КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНЕ ПРАВО ТА КРИМІНАЛІСТИКА

ВЕЙЦ А. М.,
доктор філософії,
старший помічник начальника відділу
забезпечення якості освітньої діяльності
та вищої освіти
(Військова академія (м. Одеса))

УДК 347.77
DOI https://doi.org/10.32842/2078-3736/2025.2.50

ТИПОВІ СЛІДЧІ СИТУАЦІЇ ПОЧАТКОВОГО ЕТАПУ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНУ, ВЧИНЕНОГО ЗА УЧАСТЮ ВІЙСЬКОВОЇ ПОСАДОВОЇ ОСОБИ

У статті розглянуто типові слідчі ситуації початкового етапу розслідування кіберзлочину, вчиненого за участю військової посадової особи.

До найтиповіших слідчих ситуацій на початковому етапі розслідування вказаної категорії кримінальних правопорушень віднесено наступні: коли виявлено несанкціоновані дії з інформацією за результатами роботи суб'єкта контролю у військовій та оборонній сфері в межах наданих йому повноважень (відомостей, які дозволяють визначити конкретну особу правопорушника, недостатньо); коли виявлено несанкціонований збут або розповсюдження інформації з обмеженим доступом за результатами оперативного обслуговування (моніторингу) військового кіберсередовища (відомостей, які дозволяють визначити конкретну особу правопорушника, недостатньо); коли виявлено несанкціоновані дії з інформацією у військовому кіберпросторі за результатами оперативної розробки за оперативно-розшуковою справою (відомостей, які дозволяють визначити конкретну особу правопорушника, достатньо); коли виявлено несанкціоновані дії вищезазначеного характеру під час здійснення досудового розслідування в іншому раніше дорученому кримінальному провадженні (відомостей, які дозволяють визначити конкретну особу правопорушника, недостатньо).

Запропонована класифікація має нормативне, а також науково-теоретичне підґрунтя, оскільки при її створенні було враховано як положення чинного законодавства, так і доробки відомих дослідників у галузі криміналістики. Визначення типових слідчих ситуацій дозволяє не лише систематизувати процес розслідування кіберзлочинів у військовій сфері, а й сприяє розробці ефективних методичних рекомендацій для слідчих та оперативних підрозділів. Результати проведеного дослідження можуть бути використані у практичній діяльності правоохоронних органів, а також при розробці навчальних програм для підготовки фахівців у сфері криміналістики та кібербезпеки.

Ключові слова: *слідчі ситуації, слідчий, розслідування, несанкціоновані дії, оперативно-розшукова діяльність, військова посадова особа, кіберзлочин, інформаційна безпека, кіберпростір.*

Veits A. M. The typical investigative situations of the initial stage of investigating a cybercrime committed with the involvement of a military official

The article examines typical investigative situations at the initial stage of investigating a cybercrime committed with the involvement of a military official.

The most common investigative situations at this stage of investigating such criminal offenses include the following: when unauthorized actions with information are detected as a result of the activities of a control entity in the military and defense sector within its granted powers (there is insufficient information to identify the specific offender); when unauthorized distribution or sale of restricted information is detected as a result of operational monitoring of the military cyberspace (there is insufficient information to identify the specific offender); when unauthorized actions with information in the military cyberspace are detected as a result of operational development within an investigative case (there is sufficient information to identify the specific offender); when unauthorized actions of the aforementioned nature are detected during the pre-trial investigation of another previously assigned criminal proceeding (there is insufficient information to identify the specific offender).

The proposed classification has both regulatory and scientific-theoretical foundations, as it takes into account both the provisions of current legislation and the research contributions of well-known scholars in the field of forensic science. Identifying typical investigative situations not only helps systematize the process of investigating cybercrimes in the military sphere but also contributes to the development of effective methodological recommendations for investigators and operational units. The findings of this study can be used in the practical activities of law enforcement agencies, as well as in the development of educational programs for training specialists in forensic science and cybersecurity.

Key words: *investigative situations, investigator, investigation, unauthorized actions, operational-investigative activities, military official, cybercrime, information security, cyberspace.*

Вступ. У процесі взаємодії між людьми постійно формуються суспільні відносини, багато з яких не мають чітких правових норм, оскільки закон не здатний передбачити всі варіанти поведінки учасників таких взаємодій. Основою для аналізу цих моделей є принцип системності. Яка зазначає Г. М. Грецька, системний підхід у філософії полягає в комплексному сприйнятті явищ, об'єктів і процесів, що дозволяє застосовувати його як найбільш ефективний метод для дослідження різноманітних складних систем, серед яких – технічні, економічні, соціальні, екологічні, політичні та біологічні [1, с. 21].

Системний підхід в будь-якій науковій галузі реалізується через використання набору методів, які дозволяють вивчати характеристики, структуру та функції об'єктів, явищ чи процесів, що аналізуються. Це також дає можливість розглядати систему як цілісну одиницю, досліджуючи складні зв'язки між її елементами та вплив одних елементів на інші. Поняття "зв'язок", у свою чергу, охоплює різні аспекти "залежностей" і "поділу", які визначаються як важливі характеристики соціальних відносин. У такому контексті діяльність учасників відносин не зводиться лише до активних дій, але включає також їх пасивні позиції та взаємодію, яка визначається їх ролями та становищем у суспільстві.

Ці методологічні принципи, що стосуються особливостей слідчої діяльності, виявляються через дослідження взаємозв'язку низки наукових категорій, що утворюють єдину систему, таких як "типові слідчі ситуації", "типові версії", "тактичні завдання", "типові програми розслідування", "етапи розслідування". Враховуючи складність досудового розслідування кримінальних правопорушень, скоєних у кіберпросторі за участю військових посадових осіб, вбачається за доцільне зупинитися саме на типових слідчих ситуаціях, що виникають на початковому етапі розслідування таких кіберзлочинів.

Аналіз останніх досліджень і публікацій. Питання щодо типізації слідчих ситуацій та їхнього практичного застосування розглядалися у працях багатьох науковців. Серед них слушно відмітити: Г. М. Грецьку [1], А. Ф. Волобуєва [2], В. А. Журавля [3], О. В. Пчеліна [4], В. В. Тіщенка [5], В. М. Стратонова [6] та інших. Щодо проблематики слідчих ситуацій

незаконного втручання в роботу електронно-обчислювальних машин, то вона знайшла своє відображення в роботах В. О. Голубєва [7], Л. В. Борисової [8], О. А. Самойленко [9] тощо.

Однак у науковій площині не досліджувалися слідчі ситуації початкового етапу розслідування кіберзлочину, вчиненого за участю військової посадової особи, що й зумовлює актуальність даної статті.

Постановка завдання. Метою статті є виокремлення й дослідження типових слідчих ситуацій початкового етапу розслідування кіберзлочину, вчиненого за участю військової посадової особи.

Результати дослідження. Аналіз наукових робіт, опублікованих у період з 1980 по 2000 роки, дозволяє зробити висновок, що розслідування злочинів розглядається вченими як складний процес, що має пізнавальний характер. Однак, цей процес має ряд характеристик, що визначають його структуру. По-перше, слідча діяльність обмежена певними просторовими та часовими рамками, які регулюються відповідними правовими актами. По-друге, вона відбувається в специфічному середовищі, що включає в себе сукупність навколишніх умов, які змінюються і взаємодіють між собою, впливаючи на дії учасників процесу.

Багатогранність цієї категорії викликала різні підходи серед дослідників при визначенні її сутності. Більшість вчених акцентували увагу на важливості окремих аспектів, що характеризують стан розслідування, зокрема на окремих елементах його класифікації чи типових ситуаціях. Проте, сутність слідчої ситуації залишилася незмінною. Підсумовуючи погляди науковців, можна сказати, що слідча ситуація визначається як стан розслідування, який залежить від інформаційної моделі злочину (наявність або відсутність даних про його складові, тобто елементи криміналістичної характеристики), від доказів та оперативно-розшукової інформації щодо предметів доказування, від психологічних зв'язків між учасниками розслідування, від технічної оснащеності слідчого підрозділу та інших чинників, важливих для виконання основних і тактичних завдань розслідування. А. Ф. Волобуєв зазначає, що поняття типової слідчої ситуації все частіше використовують для чіткої організації методик розслідування, в тісному зв'язку з етапами розслідування, що підвищує практичну цінність наукових досліджень. Визначення типових слідчих ситуацій для кожного етапу розслідування додає структурованості та ясності методикам розслідування [2, с. 203-204].

Слід зазначити, що в більшості криміналістичних досліджень процес розслідування зазвичай поділяють на два основних етапи – початковий та наступний. Загальноприйнятим є підхід, при якому в теорії криміналістики виділяють типові ситуації для кожного з цих етапів. Проте залишається дискусійним питання про чіткість визначення меж між цими етапами. О. А. Самойленко вважає, що точне визначення цього моменту може значно покращити ефективність діяльності слідчого при розслідуванні окремих видів злочинів [9, с. 204]. Вивчивши різноманітні наукові підходи до цієї проблеми та враховуючи сучасні елементи кримінально-процесуальної форми, які мають значний вплив на організацію пізнавального процесу під час досудового розслідування, авторка робить висновок, що момент повідомлення особі про підозру є ключовим для розвитку розслідування. На нашу думку, саме початковий етап розслідування, з огляду на системно-діяльнісний підхід у криміналістиці, є найбільш показовим.

Багато криміналістів вказують, що на початковому етапі розслідування будь-якого злочину можна виділити дві основні слідчі ситуації:

1) ситуація, коли є відома подія з ознаками кримінального правопорушення, але ще потрібно встановити особу правопорушника;

2) ситуація, коли особа вже відома, і в її діях є підстави для складу злочину, однак необхідно довести її участь у злочині – чи то самостійно, чи у складі групи осіб або організованої групи.

Водночас, такий підхід до слідчих ситуацій, на наш погляд, значно обмежує перелік обставин, які характеризують ці ситуації, особливо у випадку, коли йдеться про розслідування кіберзлочину, вчиненого за участю військової посадової особи. Складність даного аспекту обумовлена специфічною природою військової служби та пов'язаним з нею обмеженням доступу до інформації певних категорій. Виток такої інформації може спричинити масштабні наслідки

негативного характеру, такі як створення безпосередньої загрози для національної безпеки, підрив довіри до уповноважених органів і навіть формування передумов для проведення розвідувальних операцій на користь ворога.

Отже, неможливо скласти вичерпний перелік усіх можливих слідчих ситуацій для розслідування конкретних видів злочинів, оскільки це завдання є не лише складним, а й дискусійним з точки зору ситуаційного підходу. Проте, ґрунтуючись на аналізі наукових досягнень і матеріалів слідчо-судової практики, ми намагатимемося окреслити слідчі ситуації, що характерні для початкового етапу розслідування кіберзлочинів, скоєних за участю військових посадових осіб, з урахуванням сучасних реалій розслідувань таких правопорушень.

Слідча ситуація № 1. Виявлено несанкціоновані дії з інформацією за результатами роботи суб'єкта контролю у військовій та оборонній сфері в межах наданих йому повноважень (відомостей, які дозволяють визначити конкретну особу правопорушника, недостатньо). Така ситуація є характерною для несанкціонованих дій з інформацією, що зберігається в комп'ютерних системах, використовуваних для управління діями сил і засобів оборонного сектору, а також із обладнанням для її виготовлення. Такі дії часто супроводжуються професійною діяльністю конкретних осіб, що підлягають контролю – наприклад, фахівців у сфері кібербезпеки з числа військовослужбовців, – а також розповсюдженням інформації з обмеженим доступом.

Слідчу ситуацію № 1 можна визнати найбільш сприятливою типовою ситуацією, оскільки слідчий має необхідний обсяг початкової інформації, що дозволяє визначити як обставини події, так і особу правопорушника.

Незважаючи на високу якість зібраних матеріалів суб'єктом контролю, на початковому етапі розслідування слідчий стикається з низкою типових тактичних завдань, які можна сформулювати наступним чином:

забезпечити збереження паперових і електронних документів, що фіксують транзакції та роботу комп'ютерної системи, а також осіб, які обслуговують ці системи;

встановити режими роботи комп'ютерної системи, що була залучена до злочину;

визначити коло осіб, що мали доступ до комп'ютерної системи в конкретний час і дату, аби здійснити несанкціоновані дії;

встановити факти приховування злочину, такі як вплив на свідків, попередні домовленості з іншими учасниками злочину тощо.

Крім того, можна виділити три типові умови, які ускладнюють роботу слідчого та перешкоджають ефективному розслідуванню в типовій слідчій ситуації № 1. Зокрема, це:

1) наявність інших співучасників злочину, чия причетність не підтверджена наявними матеріалами перевірки;

2) багатоепізодність злочинної діяльності;

3) приховування особи злочинця через повільний темп або недостатню конфіденційність заходів, спрямованих на виявлення правопорушення з боку суб'єкта контролю.

Слідча ситуація № 2. Виявлено несанкціонований збут або розповсюдження інформації з обмеженим доступом за результатами оперативного обслуговування (моніторингу) військового кіберсередовища (відомостей, які дозволяють визначити конкретну особу правопорушника, недостатньо). В даному випадку характерною є наявність сукупності кримінальних правопорушень, вчинених з корисливою метою, зокрема: несанкціонований збут або розповсюдження інформації з обмеженим доступом (стаття 361-2 Кримінального кодексу України) та традиційні службові злочини, що часто включає прийняття пропозиції, обіцянки або отримання неправомірної вигоди службовою особою (стаття 368 Кримінального кодексу України), зловживання повноваженнями особами, які надають публічні послуги (стаття 365-2 Кримінального кодексу України), а також підкуп особи, яка надає публічні послуги (стаття 368-4 Кримінального кодексу України).

Цю ситуацію можна вважати несприятливою, оскільки на початковій стадії кримінального провадження у суб'єкта доказування є значні труднощі через недостатність доказової бази та обмежену інформацію про особу злочинця, його мотиви й мету. Тому для слідчого важливо

розуміти специфіку початкових заходів правоохоронних органів з виявлення кіберзлочинів. Лише після належного документування або проведення інших негласних слідчих (розшукових) дій ситуація може змінитися. Корупція в державних органах також серйозно ускладнює розслідування, оскільки часто злочинцем є працівник правоохоронного органу, і довести його причетність до злочину майже неможливо. У таких випадках у поле зору кримінального судочинства потрапляє лише підставна особа – так званий "дроп", – яка пропонує придбати інформацію з обмеженим доступом і отримує гроші за її продаж на свій електронний гаманець.

До тактичних завдань розслідування в ситуації № 2, що виникають на момент отримання слідчим матеріалів про кримінальне правопорушення, можна віднести такі:

документування фактів злочинної діяльності;

встановлення особи злочинця та мотивів його вчинків;

збір вичерпної інформації про обставини злочину (час, місце, спосіб вчинення);

персоналізація даних про осіб, які придбали інформацію з обмеженим доступом;

виявлення всіх співучасників злочину;

подолання засобів конспірації, які застосовують учасники злочинної групи;

визначення факту наявності незаконно отриманих доходів.

Слідча ситуація № 3. Виявлено несанкціоновані дії з інформацією у військовому кіберпросторі за результатами оперативної розробки за оперативно-розшуковою справою (відомостей, які дозволяють визначити конкретну особу правопорушника, достатньо). Цю ситуацію можна вважати досить сприятливою для розслідування, оскільки вже проведено певні оперативно-розшукові заходи в межах оперативно-розшукової справи, і результати деяких з них, які збігаються з негласними слідчими (розшуковими) діями, що включають втручання в приватне спілкування, можуть бути використані як докази. Отже, слідчий має достатньо перевірену початкову інформацію про злочинця та саму подію. Однак, можливі труднощі в розслідуванні можуть виникнути через ймовірну причетність організованої групи осіб до скоєння злочину та через затримки в прийнятті слідчим необхідних заходів для забезпечення кримінального провадження, враховуючи специфіку статусу військової посадової особи.

На початковому етапі розслідування в цій ситуації можна визначити такі тактичні завдання:

забезпечення збереження електронних носіїв інформації, на яких зафіксовано діяльність військової посадової особи в мережі;

встановлення кола осіб, з якими спілкувався злочинець;

визначення інших можливих учасників злочину та встановлення їх причетності, включаючи осіб, які можуть бути виконавцями;

виявлення всіх епізодів злочинної діяльності.

Слідча ситуація № 4. Виявлено несанкціоновані дії вищезазначеного характеру під час здійснення досудового розслідування в іншому раніше дорученому кримінальному провадженні (відомостей, які дозволяють визначити конкретну особу правопорушника, недостатньо). Слідчу ситуацію № 4 можна визнати сприятливою типовою слідчою ситуацією, оскільки слідчий володіє інформацією про подію та особу злочинця, а також розуміє її позицію щодо протидії розслідуванню. Ускладнити ситуацію може лише оголошення особи в розшук за іншими епізодами злочинної діяльності, активне використання адвокатом тактики протидії розслідуванню (особливо у випадках організованої злочинної групи), або ж повна бездіяльність слідчого, якому раніше було доручено здійснювати розслідування. В такому випадку, це може включати невиконання перших необхідних слідчих (розшукових) дій, таких як вилучення важливих документів чи речових доказів, що стосуються незаконної діяльності військової посадової особи. Основне кримінальне провадження було відкрито на підставі повідомлення про злочин у сфері службової діяльності (затримання особи під час вчинення злочину).

На початковому етапі розслідування основними тактичними завданнями в цій ситуації є:

визначення військової посадової особи як користувача у відповідній комп'ютерній системі;

забезпечення збереження електронних носіїв, що містять інформацію про її діяльність; виявлення всіх епізодів злочинної діяльності, пов'язаних з даною особою.

Висновки. Сучасні процесі, що відбуваються у світі в цілому та в Україні зокрема, дають змогу дійти висновку про безпрецедентну роль Збройних Сил у контексті забезпечення стабільності державних інституцій та національної безпеки. Виклики, з якими стикаються Сили оборони в умовах сьогодення, є більш ніж значущими. Однак, на жаль, дедалі частіше трапляються випадки вчинення правопорушень, зокрема, у кіберпросторі, власне військовими посадовими особами. Специфіка діяльності таких осіб, а також обмеження, пов'язані з проходженням військової служби, потребують неабиякої уваги слідчого задля успішного здійснення досудового розслідування, особливо на його початковому етапі. В даному контексті доцільним вбачається виокремити наступні типові слідчі ситуації початкового етапу розслідування кіберзлочину, вчиненого за участю військової посадової особи:

1. Виявлено несанкціоновані дії з інформацією за результатами роботи суб'єкта контролю у військовій та оборонній сфері в межах наданих йому повноважень (відомостей, які дозволяють визначити конкретну особу правопорушника, недостатньо).

2. Виявлено несанкціонований збут або розповсюдження інформації з обмеженим доступом за результатами оперативного обслуговування (моніторингу) військового кіберсередовища (відомостей, які дозволяють визначити конкретну особу правопорушника, недостатньо).

3. Виявлено несанкціоновані дії з інформацією у військовому кіберпросторі за результатами оперативної розробки за оперативно-розшуковою справою (відомостей, які дозволяють визначити конкретну особу правопорушника, достатньо).

4. Виявлено несанкціоновані дії вищезазначеного характеру під час здійснення досудового розслідування в іншому раніше дорученому кримінальному провадженні (відомостей, які дозволяють визначити конкретну особу правопорушника, недостатньо).

Детальний розбір даних ситуацій, з визначенням для кожної окремо тактичних завдань, версій та програм, сприятиме якісній підготовки слідчого до здійснення відповідних розслідувань, що виразиться у їхніх результатах.

Список використаних джерел:

1. Грецька Г. М. Конспект лекцій з курсу "Теорія систем і системний аналіз" (для студентів 3 курсу денної і заочної форм навчання за напрямом підготовки 6.030601 "Менеджмент", спеціалізації "Менеджмент готельного, курортного і туристського сервісу", "Менеджмент організацій міського господарства"). Харків : ХНАМГ, 2011. 148 с.

2. Волобуєв А. Ф. *Наукові* основи комплексної методики розслідування корисливих злочинів у сфері підприємництва : дис. … д-ра юрид. наук : 12.00.09. Харків, 2001. 426 с.

3. Журавель В. А. Тактичні завдання розслідування та механізм їх вирішення. Теорія та практика судової експертизи і криміналістики. 2017. Випуск 17. С. 11-18.

4. Пчеліна О. В. Особливості предмета доказування у кримінальних справах про економічні злочини та їх вплив на методику розслідування : дис. ... канд. юрид. наук : 12.00.09. Харків, 2010. 225 с.

5. Тіщенко В. В. Криміналістичні технології в теорії і практиці розслідування. *Актуальні проблеми держави і права*. 2008. Випуск 44. С. 21-27.

6. Стратонов В. М. Криміналістична теорія пізнавальної діяльності : монографія. Харків : ХДУ, 2009. 440 с.

7. Голубєв В. О. Розслідування комп'ютерних злочинів : монографія. Запоріжжя : Гуманітарний університет "ЗІДМУ". 2003. 157 с.

8. Борисова Л. В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження : дис. … канд. юрид. наук : 12.00.09. Київ, 2007. 217 с.

9. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с.