Також до проблем можна віднести складність розслідування шахрайства у мережі Інтернет. Є частим явищем діяльність таких шахраїв з-за кордону або на території України з використанням програм, які змінюють справжнє місцезнаходження. Це ускладнює їх ідентифікацію та притягнення винних до відповідальності.

В умовах воєнного стану, який значно вплинув на життя людей, важливо для громадян бути обізнаними та пильними, з чого і випливає наступна проблема. Більшість людей не знають про поширені шахрайські схеми і тому легко стають жертвами обману.

Отже, враховуючи зазначене, можна зробити висновки про необхідність посилення оперативно-розшукової протидії шахрайству в мережі Інтернет шляхом модеренізаціїї та розвитку даної сфери. Пріоритетним напрямом протидії шахрайству в мережі Інтернет, у тому числі й оперативно-розшукової протидії, є запобігання цим злочинам (профілактика, попередження та припинення), що передбачає такі форми, які призначені стримувати особу від наміру вчинити злочин чи довести злочинний намір до завершення. Протидія шахрайству в мережі Інтернет оперативно-розшуковими заходами включає систему оперативно-розшукових та інших заходів і реалізується в окремих організаційно-тактичних формах [1, с. 545]. Шахрайсво в мережі Інтернет – серйозна проблема, яка потребує комплексного вирішення.

1. Гунько К. О. Щодо визначення способів вчинення шахрайства в мережі Інтернет у період воєнного стану. *Збірник матеріалів міжнародного правничого конкурсу наукових статей серед здобувачів закладів вищої освіти : матеріали Міжнар. правн. конкурсу наук. ст. серед здобувачів вищ. освіти* (м. Кропивницький, 21 квіт. 2023 р.). Кропивницький, 2023. С. 159–166.

2. Телійчук В. Г., Гунько К.О. Проблеми протидії шахрайству в мережі Інтернет як складової інформаційної безпеки в умовах воєнного стану. *Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали VII Міжнар. наук.-практ. конф.* (м. Дніпро, 17 бер. 2023 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2023. С. 542–545.

3. Іваненко Г. Є., Телійчук В. Г. Щодо проблеми протидії незаконному обігу вогнепальної зброї в мережі інтернет. *Modern research in world science : The 8 th International scientific and practical conference* (Lviv, October 29-31, 2022). Lviv, Ukraine, 2022. P. 227–230.

УДК 343.98
DOI: 10.31733/15-03-2024/2/85-87

Родіон КОВАЛЕНКО
курсант факультету підготовки
фахівців для підрозділів
кримінальної поліції

Андрій КИСЕЛЬОВ
доцент кафедри
оперативно-розшукової діяльності
Дніпровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

СУЧАСНІ МОЖЛИВОСТІ ТЕХНОЛОГІЇ «OSINT» У КРИМІНАЛЬНОМУ АНАЛІЗІ В УМОВАХ ВОЄННОГО СТАНУ

Особливості технології відкритих джерел інформації (OSINT) в кримінальному аналізі, особливо в умовах воєнного стану, включають в себе використання різноманітних джерел, таких як соціальні мережі, новинні портали, геопросторові дані, мовний аналіз, відкриті бази даних, відео та зображення. Ці джерела надають важливу інформацію щодо змін в планах, поведінці, зв'язках осіб та груп, а також дають можливість отримати актуальну інформацію про ситуацію в місцях конфлікту, тенденції та реакцію громадськості. Аналіз цих даних може бути здійснений шляхом використання програмних засобів для автоматизації процесу збору, фільтрації та аналізу, а також з використанням технологій розпізнавання облич, об'єктів та подій у відео- та фотозображеннях. Важливо пам'ятати про етичні норми та правові вимоги при зборі та використанні інформації з відкритих джерел, а також про необхідність використання OSINT разом з іншими джерелами та методами аналізу для

забезпечення повноти та точності даних.

Використання технології OSINT в кримінальному аналізі в умовах воєнного стану дозволяє оперативно та ефективно отримувати інформацію про події, осіб та організації, що може бути вирішальним для розслідування та протидії злочинності. Важливим елементом є також моніторинг і аналіз комунікацій у віртуальному просторі, що може стати джерелом інформації про плани, дії та інші важливі аспекти діяльності кримінальних груп чи окремих осіб.

Однією з важливих переваг використання технології OSINT є можливість аналізувати великі обсяги даних за короткий час, що дає змогу оперативно реагувати на зміни в ситуації та адаптувати стратегії протидії. Крім того, використання автоматизованих систем допомагає зменшити витрати часу та ресурсів на збір та обробку інформації, що є критичним у ситуаціях кризи [1, с. 55].

Необхідно також враховувати ризики та обмеження, пов'язані з використанням технології OSINT, зокрема, можливість поширення дезінформації та зміни даних в мережі для впливу на аналітичний процес. Тому важливо ретельно перевіряти джерела та достовірність отриманої інформації.

У цілому сучасні можливості технології OSINT в кримінальному аналізі в умовах воєнного стану є надзвичайно корисними та потужними інструментами для забезпечення безпеки та правопорядку. Однак їх використання вимагає компетентності, обережності та етичного підходу.

Важливо зазначити, що в умовах військового стану технологія OSINT може допомогти в прогнозуванні можливих загроз та виявленні потенційних точок напруження. Шляхом аналізу відкритої інформації можна виявити патерни та тенденції, які можуть свідчити про небезпеку або підготовку до провокацій чи агресії [2, с. 8].

Крім того, в контексті військових дій важливим є також використання технологій обробки великих обсягів даних (Big Data) для аналізу великих потоків інформації з різних джерел. Це дозволяє вчасно виявляти та реагувати на зміни в ситуації, виявляти тенденції та прогнозувати можливий розвиток подій.

Однак важливо враховувати ризики та етичні аспекти використання технології OSINT в кримінальному аналізі в умовах військового конфлікту. Недостовірна або неправдива інформація може призвести до неправильних висновків та рішень. Також необхідно дотримуватися законодавства та правил використання інформації з відкритих джерел, особливо в сфері захисту персональних даних та конфіденційної інформації.

Окрім цього, важливим аспектом використання технології OSINT у кримінальному аналізі в умовах воєнного стану є можливість виявлення та аналізу військової активності, переміщення військової техніки, розташування військових об'єктів та іншої важливої інформації для військового командування.

Також важливою можливістю є використання технології OSINT для моніторингу та аналізу інформації про злочинні групи, терористичні організації та інші небезпечні суб'єкти, які можуть використовувати військовий конфлікт для своїх цілей [3, с. 146].

Більш того, технологія OSINT може бути використана для моніторингу та аналізу інформації про гуманітарну ситуацію в зоні конфлікту, виявлення потреб населення та оцінки ефективності гуманітарної допомоги.

Загалом технологія OSINT відкриває широкі можливості для кримінального аналізу в умовах воєнного стану, проте вона вимагає від аналітиків високого рівня компетентності та професіоналізму для ефективного використання та інтерпретації отриманої інформації. Також необхідно постійно оновлювати та удосконалювати методи та інструменти аналізу з урахуванням швидких змін у військових та політичних умовах, а також, як зазначає А. Кисельов, враховувати тактичні та інші особливості під час оперативно-розшукової протидії кримінальним правопорушенням [4–7], в тому числі й під час пошуку інформації кримінального характеру за допомогою технології OSINT.

У висновку слід зазначити, що технологія відкритих джерел інформації (OSINT) виявляється незамінним інструментом для кримінального аналізу в умовах воєнного стану. Вона надає широкий спектр можливостей для збору, аналізу та інтерпретації важливої інформації, необхідної для забезпечення безпеки, виявлення та запобігання злочинності та, зокрема, ефективного управління військовими операціями.

Застосування технології OSINT дозволяє оперативно отримувати дані з різних джерел, таких як соціальні мережі, новинні портали, геопросторові дані тощо, що дозволяє отримати об'єктивну картину ситуації та приймати обґрунтовані рішення. Проте

використання технології OSINT також потребує уважності та етичного підходу, оскільки інформація з відкритих джерел може бути спотворена через маніпуляції або бути недостовірною.

Отже, враховуючи переваги та ризики використання технології OSINT, можна зробити висновок, що вона є важливим інструментом для забезпечення безпеки та правопорядку в умовах воєнного стану, вона повинна використовуватися з обережністю та компетентністю.

1. Батанов Є. А. Сучасні можливості технології «OSINT» у кримінальному аналізі в умовах воєнного стану : дис. ... канд. юрид. наук / Київ. нац. ун-т ім. Тараса Шевченка. Київ, 2023. 205 с.

2. Білоус О. В. Використання технології OSINT у кримінальному аналізі в умовах воєнного стану : автореф. дис. ... канд. юрид. наук / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2023. 20 с.

3. Гончаренко О. М. Деякі аспекти використання технології OSINT у кримінальному аналізі в умовах воєнного стану. *Вісник Національної академії правових наук України.* 2023. № 4. С. 144–151.

4. Кисельов А. О. Особливості документування підрозділами кримінальної поліції злочинних дій, пов'язаних із незаконним заволодінням транспортним засобом. *Оперативно-розшукова діяльність Національної поліції: проблеми теорії та практики : матеріали Всеукр. наук.-практ. конф.* (м. Дніпро, 19 жовт. 2018 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. С. 29–31.

5. Кисельов А. О. Тактика спілкування поліцейського з особами. *The Top Actual Researches in Modern Science : Proceedings of the IInd International Scientific and Practical Conference* (Ajman, July 28-29, 2016, UAE). *International Scientific and Practical Conference «World Science».* 2016. № 8 (12). P. 25–28.

6. Горелік Д. С., Кисельов А. О. Міжнародне співробітництво Національної поліції у сфері оперативно-розшукової діяльності. *Оперативно-розшукова діяльність Національної поліції: проблеми теорії та практики : матеріали Всеукр. наук.-практ. конф.* : у 2-х ч. (Дніпро, 19 жовт 2018 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. Ч. 1. С. 139–141.

7. Kyselov A., Kovalevska O. An investigation of effective police communication law enforcement roles requiring language skills // Methodological bases of studying the processes of general mental laws in human interaction with the environment. International Science Group. Boston : Primedia eLounch, 2022. 194 p. P. 39–47.

УДК 343.98
DOI: 10.31733/15-03-2024/2/87-88

Володимир КОЛЕСНИК
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції

Володимир ВАРАВА
доцент кафедри
оперативно-розшукової діяльності
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

ОКРЕМІ АСПЕКТИ КОНТРОЛЮ ЗА ТЕЛЕФОННИМИ РОЗМОВАМИ ПІДРОЗДІЛАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ У КОНТЕКСТІ ВОЄННОЇ БЕЗПЕКИ ДЕРЖАВИ

У сучасних умовах неможливо захистити громадян від злочинних посягань, ефективно виявляти та розслідувати злочини без використання інформації, що циркулює в телекомунікаційних мережах, та залучення технічних ресурсів операторів телекомунікацій.

Конституція України передбачає, що кожному гарантується таємниця телекомунікацій, телефонних розмов, телеграфної та іншої кореспонденції. У випадках, передбачених законом, суд може встановити винятки лише тоді, коли іншими способами одержати інформацію неможливо, з метою запобігти вчиненню злочину чи з'ясувати істину у кримінальній справі під час її розслідування [1]. Стаття 17 Міжнародного пакту про громадянські і політичні права передбачає, що ніхто не може зазнавати безпідставного або незаконного втручання в його особисте і сімейне життя, безпідставного посягання на