УДК 343.97

СОЦІАЛЬНІ ІНТЕРНЕТ-МЕРЕЖІ ТА ЗАПОБІГАННЯ ЗЛОЧИННОСТІ: СУЧАСНІ ТЕНДЕНЦІЇ

Бугера О. І.,
кандидат юридичних наук, доцент,
доцент кафедри права
Київського національного лінгвістичного університету

Стаття присвячена дослідженню проблем використання соціальних Інтернет-мереж для запобігання злочинності, як однієї із сучасних тенденцій розвитку кримінологічної науки. Встановлено доцільність використання всього спектру можливостей соціальних Інтернет-мереж для підвищення рівня запобігання злочинності, це зокрема стосується: ведення спеціалізованих блогів; створення аудіо- та відеофайлів запобіжного характеру; моніторингу кримінологічно значимої інформації та іншого.

Статья посвящена исследованию проблем использования социальных Интернет-сетей для предупреждения преступности, как одной из современных тенденций развития криминологической науки. Установлена целесообразность использования всего спектра возможностей социальных Интернет-сетей для повышения уровня предупреждения преступности, это в частности касается: ведения специализированных блогов; создания аудио- и видеофайлов предупредительного характера; мониторинга криминологически значимой информации и дргого.

The article is devoted to research on the problems of using social internet networks for crime prevention, as one of the modern trends in the development of criminological science. The expediency of using the full spectrum of opportunities of social Internet networks for raising the level of prevention of crime is established, in particular it concerns: conducting specialized blogs; creating audio- and video files of a preventive nature; monitoring of criminological relevant information, etc.

Ключові слова: мережа Інтернет, соціальні Інтернет-мережі, злочинність, запобігання, зарубіжний досвід.

Постановка проблеми. Протидія і запобігання злочинності потребують винайдення відповідних методів запобіжного впливу на криміногенні об’єкти. Пошук і відкриття методів ефективного запобіжного впливу на відповідні криміногенні об’єкти це основа наукового підходу до свідомої, обґрунтованої, цілеспрямованої протидії злочинності, що потребує досліджень фахівців-кримінологів [1, с. 54-56].

Однією з тенденцій розвитку кримінологічної науки на сучасному етапі є дослідження можливостей використання мережі Інтернет для запобігання злочинності і, зокрема, такої складової як соціальні Інтернет-мережі. Необхідно зазначити, що Інтернет активно змінює наше життя і уявити сучасний світ без соціальних мереж стає практично неможливо. На початку 2017 року соціальні мережі охопили понад 2 мільярди користувачів. Найбільшу популярність на сьогодні отримав Facebook з аудиторією понад 1,59 мільярда постійних користувачів [2].

Аналіз останніх досліджень і публікацій. Питаннями інформаційного забезпечення кримінологічних досліджень та використанням соціальних Інтернет-мереж для запобігання злочинності займалися такі вчені, як: Автухов К.А., Андріїв Н.О., Гавловський В.Д., Гіда О.Ф., Горова С.В., Косолап О.В., Юрченко О.Ю. та інші.

Мета статті – дослідження сучасних тенденцій та міжнародного досвіду використання соціальних Інтернет-мереж для запобігання злочинності.

Виклад основного матеріалу дослідження. Необхідно зазначити, що соціальна мережа це Інтернет-співтовариство користувачів, об’єднаних за будь-якою ознакою на базі одного сайту, який і називається в цьому випадку соціальною мережею. Іншими словами, соціальна Інтернет-мережа будується на тих же принципах, що і в реальному світі, але відрізняється від реальних людських спільнот тим, що у функціонуванні мережі не має значення географічна віддаленість її учасників один від одного. Перша соціальна мережа з’явилося у середині дев’яностих років XX століття. Загалом соціальна мережа з технічної точки зору об’єднує Інтернет-користувачів на базі спеціального веб-ресурсу. Зокрема, інтерфейс соціальної мережі передбачає реєстрацію учасника, надає

учаснику можливість наповнювати своїм контентом соціальну мережу у вільному режимі, вести блоги, які також вільно можуть коментуватись іншими учасниками соціальної мережі [3].

Систематизацію соціальних мереж здійснюють за такими ознаками:

1) за типом: особисте і ділове спілкування, фото-, аудіо - і відеоконтент, розваги, покупки, геолокація, новини, сервіси питань і відповідей, віртуальні світи, тематичні соціальні мережі та ін;

2) за доступністю розрізняють відкриті і закриті соціальні мережі, а також ресурси зі змішаним доступом;

3) за охопленням: існують як веб-сайти, які охоплюють весь світ, так і внутрішньонаціональні або ресурси без прив'язки до певного регіону; окремо можна виділити майданчики корпорацій або політичних партій.

Оскільки соціальна мережа це Інтернет-ресурс, де користувачі самостійно створюють контент, то для подібного роду проектів характерний, з точки зору кримінології, ряд небезпек, серед яких: відкрите поширення конфіденційної інформації; можливість зіткнутися з неналежним контентом (насильство, образи тощо); ймовірність використання особистої інформації третіми особами з метою отримання вигоди; стрес від незадоволеності соціальної потреби в реальному світі; залежність від соціальних мереж та Інтернету в цілому; умисне створення негативного іміджу певної особи іншими учасниками спільноти (цькування, залякування, погрози тощо); комп'ютерна педофілія, сексуальні домагання; кіберзлочинність і кібертероризм; надмірність спілкування та інформації; пропаганда самогубств [4].

До негативних сторін соціальних мереж можна також віднести можливість координації діяльності злочинних угрупувань. Зокрема, терористичні угрупування, користуються соціальними мережами для поширення своєї пропаганди, рекрутування нових членів та спонукання до автономного скоєння терористичних актів. Відомо, що терористичні угрупування можуть користуватись соціальними мережами для координації власної діяльності. Соціальні мережі також можуть бути використані й для поширення дезінформації. Водночас соціальні Інтернет-мережі можуть бути використані для запобігання злочинності та проведення аналітичних кримінологічних досліджень. Зокрема, у відкритій доповіді американського аналітичного центру RAND (Research and Development) зазначено, що аналіз соціальних мереж має великий потенціал використання в інформаційних операціях американськими військовими, оскільки дозволяє дослідити ставлення, світогляд та спілкування широкого кола осіб. Наприклад, контент-аналіз може бути використаний для пошуку осіб в процесі радикалізації, оцінити ступінь підтримки екстремістських поглядів у певній групі. Геокодовані пости можуть доповнити аналіз, та допомогти оцінити географію поширення певних груп чи ідей. Завдяки аналізу мереж можливо або сприяти, або навпаки, протидіяти, поширенню окремих ідей або інформації. Аналіз дописів у соціальних мережах разом з пов'язаними даними може виявити лідерів суспільної думки. Алгоритми класифікації зображень допомагають дізнатись, які види зображень популярні в соціальних мережах, а разом з прив'язкою до місцевості – відстежити зміну вподобань та ставлення населення до різних речей [5].

На думку В.Д. Гавловського доцільним є також проведення правоохоронного моніторингу соціальних мереж: відстеження використання соціальних мереж у деструктивних цілях, яке здійснюється державою в межах виконання правоохоронної функції. Метою правоохоронного моніторингу соціальних мереж є запобігання деструктивним діянням, їх виявлення та припинення в рамках реалізації відповідними органами правоохоронної функції держави. До того ж система заходів правоохоронного моніторингу соціальних мереж, на думку автора, може включати:

1) автоматичне комп'ютерне спостереження, що має проводитися з використанням відповідного програмного забезпечення і спрямовуватися на пошук у соціальних мережах за ключовими словами чи змістом інформації, яка містить: пропаганду суспільно-небезпечних ідей; відомості з обмеженим доступом; домовленості про спільні злочинні дії; відомості щодо збуту або придбання товарів й предметів заборонених для відкритого обігу, майна здобутого злочинним шляхом; надання заборонених послуг; торгівлі людьми;

2) заходи, пов'язані із залученням громадськості до отримання інформації про використання соціальних мереж у деструктивних цілях;

3) оперативно-пошукові заходи по забезпеченню оперативної закупівлі та (або) контрольованого постачання товарів, заборонених для відкритого обігу, майна, здобутого злочинним шляхом, надання заборонених послуг, торгівлі людьми через соціальні мережі;

4) оперативне впровадження у віртуальні соціальні групи, що мають деструктивні цілі з метою отримання інформації про їх персональний склад, місця зустрічей, плани та засоби, що використовуються в деструктивній діяльності;

5) оперативно-аналітичні заходи, спрямовані на прогноз розвитку ситуації, розробка заходів з утримання її під контролем, отримання нових даних про суб'єктів деструктивної діяльності, їх зв'язки, місця відвідування, злочинні наміри тощо;

6) заходи оперативно-технічного характеру, спрямовані на виявлення та локалізацію комп'ютерних засобів (та їх користувачів), що стали джерелами (засобами) розповсюдження у соціальних мережах інформації деструктивного характеру [6].

Необхідно зазначити, що соціальні Інтернет-мережі доволі активно використовуються в США для запобігання злочинності. Опитування, проведене в Міжнародній асоціації керівників поліції (International Association of Chiefs of Police), показало, що 81% опитаних представників правоохоронних органів використовують соціальні мережі для вирішення певних завдань. Зокрема, 62% повідомили про використання Facebook для проведення кримінальних розслідувань, а близько половини зазначили використання соціальних мереж з метою запобігання злочинності [7].

Міжнародною асоціацією керівників поліції також розроблено рекомендації щодо використання соціальних Інтернет-мереж для запобігання злочинності, в яких, зокрема, вказується напрями цієї роботи: безпосереднє розміщення в соціальних мережах інформації щодо запобігання злочинності; розробка блогів; організація чатів; створення цифрових медіа-файлів, наприклад, у вигляді лекцій; розповсюдження в соціальних мережах інформації щодо різноманітних заходів із запобігання злочинності [8].

Державний департамент США також планує вимагати від усіх претендентів на отримання американської візи надавати інформацію щодо реєстрації в соціальних мережах, і зокрема, імена користувачів, попередні адреси електронної пошти, а також номери телефонів, значно розширюючи при цьому процедуру перевірки потенційних іммігрантів. Дане питання пропонується до громадського обговорення, оскільки нові вимоги вплинуть на майже 15 мільйонів іноземців, які подають заявку на отримання віз для в'їзду до США щороку. Раніше дані про соціальні мережі, електронну пошту та номери телефонів вимагались лише від заявників, визначених для додаткової перевірки, наприклад, тих, хто виїхав до територій, контрольованих терористичними організаціями (близько 65000 людей на рік у цій категорії). Нові правила застосовуватимуться до практично всіх претендентів на імміграційні та не імміграційні візи. За оцінками департаменту це вплине на 710 тисяч заявників на імміграційну візу та на 14 мільйонів не імміграційних візових заявників, у тому числі тих, хто хоче приїхати до США для ведення бізнесу чи отримання освіти. Якщо нові вимоги будуть схвалені, то заявки на всі типи віз будуть надавати інформацію про декілька платформ соціальних мереж і щодо облікових записів, які вони могли мати протягом останніх п'яти років. Заявник на отримання візи буде мати можливість самостійно надавати інформацію про облікові записи соціальних мереж на платформах, не зазначених у встановленому переліку. На додаток, до історії своїх соціальних мереж, заявникам також буде необхідно надавати інформацію про номери телефонів, що використовувались ними протягом останніх п'яти років, а також, електронні адреси, статуси міжнародного пересування та депортації, а також чи були члени сім'ї задіяні в терористичній діяльності. Вказані вимоги можуть не застосовуватись лише відносно претендентів на певні дипломатичні та офіційні види віз [9].

Штаб-квартира ЦРУ здійснює роботу по відстеженню записів в соціальних мережах. Серед соціальних мереж, які відстежуються, виявилася і найвідоміша – Facebook. Контролюванням роботи соціальних мереж займається створений спеціально для цієї мети підрозділ з назвою «Центр відкритих джерел». Робота підрозділу полягає в аналізі повідомлень, які з'являються в соціальній мережі в об'ємі до 5 мільйонів повідомлень за добу [10].

Існує також досвід Інтернет-гіганта Google, який запустив на YouTube експериментальний «Метод перенаправлення». Він полягає в тому, щоб перенаправляти людей, які шукають «про-терористичний контент», на інші інформаційні ресурси, що мають роз'яснювальний та запобіжний характер [11].

Отже з розвитком Інтернету з'явилася можливість використовувати всі його досягнення в різних його проявах. Одним з таких проявів стали соціальні мережі, які набули на сьогодні статусу невід'ємного атрибуту нашого життя. Уявити сучасну людину без соціальних мереж просто неможливо. Адже це спілкування, пошук інформації і друзів, обмін новинами, можливість слухати музику, дивитися відео і фотографії тощо [12].

Зараз соціальні мережі, зважаючи на задекларовану мету їх створення, а саме можливість спілкування, надають користувачам усі можливі для цього інструменти – відео, чати, зображення, блоги, форуми тощо [13, с. 207]., що, в свою чергу, дає підстави використовувати соціальні Інтернет-мережі для запобігання злочинності на новому якісному рівні.

Загалом про запобігання злочинів за допомогою мережі Інтернет слід говорити в контексті декількох аспектів. Зокрема доцільним є створення структурованої системи кримінологічного запобігання, підвищення правової свідомості, а також проведення заходів, спрямованих на зниження віктимності осіб у соціальних мережах. По-друге, використовуючи уже перевірену інформацію про можливість вчинення злочину у майбутньому, можна перешкодити реалізації злочинної мети. По-третє, досить поширеною на сьогодні є взаємодія правоохоронних органів з адміністрацією соціальних сервісів. Чимало правоохоронних органів прослуховують чи перечитують інформацію щодо підозрюва-

них або розшукуваних осіб у соціальних мережах. Актуальним є те, що звернення до інформації, що міститься в соціальних мережах може дати результат на всіх стадіях вчинення злочину: підготовка, замах, безпосереднє вчинення суспільно небезпечного діяння. Очевидним є також взаємозв'язок між використанням соціальних мереж правоохоронними органами та підвищенням ефективності запобігання й розслідування злочинів [14, с. 152-153].

Висновки. Отже використання соціальних Інтернет-мереж для запобігання злочинності є однією з сучасних тенденцій розвитку кримінологічної науки. Про це свідчить також міжнародний досвід. Зокрема, доцільним є використання всього спектру можливостей соціальних Інтернет-мереж для підвищення рівня запобігання злочинності, а саме: ведення спеціалізованих блогів; створення аудіо- та відеофайлів запобіжного характеру; моніторингу кримінологічно значимої інформації та ін.

Література:

1. Запобігання злочинності (теорія і практика): навч. по-сіб. / Голіна В.В. Х.: Нац. юрид. акад. України, 2011. 120 с.
2. Попова Т.В. Соціальні мережі, кібератаки та гібридні війни. URL: https://www.radiosvoboda.org/a/28598299.html (дата звернення 08.05.2018).
3. Соціальна мережа. URL: http://igroup.com.ua/seo-articles/sotsialna-merezha/ (дата звернення 08.05.2018).
4. Соціальна мережа – це що таке? URL: http://hi-news.pp.ua/tehnka-tehnologyi/2903-socalna-merezha-ce-scho-take.html (дата звернення 08.05.2018).
5. Соціальна мережа (Інтернет). URL: https://uk.wikipedia.org/wiki/ Соціальна мережа (Інтернет) (дата звернення 08.05.2018).
6. Гавловський В.Д. Теоретичні засади відстеження деструктивних процесів у соціальних мережах. URL: http://pravoznavec.com.ua/period/article/27006/%C3 (дата звернення 08.05.2018).
7. Social Media and Crime Prevention. URL: https://www.nnw.org/ publication/social-media-and-crime-prevention. (дата звернення 08.05.2018).
8. Social Media and Crime Prevention. Facts Sheet. URL: https://www.nationalpublicsafetypartnership.org/clearinghouse/Content/ResourceDocuments/Social%20Media%20and%20Crime%20Prevention%20Fact%20Sheet.pdf (дата звернення 08.05.2018).
9. US to seek social media details from all visa applicants. URL: https://apnews.com/d7 683b 1344fa4d44b87cafd0f 19b4b04/US-to-seek-social-media-details-from-all-visaapplicants?iitm_campaign-Socia!Eiow&utm source =
10. Twitter&utmmedium~AP_ Politics (дата звернення 18.04.2018).
11. ЦРУ бере соціальні мережі під тотальний контроль. URL: http://akhe.info/tsru-bere-sotsialni-merezhi-pid-totalnyj-kontrol/ (дата звернення 08.05.2018).
12. YouTube занялся «перевоспитанием» потенциальных террористов. URL: http://ru.telekritika.ua/business/youtube-zanyalsya-perevospitaniem-potentsialnih-terroristov-674820 (дата звернення 08.05.2018).
13. Беркій Т.М. Соціальні мережі: різні аспекти впливу на людину. URL: http://ukrainepravo.com/legal_publications/essay-on-itlaw/it_law_berkiy_Soci networks_and_there_involves/ (дата звернення 08.05.2018).
14. Черниш Р.Ф. Соціальні мережі як один із інструментів накопичення та протиправного використання персональних даних громадян. Проблеми законності. 2017. Вип. 136. С. 205–214.
15. Автухов К.А., Андріїв Н.О. Кримінологічний погляд на соціальні мережі. Актуальні питання публічного та приватного права. 2013. № 1. С. 150–153.