УДК 343.98.06

Самойленко О.А.
к.ю.н., доцент,
доцент кафедри криміналістики
Національний університет «Одеська юридична академія»

ДО ПИТАННЯ ОЦІНКИ СЛІДЧИМ МАТЕРІАЛІВ ПЕРВИННОЇ ПЕРЕВІРКИ ОПЕРАТИВНОЇ ІНФОРМАЦІЇ ПРО ЗЛОЧИН, ВЧИНЕНИЙ У КІБЕРПРОСТОРІ

Постановка проблеми. Використана задля досягнення злочинного результату обстановка кіберпростору призводить до вчинення злочинів у різних сферах суспільних відносин: від національної безпеки до відносин власності. У кожному другому злочині кіберпростір є середовищем, що містить ознаки вчинення кримінального правопорушення. Інформаційна природа слідів вчинення таких злочинів зумовлює складності слідчого у питанні відкриття кримінального провадження, якщо джерелом обставин, що можуть свідчити про вчинені кримінальні правопорушення, виступають матеріали первинної перевірки оперативної інформації про вчинення такого злочину. Спеціалізація слідчих щодо розслідування злочинів цієї категорії регламентована лише на рівні ГСУ Національної поліції України, в регіонах слідчі не володіють достатнім обсягом знань для оцінки матеріалів перевірки інформації про вчинення злочинів у кіберпросторі.

Огляд останніх досліджень і публікацій. Оперативна інформація традиційно розуміється як фактичні дані, отримані оперативним підрозділом внаслідок здійснення гласних і негласних пошукових, розвідувательних і контррозвідувательних заходів, на основі яких вирішується завдання оперативно-розшукової діяльності [1, с. 509]. М.А. Погорецький та А.С. Кумичко наголошують на тому, що під час здійснення заходів оперативного пошуку оперативні працівники мають докладати зусиль для отримання саме фактичних даних про кримінальні правопорушення, а не оперативну інформацію, що має імовірний характер, оскільки лише фактичні дані можуть бути використані у кримінальному процесуальному доказуванні, набути статусу процесуального доказу у спосіб та у формі, що визначені кримінальним процесуальним законом для кожного виду доказів [2, с. 60]. По суті, фактичні дані, отримані під час оперативно-розшукової діяльності, повинні мати значення доказу в кримінальному провадженні. Це особливо важливо розуміти в контексті конкретизації напрямів діяльності слідчого на початковому етапі розслідування, визначення засобів збирання цифрових (електронних) доказів.

Окремі питання відкриття кримінального провадження в результаті здійснення первинної перевірки інформації про комп'ютерний злочин були предметом уваги в роботах П.Д. Біленчука, М.В. Гуцалюка, М.Ю. Літвінова, С.М. Рогозіна, К.В. Тітуніної, Д.М. Цехана, В.С. Цимбалюка, І.Ф. Харабе-рюша, В.П. Шеломенцева та інших науковців. Водночас проблематика відкриття кримінального провадження щодо традиційних злочинів, вчинених у кіберпросторі, набуває своєї актуальності.

Формулювання завдання дослідження. Метою статті є визначення особливостей оцінки слідчим матеріалів первинної перевірки інформації про злочин, вчинений у кіберпросторі, задля відкриття кримінального провадження.

Виклад основного матеріалу. Для того щоб оперативна інформація про вчинення

злочину була перспективною з позицій відкриття кримінального провадження, вона має бути підтверджена достовірними для слідчого джерелами, які закономірно пов'язані з документальністю факту її перевірки оперативним підрозділом, що оформлюється у вигляді матеріалів первинної перевірки.

Ці матеріали підлягають передачі керівнику органу досудового розслідування з метою внесення викладеної інформації до ЄРДР. Водночас варто акцентувати на оцінній діяльності начальника слідчого відділу/слідчого щодо матеріалів такої перевірки інформації про злочин. За умови неповноти та недостовірності інформації отримані слідчим матеріали перевірки повертають до оперативного підрозділу для доопрацювання з рекомендаціями щодо подальших дій суб'єкта перевірки. Тому для вирішення питання про відкриття кримінального провадження для слідчого особливого значення набувають офіційні документи, що підтверджують оперативну інформацію, та розуміння ним компетенції суб'єктів первинної перевірки, власне такі компетенції зумовлюють особливості здійснення останньої.

З огляду на спектр злочинів, що вчиняються у кіберпросторі, суб'єктів протидії їм, спираючись на матеріали слідчої практики, визначимо джерела, які дають змогу отримати офіційні відомості, що підтверджують або спростовують інформацію про факт вчинення злочину в кіберпросторі:

1) державні органи (мають контрольні та ліцензійні функції та можуть надати копії документів про діяльність підприємств, установ та організацій, виявлені порушення процесів, що контролюється державою):

– спеціально уповноважені державні органи в сфері телекомунікацій, зокрема орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації (Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язок) і підпорядковані їй регіональні органи (управління в областях));

– орган державного регулювання у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом, що здійснює також повноваження органу ліцензування, дозвільного органу, регуляторного органу та органу державного нагляду (контролю) (Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗІ));

– Національна рада України з питань телебачення і радіомовлення;

– Державне підприємство «Український державний центр радіочастот»;

– Національний банк України;

2) громадські об'єднання/організації (можуть надати офіційні аналітичні огляди; статистичні дані, повідомити щодо виявлення факту вчинення злочинів), наприклад, Інтернет асоціація України, Всеукраїнська громадська організація «Всеукраїнське агентство з авторських та суміжних прав», Державна організація «Українське агентство з авторських та суміжних прав», Асоціація «Телекомунікаційна палата України» та інші;

3) суб'єкт господарювання (оператори та провайдери) у сфері зв'язку та телекомунікацій (може документально підтвердити реєстраційні і технічні відомості, що дають змогу ідентифікувати власника, розробника, адміністратора інтернет-ресурсу, факт надання послуг зв'язку конкретному користувачу/відправнику/отримувачу в конкретну дату та час, надання послуг хостингу, надати відомості про фінансово-господарську діяльність, технічні аспекти функціонування мережі тощо);

4) комерційні банківські установи, суб'єкти господарювання у сфері платіжних систем (можуть документально підтвердити рух (обіг) коштів на рахунках підприємств, установ і організацій, окремих громадян, поточні та депозитні рахунки, надати інформацію про штат співробітників та інше);

5) засоби масової інформації (можуть підтвердити документально факт реклами, оголошення, динаміку розвитку ринку товарів і послуг, проведення офіційних заходів (виступів,

спортивних заходів, ярмарків і аукціонів); надати результати журналістських розслідувань);

6) міжнародні правоохоронні організації (можуть документально підтвердити місце розташування адміністратора та користувачів інтернет-ресурсу, що використовується під-час вчинення злочину на території України, при цьому фізично розміщується на серверах, розташованих поза її межами).

Відповідно п. 21 ч. 2 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» окремим напрямом функціонування кібербезпеки визначено здійснення оперативно-розшукових, розвідувальних, контррозвідувальних та інших заходів, спрямованих на запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються з використанням кіберпростору, розслідування, переслідування, оперативного реагування та протидія кіберзлочинності, розвідувально-підривній, терористичній та іншій діяльності у кіберпросторі, що завдає шкоди інтересам України, використанню мережі Інтернет у воєнних цілях. На подолання відповідного спектру злочинів, вчинених у кіберпросторі, відповідно до законів України «Про оперативно-розшукову діяльність», «Про Національну поліцію України» [3], «Про Службу безпеки України» [4], наказів НП України [5] спрямована діяльність підрозділів Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБ України (далі − ДКІБ) та Департаменту кіберполіції НП України (далі − ДКП) та інших підрозділів НП України. Охарактеризуємо специфіку їх діяльності в контексті перевірки оперативної інформації про злочин, що вчинений у кіберпросторі.

Підрозділи ДКП згідно з п. 2.1. Положення про ДКП НП України прямо вповноважені до протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Ця сфера діяльності іменується у Положенні «протидією кіберзлочинності». В Україні правові основи боротьби з кіберзлочинами визначаються, перш за все, Конвенцією Ради Європи про кіберзлочинність. Тому оперативні підрозділи ДКП прямо зобов'язані здійснювати оперативно-розшукову діяльність із метою протидії конвенційним злочинам (відповідальність за них фактично передбачена ст.ст. 163, 176, 185, 190, 200, 301, 361−363-1 КК України).

Для підрозділів ДКП типово джерелами оперативної інформації виступають: 1) електронні та письмові повідомлення про злочин у значенні звернення до органу поліції; 2) письмові доручення, постанови слідчого; 3) інші джерела.

У цьому контексті варто акцентувати на значенні заяви та повідомлення, що містять оцінні (суб'єктивні) судження заявника або не містять дані про особу відправника (анонімні). Їх за оцінкою начальника органу (підрозділу) поліції вважають зверненням і перевіряють саме шляхом оперативно-розшукової діяльності. Згідно з Порядком розгляду звернень та організації проведення особистого прийому громадян в органах та підрозділах Національної поліції України [6], щодо кожного звернення суб'єкта отримання не пізніше ніж у п'ятиденний термін приймають одне з таких рішень: 1) прийняти до розгляду; 2) передати на вирішення до підпорядкованого органу (підрозділу) поліції; 3) надіслати за належністю до іншого державного органу або посадовій особі; 4) залишити без розгляду за наявності підстав, визначених у ст. 8 Закону України «Про звернення громадян». Цей механізм у правоохоронних органах можна вважати «своєрідною фільтрацією» заяв і повідомлень про вчинений злочин.

Звернення осіб до підрозділів ДКП НП України здійснюється шляхом особистого відвідування відділення кіберполіції, відправлення листа поштою або більш поширеного нині подання електронного звернення через опцію «Форма подачі електронного звер-

нення» на офіційному веб-сайті ДКП. Останній спосіб звернень функціонує на веб-сторінках правоохоронних органів відповідно до вимог Закону України «Про внесення змін до Закону України «Про звернення громадян» щодо електронного звернення та електронної петиції» [7]. Аналіз матеріалів практики свідчить, що первинна перевірка інформації, викладеної в «електронному» зверненні, є практично обґрунтованою та результативною з позицій прийняття в подальшому слідчим рішення про відкриття кримінального провадження за такими матеріалами. Це пов'язано з кількома чинниками. По-перше, особу, що повідомила інформацію про злочин, завжди можна індивідуально визначити під час перевірки (для подачі звернення обов'язковою інформацією для заявника є його реквізити (прізвище, ім'я та по-батькові, дата народження, адреса проживання, номер телефону, електрона поштова скринька; до того ж можна встановити IP-адресу, що використовувалась для подання звернення) По-друге, не діє «фактор часу»: «електронні» повідомлення миттєво отримує співробітник спеціально створеного (з метою аналізу звернення та його перевірки) відділу. По-третє, як правило, заявник сам зацікавлений у розгляді свого звернення.

Зазначимо, щодо багатьох видів злочинів, протидія яким належить до компетенції підрозділів ДКП, кримінальне провадження здійснюється у формі приватного обвинувачення. Тому на практиці метою перевірки інформації про злочин, отриманої оперативним підрозділом з інших джерел, часто стає встановлення потерпілого та визначення його позиції щодо подання заяви про вчинення кримінального правопорушення. Останнє виступає обов'язковою умовою початку кримінального провадження щодо таких видів злочинів:

– порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер, без обтяжуючих обставин (ч. 1 ст. 163 КК України);

– порушення авторського права і суміжних прав без обтяжуючих обставин (ч. 1 ст. 176 КК України);

– порушення прав на винахід, корисну модель, промисловий зразок, топографію інтегральної мікросхеми, сорт рослин, раціоналізаторську пропозицію (ч. 1. ст. 177 КК України);

– незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару (ст. 229 КК України);

– незаконне збирання з метою використання відомостей, що становлять комерційну або банківську таємницю (ст. 231 КК України);

– розголошення комерційної або банківської таємниці, інсайдерської інформації (ст.ст. 232, 232-1 КК України);

– несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, без обтяжуючих обставин (ч. 1 ст. 361 КК України) або за обтяжуючих обставин, якщо вини вчинені чоловіком (дружиною) потерпілого (ч. 2 ст. 361 КК України);

– несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, без обтяжуючих обставин (ч. 1 ст. 362 КК України) або за обтяжуючих обставин, якщо вони вчинені чоловіком (дружиною) потерпілого (ч. 2 ст. 362 КК України).

НП України без деталізації її структурних одиниць відповідно до § 3 Стратегії кібербезпеки України належить до Національної системи кібербезпеки як орган, що забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі та здійснює заходи із запобігання, виявлення, припинення та розкриття таких злочинів. Тому щодо протидії

іншим альтернативним Конвенції злочинам, що вчиняються у кіберпросторі та підслідні слідчим НП України, завдання ДКП визначається як «сприяння в порядку, передбаченому чинним законодавством, іншим підрозділам НП України у попередженні, виявленні та припиненні кримінальних правопорушень» [5, с. 9]. З огляду на те, що здійснення оперативно-розшукової діяльності щодо альтернативних Конвенції злочинів згідно з окремими наказами НП України [5; 8–10] зараховано до компетенції, або Департаменту карного розшуку, або Департаменту захисту економіки, або Департаменту протидії наркозлочинності, оперативно-розшукова діяльність співробітників структурних підрозділів ДКП обмежується лише отриманням інформації про злочини, що вчинені у кіберпросторі, перевірка ж інформації здійснюється вже вищевказаними департаментами НП України. Отже, для інших підрозділів у складі кримінальної поліції НП України основним джерелом інформації про злочин, вчинений у кіберпросторі, часто є матеріали ДКП НП України.

Підрозділи ДКІБ є суб'єктом здійснення оперативно-розшукової діяльності щодо більшості злочинів, вчинених у кіберпросторі з антидержавно-політичних мотивів. Це ті злочини, що, як правило, підслідні слідчим органів безпеки (передбачені ст.ст. 109, 110, 110-2, 111−114-1, 258-258-5, 330, 436 КК України). Стратегією кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 р. за № 96/2016 [11], на СБ України покладений широкий спектр завдань щодо протидії злочинам проти миру і безпеки людства, які вчиняються у кіберпросторі, кібертероризму та кібершпигунства, а також щодо перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів щодо державних електронних інформаційних ресурсів та у сфері державної безпеки. Ці завдання не можуть бути розв'язані без постійно здійснюваних оперативних заходів, спрямованих на отримання інформації про осіб, факти й предмети, що становлять оперативний інтерес [12].

ДКІБ СБ України одночасно з ДКП НП України можуть із різних джерел отримати інформацію фактично про один і той самий злочин, що вчинений у кіберпросторі. Законодавчо закріплена можливість інформаційного обміну між НП України та СБ України (п. 3 ч. 5 ст. 5 та п. 12 ч. 3 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України») [13] фактично відображається в формі координації оперативно-розшукової діяльності вказаних суб'єктів задля організації перевірки інформації про злочин та взаємодії зі слідчим.

Висновки. Отже, з позиції організації перевірки оперативної інформації про злочини, вчинені у кіберпросторі, важливе значення має компетенція суб'єктів здійснення цієї діяльності, зокрема, ними можуть виступати:

1) підрозділи Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України;

2) оперативні підрозділи Департаменту кіберполіції Національної поліції України;

3) інші підрозділи в складі кримінальної поліції Національної поліції України. Одним із ключових аспектів відкриття кримінального провадження у процесі виявлення оперативним підрозділом злочину, вчиненого у кіберпросторі, є документальність факту перевірки оперативної інформації. Ми конкретизували офіційні джерела інформації про злочин, вчинений у кіберпросторі.

Анотація

У статті висвітлюються важливі для відкриття кримінального провадження аспекти первинної перевірки інформації про злочин, вчинений у кіберпросторі. Конкретизована компетенція суб'єктів здійснення первинної перевірки оперативної інформації, а також визначено джерела, які дають змогу отримати офіційні відомості, що підтверджують або спростовують інформацію про факт вчинення злочину у кіберпросторі.

Ключові слова: джерело, Департамент кіберполіції (ДКП), злочин, кіберпростір, Національна поліція (НП України), первинна перевірка, оперативна інформація.

Аннотация

В статье освещаются важные в целях начала уголовного производства аспекты первоначальной проверки информации о преступлении, совершенном в киберпространстве. Конкретизирована компетенция субъектов первоначальной проверки оперативной информации, а также определены источники, которые позволяют получить официальные сведения, подтверждающие или опровергающие информацию о факте совершения преступления в киберпространстве.

Ключевые слова: источник, Департамент киберполиции (ДКП), преступление, киберпространство, Национальная полиция (НП Украины), первичная проверка, оперативная информация.

Samoilenko O.A. To the question of the investigator's assessment of the materials of the initial verification of operative information about a crime committed in cyberspace

Summary

The article highlights the aspects of primary verification of information about a crime committed in cyberspace that are important for the purpose of opening criminal proceedings. The competence of subjects of primary verification of operational information has been specified, and sources have been identified that provide official information confirming or disproving information about the fact of a crime in cyberspace.

Key words: source, Department of Cyber Police (DCT), crime, cyberspace, National Police (NP of Ukraine), primary inspection, operational information

Список використаних джерел:

1. Міжнародно-поліцейська енциклопедія. У 10 томах / відп. ред. В.В. Коваленко, Є.М. Моїсєв, В.Я. Тацій, Ю.С. Шемшученко. Київ : Атака, 2011. Т. 6. Оперативно-розшукова діяльність поліції. 1232 с.
2. Погорецьким М.А., Кумичко А.С. Фактичні дані та їх значення для документування оперативними підрозділами злочинів у сфері рефінансування Національним банком України вітчизняних банків. *Вісник кримінального судочинства.* 2015. № 4. С. 54–62.
3. Про Національну поліцію України : Закон України від 02.07.2015 р. № 580-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/580-19.
4. Про Службу безпеки України : Закон України від 25.03.1992 р. № 2229-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2229-12.
5. Про затвердження Положення про Департамент кіберполіції НП України : Наказ НП України від 10.11.2015 р. № 85 / Офіційний матеріал Департаменту Документального забезпечення НП України.
6. Про затвердження Порядку розгляду звернень та організації проведення особистого прийому громадян в органах та підрозділах Національної поліції України : Наказ Міністерства внутрішніх справ України від 15.11.2017 р. № 93. URL: http://zakon.rada.gov.ua/laws/show/z1493-17.

7. Про внесення змін до Закону України «Про звернення громадян» щодо електронного звернення та електронної петиції : Закон України 02.07.2015 р. № 577-VIII. URL: http://zakon.rada.gov.ua/laws/show/577-19#n2.
8. Про затвердження Положення про Департамент карного розшуку НП України : Наказ НП України від 14.11.2015 р. № 90 / Офіційний матеріал Департаменту Документального забезпечення НП України.
9. Про затвердження Положення про Департамент захисту економіки НП України : Наказ НП України від 07.11.2015 р. № 81 / Офіційний матеріал Департаменту Документального забезпечення НП України.
10. Про затвердження Положення про Департамент протидії наркозлочинності НП України : Наказ НП України від 17.11.2015 р. № 95 / Офіційний матеріал Департаменту Документального забезпечення НП України.
11. Про рішення Ради національної безпеки і оборони України від 27 січ. 2016 р. «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 р. № 96/2016 / Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/96/2016#n11.
12. Отримання та використання первинної оперативно-розшукової інформації оперативними підрозділами ОВС України : монографія / А.В. Баб'як, В.П. Сапальов, М.В. Стащак, В.В. Шендрик. Львів : Каменяр, 2010. 167 с.
13. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19.