захисту молоді (jugendschutz. net.), що фінансується всіма федеральними землями Німеччини.

Якщо інспектори jugendschutz. net знаходять такий протиправний контент, вони намагаються зробити так, щоб його видалили якомо-

га швидше – за умови, що інтернет-провайдери готові на це. У 2011 р., за підрахунками та з ініціативи jugendschutz. net, понад 970 разів було видалено неонацистські матеріали в різних соціальних мережах.

Однак більша частина праворадикального контенту після видалення часто завантажується заново – і це той випадок, коли провайдери повинні взяти на себе відповідальність. Адже, технічно цілком можливо розпізнавати повторне завантаження ідентичних матеріалів і запобігати цьому [13].

Ще більше перспектив для протидії злочинності за допомогою засобів і знарядь із протидії злочинності, що притаманні виключно сфері кіберпростору, вже тривалий час використовуються правоохоронцями низки держав. Там правоохоронці намагаються використовувати нові технології, зокрема і ті, що отримані завдяки наявності соціальних мереж, для виявлення, розкриття, розслідування та попередження злочинів. Ними здійснюється постійний моніторинг підозрілих блогів, чатів, сайтів тощо з метою отримання оперативно вагомої для правоохоронців інформації.

Зокрема, сьогодні соціальні мережі широко використовуються правоохоронними органами зарубіжних країн як засіб для зв'язків із громадськістю, у тому числі з метою отримання криміналістично значимої інформації. Так, наприклад, співробітники районного управління внутрішніх справ Приморського району м. Санкт-Петербургу ще у листопаді 2007 року в соціальній мережі "Вконтакті" відкрили групу "Злочинність у Приморському", яка й сьогодні є досить популярною. Група містить корисну інформацію довідкового характеру, відеозаписи, на яких зафіксовано окремі злочини, фотографії осіб, оголошених у розшук, відомості про розкриті злочини. Користувачі позитивно оцінюють запровадження "поліцейської" сторінки та надають допомогу. Завдяки допомозі громадськості правоохоронцями досягнуто суттєвих результатів у встановленні місць перебування та затриманні розшукуваних осіб [14].

У Британії правоохоронці також використовують соціальні мережі як засіб зв'язків із громадськістю. Так, поліція графства Великий Манчестер створила обліковий запис мережі Twitter. У мікроблозі даного ресурсу публікують важливі повідомлення, кримінальні відомості, дані про осіб, оголошених у розшук. При цьому британські правоохоронці офіційно визнали важливу роль соціальних мереж у попередженні та розкритті злочинів і включили відповідний курс у програму підготовки молодих співробітників. У поліції переконані, що соціальні мережі можуть бути особливо корисними для розкриття злочинів, пов'язаних із вимаганням і насильством у сім'ї [15].

Усе це свідчить про перспективність використання соціальних мереж з метою протидії деструктивній діяльності.

Досить ефективним є моніторинг соціальних мереж, що проводиться новим підрозділом поліції Нью-Йорка, який було сформовано у серпні минулого року. Завданням цього підрозділу є стеження за пра-

вопорушниками в соціальних мережах. Співробітники вже заарештували близько 50 членів злочинних угруповань після спостереження за їхньою активністю в соціальній мережі Facebook [16].

Цікавими є програми, розроблені вченими для виявлення протиправних діянь і допомоги правоохоронним органам.

Так, швейцарські вчені – дослідницька група з Лабораторії аудіовізуальних комунікацій при Федеральній політехнічній школі Лозанни, розробили алгоритм, що дозволяє допомогти у роботі правоохоронцям. Використовуючи цей алгоритм, можливо точно визначати джерело суспільно небезпечної інформації, що масово тиражується в соціальних мережах. Цей метод може також використовуватися для моніторингу терористичних атак, опозиційної політичної активності, спамрозсилок, шкідливих програм і комп'ютерних вірусів.

Як стверджують вчені, цей метод можна використовувати для пошуку джерела будь-якого інформаційного сигналу в масиві даних, що циркулюють у соціальній мережі, членом якої є людина. Проаналізувавши з урахуванням фактору часу і деяких інших доступних параметрів повідомлення, надіслані всього 15–20 учасникам мережі, алгоритм відновить траєкторію поширення цієї інформації і знайде її джерело [17].

Соціальна мережа Facebook використовує в США автоматичні алгоритми сканування чатів та іншої особистої інформації користувачів з метою пошуку та раннього виявлення злочинів. Головним чином система налаштована на пошук педофілів, але вона також може бути налаштована і на пошук ознак інших злочинів, наприклад, обговорення покупки наркотиків, зброї та інших заборонених дій.

Система сканує листування та публікації користувачів Facebook і, якщо виявляє підозрілу активність, позначає профіль і повідомляє про нього спеціальному співробітникові Facebook. Цей співробітник, у свою чергу, оцінює ступінь потенційної небезпеки і в разі її наявності повідомляє про злочинця до правоохоронних органів США.

Для того, щоб особисте листування законослухняних користувачів мережі не піддавалося перевірці, система налаштована з дуже низьким відсотком "помилкових спрацьовувань".

За словами представника соціальної мережі, програмне забезпечення, використовуване для моніторингу дій користувачів, сфокусоване на діалогах між користувачами з "бідними" зв'язками.

Наприклад, якщо два користувачі не є друзями один одному або стали друзями лише недавно і при цьому в них немає спільних друзів, а інші друзі взаємодіють з користувачем і один з одним вкрай рідко, а також якщо два користувачі мають велику різницю у віці, програмний алгоритм "зацікавиться" даним зв'язком і повідомить про це вповноваженій особі Facebook.

Прикладом успішного використання системи може слугувати такий випадок: у березні цього року система звернула увагу співробітників Facebook на листування між 30-річним чоловіком і дівчинкою 13 років. У листуванні між ними регулярно фігурувало слово "секс". З листування випливало, що чоловік планував зустріти дівчинку біля її школи після занять вже наступного дня. Співробітник Facebook оперативно поінформував про це правоохоронні органи, і ті через добу заарештували чоловіка [18].

За допомогою власних програм зарубіжні правоохоронні органи та спецслужби постійно моніторять підозрілі блоги, форуми і сайти, отримуючи безліч корисної інформації. Разом з тим, якщо процес збору та обробки інформації і приносить свої плоди, то питання оперативності залишається поки відкритим. Наприклад, за даними інформагентства "Ассошіейтед Прес", велика кількість онлайн-груп джихадистів напередодні недавнього вбивства посла США в Лівії К. Стівенса обговорювали плани нападу на американські дипмісії в Лівії, Єгипті та Алжирі. Незважаючи на це, уникнути смерті чотирьох своїх дипломатів США не вдалося [19].

Досить цікавою є розробка Facebook сайту Connected To The Case для допомоги громадян поліції у розслідуваннях за допомогою краудсорсингу (англ. crowdsourcing, crowd – "натовп" і sourcing – "використання ресурсів") – рішення суспільно значущих завдань силами добровольців).

Користувачі зможуть зайти на сайт, вказавши свій акаунт у соцмережі. Сервіс буде отримувати дані з профілю в Facebook і визначати, у розслідуванні яких справ людина зможе допомогти поліції. Система заводить на кожного користувача декілька ключових міток і з'ясовує, які місця і коли він відвідував, з ким спілкувався і т. ін.

Потім система зіставляє цю інформацію з базою нерозкритих злочинів, визначаючи, по якому з них користувач міг би стати свідком. Крім того, в Connected To The Case реалізовано можливість відправити анонімне повідомлення про правопорушення [20].

Для відстеження активності в соціальних мережах у Росії розробили і використовують систему моніторингу соціальних мереж – спеціальні термінали "Призма".

Система "Призма" в реальному часі відслідковує 60 млн джерел. Вона показує динаміку позитивних і негативних відгуків у блогах на ту чи іншу подію, а також здатна будувати графіки атак ботів. При цьому відстеження тем моніторингу настроюються індивідуально.

"Призма" відслідковує в соцмедіа активності, що призводять до зростання соціальної напруженості: нагнітання безладів, протестні настрої, екстремізм та ін. [21].

Аналогічну систему розробляли і в Україні під керівництвом доктора фізико-математичних наук, професора, член-кореспондента НАН України А. В. Анісімова. Перша версія системи моніторингу активнос-

ті користувачів соціальної мережі Twitter сьогодні вже працює. Вона призначена для збору інформації про хід соціальних процесів і явищ через їх відображення в соціальній мережі Twitter. Зібрані системою статистичні дані призначені для подальшої обробки експертами. Система здатна візуалізувати зібрані дані у вигляді діаграм. Збір інформації відбувається за допомогою ключових слів і фраз.

Крім збору даних, система здатна виробляти їх первинний семантичний аналіз за шкалою полярностей: позитивний, нейтральний, негативний. Також система містить модуль кластеризації, застосовуваний для формування груп з тематично схожих текстів, що дозволяє визначати найбільш актуальні події, в рамках проведеного дослідження, на певному часовому проміжку.

На жаль, через відсутність фінансування подальшу розробку призупинено.

Сьогодні Україна перебуває осторонь цих суспільно-корисних позитивних процесів. Це пов'язано, з одного боку, із майже повною відсутністю у співробітників правоохоронних органів спеціальних інформаційно-пошукових систем, особливо контент-моніторингу, контент-аналізу, недостатньої кількості спеціалістів, підготовлених у цьому напрямку, а, з іншого, – із відсутністю нормативного закріплення прав, повноважень та обов'язків конкретних правоохоронних органів нашої держави щодо здійснення відповідних заходів протидії злочинності з використанням кіберпростору. Також слід підтримати думку про те, що однією з причин неефективного правового впливу на сучасний кіберпростір є відсталість методик і засобів практичної реалізації наявної системи правової бази правоохоронними органами [22, С. 15].

Висновки. Сьогодні, в контексті сучасного стану протиправного використання соціальних мереж, прогнозованого зростання у найближчому майбутньому кількості та суспільної небезпеки реальних і потенційних загроз, що виходять із кібернетичного простору, ми маємо констатувати, що створення ефективної системи протидії таким деструктивним явищам і локалізації відповідних загроз можливе лише через безпосереднє використання правоохоронними органами нашої держави, у взаємодії із компетентними органами інших зарубіжних країн, специфічних можливостей самих соціальних мереж. Отже, фактично йдеться, про те, що правоохоронці мають постійно використовувати у своїй діяльності в якості засобів і знарядь для виявлення, розкриття та попередження злочинів соціальні мережі.

В Україні станом на сьогодні не існує законодавства, яке б здійснювало нормативно-правове регулювання такої діяльності взагалі, та спеціальні методи "дослідження цільової аудиторії", зокрема.

На наше переконання, одним із достатньо ефективних засобів припинення протиправної діяльності, а, отже, забезпечення прав і свобод наших

громадян, повинен стати так званий правоохоронний моніторинг, функцію якого законодавець має покласти, із відповідним визначенням компетенції, на правоохоронні органи, наділені правом здійснення оперативно-розшукової діяльності, у першу чергу, на міліцію та Службу безпеки України.

Список використаних джерел

1. Кількість користувачів інтернету в Україні досягнула майже 20 мільйонів / [Електронний ресурс]. – Режим доступу :
http://blogosphere. com. ua/2012/11/01/ukrainian-internet-user-stats-2012/.
2. Гавловський В. Д. До питання захисту персональних даних у соціальних мережах / В. Д. Гавловський // Б-ба з орг. злоч. і корупцією (теорія і практика) : наук.-практ. журнал. – К. : МНДЦ при РНБО України, 2011. – № 24. – С. 252–262.
3. Персональные данные – золотая жила интернет-компаний / [Электронный ресурс]. – Режим доступа :
http://internetua. com/personalnie-dannie--zolotaya-jila-internet-kompanii.
4. Киллерша убивала своих двойников, чтобы завладеть их квартирой / [Электронный ресурс]. – Режим доступа :
http://ww. yagazeta. com/news. php? extend.2169.
5. На Закарпатье одноклассники убили девочку в Интернете / [Электронный ресурс]. – Режим доступа :
http://ua-reporter. com/novosti/115780). – 2012. – 12.04.
6. Український ринок порнографічної продукції оцінюється в 100 млн дол. на рік / [Електронний ресурс]. – Режим доступу :
http://sevlush. info/ukraina. html.
7. Україна скопіює у Росії ідею списку шкідливих сайтів / [Електронний ресурс]. – Режим доступу :
http://ua. ht. comments. ua/2012/11/06/187682/ukraina-skopiyuie-u-rosii-ideyu. html.
8. Российские власти составили "черный" список противозаконных сайтов / [Электронный ресурс]. – Режим доступа :
http://for-ua. com/world/2012/11/01/100120. html.
9. Роскомнадзор заблокировал первый сайт из реестра запрещенных / [Электронный ресурс]. – Режим доступа :
http://www. itar-tass. com/c95/564801. html.
10. Корея боротиметься із суїцидами через соціальні мережі / [Електронний ресурс]. – Режим доступу :
http://www. lenta. ru/news/2012/06/05/congressmen/.
11. Австралия отказалась от планов фильтровать Интернет / [Электронный ресурс]. – Режим доступа :
http://internetua. com/avstraliya-otkazalas-ot-planov-filtrovat-internet.
12. Голландская полиция хочет взламывать компьютеры за границей / [Электронный ресурс]. – Режим доступа :
http://internetua. com/gollandskaya-policiya-hocset-vzlamivat-kompuaterи-za-granicei.
13. Веркгойзер Н. Неонацисти все частіше використовують соцмережі для пропаганди [Электронный ресурс] / Н. Веркгойзер, К. Каплюк. – Режим доступа :
http://www. dw. de/dw/article/0,,16091158,00. html.

14. Милиция осваивает сеть “В Контакте” / [Электронный ресурс]. – Режим доступа :
http://net. compulenta. ru.
15. Британскую полицию научат находить преступников в Twitter и Facebook / [Электронный ресурс] – Режим доступа :
http://internet-search. ru.
16. Поліція США затримала півсотні злочинців завдяки Facebook / [Електронний ресурс]. – Режим доступу :
http://ua. korrespondent. net/world/1394544-policiya-ssha-zatrimala-pivsotni-zlochinciv-zavdyaki-facebook).
17. Найден способ борьбы со спамом в соцсетях / [Электронный ресурс]. – Режим доступа :
http://www. from-ua. com/news/97d8bbf410e3c. html.
18. Facebook проверяет чаты пользователей на криминал / [Электронный ресурс]. – Режим доступа :
http://www. segodnya. ua/news/14409483. html.
19. Белоус Н. Киберджихад [Электронный ресурс] – Н. Белоус. – Режим доступа :
http://2000. net. ua/2000/derzhava/ekspertiza/84034.
20. Стартап сразится с преступностью при помощи Facebook / [Электронный ресурс]. – Режим доступа :
http://internetua. com/startap-srazitsya-s-prestupnostua-pri-pomosxi-Facebook.
21. Кремль уличили в использовании новейших систем мониторинга соцсетей / [Электронный ресурс]. – Режим доступа :
http://lb. ua/news/2012/08/16/166125_kreml_ulichili_ispolzovanii. html.
22. Горовий В. М. ІТ-субкультура як фактор розвитку сучасного правотворення / В. М. Горовий // Актуальні проблеми управління інформаційною безпекою держави : зб. мат. наук-практ. конф. (30 берез. 2012 р.). – К. : Наук-вид. відділ НА СБ України, 2012. – 308 с.

В статье проведен анализ актуальных сегодня вопросов, связанных с созданием государственного механизма противодействия деструктивному использованию социальных сетей преступными элементами. В практическом аспекте рассмотрены потенциальные возможности использования такого вида информационных сетей для выявления и раскрытия преступлений.

The article deals with the analysis of the actual today questions concerning the creation of state mechanism of counteraction the destructive use of social networks by the criminal elements. In the practical aspect the potential possibilities of the use of such type of informative networks for the discovering offences, crime detection are considered.

Стаття надійшла до редакції журналу 6 листопада 2012 року.