стосуються ситуації;

– не робити великих передплат під час покупки в інтернет-магазині;

– не користуватися підозрілими сервісами або пропозиціями інших громадян.

Зазвичай, люди або сервіси, які пропонують швидкий заробіток, на практиці і є шахраями.

Тож, підсумовуючи вищевикладене, потрібно правоохоронним органам та іншим органам проводити масові інформування населення щодо діяльності шахраїв, їх методів та прийомів, щоб люди не стали жертвою шахраїв. Наприклад, як це зробили у Вільногірському бюро правової допомоги, де провели бесіду з населенням про найпоширеніші нині види шахрайства, в тому числі і про «телефонних» злочинців та про наслідки таких SMS-повідомлень [3].

Бібліографічні посилання

1. Кримінальний кодекс України : Кодекс від 05.04.2001р. № 2341-III в редакції від 04.10.2021р. *Відомості Верховної Ради України (ВВР)*. 2001. № 25–26. Ст.131.

2. Прудка Л. М. Психологічні особливості шахрайства в мережі Інтернет. *Південноукраїнський правничий часопис*. 2018. № 2. С. 30–33.

3. Нужна О. Про шахрайство, яке завжди на часі, розповідають у Вільногірському бюро правової допомоги. URL: https://www.legalaid.gov.ua/novyny/pro-shahrajstvo-yake-zavzhdy-na-chasi-rozpovidayut-u-vilnogirskomu-byuro-pravovoyi-dopomogy/

Романенко П. П., курсант 3-го курсу
факультету підготовки фахівців
для підрозділів кримінальної поліції
Науковий керівник – Гребенюк А. М.,
доцент кафедри економічної
та інформаційної безпеки,
кандидат технічних наук, доцент
*(Дніпропетровський державний
університет внутрішніх справ)*

ІНФОРМАЦІЙНІ ПІДСИСТЕМИ, ЯКІ ДОПОМОГАЮТЬ РОЗСЛІДУВАННЮ ПІД ЧАС КРИМІНАЛЬНОГО АНАЛІЗУ

Розгляд цієї теми зумовлений розслідуванням правопорушень, які потребують використання кримінального аналізу. Інформаційні підсистеми допомагають досягнути очікуваного результату, але важливо правильно використовувати обрану підсистему аби прискорити процес пошуку.

Інформаційні підсистеми, які функціонують на базі Національної поліції України, допомагають розкриттю правопорушень різної складності,

бо в підсистемах міститься інформація, яка може прямо стосуватись правопорушення. Головним є правильність використання кожної підсистеми та спрямування її у правильне русло.

Наказ Міністерства внутрішніх страв України від 14.06.2019 р. № 508 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» містить в собі положення, які регламентують порядок формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України», призначеної для обробки відомостей під час прийняття та реєстрації заяв і повідомлень про кримінальні правопорушення та інші події. Тобто працівник поліції повинен забезпечити повноту та своєчасне внесення до Єдиного обліку відомостей, з якими працівники поліції будуть працювати або використовувати у кримінальному аналізі, тому від правильності введеної інформації буде залежати подальший хід справи [1].

Наявні деякі проблемні питання стосовно доступу до деяких підсистем, з якими працює Національна поліція. Проблема щодо здійснення доступу до ІПС ОНП («Цунамі», «Армор»), яка полягає у можливості входу одночасно з декількох робочих станцій під одним логіном та паролем, що може призводити до витоку інформації службового характеру, повинна бути у найкоротший час остаточно вирішена. Доступ до інформаційних підсистем має мати абсолютну захищеність, бо важливість збереження персональних даних у цьому контексті на першому плані [2].

Загалом досить поширеними інформаційними ресурсами залишаються соціальні мережі, за допомогою яких можна знаходити інформацію та використовувати її під час розслідування. Зараз, за результатами різних експертних оцінок, американські розвідувальні служби з відкритих джерел добувають від 35 % до 95 % розвідданих. У провідних країнах світу система OSINT є важливим інструментом захисту національних інтересів та основною складовою в діяльності профільних силових відомств [3].

Звісно, що інформаційні системи Національної поліції України досить ефективно виконують свої завдання та функції, але перед тим як безпосередньо переходити до пошуку, потрібно відібрати максимум інформації з відкритих джерел. Можливо, що саме технологія OSINT стане поштовхом до розкриття кримінального правопорушення або іншого протиправного діяння.

OSINT (Open Source INTelligence) – це збір, аналіз, обробка даних, які є в загальному доступі, але ці дані завжди специфічні, тобто зібрані та структуровані особливим способом для відповіді на конкретне питання [6].

Швидкість розслідування цілком залежить від аналітичних вмінь та вмінь правильно користуватися пошуком за відповідними даними. За кожною отриманою інформацією кримінальному аналітику необхідно

ухвалити рішення про її необхідність, зберігання і подальше використання. Засоби аналітичної обробки допомагають знизити витрати й заощадити час на пошук інформації, істотної для розкриття та розслідування злочинів [4].

Одним з головних критеріїв ефективності розслідування є захищеність даних інформаційних підсистем, які використовуються в діяльності поліції. Одним з головних шляхів захисту є криптографія. Стійкість будь-якої системи закритого зв'язку визначається ступенем таємності використовуваного в ній ключа. Проте цей ключ повинен бути відомий іншим користувачам мережі, щоб вони могли вільно обмінюватися зашифрованими повідомленнями. У цьому змісті криптографічні системи також допомагають вирішити проблему автентифікації (встановлення дійсності) прийнятої інформації. Для класичної криптографії характерне використання однієї секретної одиниці – ключа, що дозволяє відправникові зашифрувати повідомлення, а одержувачеві розшифрувати його [5].

Отже, інформаційні підсистеми під час розслідування мають важливе значення під час кримінального аналізу. Інформаційні підсистеми є неабиякою допомогою працівникам не тільки поліції, але й всіх правоохоронних органів загалом. В епоху інформатизації суспільства інформаційні ресурси стали допоміжним елементом пошуку для поліції. Тому потрібно, щоб інформаційні підсистеми правильно використовували, інформація повинна містити загально визначений характер, а також інформація повинна перебувати під абсолютним захистом, аби дані, які зберігаються, не потрапили до рук злочинців.

Бібліографічні посилання

1. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» : наказ МВС України від 14.06.2019 р. № 508. URL: https://zakon.rada.gov.ua/laws/show/z0739-19#Text (дата звернення: 22.03.2021).

2. Рижков Е. В., Дзех Я. С. Проблемні питання інформаційно-аналітичного забезпечення в системі органів Національної поліції та проблемні питання щодо захисту під час виконання службових обов'язків : зб. наукових статей за матеріалами доп. Всеукр. науково-практ. конф. 21 грудня 2018 року / упорядник Т. В. Магеровська. Львів : ЛьДУВС, 2018 С. 83–86.

3. Пащенко Т. П. Гібридна війна та соціальні мережі. *Інформаційний вимір гібридної війни: досвід України* : матеріали Міжнар. науково-практ. конф. Київ : НУОУ, 2017. С. 62–65.

4. Фаріон О. Б. Сфери застосування таких систем різноманітні. *Алгоритм опрацювання оперативно-розшукової інформації для забезпечення потреб кримінального аналізу злочинної діяльності* : зб. наукових пр. Націон. академії держав. прикордонної служби України. Серія : військові та технічні науки. 2013. № 1 (59). С. 194–203.

5. Кавун С. В., Носов В. В., Манжай О. В. Інформаційна безпека : навч. посіб. : у 2 ч. Харків : Вид-во ХНЕУ, 2008. Ч. 2. С. 78–79.

6. Политическое Экспертное Сообщество (Модель OSINT. Открытые источники в мире разведки). URL: http://strateger.net/model_osint_otkritie_istochniki_v_mire_razvedki (дата звернення: 29.10.2021).