Соціально-правові студії. 2021. Випуск 2 (12). С. 94-100
Social & Legal Studios. 2021. Issue 2 (12). P. 94-100

UDC (УДК) 343.983

Пелещак Олег Романович,
здобувач наукового ступеня доктора філософії у галузі права
кафедри кримінального процесу та криміналістики
Львівського державного університету внутрішніх справ
(Львів, Україна)
e-mail: pelsh79@ukr.net
ORCID ID: 0000-0002-2785-7464

ТИПОВІ СЛІДЧІ СИТУАЦІЇ ПОЧАТКОВОГО ЕТАПУ РОЗСЛІДУВАННЯ КІБЕРДИВЕРСІЙ

Анотація. Зазначено, що через гібридну війну з Російською Федерацією на території України значно почастішали випадки вчинення злочинів проти національної безпеки України, зокрема диверсій, які старанно маскуються під інші кримінальні правопорушення, що не дає змоги одразу організувати та провести об'єктивне досудове розслідування належним суб'єктом. Запропоновано узагальнені слідчі ситуації та першочергові тактичні завдання, вирішення яких сприятиме виконанню завдань кримінального провадження та уникненню дублювання роботи різними правоохоронними органами.

Ключові поняття: кібердиверсія, належний суб'єкт розслідування, слідча ситуація, першочергові тактичні завдання.

Peleshchak Oleh,
Postgraduate Student
of the Department of Criminal Procedure and Criminalistics,
Lviv State University of Internal Affairs
(Lviv, Ukraine)
e-mail: pelsh79@ukr.net
ORCID ID: 0000-0002-2785-7464

TYPICAL INVESTIGATIVE SITUATIONS OF THE INITIAL STAGE OF CYBER DIVERSIONS INVESTIGATION

Abstract. Ensuring Ukraine's national security is becoming an increasingly important task in the context of the implementation of the European vector of development and the hybrid war with Russia. In the conditions of an undeclared war, sabotage on the territory of Ukraine is more real than ever. Such crimes are professionally disguised as other criminal offenses, in particular in the field of use of computers, systems, and computer networks and telecommunication networks, and the ways of their commission are quite diverse and are qualified by separate articles of the Criminal Code of Ukraine. It is sometimes problematic for law enforcement agencies to objectively classify a criminal offense at the initial stage of the investigation, which leads to duplication of work by different bodies of the pre-trial investigation, its improper subject, resulting in the unsatisfactory implementation of the prosecution and thus failure to perform criminal proceedings.

The purpose of the study is to summarize typical investigative situations and identify tactical tasks to be addressed as a matter of priority, the initial stage of investigation of criminal offenses in the use of computers, systems, and computer networks, and telecommunications networks to confirm or refute the presence of signs of sabotage.

According to the results of the study, it was concluded that the need to identify specific investigative situations is due primarily to the fact that clarifying its elements significantly saves time and resources of law enforcement to address typical tactical tasks that must be performed to determine the appropriate subject of investigation (jurisdiction). The typification of investigative situations of the next stage of investigation of criminal offenses by the proper subject of investigation directly depends on the timely and objective solution of the priority tactical tasks. The latter is directly affected by the state of the investigation of criminal proceedings, which is determined by the degree of fulfillment of the tactical tasks of the initial stage of the investigation. The state of the criminal investigation should be assessed in order to determine a model of the situation in which the appropriate subject of the investigation will have to initiate the next stage of the investigation.

Key concepts: cyber diversion, proper subject of investigation, investigative situation, priority tactical tasks.

DOI 10.32518/2617-4162-2021-2-94-100

Вступ

Забезпечення національної безпеки України набуває дедалі більшої актуальності в умовах реалізації європейського напряму розвитку та гібридної війни з Росією. Через неоголошену війну диверсії на території України є надреальними. Такі злочини професійно маскуються під інші кримінальні правопорушення, зокрема у сфері використання комп'ютерних мереж і систем, електронно-обчислювальних машин (комп'ютерів) тощо, а способи їх учинення є доволі різноманітними та кваліфікуються за окремими статтями Кримінального кодексу України. Правоохоронним органам інколи проблематично об'єктивно кваліфікувати кримінальне правопорушення на початковому етапі розслідування, що призводить до дублювання роботи різними органами досудового розслідування, її проведення неналежним суб'єктом, результатом чого є незадовільна реалізація функції обвинувачення, а відтак і невиконання завдань кримінального провадження. Однією із гарантій, яка не може бути обмежена, є недопустимість обґрунтування обвинувачення особи у вчиненні кримінального правопорушення на доказах, одержаних поза встановленим законом порядком. Під час оцінювання на предмет допустимості як доказів отриманих фактичних даних про вчинення чи підготовку кримінального правопорушення враховується ініціативний або ситуативний (випадковий) характер дій фізичних (юридичних) осіб, їх мету та цілеспрямованість при фіксуванні зазначених даних. Отже, обвинувачення не може ґрунтуватися на фактичних даних, одержаних у результаті слідчих (розшукових) дій уповноваженою на те особою без дотримання конституційних положень або з порушенням порядку, встановленого законом, а також не уповноваженою особою (суб'єктом). Лише у разі доведеності вини може мати місце визнання особи винуватою у вчиненні кримінального правопорушення, а саме обвинувачення не може ґрунтуватися на припущеннях, а також на незаконних доказах.

Як свідчить практика, трапляються ситуації, коли різні правоохоронні органи майже одночасно відкривають кримінальні провадження, хоча останні, як виявляється, взаємопов'язані спільним умислом, об'єктами та суб'єктами посягання тощо. В кінцевому результаті слідчі підрозділи Національної поліції, витративши значні ресурси правоохоронного органу і встановивши з часом ознаки диверсії, передають кримінальне провадження за підслідністю до слідчих підрозділів Служби безпеки України або через суб'єктивні обставини не помічають наявність у кримінальному провадженні матеріалів, які є підставою для передачі останнього до іншого правоохоронного органу, що, звичайно, є негативною практикою правоохоронної діяльності і не відповідає завданням кримінального провадження. Для її викорінення дуже важливим є узагальнення типових слідчих ситуацій і відповідних тактичних завдань, які першочергово потрібно вирішити слідчим на початковому етапі розслідування згадуваних кримінальних правопорушень.

Наукову розвідку проблемних питань щодо виявлення, кримінально-правової кваліфікації, розслідування та відповідальності за вчинення диверсій здійснили Д. С. Артеменко, О. Ф. Бантишев, О. Д. Довгань, О. О. Дудоров, О. Ю. Звонарьов, В. С. Картавцев, А. С. Климосюк, О. О. Климчук, В. В. Колосков, А. М. Лисенко, В. А. Ліпкан, О. І. Манартович, М. І. Мельник, В. О. Навроцький, В. В. Сташис, В. Я. Тацій, В. П. Тихий, М. І. Хавронюк, В. Г. Хлань, О. О. Черноног, О. А. Чуваков, О. Г. Ященко.

Дослідженням проблемних аспектів розслідування кримінальних правопорушень, учинених із використанням комп'ютерних мереж і систем комп'ютерів, займалися П. Д. Біленчук, А. С. Білоусов, М. В. Гуцалюк, М. Ю. Літвінов, І. М. Осика, Л. П. Паламарчук, А. В. Реуцький, С. М. Рогозін, Б. В. Романюк, С. В. Самойлов, К. В. Тітунініна, Д. М. Цехан, В. С. Цимбалюк, В. П. Шеломенцев, С. С. Чернявський.

Проблеми боротьби із кіберзлочинами досліджували В. М. Бутузов, А. Ф. Волобуєв, В. Д. Гавловський, М. В. Карчевський, О. І. Котляревський, М. О. Кравцова, О. М. Лепеха, О. В. Манжай, А. І. Марущак, Д. В. Пашнєв, Є. Д. Скулиш, І. Ф. Хараберюш, В. Г. Хахановський, В. В. Чернєй.

Однак проблематика виявлення на початковій стадії розслідування ознак диверсії, вчиненої із використанням комп'ютерних мереж та систем, мереж електрозв'язку, електронно-обчислювальних машин (комп'ютерів), та її вплив на вибір ефективних форм розслідування належним суб'єктом потребує подальших досліджень із метою задоволення сучасних потреб науки та практики боротьби зі злочинністю.

Метою статті є узагальнення типових слідчих ситуацій і виокремлення тактичних завдань, які підлягають першочерговому вирішенню, початкового етапу розслідування кримінальних правопорушень у сфері використання комп'ютерних мереж і мереж електрозв'язку, електронно-обчислювальних машин (комп'ютерів), систем для підтвердження або спростування наявності ознак диверсії.

1. Теоретичні засади змісту слідчої ситуації

Слідчі ситуації взаємопов'язані з деякими іншими процесами, що відбуваються в певний момент, об'єктивною дійсністю та її конкретними умовами. Для визначення шляхів і засобів найефективнішого криміналістичного використання чи зміни ситуації в сприятливий для слідства бік, а також вибору найбільш оптимальних прийомів і методів подальшого розслідування потрібно досконально розібратися у всіх елементах конкретної слідчої ситуації і правильно її оцінити з урахуванням інших умов об'єктивної дійсності, що впливають на неї. До них, зокрема, належить питання розуміння, змісту слідчої ситуації й особливості їхнього оцінювання у зв'язку з необхідністю прийняття відповідних слідчих рішень [1, с. 85]. На початкових етапах розслідування потрібно спиратися на вихідні дані, що характеризують явні ознаки кримінального правопорушення. Зазвичай науковці виокремлюють два основні підходи до розуміння слідчих ситуацій. Перший (практичний) – слідча ситуація розглядається як багатокомпонентна сукупність умов (інформаційного, процесуального, психологічного, тактичного, матеріально-технічного характеру), в яких здійснюється розслідування в певний його момент [2, с. 116]. Він орієнтує на аналіз конкретної слідчої ситуації. При другому підході до уваги береться лише інформаційний компонент умов розслідування як найбільш значущий – слідча ситуація розглядається як сукупність інформації (доказів та оперативно-розшукових відомостей), яка найбільш характерна для певного етапу розслідування в кримінальних провадженнях окремих категорій [3, с. 38; 4, с. 72].

2. Практика відкриття кримінальних проваджень

У зв'язку із військовою агресією Російської Федерації значно почастішали диверсії на території та об'єктах нашої держави, вчинені із використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Кримінальні провадження за готування або вчинення диверсії підслідні органам безпеки і зазвичай відкриваються в результаті самостійного виявлення ознак кримінального правопорушення правоохоронним органом, в процесі розслідування іншого кримінального правопорушення, і, подекуди, за заявою осіб. Кримінальні провадження за готування або вчинення кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку відкриваються органом досудового розслідування Національної поліції, переважно, за заявою юридичної або фізичної особи. Відтак внесення відповідних відомостей до Єдиного реєстру досудових розслідувань (далі – ЄРДР) за ст.ст. 361–363-1 КК України [5] здійснюють слідчі органів Національної поліції, а за ст. 113 КК України – слідчі Служби безпеки України.

3. Типові слідчі ситуації та тактичні завдання, які підлягають першочерговому вирішенню

Початкові етапи розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (ст.ст. 361–363-1 КК України), залежно від характеру вихідних даних про наявність в діянні ознак кримінального правопорушення, передбаченого ст. 113 КК України, можуть відрізнятися, а тому не цілком коректно говорити про саме типові слідчі ситуації, які виникають на початковому етапі розслідування. Ми схиляємося до думки віднести їх все ж таки до комбінованих слідчих ситуацій, зважаючи на високу ймовірність учинення саме диверсій через або із використанням електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж тощо. Нагадаємо, що під поняттям «кібердиверсія» в попередніх дослідженнях нами обґрунтовується взаємозв'язок ст. 113 КК України «Диверсія» зі ст.ст. 361, 361-1, 361-2, 362, 363, 363-1 КК України [6, с. 31; 7, с. 233–234].

Спробуємо узагальнити та деталізувати такі ситуації.

1. Ситуації, що характеризуються наявністю персоналізованих відомостей про ймовірного злочинця

Ситуація 1.1. Кримінальне провадження розпочато в результаті отримання заяви/повідомлення особи про кримінальне правопорушення, а матеріали кримінального провадження містять фактичні дані із персоналізованими відомостями про особу злочинця. Така ситуація типова при розслідуванні кримінальних правопорушень, учинених особою, яка має доступ до відповідних систем або мереж, наміри якої спрямовані на заволодіння чужим майном. Потерпіла сторона, як правило, є юридичною особою. Наявність матеріалів внутрішньої перевірки (аудит, технічна перевірка, моніторинг мереж тощо) значно спрощує планування початкового етапу розслідування.

Ситуація 1.2. Кримінальне провадження розпочато в результаті перевірки оперативної інформації, а матеріали первинної перевірки містять персоналізовані фактичні дані про особу злочинця. Ситуація типова при розслідуванні так званих кіберзлочинів. Підставою

для відкриття кримінального провадження є матеріали з територіального підрозділу кіберполіції, водночас особа або група осіб (співучасників) затримана оперативним підрозділом.

Ситуація 1.3. Кримінальне провадження розпочато в рамках реалізації матеріалів оперативно-розшукової справи (далі – ОРС), а ідентифікація особи злочинця є результатом діяльності оперативних підрозділів відповідно до проведених заходів, передбачених планом реалізації матеріалів ОРС, складеним спільного зі слідчим. Ситуація є типовою при розслідуванні тяжких та особливо тяжких злочинів, учинених із корисливих мотивів, тяжких конвенційних злочинів, учинених професійними злочинцями із специфічними навиками.

Припускаючи можливість вчинення завуальованої кібердиверсії, на початковому етапі розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку основними тактичними завданнями для слідчого, а відповідно і для оперативного підрозділу, який здійснює оперативне супроводження кримінального провадження, є встановлення предмета кримінального правопорушення, передбаченого ст. 113 КК України, посягання на який учинено за допомогою електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж, мереж електрозв'язку.

Для початкового етапу розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку важливим є встановлення режиму роботи згаданих машин, систем, мереж та конкретних фактів здійснення незаконних дій щодо останніх (ст. 361 КК України); встановлення фактів створення з метою використання, розповсюдження або збуту, а також розповсюдження або збуту шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу таких машин, систем, мереж (ст. 361-1 КК України); встановлення фактів несанкціонованого збуту або розповсюдження інформації з обмеженим доступом, яка зберігається в згаданих комп'ютерах, системах, мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства (ст. 361-2 КК України); встановлення фактів несанкціонованої зміни, знищення або блокування інформації, яка оброблюється в системах або мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, а також несанкціоновані перехоплення або копіювання інформації, яка оброблюється на комп'ютерах, в мережах, системах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації (ст. 362 КК України); встановлення порушення правил експлуатації комп'ютерів, відповідних систем, мереж або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України); встановлення фактів перешкоджання роботі комп'ютерів, відповідних систем, мереж шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1 КК України); встановлення особи чи кола осіб, що мали змогу вчинити зазначене кримінальне правопорушення; встановлення фактів приховування кримінального правопорушення, передбаченого ст. 113 КК України (вчинене із використанням комп'ютерів, відповідних систем, мереж, за допомогою шкідливих програм та технічних засобів, призначених для несанкціонованого втручання в роботу комп'ютерів, відповідних систем, мереж); встановлення способів витоку інформації з обмеженим доступом, яка зберігається в комп'ютерах, відповідних системах, мережах або на носіях такої інформації, встановлення фактів несанкціонованих змін, знищення перехоплення, копіювання інформації або блокування інформації; встановлення фактів порушення правил експлуатації комп'ютерів, відповідних систем, мереж або порядку чи правил захисту інформації, яка в них оброблюється; встановлення фактів умисного масового розповсюдження повідомлень, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи відповідних комп'ютерів, систем, мереж; встановлення місцезнаходження співучасників, фактичних даних щодо них та їхніх зв'язків; встановлення зв'язку кримінальної події із іншими кібердиверсіями; встановлення способів вчинення диверсії із їх подальшою кримінально-правовою кваліфікацією; забезпечення можливостей відшкодування матеріальних збитків.

Для вирішення тактичних завдань із виявлення кібердиверсії першочергово проводяться такі слідчі (розшукові) дії – з метою виявлення та фіксації відомостей щодо обставин учинення кримінального правопорушення проводиться огляд місця події, якщо це не було здійснено до початку кримінального провадження; допит працівників організації у сфері використання комп'ютерів, відповідних систем, мереж, а також людей, які можуть бути свідками виявленого кримінального правопорушення; допит потерпілого; призначаються різновиди комп'ютерно-технічної експертизи (апаратно-комп'ютерна експер-

тиза, програмно-комп'ютерна експертиза, комп'ютерно-мережева експертиза, інформаційно-комп'ютерна експертиза).

Для забезпечення кримінального провадження ухвалюються процесуальні рішення щодо тимчасового доступу до документів і розшуку підозрюваного, установлення місця, звідки дистанційно вчинялося кримінальне правопорушення. Щоб зробити висновки, висунути версії щодо причетності особи або групи осіб до вчиненого кримінального правопорушення повинні бути проведені відповідні негласні слідчі (розшукові) дії, зокрема аудіо-, відеоконтроль особи (ст. 260 КПК України), накладення арешту на кореспонденцію (ст. 261 КПК України), огляд і виїмка кореспонденції (ст. 262 КПК України), зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України) та електронних інформаційних систем (ст. 264 КПК України), фіксація та збереження інформації, отриманої з телекомунікаційних мереж за допомогою технічних засобів та в результаті зняття відомостей з електронних інформаційних систем (ст. 265 КПК України), спостереження за особою, річчю або місцем (ст. 269 КПК України), аудіо-, відеоконтроль місця (ст. 270 КПК України) [8].

2. Ситуації, що характеризуються відсутністю відомостей, які ідентифікують імовірного злочинця

Ситуація 2.1. Кримінальне провадження розпочато на підставі отриманої заяви/повідомлення особи про кримінальне правопорушення, матеріали звернення містять неперсоналізовані дані про особу злочинця. Така ситуація характерна для розслідування кримінальних правопорушень, учинених непрофесійним злочинцем з насильницьких егоїстичних чи насильницьких дискримінаційних мотивів. Наслідок кримінального правопорушення конкретизований заявою особи, якій, як правило, завдано матеріальних або моральних збитків, тому на момент відкриття кримінального провадження мотив учинення кримінального правопорушення є з великою імовірністю очевидний. Тактичні завдання розслідування у цьому разі схожі на завдання у попередньо розглянутій групі ситуацій, але їх вирішення полегшується тим, що вже є інформація, зібрана персоналом (службою безпеки та фахівцями) підприємства (організації, установи), щодо якого було вчинено комп'ютерне кримінальне правопорушення. Важливим чинником є й факт установлення особи, причетної до виявленого кримінального правопорушення. Першочерговими тактичними завданнями слідчого є перевірка наявної інформації шляхом проведення слідчих (розшукових) дій. Різновидом цієї ситуації є випадок, коли підозрюваний був затриманий на місці вчинення кримінального правопорушення або одразу після його вчинення. Зазвичай у цьому випадку застосовуються такі слідчі (розшукові) дії: особистий обшук затриманого, допит підозрюваного, проведення обшуків із метою виявлення слідів підготовки й реалізації його злочинних намірів та дій.

Ситуація 2.2. Кримінальне провадження розпочато за результатами перевірки оперативної інформації, а самі матеріали містять неперсоналізовані відомості про особу злочинця. Ситуація характерна при розслідуванні вчинення професійним злочинцем конвенційних кіберзлочинів (кримінальних правопорушень, пов'язаних з анархістськими діями в кіберпросторі, інтелектуальне піратство тощо) або злочинцем-користувачем мереж кримінальних правопорушень з антидержавних та політичних мотивів. Способи приховування злочинної діяльності у мережі злочинець не застосовував, тому дані, які дозволяють його ідентифікувати, були встановлені за допомогою спеціальних навиків співробітників, зокрема агентів, підрозділів кіберполіції. Кримінальне провадження розпочинається на підставі матеріалів оперативного підрозділу, в яких містяться фактичні дані щодо самостійного виявлення правоохоронним органом кримінального правопорушення, вчиненого невстановленою особою.

Ситуація 2.3. Кримінальне провадження розпочато в рамках реалізації матеріалів оперативної розробки за ОРС, а її результати містять неперсоналізовані відомості про особу злочинця. Ситуація є характерною при виявленні ознак готування до тяжких або особливо тяжких злочинів, пов'язаних зі сферою захисту інформації з обмеженим доступом, яку обробляють в автоматизованих системах, до кримінальних правопорушень, що порушують встановлений порядок обігу певних речей. На момент початку кримінального провадження інформація, що містить ознаки готування до вчинення тяжких або особливо тяжких злочинів зафіксована за результатами проведення оперативно-розшукових заходів, зокрема – установлення місцезнаходження радіоелектронного засобу, контролю за телефонними розмовами, зняття інформації з каналів зв'язку, зняття інформації з електронних інформаційних систем. Ініціативний рапорт від співробітника оперативного підрозділу є формальним кроком на шляху реалізації матеріалів ОРС, основним завданням слідчого в даній ситуації вбачається фіксація мотиву злочинної діяльності ідентифікованої особи та, у разі спроби вчинення нею тяжкого або особливо тяжкого злочину, виявлення

раніше невідомих співучасників. Такі особи традиційно належать до типу злочинців – упевнених користувачів мереж (систем), які, зазвичай, були в минулому або на момент вчинення злочину пов'язані з організацією (підприємством, установою), через яку можуть отримувати інформацію з обмеженим доступом. Зазначену інформацію вони використовують з різною метою, об'єктивне встановлення якої і обумовлює застосування комплексу негласних слідчих (розшукових) дій. Такий злочинець здебільшого діє в складі корпоративної організованої групи як виконавець або співучасник кримінального правопорушення, тому, як правило, бере на себе зобов'язання співпрацювати з правоохоронними органами щодо попередження та викриття кримінальних правопорушень, учинених іншими особами, про які йому відомо або стане відомо.

3. Ситуації, що характеризуються відсутністю будь-яких відомостей про особу злочинця

Кримінальне провадження відкрито в результаті виявлення ознак диверсійного злочину правоохоронним органом у процесі розслідування іншого злочину із використанням електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж, мереж електрозв'язку. Ця ситуація характеризується тим, що відомості про кібердиверсію були отримані в результаті проведення процесуальних дій за попереднім кримінальним провадженням, відкритим за ст.ст. 361–363-1 КК України. Крім того, із використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, мереж електрозв'язку не тільки можна вчиняти диверсії, а й запобігати їм, виявляючи різні стадії кримінального правопорушення. На жаль, відсутні підстави для проведення негласних слідчих (розшукових) дій у межах кримінального провадження за ч. 1 ст. 361–363-1 КК України, на відміну від кримінального провадження за ч. 2 ст. 361 КК України для встановлення особи злочинця й обставин учинення нею диверсії, щоб в майбутньому передати за підслідністю слідчим Служби безпеки України. Тому слідча ситуація у кримінальному провадженні за ч. 2 ст. 361 КК України передбачає проведення комплексу негласних слідчих (розшукових) дій, результати яких імовірно вкажуть на вчинення диверсії. Акцентуємо, що слідчі ситуації, які виникли на початковому етапі, впливають на подальший хід розслідування. Від того, наскільки вдало вони будуть розв'язані, залежить те, які слідчі ситуації сформуються на наступних етапах та чи будуть вирішені завдання кримінального провадження.

Ситуація 3.1. Кримінальне провадження розпочато на підставі заяви/повідомлення про кримінальне правопорушення, в матеріалах немає даних про особу злочинця. Наявність такої ситуації зумовлена необхідністю реалізації оперативної інформації про кримінальні проступки та злочини невеликої тяжкості, що вчиняються з соціально-економічних мотивів, пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі. Окреслюючи цю ситуацію, потрібно враховувати, що інформація про кримінальне правопорушення, зазвичай отримана в результаті негласної, агентурно-оперативної роботи або завдяки спеціальним навикам оперативного працівника підрозділу кіберполіції досить часто оцінюється слідчим як недостовірна, а тому заява особи, по суті, виконує формальну роль для початку кримінального провадження. Заявником найчастіше є фізична особа, яка конфіденційно співпрацює з оперативним підрозділом, складає формальне повідомлення про організовану злочинну діяльність, її персональні дані можуть бути легендованими, слідчий допитує її як свідка, який виявив підозрілу, на його думку, інформацію в мережі Інтернет.

Ситуація 3.2. Кримінальне провадження розпочато за результатами перевірки оперативних фактичних даних, а в матеріалах немає установчих відомостей про злочинця. Це типова ситуація під час розслідування організованої злочинної діяльності, що пов'язана із заволодінням майном шляхом незаконних операцій із використанням комп'ютерів, мереж і систем. На початковому етапі відомі відомості про потерпілих у інших кримінальних провадженнях, їх допитано, відомо про механізм учинення кримінального правопорушення, однак через способи його маскування немає достатніх даних про членів організованої групи, їх кількість, епізоди злочинної діяльності. Об'єднавши кілька кримінальних проваджень, слідчий отримує широкий спектр основних тактичних завдань для організації об'єктивного розслідування.

Ситуація 3.3. Кримінальне провадження розпочато в рамках реалізації матеріалів оперативної розробки ОРС, в яких немає ідентифікуючих даних про особу злочинця. Співробітник оперативного підрозділу ініціативним рапортом доповідає про групу радикально налаштованих невстановлених осіб, які зорганізувалися для вчинення кримінальних правопорушень з антидержавно-політичних мотивів. Рівень суспільної небезпеки таких кримінальних правопорушень, маскування способів їх учинення й притаманна наявність в окремих осіб із групи специфічних навиків вчинення протиправної

діяльності проти основ національної безпеки України вимагають своєчасного виявлення її стадій із метою недопущення настання невідворотних суспільно небезпечних наслідків. Тактичне завдання щодо встановлення мотивів злочинної діяльності не характерне для цієї слідчої ситуації. Основною метою для органу досудового розслідування є сприяння у реалізації завдань суб'єкта оперативно-розшукової діяльності, що полягає в запобіганні кримінальному правопорушенню, чим обумовлюється застосування комплексу негласних слідчих (розшукових) дій, що можна вважати тактичною специфікою цієї ситуації.

Висновки

Необхідність виокремлення конкретних слідчих ситуацій обумовлена передусім тим, що з'ясування її елементів істотно економить час і ресурси правоохоронного органу для вирішення типових тактичних завдань, які першочергово необхідно виконати з метою визначення належного суб'єкта розслідування (підслідності). Від своєчасного й об'єктивного вирішення першочергових тактичних завдань безпосередньо залежить типізація слідчих ситуацій наступного етапу розслідування кримінальних правопорушень належним суб'єктом розслідування. На останнє безпосередньо впливає стан розслідування кримінального провадження, що зумовлюється ступенем виконання тактичних завдань початкового етапу розслідування. Стан розслідування кримінального провадження має оцінитися з метою визначення моделі ситуації, в якій належному суб'єкту доведеться розпочинати наступний етап розслідування.

Список використаних джерел

1. Артюх О. М. Класифікація типових слідчих ситуацій, що виникають при виявленні та розслідуванні протидії законній господарській діяльності. *Південноукраїнський правовий часопис.* 2015. Вип. 1. С. 85–88.
2. Белкин Р. С. Криминалистика : учеб. словарь-справочник. М. : Юристъ, 1999. 268 с.
3. Гавло В. К. Следственная ситуация. М., 1985. С. 38–42.
4. Филиппов А. Г. Понятие и криминалистическое значение следственной ситуации. Проблемы криминалистики. Избранные статьи. М. : Юрлитинформ, 2007. 352 с.
5. Кримінальний кодекс України від 05.04.2001 № 2341-III. URL: http://zakon5.rada.gov.ua/laws/show/2341–14 (дата звернення: 25.05.2021).
6. Пелещак О. Р. Деякі аспекти кримінально-правової характеристики кібердиверсій. *Соціально-правові студії.* 2020. Вип. 3 (9). С. 26–33.
7. Пелещак О. Р. Кібердиверсія як форма сучасної диверсійної діяльності. *Науковий вісник ЛьвДУВС.* Вип. 3. 2017. С. 225–243.
8. Кримінальний процесуальний кодекс України : Закон від 13.04.2012 № 4651-VI. URL: http://zakon4.rada.gov.ua/laws/show/4651–17/page8 (дата зверенення: 25.05.2021).

References

1. Artyux, O. M. (2015). Klasy`fikaciya ty`povy`x slidchy`x sy`tuacij, shho vy`ny`kayut` pry` vy`yavlenni ta rozsliduvannya proty`diyi zakonnij gospodars`kij diyal`nosti. *Pivdennoukrayins`ky`j pravovy`j chasopy`s,* 1, 85–88 [in Ukr.].
2. Belky`n, R. S. (1999). Kry`my`naly`sty`ka : ucheb. slovar`-spravochny`k. M. : Yury`stъ, 268 [in Russ.].
3. Gavlo, V. K. (1985). Sledstvennaya sy`tuacy`ya. M. [in Russ.].
4. Fy`ly`ppov, A. G. (2007). Ponyaty`e y` kry`my`naly`sty`cheskoe znacheny`e sledstvennoj sy`tuacy`y`. Problemы kry`my`naly`sty`ky`. Y`zbrannыe stat`y`. M. : Yurly`ty`nform [in Russ.].
5. Kry`minal`ny`j kodeks Ukrayiny` vid 05.04.2001 № 2341-III [Criminal Code of Ukraine 01.05.04 № 2341-III]. Retrieved from http://zakon5.rada.gov.ua/laws/show/2341–14 [in Ukr.].
6. Peleshhak, O. R. (2020). Deyaki aspekty` kry`minal`no-pravovoyi xaraktery`sty`ky` kiberdy`versij [Somea spects of criminal and legal characteristics of cyber diversion]. *Social`no-pravovi studiyi (Social & Legal studios),* 3 *(9)*, 26–33 [in Ukr.].
7. Peleshhak, O. R. (2017). Kiberdy`versiya yak forma suchasnoyi dy`versijnoyi diyal`nosti. *Naukovy`j visny`k L`vDUVS,* 3, 225–243 [in Ukr.].
8. Kry`minal`ny`j procesual`ny`j kodeks Ukrayiny`: Zakon vid 13.04.2012 № 4651-VI. Retrieved from: http://zakon4.rada.gov.ua/laws/show/4651–17/page8 [in Ukr.].

Стаття: надійшла до редакції 03.04.2021
прийнята до друку 09.06.2021
The article: is received 03.04.2021
is accepted 09.06.2021