Артюшенко Аліна Станіславівна
старший лаборант кафедри
адміністративного права, процесу
та адміністративної діяльності
Дніпропетровського державного
університету внутрішніх справ

науковий керівник –
Рижков Едуард Володимирович
к.ю.н., доцент, завідувач кафедри
економічної та інформаційної безпеки

ДО ПИТАННЯ ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ, РОЗКРИТТЯ ТА ПОПЕРЕДЖЕННЯ ЗЛОЧИНІВ

В час сучасних технологій кількість Інтернет-аудиторії постійно збільшується, охоплюючи значну кількість населення нашої планети. Зокрема із 7 млрд. жителів планети Земля 2,3 млрд. користуються послугами Інтернет, тобто фактично кожен третій житель. Не залишається осторонь таких глобальних змін і наша держава. Станом на січень 2018 року в Україні налічується 21,8 млн. користувачів Інтернету, інакше кажучи половинна населення України має доступ до мережі, а ще половина з них до соціальних мереж. Поряд із незаперечними позитивними рисами користування, соціальними мережами притаманні також негативні, зокрема: марнування часу, виток конференційної інформації, виникнення психологічної залежності, інтелектуальної деградації, інше. Крім того анонімність користування дає можливість для вчинення злочинів.

Аналізуючи нові загрози для користувачів соціальних мереж, необхідно констатувати, що, такі мережі вже тривалий час активно використовуються злочинцями не тільки як засіб, але й знаряддя чи місце вчинення злочинів. Отже, наразі необхідна розробка засад організаційно-правової протидії Інтернет злочинності. Дослідженням окремих аспектів організаційно-правової протидії вчиненню злочинів з використанням специфічних інформаційних можливостей займались: В.М. Бутузов, В.М. Горовий, А.І. Марущак, О.М. Юрченко, В.П. Шеломанцев, та інші. Однак сьогодні залишаються остаточно невирішеними питання, щодо правової регламентації використання соціальних мереж, для виявлення, розкриття та попередження злочинів.

Інформація стає головним товаром Інтернет-економіки. За прогнозами Boston Consulting, через 8-10 років частка Інтернет-економіки у ВВП Єврозони досягне 8 відсотків, і більша частина буде припадати на збір та аналіз персональних даних, які сьогодні приносять Інтернет-компаніям понад 300 млрд. на рік. Європейські компанії наразі заробляють на кожному користувачу близько 1 тис євро. Ринок цей росте не тільки бурхливо, але й безконтрольно. Єврокомісія, наприклад, вже рік розслідує питання, як саме Google та Facebook використовують особисті данні відвідувачів.[1]

Все швидше набуває обертів спеціальний вид шахрайства, що характеризується використанням Інтернет-магазинів. При цьому злочинці використовують надзвичайно просту технологію, яка за своєю цифровою формою нагадує «спам». Так, вкравши данні користувача, зловмисники заманюють «друзів» користувача, які нічого не підозрюють на сайти Інтернет-магазинів, які спеціалізуються на обмані користувача або клієнта. 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 скористуватися зловмисники при вчинені квартирної крадіжки, угону автотранспорту.[2; С. 258]

Соціальні мережі нерідко використовуються також при підготовці та вчинені особливо тяжких злочинів корисливо-насильницької спрямованості. Також екстремістські та терористичні організації для здійснення своє деструктивної діяльності активно використовують мережу Інтернет, зокрема соціальні мережі, які виступають засобом зв'язку для вербування, координацією при вчиненні терактів, джерелом отримання інформації, тощо. Варто зазначити, що сьогодні практично вся інформація діяльність терористичних угрупувань перенесена у віртуальних світ. Це пов'язано з тим, що працювати там більш безпечно, ніж у традиційних ЗМІ.

У соціальних мережах люди знаходять один одного, знайомляться, спілкуються, беруть участь у обговореннях – проте інтереси у всіх різні. І один із небезпечних «інтересів» суспільства як наркотики не обійшов мережу Інтернет. Користувачі соціальних мереж активно створюють групи, де радять з приводу придбання наркотичних речовин. В таких групах пропогандують наркотики, радять де їх придбати, виступають за легалізацію наркотичних речовин, вказують ціни та торговців наркотичними препаратами та інше.

Останнім часом усе частіше кіберпростір використовують для цькування опонентів. Занепокоєність викликає кібер-буллінг (кібер-знущання) – це одна з форм залякування, переслідування, насильства, цькування дітей, підлітків з використанням інформаційних ресурсів: електронна пошта, веб-сайти, соціальні мережі та інше. Кібер-буллінг включає в себе 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. Прикладом буллінгу може бути випадок, що стався на Закарпатті, де школярі зацькували у соціальній мережі свою однокласницю -14 річну дівчину до самогубства. [3]

За даними фонду Internrt 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. Отже, Інтернет наповнюється протиправним контентом і використовується з метою протиправної діяльності.

У Південній Кореї, де сьогодні найбільша кількість випадків суїциду влада сформувала спеціальну групу експертів з Інтернет, понад 100 осіб, яким належить шукати суїцидально налаштованих користувачів соціальних мереж і сайти, які спонукають людей до таких дій. [4]

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.

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 при необхідності її можна перепрограмувати на пошук інших ознак злочинів. Система сканує листування та публікації користувачів Facebook. Цей співробітник, у свою чергу, оцінює ступінь потенційної небезпеки і вразі наявності про злочинця повідомляє про це правоохоронні органи США.

Сьогодні Україна перебуває осторонь цих суспільно-корисних процесів. Це пов'язано з одного боку відсутністю у співробітників поліції спеціальних інформаційно-пошукових систем, особливо контент-моніторингу, контент-аналізу, а з іншого – із відсутністю нормативного закріплення подібних дій. В контексті протиправного використання соціальних мереж, зростання у майбутньому кількості Інтернет-злочинів та суспільної небезпеки необхідно створювати ефективні системи протидії таким деструктивним явищам і локалізації відповідних загроз лише з використанням специфічних можливостей соціальних мереж.

1. Гавловський В.Д. До питання захисту персональних даних у соціальних мережах / В.Д Гавловський // Б-ба з огр. злоч. і корупцією (теорія та практика) : наук.-практ.журнал.-К.: МНДЦ при РНБО України, 2011.-№24. С.252-262.

2. Кількість користувачів інтернету в Україні досягнула 20 млн/ [Електронний ресурс].-Режим доступу: blogosphere.com.ua/

3. На Закарпатье одноклассники убили девочку в Интернете /[Електронний ресурс].-Режим доступу: blogosphere.com.ua/

4.Корея боротиметься із суїцидами через соціальні мережі /[Електронний ресурс].-Режим доступу: blogosphere.com.ua/