УДК 343.1
DOI https://doi.org/10.32844/2618-1258.2021.4.33

ЛИСЕЮК А.М.

ЗАСТОСУВАННЯ МЕТОДІВ КРИМІНАЛЬНОГО АНАЛІЗУ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ ПРАВООХОРОННИМИ ОРГАНАМИ

APPLICATION OF THE METHODS OF CRIMINAL ANALYSIS DURING THE INVESTIGATION OF CYBERCRIME BY LAW ENFORCEMENT AGENCIES

У статті розглядається застосування кримінального аналізу під час розслідування кіберзлочинів у інформаційній сфері. Автором визначено основні характеристики кіберзлочинності як суспільно шкідливого явища: транснаціональність, латентність, динамічність темпів зростання та трансформацій, анонімність, масштабність наслідків. Автор описує негативний вплив неконтрольованого розвитку способів вчинення злочинів з використанням кіберпростору на розробку актуальних методів, способів та прийомів розслідування кіберзлочинів.

У статті обґрунтовано визначення інформаційно-аналітичної діяльності як основного інструменту в розслідуванні злочинів, що вчиняються в інформаційній сфері. Висока ефективність практичного застосування оперативно-розшуковими підрозділами правоохоронних органів методу кримінального аналізу в протидії злочинності загалом та кіберзлочинності зокрема підтверджується результатами багатоепізодних проваджень, що охоплювали велику територію, включали значну кількість подій і суб'єктів злочинного угруповання зі складною структурною побудовою.

Поява можливості отримання нової, раніше невідомої інформації, не лише про події, але і про причинно-наслідкові зв'язки, додаткові кваліфікуючі ознаки, визначається як основна відмінність кримінального аналізу від інформаційно-аналітичної діяльності.

Автор наголошує на необхідності вирішення низки проблемних питань під час застосування кримінального аналізу в діяльності оперативних підрозділів правоохоронних органів: необхідність подальшої розбудови нормативно-правової бази у сфері використання кримінального аналізу в правоохоронних органах; не належний рівень використання можливостей кримінального аналізу в оперативних органах; недостатня забезпеченість оперативних підрозділів сучасною оргтехнікою, комп'ютерним програмним забезпеченням та перш за все методами кримінального аналізу в протидії кіберзлочинам; формування відповідних інформаційних банків даних тощо.

У статті зазначається доцільність дослідження засад кримінального аналізу як позитивного досвіду застосування аналітичних інструментів у сфері протидії кіберзлочинності у країнах Євросоюзу та покладення в основу розробки теоретико-методологічних засад його прикладного використання в національному кіберпросторі.

Ключові слова: *кримінальний аналіз, кіберзлочини, правоохоронні органи, інформаційно-аналітична діяльність, методи кримінального аналізу.*

The article considers applying criminal analysis during the investigation of cybercrimes in information sphere. The author defines main peculiarities of cybercrime as socially harmful phenomenon: transnationalism, latency, dynamic pace of increase

© ЛИСЕЮК А.М. – кандидат юридичних наук, головний спеціаліст (Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України), доцент кафедри оперативно-розшукової діяльності (Університет державної фіскальної служби України)

and transformations, anonymity, the magnitude of the consequences. The author describes the negative effect of uncontrolled development of ways of committing crimes using cyberspace on the process of designing relevant methods, ways and techniques of cybercrimes investigation.

The definition of information-analytical activity as a major tool for investigation of the crimes, committed in information sphere is substantiated in the article. High efficiency of practical application by units of law enforcement agencies of the criminal analysis methods in combating crime in general and cybercrime in particular is confirmed by the results of multi-episode proceedings, which covered a big territory, included a significant number of events and subjects of criminal group with complex structure.

The emergence of opportunity to gain new, unknown before information not only about events, but also about cause-and-effect relationships, additional qualifying features is determined as the main difference between criminal analysis and information-analytical activity.

The author emphasizes the need to address a number of issues in the application of criminal analysis in the activities of operational units of law enforcement agencies: the need to further develop the regulatory framework for the use of criminal analysis in law enforcement agencies; inadequate level of use of criminal analysis opportunities in operational bodies; insufficient provision of operational units with modern office equipment, computer software and, above all, methods of criminal analysis in the fight against cybercrime; formation of appropriate information data banks, etc.

The article notes the expediency of studying the principles of criminal analysis as a positive experience in the use of analytical tools in the field of combating cybercrime in the European Union and laying the foundation for the development of theoretical and methodological principles of its application in national cyberspace.

Key words: *criminal analysis, cybercrimes, law enforcement agencies, information-analytical activity.*

Вступ. Основним чинником, що свідчить про ефективність здійснення запобігання кримінальним правопорушенням, є рівень системи накопичення, концентрації та використання різної інтегрованої оперативно-розшукової інформації, що здобувається оперативним та оперативно-технічним шляхом. Тому під час кримінального аналізу забезпечується цілеспрямований пошук, виявлення, обробка та фіксація, вилучення, упорядкування, аналіз та оцінка здобутої кримінальної інформації, її представлення або візуалізація, передача та реалізація [1, с. 175].

Сучасні глобалізаційні процеси в поєднанні з інтенсивною інформатизацією зумовлюють динамічні явища, що визначають пріоритет напряму державної політики у сфері забезпечення не тільки національної безпеки загалом, а також і кожного з її складників зокрема, бо це є важливим складником безпеки як цілісної системи. Сьогодні інформаційна сфера утворює з'єднуючу ланку основи життєдіяльності суспільства, а забезпечення інформаційної безпеки визнається одним із фундаментальних чинників його подальшого розвитку. За таких умов особливого значення набуває усунення негативних впливів та подолання суспільно небезпечних явищ, що мають прояви в інформаційній сфері, одним з яких є кіберзлочинність.

Постановка завдання. Важко недооцінити суспільну шкідливість кіберзлочинності, зважаючи на те, що основною їх характеристикою є транснаціональність, латентність, динамічність темпів зростання та трансформацій, анонімність, масштабність наслідків.

Неконтрольований розвиток способів вчинення злочинів з використанням кіберпростору є великою проблемою для розробки актуальних методів, способів та прийомів розслідування кіберзлочинів, адже з часом виникають як зовсім нові способи вчинення злочину, так і способи, що запозичені з певних вже діючих механізмів вчинення злочину, які удосконалюють і таким чином підвищують їхню ефективність у декілька разів, як-от: розповсюдження комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, викрадення інформації, розміщеної на матеріальних носіях, та порушення правил експлуатації автоматизованих електронно-обчислювальних систем і ще велика кількість інших способів вчинення кіберзлочинів, відомих лише правоохоронним органам.

Результати дослідження. Кримінальний аналіз є специфічним видом інформаційно-аналітичної діяльності, яка полягає в ідентифікації та якомога більш точному визначенні внутрішніх зв'язків між інформаціями (відомостями, даними), що стосуються злочину, і будь-якими іншими

даними, отриманими з різних джерел, їх використанням в інтересах ведення оперативно-розшукової та слідчої діяльності, їх аналітичної підтримки [2, с. 82].

Інформаційно-аналітична діяльність є основним інструментом у розслідуванні злочинів, що вчиняються у різних сферах, тому визначення цього виду діяльності є необхідним для загального поняття та формування питання у роз'ясненні поставленої проблеми, адже інформаційно-аналітична діяльність – це особливий напрям інформаційної діяльності із застосуванням аналітичних методів, що пов'язаний з пошуком, виявленням, опрацюванням, аналізом, збереженням та використанням інформації.

Інструментальний зміст у системі уточнюється через сутність інформаційно-аналітичного забезпечення діяльності аналітичних підрозділів правоохоронних органів та проведення кримінального аналізу отриманої (наявної) інформації.

Значною відмінністю кримінального аналізу від інформаційно-аналітичної діяльності є те, що створюється можливість отримання нової, раніше невідомої інформації, не лише про події, явища, але і про причинно-наслідкові зв'язки, додаткові кваліфікуючі ознаки [3, с. 236].

У ході здійснення кримінального аналізу забезпечується цілеспрямований процес пошуку, виявлення, фіксації, вилучення, упорядкування, аналізу та оцінки кримінальної інформації, її представлення (візуалізація), передача та реалізація.

Практичне застосування оперативно-розшуковими підрозділами правоохоронних органів методів кримінального аналізу в протидії злочинності загалом та кіберзлочинності зокрема підтвердило його високу ефективність у багатоепізодних провадженнях, що охоплювали велику територію, включали значну кількість подій і чітке визначення суб'єктів злочинного угруповання зі складною структурною побудовою.

Враховуючи вищесказане, слід зазначити, що з метою протидії кіберзлочинам підрозділи, що здійснюють кримінальний аналіз, повинні вирішувати такі завдання:

– якісне комплектування підрозділу, формування професійного ядра та організація підготовки фахових кадрів, що включатиме жорсткі умови відбору працівників до підрозділів, що здійснюють кримінальний аналіз, та організацію співпраці з профільними закладами вищої освіти для підготовки фахівців аналітиків з початкового рівня до вищого, залучення їх можливостей для проведення проходження навчальних та виробничих практкурсів підвищення кваліфікації.

Проте вивчення різноманітних аспектів застосування кримінального аналізу в діяльності оперативних підрозділів правоохоронних органів дає підстави виділити низку таких проблемних питань:

– необхідність подальшої розбудови нормативно-правової бази у сфері використання кримінального аналізу в правоохоронних органах;

– неналежний рівень використання можливостей кримінального аналізу в оперативних органах;

– недостатня матеріально-технічна забезпеченість оперативних підрозділів сучасною оргтехнікою, комп'ютерним програмним забезпеченням та перш за все методами проведення кримінального аналізу в протидії кіберзлочинам;

– формування відповідних інформаційних банків баз даних тощо.

Таким чином, для подальшого розвитку і впровадження кримінального аналізу в правоохоронну практику держави доцільно провадити його розбудову.

Викладене не охоплює всіх проблемних аспектів створення та розвитку кримінального аналізу в національному правовому полі, однак дає підстави для здійснення подальших наукових розробок. Варто також погодитись із висновками вчених [4, с. 24], які вважають, що дослідження засад кримінального аналізу як позитивного досвіду застосування аналітичних інструментів у сфері протидії кіберзлочинності у країнах Євросоюзу доцільно покласти в основу розробки теоретико-методологічних засад його прикладного використання в національному кіберпросторі.

Успішна реалізація та впровадження нових методів кримінального аналізу дасть можливість у майбутньому поширити її на всю систему та активно використовувати аналітичні способи і прийоми, завдяки яким можливо забезпечити виконання завдань оперативно-розшукової діяльності, створити передумови для більш ефективного виконання суб'єктами оперативно-розшукової діяльності своїх завдань і правоохоронних функцій, що сприятиме підвищенню ефективності протидії кіберзлочинності.

Висновки. Підсумовуючи вищесказане, слід зазначити, що кримінальний аналіз як спосіб боротьби з кіберзлочинами є дуже ефективним та заслуговує уваги не тільки зі сторони науковців, а й держави, адже впровадження та вдосконалення нормативної бази для належного функціону-

вання правоохоронних органів, які провадять свою діяльність в інформаційній та правоохоронній сферах та здійснюють кримінальний аналіз, фінансування держави, надання матеріально-технічної бази та створення належних умов для виключного виконання своїх завдань правоохоронними органами, спонукатиме до збільшення ефективності розслідування саме кіберзлочинів.

Список використаних джерел:

1. Деревягін О.О. Перспективи застосування методики кримінального аналізу у протидії кіберзлочинам. *Кібербезпека в Україні: правові та організаційні питання: матеріали ІІ Всеук. наук. практ. конф*. (м. Одеса, 17 лист. 2017 р.). Одеса : ОДУВС, 2017. С. 175–176.

2. Власюк О.В. Роль і місце кримінального аналізу у розкритті та розслідуванні злочинів на державному кордоні України. *Матеріали постійно діючого науково-практичного семінару*. Харків : Інститут підготовки юрид. кадрів для СБУ Нац. юрид. акад. України ім. Я. Мудрого, 2011. Вип. 3. Ч. 1. С. 82–85.

3. Цигикал П. Кримінальний аналіз як елемент системи інформаційного забезпечення оперативно – розшукової діяльності. *Збірник наукових праць національної академії державної прикордонної служби України серія: військові та технічні науки*, № 2 (72) 2017. С. 234–240.

4. Заєць О.М. Інститут аналітичного супроводження досудового розслідування кримінального провадження в Україні: сучасний стан і перспективи розвитку. *Вісник кримінального судочинства*, 2016. № 4. С. 17–25.

УДК 343.13
DOI https://doi.org/10.32844/2618-1258.2021.4.34

НИКИФОРЕНКО Ю.Л.

КРИМІНАЛЬНЕ ПРОВАДЖЕННЯ У ПОРЯДКУ ПЕРЕЙНЯТТЯ ЯК ОДНА ІЗ ФОРМ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА

TAKEOVER OF CRIMINAL PROCEEDINGS AS A FORM OF INTERNATIONAL COOPERATION

У статті звертається увага на те, що перейняття кримінального переслідування є однією з форм міжнародного співробітництва, яка полягає у здійсненні компетентними органами однієї держави розслідування з метою притягнення особи до кримінальної відповідальності за злочини, вчинені на території іншої держави, за її запитом. Перейняття кримінального провадження може здійснюватися у таких формах: перейняття кримінального провадження від компетентних органів іноземної держави; передання компетентному органу іншої держави кримінального провадження у порядку перейняття. У теорії кримінального процесу виділяють два види перейняття: лише матеріалів кримінального провадження; перейняття матеріалів, поєднане з передачею підозрюваного (обвинуваченого).

Запропоновано виділяти такі умови перейняття кримінального провадження: фактор громадянства та місця проживання; наявність складу злочину; відсутність преюдиційних фактів. Для визначення форми міжнародного співробітництва у кримінальних провадженнях ключове значення відіграє громадянство підозрюваного (обвинуваченого).

Наголошується на необхідності відмежування перейняття кримінального провадження від екстрадиції та визнання і виконання вироків судів іноземних дер-

© НИКИФОРЕНКО Ю.Л. – аспірант кафедри кримінального процесу (Національна академія внутрішніх справ)