Вісник Національного університету "Львівська політехніка". Серія: "Юридичні науки"
№ 2 (30), 2021

УДК 343.983

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

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ОКРЕМИХ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ДЛЯ ВСТАНОВЛЕННЯ ОБСТАВИН ПОДІЇ КІБЕРДИВЕРСІЇ

http://doi.org/10.23939/law2021.30.197

В дослідженні обґрунтовується, що встановлення об'єктивних обставин диверсії, яка готується або вчинена із використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, неможливе без застосовування негласних слідчих (розшукових) дій. Розглянуто особливості застосування окремих негласних слідчих (розшукових) дій, таких як аудіо-, відеоконтроль особи, аудіо-, відеоконтроль місця, спостереження за особою, річчю або місцем, зняття інформації з транспортних телекомунікаційних мереж, зняття інформації з електронних інформаційних систем, обстеження публічно недоступних місць, житла чи іншого володіння особи (шляхом таємного проникнення), установлення місцезнаходження радіоелектронного засобу, виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації.

Встановлено. що залежно від слідчої ситуації необхідно вибирати та організовувати найдоцільніші НСРД, які за змістом теоретично здатні вирішити першочергові тактичні завдання кримінального провадження. Організація саме комплексного застосування НСРД є одним із організаційно-тактичних завдань слідчого, за вирішення якого останній повинен відповідати персонально, оскільки воно безпосередньо впливає на ефективність встановлення всіх обставин кібердиверсії, способи приховання стадій кримінального правопорушення, невідомих співучасників, ролі кожного з них, зв'язків зі спецслужбами інших країни.

Ключові поняття: кібердиверсія; негласні слідчі розшукові дії; оперативні підрозділи.

Постановка проблеми. Національним законодавством закріплено повноваження правоохоронних органів щодо одержання фактичних даних, що можуть бути визнані доказами і які суд оцінює на предмет законності (допустимості). Збирання, перевірка та оцінювання доказів можливі лише в порядку, передбаченому кримінальним процесуальним законодавством. Ефективне розслідування кібердиверсії, вчиненої із використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, неможливе без застосовування негласних слідчих (розшукових) дій, оскільки, здебільшого, відомості про особу, яка її вчинила, співучасників та обставини кримінальної події приховуються, ретельно маскуються і їх неможливо отримати в інший спосіб.

Аналіз дослідження проблеми. Окремі теоретичні та практичні аспекти застосування негласних слідчих розшукових дій досліджували С. В. Албул, Л. І. Аркуша, М. В. Багрій, Б. І. Бараненко, Р. І. Благута, В. Д. Берназ, О. В. Бочковий, Н. Ф. Войтович, В. О. Глушков, С. О. Гриненко, К. А. Гусєва, Г. О. Душейко, О. М. Дроздов, О. В. Кириченко, В. А. Колесник, О. В. Кондратюк, О. Є. Користін, С. С. Кудінов, Є. Д. Лук'янчиков, В. В. Луцик, М. А. Мергеєва, В. А. Мусієнко, В. А. Некрасов, Д. Й. Никифорчук, Ю. Ю. Орлов, М. А. Погорецький, О. О. Подобний, О. І. Полюхович, В. С. Рудей, М. Б. Саакян, М. В. Стащак, Д. Б. Сергєєва, Є. Д. Скулиш, Р. Л. Степанюк, С. Р. Тагієв, Ж. В. Удовенко, Л. Д. Удалова, А. М. Ханькевич, В. О. Черков, О. М. Чистолінов, В. В. Шендрик, М. О. Шилін, І. Р. Шинкаренко, Р. М. Шехавцов.

Попри вагомий внесок вчених у вирішення дискусійних питань щодо застосування негласних слідчих (розшукових) дій, вказана проблематика залишається малодослідженою в умовах розслідування кібердиверсій, що і визначило актуальність цієї теми та її вибір.

Мета статті – з'ясувати особливості застосування окремих негласних слідчих (розшукових) дій для встановлення обставин події кібердиверсії.

Виклад основного матеріалу.

Нормативно-правова регламентація застосування негласних слідчих розшукових дій. Відповідно до положень ст. 246 КПК України негласні слідчі (розшукові) дії (далі – НСРД) є різновидом слідчих (розшукових) дій (далі – СРД), проте відомості про способи та методи їх проведення не підлягають оприлюдненню. Правову основу проведення НСРД, захисту інформації під час їх здійснення становлять Конституція України [3], Кримінальний процесуальний кодекс України [5], Кримінальний кодекс України [4], Закони України "Про прокуратуру" [11], "Про державну таємницю" [9], "Про оперативно-розшукову діяльність" [10], інші відомчі нормативно-правові акти правоохоронних органів із обмеженим доступом або грифом секретності.

НСРД здебільшого проводяться з дозволу слідчого судді за клопотанням прокурора або слідчого, погодженим з прокурором, за винятком контролю за вчиненням кримінального правопорушення (ч. 4 ст. 246 та ч. 7 ст. 271 КПК України) та виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації (ч. 2 ст. 272 КПК України). Згадане клопотання розглядається не пізніше ніж через шість годин з моменту його отримання слідчим суддею із обов'язковою участю у розгляді особи, яка його подала (ч. 1 ст. 248 КПК України). Кримінально-процесуальне законодавство дозволяє проведення окремих НСРД (установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК України) та спостереження за особою (ст. 269 КПК України)) до постановлення ухвали слідчого судді (за рішенням слідчого, узгодженим з прокурором, або прокурора) у конкретних виняткових невідкладних ситуаціях, пов'язаних із врятуванням життя людей та запобіганням вчиненню тяжкого або особливо тяжкого злочину, передбаченого, зокрема, і ст.113 КК України (Розділ І КК України), незалежно від способу вчинення, зокрема із використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Після початку застосування вказаних НСРД прокурор зобов'язаний звернутися з відповідним клопотанням до слідчого судді для постановлення відповідної ухвали.

У практичній діяльності органів досудового розслідування проведення НСРД доручається оперативним підрозділам (ч. 3 ст. 40 КПК України). Суб'єктами проведення НСРД у згаданій категорії кримінальних проваджень є оперативні та оперативно-технічні підрозділи Служби безпеки України. Під час виконання доручень слідчого, прокурора щодо проведення НСРД співробітники оперативних підрозділів Служби безпеки України користуються повноваженнями слідчого, проте не уповноважені здійснювати процесуальні дії з власної ініціативи або звертатися з клопотаннями про отримання дозволу на проведення СРД (НСРД) до слідчого судді чи прокурора. Але ніхто не забороняє оперативному підрозділу (співробітнику) звернутися з ініціативним рапортом про необхідність проведення конкретної НСРД до слідчого (прокурора), який може його врахувати під

час подальшої організації досудового розслідування кібердиверсії. Для оперативного підрозділу доручення слідчого, прокурора є обов'язковими для виконання, а результати проведення НСРД використовують у доказуванні, оскільки відповідні протоколи з додатками (аудіо- або відеозаписи, фотознімки, інші результати, отримані за допомогою застосування технічних засобів, вилучені предмети і документи тощо) можуть використовуватися в доказуванні так само, як результати проведення СРД. Особи, які виконували вказані дії, можуть бути допитані як свідки, за винятком працівників оперативно-технічних підрозділів, замість них, як правило, допитують їхнього прямого або безпосереднього керівника. Про виконання доручення оперативний працівник інформує керівника оперативного підрозділу рапортом із зазначенням отриманих результатів, проведених заходів, залучених сил і засобів, а останній, перевіривши заходи із забезпечення дотримання вимог щодо збереження державної таємниці, вирішує питання про передавання результатів НСРД (протоколів з додатками) прокурору, зазначеному в дорученні, а саме передавання (направлення) матеріалів відбувається не пізніше ніж через 24 години з моменту складання протоколу.

Теоретичне підґрунтя дослідження. Інститут НСРД в оновленій системі кримінального процесу України повинен забезпечити оптимальні шляхи використання у кримінальному процесуальному провадженні інформації, здобутої із використанням негласних сил і засобів [8, с. 61]. Наукова спільнота після введення в кримінальний процес інституту НСРД активно долучилася до розроблення тактики його проведення [6, с. 1–17; 13, с. 101–103; 12, с. 41–49; 18, с. 76–78; 20, с. 347–350], хоча "навіть такий стислий, майже на слух, аналіз ознак запропонованих НСРД дозволяє дійти висновку про їх практично повну тотожність оперативно-розшуковим заходам, які здійснюються уповноваженими оперативними підрозділами. Основна та майже єдина відмінність полягає у суб'єкті – слідчий або оперативний підрозділ, та, відповідно, це слідча дія або оперативно-розшуковий захід" [19]. Введення до системи досудового розслідування НСРД є надзвичайно прогресивним кроком законодавця, що дає можливість слідчому відшукувати докази, застосовуючи методи негласної діяльності [14, с. 151]. Висловлюються думки про великі можливості й доцільність введення до змісту окремої криміналістичної методики рекомендацій щодо особливостей тактики окремих НСРД, які є найтиповішими й найефективнішими для досудового розслідування певних категорій кримінальних правопорушень [15, с. 293]. До методів проведення НСРД науковці зараховують пошукові, дослідницькі, організаційні, практичні прийоми, зокрема із застосуванням технічних засобів, які дають змогу в порядку, передбаченому кримінальним процесуальним законодавством України, отримати інформацію про злочин або особу, яка його вчинила, без її відома [17, с. 79]. Розглянемо детальніше особливості застосування окремих НСРД під час розслідування кібердиверсій – "диверсій, вчинених із використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку" [7, с. 242].

Соціологічне дослідження. Проведення НСРД під час розслідування кібердиверсій доволі поширено в практичній діяльності підрозділів Служби безпеки України, оскільки дає змогу вирішити важливі завдання щодо збирання первинної інформації, процесуального документування злочинної діяльності проти основ національної безпеки. Опитування слідчих територіальних підрозділів Служби безпеки України показало, що у кримінальних провадженнях, відкритих за ст. 113 КК України, вчинених із використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (ст.ст. 361–363-1 КК України), найчастіше проводилися такі НСРД: аудіо-, відеоконтроль особи – 33,4 %; аудіо-, відеоконтроль місця – 41,1 %; спостереження за особою, річчю або місцем – 34,1 %; зняття інформації з транспортних телекомунікаційних мереж – 21 %; зняття інформації з електронних інформаційних систем – 27,9 %; обстеження публічно недоступних місць, житла чи іншого володіння особи (із таємним проникненням) – 7,9 %; установлення місцезнаходження радіоелектронного засобу – 61,4 %; виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації – 4 %.

Особливості застосування окремих НСРД. Аудіо-, відеоконтроль особи (ст. 260 КПК України) здійснюються щодо персоналізованого співучасника кібердиверсії, незалежно від стадії кримінального правопорушення, у публічно доступних і публічно недоступних місцях, шляхом прихованої (таємної) фіксації фактичних даних за допомогою аудіо-, відеозапису, за наявності відомостей про те, що розмови і поведінка особи, а також інші події, що відбуваються, можуть містити процесуально значущі дані, які мають значення для вирішення завдань кримінального провадження. Джерелом інформації є підозрюваний як об'єкт НСРД, його дії, поведінка, рухи, висловлювання, інша аудіовізуальна інформація.

Аудіо-, відеоконтроль місця (ст. 270 КПК України) здійснюють із установленням спеціальних технічних засобів оперативно-технічними підрозділами Служби безпеки України у публічно доступних місцях без відома їхнього власника, а також у місцях імовірної появи співучасників кібердиверсії. НСРД проводяться у громадських місцях і місцях загального користування, доступ до яких не обмежений, і з обов'язковим визначенням в ухвалі слідчого судді повної та точної адреси місця, де відбуватиметься НСРД, часу та строку її здійснення. Зазначені НСРД проводять за наявності відомостей про те, що розмови і поведінка співучасника кібердиверсії у цьому місці, а також інші події, що відбуваються саме в цьому місці, можуть містити інформацію про обставини події кримінального правопорушення, які мають значення для вирішення завдань кримінального провадження. Об'єктом цих НСРД є приватне спілкування підозрюваного у публічно доступному місці у вигляді розмов або інших звуків, рухів, дій, пов'язаних із його діяльністю або місцем перебування, а також інші події, які там відбуваються, зміст яких має значення для розслідування. На практиці такі НСРД здійснюють у громадських місцях та в місцях загального користування, доступ до яких необмежений – всередині місць, до яких можна увійти або перебувати там офіційно (реально), спеціально не повідомляючи про такий факт їх власника, орендаря тощо.

Спостереження за особою в публічно доступних місцях (ст. 269 КПК України) полягає в збиранні фактичних даних, необхідних для вирішення завдань кримінального провадження, за допомогою прихованого стеження за персоналізованим підозрюваним в публічно доступних місцях, зокрема із застосуванням технічних засобів. НСРД проводиться для пошуку, фіксації та перевірки відомостей про підозрюваного, його поведінку та раніше невідомих (відомих) співучасників, з якими відбувається безпосередній або опосередкований контакт об'єкта контролю. Це можуть бути співучасники, близькі особи, розшукувані, відомі учасники терористичних та інших незаконних озброєних формувань, представники дипломатичних установ іноземних держав (Російської Федерації), особи, які мають спеціальні технічні навички та знання, доступ до комп'ютерного обладнання, систем та мереж, особи, які володіють даними про стадії кримінального правопорушення та кримінального провадження тощо. Для спостереження за особою в публічно доступних місцях основним завданням є з'ясування і фіксація відомостей щодо її пересування, місць перебування, фактів зустрічей з іншими особами як із застосуванням технічних засобів, так і без нього. Контроль та фіксація переміщень підозрюваного та його контакти мають основне значення у застосуванні НСРД.

Застосування спостереження за річчю або місцем у публічно доступних місцях (ст. 269 КПК України) являє собою збирання фактичних даних, за допомогою прихованого стеження в публічно доступних місцях (зокрема із застосуванням оперативної техніки) за невстановленими (невідомими) фізичним особами, які відвідували місце або контактували з річчю, для вирішення завдань кримінального провадження. Такий захід (НСРД) з давніх часів використовували з метою отримання достовірних даних про особу, її спосіб життя, діяльність, контакти, місця відвідування тощо. Спостереження здійснюється неозброєним оком або за допомогою спеціальних оптичних та оптико-електронних приладів. Втрата предмета контролю є несприятливою умовою проведення НСРД, тому, щоб мінімізувати можливість втрати об'єкта (предмета) контролю, використовують різні технічні засоби його дистанційного контролю, до прикладу радіомаяки.

Надважливе значення для відстеження діяльності суб'єкта злочину (кібердиверсанта) під час вчинення кібердиверсії та після неї мають такі НСРД, як зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України), зняття інформації з електронних інформаційних систем (ст. 264 КПК України).

Контроль за телефонними розмовами (як вид зняття інформації з транспортних телекомунікаційних мереж) полягає в негласному спостереженні, відборі, фіксації, обробці і відтворенні із застосуванням відповідних технічних засобів, зокрема встановлених на транспортних телекомунікаційних мережах, змісту телефонних розмов, а також інших відомостей та сигналів, які передаються телефонним каналом зв'язку, що контролюється (SMS, MMS, факсимільний зв'язок, модемний зв'язок). Об'єктом зняття інформації із застосуванням цього НСРД є телефонні лінії загального користування, різноманітні відомчі мережі, що мають вихід на телефонні лінії загального користування, виділені мережі зв'язку невиробничого призначення, мережі пересувного радіотелефонного зв'язку, системи пересувного супутникового зв'язку. Через комплексно-програмні пристрої операторів і провайдерів телекомунікаційних мереж проходить потік інформації, частина якої залишається у пам'яті для технологічних цілей (статична), а інша частина проходить як наскрізна – динамічна інформація, що в інтересах слідства може бути перехоплена лише на підставі ухвали слідчого судді апеляційного суду [16, с. 19–20]. В результаті контролю за телефонними розмовами можна здобути телефонні номери стільникового мобільного зв'язку, яким користуються підозрювані та невстановлені співучасники, причетні до різних стадій кібердиверсії та способів її вчинення; номери терміналів мобільного зв'язку, яким користуються зловмисники; встановити міжособисті зв'язки співучасників, зв'язки із іншими невідомими особами, що дає змогу виявити усіх (переважну більшість) співучасників кібердиверсії та визначити роль кожного з них у кримінальному правопорушенні; можна встановити місцеперебування підозрюваного незалежно від часу розмови. Застосування кількісно-якісного аналізу телефонних розмов з його накладенням на електронну карту району дає змогу встановити фактичне місцеперебування (проживання, переховування) підозрюваного, маршрути переміщення та місця тривалих зупинок тощо.

Керівники та працівники операторів телекомунікаційного зв'язку зобов'язані сприяти виконанню дій зі зняття інформації із транспортних телекомунікаційних мереж, вживати необхідних заходів щодо нерозголошення факту проведення таких дій та отриманої інформації, зберігати її в незмінному вигляді. Під час вчинення кібердиверсій може відбуватися зміна матеріального стану елементів телекомунікаційної системи мобільного зв'язку або інтернету, що утворює системи електронних слідів-відображень, придатних для сприйняття за допомогою відповідних програмно-технічних засобів. Проведення НСРД дає змогу отримати фактичні дані про джерело сигналу (відправника), інформаційний зміст, час та спосіб (відкритий чи зашифрований) його відправлення або отримання, а також частково персоналізувати отримувача. Відповідно до ст. 265 КПК України, що визначає порядок фіксації та збереження інформації, одержаної з телекомунікаційних мереж за допомогою технічних засобів, та в результаті зняття відомостей з електронних інформаційних систем, зміст інформації, яку особи передають через транспортні телекомунікаційні мережі, з яких здійснюється зняття інформації, зазначається у протоколі про проведення цієї НСРД. У разі виявлення в інформації відомостей, що мають значення для конкретного досудового розслідування, у протоколі відтворюється відповідна частина такої інформації, а прокурор вживає заходів для збереження знятої інформації. Дослідження інформації, отриманої зі застосуванням технічних засобів, за необхідності здійснюється за участю спеціаліста. Слідчий вивчає зміст одержаної інформації, про що складає протокол.

Зняття інформації з каналів зв'язку дає змогу прослуховувати, фіксувати та відтворювати інформацію, що передавалася цим каналом зв'язку. Така інформація може містити дані як про взаємоз'єднання телекомунікаційних мереж, так і щодо змісту інформації, яка була передана каналом зв'язку. Її об'єктом є телексні, факсимільні, селекторні, радіорелейні, пейджингові канали обміну інформацією між абонентами, комп'ютерні мережі різних рівнів (Global Area Network, Wide Area Network, Metropolitan Area Network, Local Area Network).

Сьогодні найрозвиненішою комп'ютерною мережею є інтернет, діяльність якого забезпечують провайдери доступу до неї (мережі), хостинг-провайдери, провайдери електронних повідомлень, власники інформаційних контентів [2, с. 14]. Кожному комп'ютеру підприємство-виробник присвоює унікальний ідентифікатор – MAC-адресу. Крім того кожному вузлу в комп'ютерній мережі присвоюється унікальна мережева адреса – IP-адреса. Всі повідомлення користувача надходять на центральний пристрій – сервер, а потім за допомогою іншого пристрою – маршрутизатора – направляються абонентам. Відомості про відправника фіксуються і зберігаються на сервері провайдера. Отже, повідомлення в комп'ютерних мережах можна відстежити за MAC-адресою, IP-адресою, адресою електронної поштової скриньки, ідентифікаційним номером UIN, наявним у користувачів ICQ, даними, що містяться в облікових записах відвідувачів чатів, форумів, блогів, соціальних мереж [1, с. 144–145].

Залежно від типу телекомунікаційної мережі визначення місця розташування термінала абонента спостереження поділяється на: географічне місцезнаходження (ідентифікатор країни, міста або оператора телекомунікацій, зони приймання для мереж рухомого зв'язку тощо); фізичне місцезнаходження (номер у мережі фіксованого телефонного зв'язку, доступ до якої здійснюється із застосуванням стаціонарного кінцевого обладнання тощо); логічне місцезнаходження (IP-адреси для мереж передавання даних, єдиний UPT-номер для універсального персонального зв'язку). Встановлені у провайдерів телекомунікаційні засоби управління системою перехоплення повинні виконувати вищенаведені визначення особи, щодо якої здійснюється перехоплення телекомунікацій (абонента спостереження), у випадках успішної або неуспішної спроби встановлення сеансу зв'язку для вихідного виклику від абонента спостереження, та успішної спроби встановлення зв'язку для вхідного виклику до абонента спостереження; обміну службовими повідомленнями між терміналом та обладнанням телекомунікаційної мережі; надання послуги, що асоціюється з місцезнаходженням абонента спостереження; передавання спеціального запиту від засобів управління системою перехоплення щодо визначення місцезнаходження абонента спостереження. Всі способи зняття інформації з електронних інформаційних систем можна об'єднати в дві основні групи. Перша група – це способи безпосереднього доступу. В разі їх реалізації інформацію отримують, подаючи відповідні команди з комп'ютера, на якому ця інформація міститься. До другої групи входять способи опосередкованого (віддаленого) доступу до комп'ютерної інформації. До них можна зарахувати підключення до лінії зв'язку користувача й отримання цим шляхом доступу до електронної інформаційної системи; проникнення в комп'ютерну систему за допомогою підбору паролів. До способів опосередкованого (віддаленого) доступу до комп'ютерної інформації належать способи безпосереднього та електромагнітного перехоплення. Перше здійснюється або прямо через зовнішні комунікаційні канали системи, або із підключенням до ліній периферійних пристроїв. Сучасні технічні засоби дають змогу отримати інформацію без безпосереднього підключення до електронної інформаційної системи, за рахунок випромінювання центрального процесора, дисплея, комунікаційних каналів, принтера тощо [1, с. 157]. Всі ці дії можна виконати, перебуваючи на значній відстані від об'єкта перехоплення, наприклад: від процесора, щопрацює, – до 150 м, випромінювання моніторів і з'єднувальних кабелів – до 500 м.

Віддалений оперативний огляд комп'ютера підозрюваного (невстановленої особи), підключеного до мережі, передбачає збирання всієї можливої інформації про пристрій із відкритих мереж та здійснення прослуховування мережевого трафіку комп'ютера, отримання інформації із серверів глобальних доменних імен, визначення розташування маршрутизаторів, брандмауерів мережі, виду операційної системи пристрою, відкритих портів, служб, які працюють, версії програмного забезпечення, системи захисту. Зміст такого втручання у приватне спілкування передбачає здійснення перехоплення та дослідження зв'язку (трафіку). На основі аналізу змісту, а також статистики мережевого трафіку можна виявити, ідентифікувати та зафіксувати дії користувача, а також отримати інформацію про програмне забезпечення та характеристику використаних мереж. Внаслідок застосування НСРД можна одержати інформацію про: несанкціонований доступ до віддале-

них вузлів; зміст електронної пошти; розміщення відповідної інформації у мережі; відомості щодо відвідування сайтів тощо.

Обстежуючи публічно недоступні місця, житло чи інше володіння особи (ст. 267 КПК України), виявляють та фіксують сліди готування та/або вчинення тяжкого або особливо тяжкого злочину, предмети і документи (зокрема електронні документи); виготовляють копії документів; вилучають зразки для експертизи; виявляють розшукуваних; встановлюють технічні засоби забезпечення проведення інших НСРД.

Установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК України) найчастіше застосовують для встановлення особи підозрюваного та його зв'язків; визначення місця мешкання підозрюваного та його зв'язків; конкретних місць, які відвідує підозрюваний, та його зв'язків; місцезнаходження підозрюваного та його зв'язків у конкретний час; наявності додаткових радіоелектронних засобів (мобільних телефонів), якими користується підозрюваний, та його зв'язків, підвищення ефективності проведення інших НСРД у комплексі.

Виявити прямі докази діяльності злочинного угруповання і забезпечити кримінальне переслідування винних без участі негласного співробітника часом неможливо або вкрай складно. Основними завданнями, які вирішують, виконуючи спеціальне завдання з розкриття злочинної діяльності організованої групи чи злочинної організації (ст. 272 КПК України), є збирання, обробка, аналіз, узагальнення та надання слідчому підрозділу Служби безпеки України інформації про криміногенні процеси в організованому злочинному середовищі та вплив на соціально-економічне становище в регіоні (державі), що може безпосередньо або опосередковано загрожувати національній безпеці, виявлення схем, механізмів та конкретних фактів вчинення кібердиверсій та способів приховання злочину. До спеціальних завдань, які вирішують, застосовуючи згадану НСРД, є: виявлення тенденцій, новітніх видів, технологій та напрямів злочинної діяльності; встановлення фактичних даних, що розкривають дійсний характер предмета (об'єкта) посягання кібердиверсії, різновид, інфраструктуру і склад злочинної групи, її територіальні межі функціонування; одержання відомостей про причетність до злочинної діяльності фізичних та юридичних осіб; виявлення та фіксація слідів кримінального правопорушення; отримання інформації щодо протидії членами ОЗУ органам досудового розслідування та правоохоронним органам; встановлення фактів зв'язку зі спецслужбами інших держав.

Висновки. Уміння своєчасно організувати і, відповідно, застосувати НСРД є запорукою ефективності недопущення та припинення кібердиверсії, запобігання (мінімізації) настання суспільно небезпечних наслідків щодо об'єкта посягання. Залежно від слідчої ситуації необхідно вибирати та організовувати найдоцільніші НСРД, які за змістом теоретично здатні вирішити першочергові тактичні завдання кримінального провадження. Організація саме комплексного застосування НСРД є одним із організаційно-тактичних завдань слідчого, за вирішення якого останній повинен персонально відповідати, оскільки воно безпосередньо впливає на ефективність встановлення усіх обставин кібердиверсії, способи приховання стадій кримінального правопорушення, невідомих співучасників, роль кожного з них, зв'язки зі спецслужбами інших країни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Багрій М. В., Луцик В. В. (2017). Процесуальні аспекти негласного отримання інформації: вітчизняний та зарубіжний досвід: монографія. Х. 376 с.

2. Дмитрик Н. А. (2007). Способы осуществления субъективных гражданских прав и исполнения обязанностей с использованием сети Интернет: автореф. дис. … канд. юрид. наук. Москва. С. 14–15.

3. Конституція України від 28 червня 1996 року. *Відомості Верховної Ради України*, 1996, № 30, ст. 141.

4. Кримінальний кодекс України: Закон від 5 квіт. 2001 р. № 2341-14. URL: http: zakon.rada.gov.ua/laws /show/2341−14.

5. Кримінальний процесуальний кодекс України: Закон від 13.04.2012 № 4651-VI. URL: http://zakon4.rada.gov.ua/laws/show/4651–17/page8.

6. Лук'янчиков Є. Д., Лук'янчиков Б. Є. (2014). Визначення та система негласних (розшукових) дій. *Часопис Національного університету "Острозька академія". Серія "Право".* № 9. С. 1–17.

7. Пелещак О. Р. (2017). Кібердиверсія як форма сучасної диверсійної діяльності. *Науковий вісник ЛьвДУВС.* Вип. 3. С.225−243.

8. Погорецький М. А. (2012). Впровадження інституту негласних (розшукових) слідчих дій в правозастосовну практику. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* Вип. № 2 (28). С. 56–63.

9. Про державну таємницю: Закон України від 21.01.1994 № 3855–XII. URL: http://zakon2.rada.gov.ua.

10. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135–XII. URL: http://zakon2.rada.gov.ua.

11. Про прокуратуру: Закон України від 14.10.2014 р. *Відомості Верховної Ради (ВВР),* 2015, № 2–3, ст.12.

12. Сергеева Д. Б. (2014). Негласные следственные (розыскные) действия как средства познания в уголовном процессе. *Вестник Московского государственного областного университета. Серия "Юриспруденция".* Москва. № 1. С. 41–49.

13. Сергєєва Д. Б. (2012). Негласні слідчі (розшукові) дії у проекті нового КПК України. *Проблеми реформування кримінального процесуального законодавства в контексті європейських стандартів:* тези доповідей та повідомлень наук. семінару (м. Київ, 13 березня 2013 р.). Х.,. С. 101–103.

14. Скулиш Є. Д. (2012). Система негласних слідчих (розшукових) дій за кримінальним процесуальним кодексом України. *Наук. вісник Чернівецького ун-ту. Серія Правознавство.* Вип. 618. URL: http://archive.nbuv.gov.ua/ portal/soc_gum/Vnapu/2012.

15. Степанюк Р. Л. (2013). Особливості тактики негласних слідчих дій у структурі криміналістичної методики. Сучасні проблеми криміналістики: матеріали Міжнар. наук.-практ. конф., присвяченої 100-річчю з дня народження доктора юридичних наук, професора В. П. Колмакова (м. Одеса, 27–28 вересня 2013 р.). Одеса,. С. 292–294.

16. Тагієв С. Р. (2013). Тимчасовий доступ до інформації, яка знаходиться у операторів і провайдерів телекомунікацій, у кримінальному провадженні. *Слово Національної школи суддів України.* № 2 (3). С. 13–24. URL: file:///C:/Users/ WINDOWS/Downloads/cln_2013_2_4.pdf.

17. Тертишник В. М. (2014). Кримінальний процес України. Особлива частина: підручник. Київ: Алерта, 430 с.

18. Удовенко Ж. В. (2013). Дотримання прав і свобод людини при проведенні негласних слідчих (розшукових) дій. *Актуальні проблеми розслідування злочинів за новим Кримінальним процесуальним кодексом України*: зб. наук. праць за матеріалами Всеукр. наук.-практ. конф. (м. Київ, 5 липня 2013 р.). Київ: Нац. акад. внутр. справ.. С. 76–78.

19. Черков В. О., Чистолінов О. М. До питання про співвідношення оперативно-розшукової діяльності й негласних слідчих (розшукових) дій за проектом нового КПК України. URL: http://www.corp-lguvd.lg.ua/d120106.html.

20. Шехавцов Р. М. (2012). Особливості використання результатів негласних слідчих (розшукових) дій у кримінальному провадженні України. *Докази і доказування за новим Кримінальним процесуальним кодексом України (до 75-річчя з дня народження доктора юридичних наук, професора М. М. Михеєнка):* матеріали міжнар. наук.-практ. конф. (м. Київ, 6–7 грудня 2012 р.). С. 348–350.

REFERENCES

1. Bagrij M. V., Lucy`k V. V. (20170. ***Procesual`ni aspekty` neglasnogo otry`mannya informaciyi***: vitchy`znyany`j ta zarubizhny`j dosvid: monografiya. X. 376 p.

2. Dmy`try`k N. A. (2007). ***Sposoby osushhestvleny`ya subъekty`vnыx grazhdansky`x prav y` y`spolneny`ya obyazannostej s y`spol`zovany`em sety` Y`nternet***: avtoref. dy`s. … kand. yury`d. nauk. M.. P. 14−15.

3. ***Konsty`tuciya Ukrayiny`*** vid 28 chervnya 1996 roku. Vidomosti Verxovnoyi Rady` Ukrayiny`, 1996. № 30. P. 141.

4. ***Kry`minal`ny`j kodeks Ukrayiny`***: Zakon vid 5 kvit. 2001 r. No. 2341−14. URL: http: zakon.rada.gov.ua/laws /show/2341−14.

5. ***Kry`minal`ny`j procesual`ny`j kodeks Ukrayiny***`: Zakon vid 13.04.2012 No. 4651-VI. URL: http://zakon4.rada.gov.ua/laws/show/4651–17/page8.

6. Luk'yanchy`kov Ye. D., Luk'yanchy`kov B. Ye. (2014). ***Vy`znachennya ta sy`stema neglasny`x (rozshukovy`x) dij.*** Chasopy`s Nacional`nogo universy`tetu "Ostroz`ka akademiya". Seriya "Pravo". No. 9. P. 1–17.

7. Peleshhak O. R. (2017). ***Kiberdy`versiya yak forma suchasnoyi dy`versijnoyi diyal`nosti***. Naukovy`j visny`k L`vDUVS. Vy`p. 3. P. 225−243.

8. Pogorecz`ky`j M. A. (2012). ***Vprovadzhennya insty`tutu neglasny`x (rozshukovy`x) slidchy`x dij v pravozastosovnu prakty`ku:*** zhurnal Borot`ba z organizovanoyu zlochy`nnistyu i korupciyeyu (teoriya i prakty`ka). Vy`p. No. 2 (28). P. 56–63.

9. ***Pro derzhavnu tayemny`cyu***: Zakon Ukrayiny` vid 21.01.1994 No. 3855–XII. URL: httr://zakon2.gada.gov.ua.

10. ***Pro operaty`vno-rozshukovu diyal`nist***`: Zakon Ukrayiny` vid 18 lyutogo 1992 roku No. 2135–XII. URL: httr://zakon2.gada.gov.ua.

11. ***Pro prokuraturu***: Zakon Ukrayiny` vid 14.10.2014 r. Vidomosti Verxovnoyi Rady` (VVR), 2015, No. 2−3. P. 12.

12. Sergeeva D. B. (2014). ***Neglasnыe sledstvennыe (rozыsknыe) dejstvy`ya kak sredstva poznany`ya v ugolovnom processe.*** Vestny`k Moskovskogo gosudarstvennogo oblastnogo uny`versy`teta. Sery`ya "Yury`sprudency`ya". M.. No. 1. P. 41–49.

13. Sergyeyeva D. B. (2012). ***Neglasni slidchi (rozshukovi) diyi u proekti novogo KPK Ukrayiny`.*** Problemy` reformuvannya kry`minal`nogo procesual`nogo zakonodavstva v konteksti yevropejs`ky`x standartiv: tezy` dopovidej ta povidomlen` nauk. seminaru (m. Ky`yiv, 13 bereznya 2013 r.). X. P. 101–103.

14. Skuly`sh Ye. D. (2012). ***Sy`stema neglasny`x slidchy`x (rozshukovy`x) dij za kry`minal`ny`m procesual`ny`m kodeksom Ukrayiny***`. Nauk. visny`k Chernivecz`kogo un-tu. Seriya Pravoznavstvo. Vy`p. 618. URL: http://archive.nbuv.gov.ua/ portal/soc_gum/Vnapu/2012.

15. Stepanyuk R. L. (2013). ***Osobly`vosti takty`ky` neglasny`x slidchy`x dij u strukturi kry`minalisty`chnoyi metody`ky***`. Suchasni problemy` kry`minalisty`ky`: materialy` Mizhnar. nauk.-prakt. konf., pry`svyachenoyi 100-richchyu z dnya narodzhennya doktora yury`dy`chny`x nauk, profesora V. P. Kolmakova (m. Odesa, 27–28 veresnya 2013 r.). Odesa. P. 292–294.

16. Tagiyev S. (2013). ***Ty`mchasovy`j dostup do informaciyi, yaka znaxody`t`sya u operatoriv i provajderiv telekomunikacij, u kry`minal`nomu provadzhenni***. Slovo Nacional`noyi shkoly` suddiv Ukrayiny`.. No. 2 (3). P. 13−24. URL: file:/C:/Users/ WINDOWS/Downloads/cln_2013_2_4.pdf.

17. Terty`shny`k V. M. (2014). ***Kry`minal`ny`j proces Ukrayiny***`. Osobly`va chasty`na: pidruchny`k. Akademichne vy`dannya. K.: Alerta. 430 p.

18. Udovenko Zh. V. (2013). ***Dotry`mannya prav i svobod lyudy`ny` pry` provedenni neglasny`x slidchy`x (rozshukovy`x) dij.*** Aktual`ni problemy` rozsliduvannya zlochy`niv za novy`m Kry`minal`ny`m procesual`ny`m kodeksom Ukrayiny`: zb. nauk. pracz` za materialamy` Vseukr. nauk.-prakt. konf. (m. Ky`yiv, 5 ly`pnya 2013 r.). K.: Nacz. akad. vnutr. sprav. P. 76–78.

19. Cherkov V. O., Chy`stolinov O. M. ***Do py`tannya pro spivvidnoshennya operaty`vno-rozshukovoyi diyal`nosti j neglasny`x slidchy`x (rozshukovy`x) dij za proektom novogo KPK Ukrayiny`.*** URL: http://www.corp-lguvd.lg.ua/d120106.html.

20. Shexavczov R. M. ***Osobly`vosti vy`kory`stannya rezul`tativ neglasny`x slidchy`x (rozshukovy`x) dij u kry`minal`nomu provadzhenni Ukrayiny`.*** Dokazy` i dokazuvannya za novy`m Kry`minal`ny`m procesual`ny`m kodeksom Ukrayiny` (do 75-richchya z dnya narodzhennya doktora yury`dy`chny`x nauk, profesora M. M. My`xeyenka): materialy` mizhnar. nauk.-prakt. konf. (m. Ky`yiv, 6–7 grudnya 2012 r.). P. 348–350.

Дата надходження: 23.04.2021 р.

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

PECULIARITIES OF APPLICATION OF INDIVIDUAL SILENT INVESTIGATIVE (SEARCH) ACTIONS TO ESTABLISH THE CIRCUMSTANCES OF THE CYBERDIVERSION EVENT

National law enshrines the powers of law enforcement agencies to obtain factual data that can be recognized as evidence and which the court assesses for legality (admissibility). Collection, verification and evaluation of evidence is possible only in the manner prescribed by law. Effective investigation of cyber diversion committed with the use of computers, systems and computer networks and telecommunication networks is impossible without the use of covert investigative (search) actions, as most of the information about the person who committed it, accomplices and the circumstances of the criminal event cannot be obtained in any other way.

Peculiarities of application in criminal proceedings, open for the criminal state "Diversion", committed with the help of computers, systems and computer networks and telecommunication networks, such unspoken following search actions are considered − audio surveillance of a person, video surveillance of a person, audio surveillance of a place, video surveillance of a place, surveillance of a person, thing or place, removal of information from transport telecommunication networks, removal of information from electronic information systems, inspection of publicly inaccessible places, housing or other performing a special task to detect the criminal activities of an organized group or criminal organization.

It is concluded that the ability to organize in a timely manner and, accordingly, the use of covert investigative (search) actions is the key to effective prevention and cessation of cyber diversion, prevention (minimization) of socially dangerous consequences for the object of encroachment. Depending on the investigative situation, it is necessary to select and organize the most appropriate covert investigative (search) actions, which in their content are theoretically able to solve the priority tactical tasks of criminal proceedings. The organization of the complex application of covert investigative (search) actions is one of the organizational and tactical tasks of the investigator, for the solution of which the latter must bear personal responsibility, as it directly affects the effectiveness of establishing all the circumstances of cyber diversion, ways to conceal stages of criminal offense, unknown accomplices of them, relations with special services of other countries.

Key words: cyber diversion; covert investigative actions; operational units.