УДК 343.72
DOI 10.37749/2308-9636-2020-1(205)-3

А. С. Осадько,
кандидат юридичних наук, старший науковий співробітник
з вивчення проблем захисту національних інтересів в економічній сфері
та протидії корупції Міжвідомчого науково-дослідного центру
з проблем боротьби з організованою злочинністю при РНБО України

Ю. С. Довгаль,
науковий співробітник відділу з вивчення проблем забезпечення інформаційної
та кібернетичної безпеки, захисту вітчизняного інформаційного простору
Міжвідомчого науково-дослідного центру з проблем боротьби
з організованою злочинністю при РНБО України

ВИКОРИСТАННЯ МІЖНАРОДНИМИ ЗЛОЧИННИМИ УГРУПОВАННЯМИ ІНТЕРНЕТУ ТА СОЦІАЛЬНИХ МЕРЕЖ У ПРОТИПРАВНІЙ ДІЯЛЬНОСТІ

У статті досліджуються: кримінологічна характеристика злочинів, пов'язаних із використанням соціальних мереж. За основу взятий основний мотив, що спонукає особистість проводити в Інтернеті значну кількість часу, розглядаються фізична і психологічна залежності, що розвиваються внаслідок звикання до тих чи інших зовнішніх факторів. Проаналізована специфіка видів злочинів у соціальних мережах, також проведено аналіз низки актуальних на сьогодні питань, пов'язаних зі 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. Стаття присвячена дослідженню проблем використання соціальних Інтернет-мереж для запобігання злочинності шляхом здійснення моніторингу кримінологічно значимої інформації та її аналізу. Також зроблено висновок щодо можливості використання соціальних Інтернет мереж для підвищення рівня правової культури суспільства. Розглянута загрозлива тенденція поширення злочинності в Інтернет-мережах є актуальною проблемою, що обумовлює необхідність прискореного реагування на зростання інформаційних технологій у злочинному світі, з розвитком соціальних мереж з'являється потреба формування відповідної правової бази, яка б регламентувала саме такі форми інформаційних обмінів, якої в нашій країні ще не існує. Через зростаючу популярність соціальних мереж у суспільстві потрібна організація присутності державних органів, наукових установ, громадських організацій у цій сфері спілкування. Ця присутність повинна збалансувати фактично неконтрольовані інформаційні злочинні процеси в соціальних мережах, а також наявні там інформаційні масиви якісною, достовірною, суспільно значимою інформацією. Розвиток сфери соціальних мереж обумовлює зростаючу необхідність створення державних інформаційних структур для виробництва інформації, що сприяла б формуванню достовірних уявлень усіх користувачів соціальних комунікацій, у тому числі й мережевих, про актуальні проблеми розвитку суспільства та справжній стан злочинності в нашій країні.

Ключові слова: *мережа Інтернет, соціальні Інтернет-мережі, злочинність, запобігання, кримінологічна інформація, соціальна мережа, кіберзлочинність, інформаційний простір, мережеві комунікації.*

Актуальність. Протягом останніх десятиліть сучасні інформаційні технології здійснили справжню революцію серед звичних раніше засобів та способів спілкування, зв'язку, передачі та поширення інформації між членами суспільства. Внаслідок цього великий обсяг інформації, який перебуває в Інтернет-просторі, потребує належного механізму збирання, використання, узагальнення, зберігання та контролю і, насамперед, з боку держави. Зокрема, соціальні Інтернет-мережі можуть використовуватися для запобігання злочинності та проведення аналітичних кримінологічних досліджень. У відкритій доповіді американського аналітичного центру «RAND» (Research and Development) за 2018 рік зазначено, що контент-аналіз соціальних мереж має великий потенціал застосування під час спеціальних інформаційних операцій американськими військовими, оскільки дає змогу дослідити ставлення, світогляд та спілкування широкого кола осіб.

Наприклад, контент-аналіз може бути використаний для пошуку осіб у процесі радикалізації, оцінки ступеня підтримки екстремістських поглядів у певній групі. Геокодовані пости можуть доповнити аналіз та допомогти оцінити географію поширення певних груп чи ідей. Завдяки аналізу мереж можна або сприяти, або, навпаки, протидіяти поширенню окремих ідей або інформації. Аналіз дописів у соціальних мережах разом із пов'язаними метаданими може виявити лідерів суспільної думки [1].

Враховуючи викладене, доцільним є створення структурованої системи кримінологічного запобігання, підвищення соціальної та правової свідомості, а також вжиття заходів, спрямованих на зниження віктимності осіб у соціальних мережах; використовуючи вже перевірену інформацію про можливість вчинення злочину в подальшому, можна запобігти реалізації злочинної мети; досить поширеною сьогодні є взаємодія правоохоронних органів з адміністрацією соціальних сервісів. Чимало правоохоронних органів отримують інформацію про підозрюваних або розшукуваних осіб саме із соціальних мереж. Важливим є те, що аналіз інформації, що міститься в соціальних мережах, може дати результат на всіх стадіях вчинення злочину: готування, замах, безпосереднє вчинення суспільно небезпечного діяння.

Очевидним є також взаємозв'язок між використанням соціальних мереж правоохоронними органами та підвищенням ефективності запобігання злочинам і їх розслідуванню. Використання сучасних інформаційних технологій, зокрема соціальних мереж, під час виявлення та розслідування злочинів є необхідною умовою для ефективності вказаних дій і потребує подальшого детального дослідження та аналізу з метою визначення й удосконалення напрямів використання зазначених категорій у діяльності правоохоронних органів. Слід визнати, що сфера застосування соціальних мереж у криміналістичній науці охоплює дедалі більше напрямів. Необхідно також наголосити, що соціальні мережі для запобігання злочинності використовуються вже тривалий час правоохоронцями низки держав.

Правоохоронні органи намагаються використовувати нові технології, зокрема й 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 оперативного отримання вагомої для правоохоронців інформації.

Крім цього, соціальні мережі широко використовуються правоохоронними органами зарубіжних країн як засіб для зв'язків із громадськістю, у тому числі з метою отримання криміналістично значимої інформації. Необхідно зазначити, що, крім позитивних сторін соціальних мереж, передусім з точки зору можливостей комунікації, є також їх негативні сторони, зокрема, вони використовуються як середовище вчинення злочинів або як інструмент (знаряддя) вчинення злочину.

У сучасній науці існують різні класифікації злочинів, учинених у соціальних

мережах, в основу більшості з них покладено основний вид діяльності особистості в мережі Інтернет або провідний мотив використання соціальних мереж. Інформаційні технології сучасності сприяють зростанню соціальної активності членів суспільства. Особливу увагу в плані криміногенності привертають саме соціальні мережі, в яких активно діють як окремі злочинці, так і організовані злочинні угруповання. Крім того, соціальні мережі сьогодні — це величезні можливості для віртуальних соціальних спільнот й інструменти конструювання та зміни віртуальної реальності.

У сучасних умовах злочинців приваблюють можливості самого Інтернету та Інтернет-середовища, що забезпечує доступ до об'єктів злочинних посягань (банківських фінансових і платіжних систем, систем зберігання конфіденційної інформації тощо), а також можливість приховування слідів злочину, використовуючи такі якості Інтернету, як анонімність, можливість діяти «під легендою», простота знищення доказів (листування, слідів злому систем безпеки, слідів підробки електронних документів тощо). Для цього злочинці використовують як програмно-апаратні засоби (проксі-сервери, закладки тощо), так і результати революційного розвитку інформаційних технологій (шкідливі програми-віруси, програми-шпигуни, програми-диверсанти, закладки). Перелік цих інструментів далеко не повний, його можна доповнювати як за рівнем технічного виконання, так і за рівнем реальної або прихованої небезпеки.

Не менш важливим для злочинця є той факт, що до інформації, отримуваної із всесвітньої мережі, користувач за замовчуванням ставиться з високим ступенем довіри, що знижує рівень його критичності й пильності і створює ідеальні умови для залучення (за допомогою маніпулювання) до різних шахрайських схем, а нерідко й безпосередньо до протиправної діяльності. Людина, що характеризується обережністю й вибірковістю в спілкуванні з іншими людьми в реальному світі, досить часто втрачає ці якості, починаючи листування із суб'єктом із соціальних мереж, відомості про якого обмежуються фотографією (яка в багатьох випадках не має нічого спільного з реальним власником сторінки), «аватаром» і недостовірними анкетними даними, розміщеними на його особистій сторінці.

Це пов'язано з тим, що для психіки людини Інтернет та існуючі в ньому віртуальні об'єкти — явище нове, протягом еволюції людина з цим ніколи не стикалася і, отже, не звикла сприймати його як небезпеку. На рівні підсвідомості людина звикла розпізнавати як можливі джерела небезпеки реальні об'єкти — інших людей, тварин або стихію, проявляючи при цьому такі якості, як обережність, увага, критичність. Проте зображення в мережі не сприймається людиною на рівні підсвідомості як джерело небезпеки, що надає зловмисникам широкі можливості для підготовки та вчинення злочинів шляхом зловживання довірою користувачів.

Більшість соціальних мереж забезпечує своїм користувачам анонімність: активний користувач може виступати в контактах з іншими учасниками мережі як під своїм ім'ям (акаунтом, дані якого збігаються з особистими даними самого користувача), так і під профілем, що використовує дані іншої людини (для того, щоб «заплутати» слідство або забезпечити свою безпеку на випадок перевірки заявлених особистих даних); крім того, профіль користувача може бути повністю вигаданим (як нерідко буває). Інші користувачі соціальної мережі, вступаючи з ним у контакт, можуть навіть не здогадуватися про те, що з ними спілкується зовсім інша людина, що не відповідає сформованому індивідуальним профілем образу.

При роботі в соціальній мережі суб'єктивне ставлення зловмисника до підготовлюваного або вчинюваного ним діяння також віртуалізується; свідомість зловмисника розщеплюється, інтуїтивно відокремлюючи самого зловмисника, який живе в реальності, від його «аватара», що існує в мережі;

потім саме «аватар» починає сприйматися свідомістю й підсвідомістю зловмисника як суб'єкт вчинення злочину.

Якщо йдеться про дитячу порнографію, в якій в якості каналів передачі компрометуючої інформації та загроз використовуються соціальні мережі, то на рівні підсвідомості зловмисник, як правило, не пов'язує ці дії у віртуальному середовищі з власною особистістю — джерелом загроз стає саме його «аватар».

У свідомості злочинця акаунт, який він створив у соціальній мережі, і є суб'єктом, що чинить злочин: зв'язок його з реальною особою злочинця для підсвідомості, що породжує відчуття провини і невідворотності покарання, як правило, не очевидна. «Аватар», у свою чергу, з об'єктивних причин не може відчувати ні почуття провини, ні почуття страху, пов'язаного з невідворотністю покарання, що стимулює злочинця, який скоює злочинні дії під прикриттям «аватара», до вчинення більш жорстоких і радикальних злочинів. Злочинець підсвідомо впевнений, що це не він вчиняє злочин — це діє його «аватар», який у соціальних мережах живе своїм, вигаданим життям. Тобто злочинець перед вчиненням злочину переконує себе, що злочин насправді вчиняється не ним, а віртуальним суб'єктом, що існує в паралельній (інформаційній) реальності.

Аналогічним чином діють екстремісти, що використовують соціальні мережі в якості каналів поширення радикальних екстремістських гасел і закликів: екстреміст, створивши анонімний «акаунт» у соціальній мережі, переконує себе, що радикальні заклики йдуть від «аватара» — вигаданого персонажа, — зв'язок якого з реальною особою злочинця не є очевидним і може бути прихованим за допомогою методів та інструментів, що забезпечують користувачам соціальних мереж анонімність. У результаті в підсвідомості екстреміста «вимикається» найголовніший стримуючий фактор — усвідомлення особистої відповідальності за скоєне діяння, розуміння можливих наслідків, а також невідворотності покарання.

Таким чином, у злочинця формується стійка мотивація до радикалізації своєї діяльності; в мережах він готовий до вчинення більш тяжкого злочину, який він ніколи не вчинив би в реальному житті. Для здійснення цього діяння він створює спеціальний акаунт у мережі, який потім використовує для поширення закликів екстремістського змісту та погроз.

У результаті при вчиненні злочину в соціальних мережах суб'єктивна оцінка злочинця скоєного ним діяння виявляється деформованою, створюючи злочинцеві ілюзію невразливості і вседозволеності. Це призводить до того, що злочини екстремістської спрямованості (і не тільки: шантаж, вимагання та інші види злочинів цього типу також підпадають під цю категорію ризику), що вчиняються з використанням можливостей і ресурсу соціальних мереж, відрізняються підвищеною зухвалістю, зневагою до небезпеки і ризиків розкриття.

Крім звичайних злочинців, у соціальних мережах активно «працюють» вербувальники міжнародних терористичних організацій (таких як Даіши, Джебхат ан-Нусра та інші осередки Аль-Каїди, Хізб-ут-Тахрір), які розглядають соціальні мережі як ідеальне середовище для організації вербувальних операцій, і технологи «кольорових революцій», що формують протестний електорат. Цікаво, що й ті, й інші існують у формі мережевих організацій, які надзвичайно важко виявити: такі організації складаються з окремих, ізольованих один від одного осередків, які підтримують зв'язок із керуючим центром (або центрами) за допомогою досить складних ланцюжків різних рівнів. Подібність в організаційній формі існування у терористичних організацій і центрів координації протестного руху пояснюється досить просто: і ті, й інші змушені діяти в умовах суворої конспірації, вимогам якої найбільш точно відповідають саме мережеві форми. Адже саме завдяки мережевій формі організації терористичні підпілля в різних регіонах світу існують досить тривалий час [2].

Довідково. *У рамках протидії міжнародному тероризму в соціальних мережах у ході спільної операції правоохоронних та судових органів Євросоюзу, проведеної 21—24 листопада 2019 року, вдалося приховати 26 тис. одиниць контенту, пов'язаного з діяльністю «ІД», у тому числі відео та акаунти в соціальних мережах. За даними правоохоронної організації Євросоюзу, протягом чотириденної організації правоохоронці зв'язалися з дев'ятьма компаніями, в тому числі «Google» та «Telegram», з вимогою видалити їх із мережі. Угруповання «Ісламська держава» втратило більшу частину територій, які контролювало в Сирії та Іраку, проте продовжує розповсюджувати пропаганду онлайн.*

Крім того, поліція заарештувала в Іспанії чоловіка, якого підозрюють у тому, що він був одним із «головних поширювачів» онлайн-пропаганди «ІД». Як зазначено в заяві Євроюсту — іншої установи ЄС, що співпрацює з правоохоронними та судовими установами країн — членів НАТО, — «Європол і надалі працюватиме над заохоченням тісної публічної та приватної співпраці з метою запобігання поширенню терористичної онлайн-пропаганди і продовжить підтримувати забезпечення правосуддя установами країн — членів ЄС, щоби протидіяти терористичним атакам у мережі Інтернет». Операцію очолювали бельгійська поліція та прокуратура. До неї долучилися правоохоронні та судові установи Євросоюзу, Європол та Євроюст [3].

Також не малий відсоток складають «асоціальні злочини», в основі яких — прагнення особистості до самоствердження, однак використовуються при цьому соціально неприйнятні засоби. Одним із його проявів є кібербулінг, який характеризується агресивною поведінкою, спрямованою на конкретну людину чи групу людей.

Кібербулінг може мати яскраві негативні наслідки та навіть викликати суїцидальні спроби з боку осіб, на яких спрямований психологічний тиск, що проявляється в образах та цькуванні. Для особистості, що демонструє таку форму девіантної поведінки, цей тип самоствердження стає звичним та за певних обставин набуває нав'язливої форми, займаючи всі думки особи та практично весь її час.

Помилкові звинувачення, непристойні листи, погрози, образливі телефонні дзвінки підпадають під тип діяльності кіберпереслідування. «Cyberstalkers» часто здійснюються зловмисниками за допомогою чатів, Інтернет-форумів і вебсайтів соціальних мереж для збору інформації про користувачів і здійснення пихологічного тиску на своїх жертв на основі зібраної інформації. Прикладами таких злочинів є ксенофобія, расизм, гендерна нерівність тощо [4].

Іншою формою цього виду є тролінг, який проявляється в процесі віртуального спілкування у формі ініціювання конфлікту та нагнітання ситуації взаємодії в Інтернет-середовищі. Це дозволяє особистості проявити приховану агресію, яку вона не дозволяє собі демонструвати в реальному житті, боячись осуду, несхвалення та наслідків такої поведінки. Однак якщо в особистості постійно накопичуються деструктивні імпульси, від яких вона не може звільнитися соціально прийнятними засобами, тролінг стає звичним способом зняття напруги та набуває все більшої значущості. У цьому контексті основним мотивом є реалізація деструктивних тенденцій.

Ще однією формою злочинної діяльності в соціальних мережах є кіберсуїцид. У даному випадку спостерігається аутоагресія, яка знаходить вихід через пошук у мережі однодумців та спільне здійснення суїцидальних дій. У такій ситуації провідним мотивом є прагнення позбавитися болю, який виникає в кризових ситуаціях і суб'єктивно сприймається як нестерпний, або ж бажання завдяки смерті позбавитися всіх проблем, з якими особистість не здатна впоратися.

Одним із найбільших сайтів для самогубців видання «Wired» (США, Великобританія) називає «alt.suicide.holiday» (скорочено «a.s.h»), що можна перекласти як «прах». Учасники цієї групи називають себе Ешера (Ashers), а

ЗМІ вважають цей ресурс причетним як мінімум до трьох випадків суїциду. Але перевірити, чи так це, на жаль, неможливо через анонімність.

Ще однією формою прояву злочинів у соціальних мережах є група, що отримала назву «біологічно-фрустровані злочини». У цьому випадку в основі розвитку злочинності лежить незадоволена біологічна потреба — найчастіше сексуальна. Нездатність особистості реалізувати власні бажання з дорослою людиною в інтимній сфері в реальному житті призводить до появи кіберсексуальної залежності, яка характеризується спрямованістю на побудову віртуальної взаємодії з неповнолітніми особами будь-якої статі.

До іншої групи увійшли «змістоутворювально-фрустровані» злочини, пов'язані з порушенням авторського права і суміжних прав. В основі таких злочинів лежить прагнення наповнити своє життя особистісним сенсом. Виникає такий мотив тоді, коли особистість перебуває в стані екзистенційного вакууму, не здатна усвідомити сенс свого життя, ставити перед собою цілі, яких вона хотіла б досягнути.

Загрозлива тенденція поширення злочинності в Інтернет-мережах є актуальною проблемою, що обумовлює необхідність прискореного реагування на зростання інформаційних технологій у злочинному світі.

По-перше, з розвитком соціальних мереж з'являється потреба формування відповідної правової бази, яка б регламентувала саме такі форми інформаційних обмінів, якої в нашій країні ще не існує.

По-друге, через зростаючу популярність соціальних мереж у суспільстві потрібна організація присутності державних органів, наукових установ, громадських організацій у цій сфері спілкування. Ця присутність повинна збалансувати фактично неконтрольовані інформаційні злочинні процеси в соціальних мережах, а також наявні там інформаційні масиви якісною, достовірною, суспільно значимою інформацією.

По-третє, розвиток сфери соціальних мереж обумовлює зростаючу необхідність створення державних інформаційних структур для виробництва інформації, що сприяла б формуванню достовірних уявлень усіх користувачів соціальних комунікацій, у тому числі й мережевих, про актуальні проблеми розвитку суспільства та справжній стан злочинності в нашій країні.

По-четверте, прискорене розповсюдження інформації в соціальних мережах обумовлює необхідність організації роботи з прогнозування нових реалій і ситуацій у злочинному інформаційному просторі та розробки згідно з цим прогнозуванням методик протидії злочинам в інформаційній сфері, вироблення аргументацій, спрямованих на нейтралізацію негативних інформаційних впливів на інформаційний простір України в цілому.

Висновки. Сьогодні, в контексті сучасного стану протиправного використання соціальних мереж, прогнозованого зростання в найближчому майбутньому кількості та суспільної небезпеки реальних і потенційних загроз, що виходять із кібернетичного простору, необхідне створення ефективної системи протидії таким деструктивним явищам і локалізації відповідних загроз. В Україні на сьогодні не існує законодавства, яке б здійснювало нормативно-правове регулювання такої протидії взагалі та визначало спеціальні методи «дослідження цільової аудиторії», зокрема [5].

З огляду на це вважаємо доцільним прискорення прийняття в оновленій редакції закону «Про медіа», концепція якого 13 листопада 2019 р. була презентована на засіданні Комітету Верховної Ради України з питань цифрової трансформації. Цим законопроєктом пропонується об'єднати діючі закони про медіа, обмежити монополію і заборонити росіянам володіти українськими ЗМІ, а також визначити порядок регулювання сфери онлайн-медіа та соціальних мереж [6], що дозволить вирішити питання щодо прозорості власності, контролю, звітування, ліцензування та реєстрації, контенту в розрізі квот європейського і

національного продукту, мови, захисту неповнолітніх і механізмів співрегулювання медіа.

Одним із достатньо ефективних засобів припинення протиправної діяльності може стати використання методів контент-моніторингу і контент-аналізу інформаційних потоків у соціальних мережах, функцію проведення яких із відповідним визначенням компетенції, законодавець має покласти на правоохоронні органи, наділені правом здійснення оперативно-розшукової діяльності, насамперед, на Національну поліцію України та Службу безпеки України.

Список використаної літератури

1. Бугера О. Використання соціальних Інтернет-мереж для запобігання злочинності. URL: http://pgp-journal.kiev.ua/archive/2018/5/47.pdf.

2. Гаркуша Ю. О. Кримінологічна характеристика злочинів, пов'язаних з використанням соціальних мереж. URL: http://www.pap.in.ua/6_2015/78.pdf.

3. Європол заявляє про блокування 26 тисяч одиниць контенту, пов'язаного з «ІД». URL: https://www.unn.com.ua/uk/news/1837788-yevropol-zayavlyaye-pro-blokuvannya-26-tisyach-odinits-kontentu-povyazanogo-z-id.

4. Найденова Л. О. Кибер-буллинг: опасное виртуальное «быкование» / Л. О. Найденова II «ПСИ-ФАКТОР». URL: http://psyfactor.org/lib/cyber-bullying.htm.

5. Гавловський В.Д. Щодо використання соціальних мереж для виявлення, розкриття та попередження злочинів. URL: http://nbuv.gov.ua/UJRN/boz_2012_2_33.

6. Електронний ресурс. URL: https://www.ukrinform.ua/rubric-society/2817663-radi-proponuut-pririvnati-socmerezi-i-strimingovi-servisi-do-zmi.html.

References

1. Bougera O. Using Social Internet Networks to Prevent Crime. URL: http://pgp-journal.kiev.ua/archive/2018/5/47.pdf.

2. Garkusha Y. O. Criminological characteristics of crimes related to the use of social networks. URL: http://www.pap.in.ua/6_2015/78.pdf.

3. Europol announces blocking of 26 units of content related to «ID». URL: https://www.unn.com.ua/uk/news/1837788-yevropol-zayavlyaye-pro-blokuvannya-26-tisyach-odinits-kontentu-povyazanogo-z-id.

4. Naydenova LO Cyber Bulling: A Dangerous Virtual Bullshit / L.O. Nayden II «PSI-FACTOR». URL: http://psyfactor.org/lib/cyber-bullying.htm.

5. Gavlovsky V. D About using social networks to detect, uncover and prevent crime. URL: http://nbuv.gov.ua/UJRN/boz_2012_2_33.

6. Electronic resource. URL: https://www.ukrinform.ua/rubric-society/2817663-radi-proponuut-pririvnati-socmerezi-i-strimingovi-servisi-do-zmi.html.

Осадько А. С., Довгаль Ю. С. Использование международными преступными группировками интернета и социальных сетей в противоправной деятельности.
В статье исследуются: криминологическая характеристика преступлений, связанных с использованием социальных сетей. За основу взят основной мотив, побуждающий личность проводить в Интернете значительное количество времени, рассматриваются физическая и психологическая зависимости, развивающиеся вследствие привыкания к тем или иным внешним факторам. Проанализирована специфика видов преступлений в социальных сетях, а также проведен анализ ряда актуальных на сегодняшний день 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. Статья посвящена исследованию проблем использования социальных Интернет-сетей для предотвраще-

ния преступности путем осуществления мониторинга криминологически значимой информации и ее анализа. Также сделан вывод о возможности использования социальных Интернет-сетей для повышения уровня правовой культуры общества. Рассмотреная угрожающая тенденция распространения преступности в Интернет-сетях является актуальной проблемой, что обусловливает необходимость ускоренного реагирования на рост информационных технологий в преступном мире, с развитием социальных сетей появляется необходимость формирования соответствующей правовой базы, которая бы регламентировала именно такие формы информационных обменов, которой в нашей стране еще не существует. За растущей популярностью социальных сетей в обществе нужна организация присутствия государственных органов, научных учреждений, общественных организаций в этой сфере общения. Это присутствие должно сбалансировать фактически неконтролируемые информационные преступные процессы в социальных сетях, а также имеющиеся там информационные массивы качественной, достоверной, общественно значимой информации. Развитие сферы социальных сетей обусловливает растущую необходимость создания государственных информационных структур для производства информации, которая способствовала бы формированию достоверных представлений всех пользователей социальных коммуникаций, в том числе и сетевых, об актуальных проблемах развития общества и настоящее состояние преступности в нашей стране.
Ключевые слова: *сеть Интернет, социальные Интернет-сети, преступность, предупреждение, криминологическая информация, социальная сеть, киберпреступность, информационное пространство, сетевые коммуникации.*

Osad'ko A. S., Dovhal Yu. S. Use of international criminal groups by the Internet and social networks in illegal activities.
The article explores: *criminological characteristics of crimes related to the use of social networks. The basic motive that drives a person to spend a considerable amount of time on the Internet is based on the physical and psychological dependence that develops as a result of getting used to certain external factors. The specificity of types of crimes in social networks was analyzed, and a number of current issues related to the creation of a state mechanism for counteracting the destructive use of social networks by criminal elements were analyzed. In a practical aspect, the potential possibilities of using this type of information networks for the detection and detection of crimes are considered. The article is devoted to the research of problems of using social Internet-networks for prevention of crime by carrying out monitoring of criminologically relevant information and its analysis. It also concluded that the use of social internet networks to enhance the legal culture of society. The threatening tendency of spreading crime on the Internet networks is considered an urgent problem, which necessitates the speedy response to the growth of information technologies in the criminal world, with the development of social networks there is a need to create an appropriate legal framework that would regulate exactly such forms of information exchanges, which in our country does not yet exist. Due to the growing popularity of social networks in society, it is necessary to organize the presence of state bodies, scientific institutions, public organizations in this field of communication. This presence must balance virtually uncontrolled information criminal processes in social networks, as well as the available information arrays with high-quality, reliable, socially significant information. The development of the sphere of social networks necessitates the growing need for the creation of state information structures for the production of information, which would contribute to the formation of reliable perceptions of all users of social communications, including network ones, about the actual problems of social development and the true state of crime in our country.*
Key words: *Internet, social Internet, crime, prevention, criminological information, social network, cybercrime, information space, network communications.*