МВС УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
Факультет№1

Кафедра кібербезпеки та інформаційного забезпечення

ВИЛУЧЕННЯ ДОКАЗІВ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кваліфікаційна робота
здобувача вищої освіти
2 – го курсу навчання
освітнього ступеню «магістр»
факультету № 2 ННІПК
спеціальність «Системний аналіз»
Щербини Діани Андріївни

Науковий керівник:
професор кафедри кібербезпеки та інформаційного забезпечення
доктор технічних наук,
Балтовський О.А.

Рецензент:
кандидат юридичних наук, доцент
Форос Г.В.

Кваліфікаційна робота допущена до захисту
“___”_____2022р. протокол № _____
В.о. завідувача кафедри кібербезпеки та інформаційного забезпечення
доктор юридичних наук, доцент
А.М. Бабенко

Одеса 2022

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Протягом останніх років на фоні модернізації усіх сфер суспільного життя вдосконалюються і способи вчинення кримінальних правопорушень, у тому числі з використанням новітніх технологій. За таких умов забезпечення вирішення ряду важливих питань, що постають перед законодавцем та правоохоронними органами залежить від вмілого використання новітніх науково-технічних засобів, у тому числі і комп'ютерних технологій при здійсненні досудового розслідування.

Підвищенні ефективності й результативності досудового розслідування, неможливо без використання відповідних технічних засобів. Зокрема це стосується комп'ютерних технологій, які використовується при виявленні та вилученні доказів. Проте безупинний розвиток інформаційних технологій зумовлює необхідність розвитку законодавчої бази та вдосконалення методик розслідування злочинів. Основою ефективного досудового розслідування є налагоджена організація і тактика використання комп'ютерних технологій; правова визначеність підстав, вимог та процедури використання матеріалів, отриманих при використанні комп'ютерних технологій.

У світлі сучасних наукових розробок, що покликані забезпечити ефективне використання комп'ютерних технологій під час досудового розслідування мають враховуватись як сучасні базові правові норми національного законодавства України, більшість яких фактично стала результатом адаптації національного законодавства до міжнародних правових стандартів у даній сфері та напрацьований досвід правозастосовної практики, так і цінний доробок вітчизняних та зарубіжних учених, які протягом попередніх років працювали над зазначеною проблематикою.

Загальнотеоретичні, правові та організаційно-тактичні аспекти використання науково-технічних засобів та інформаційних технологій у

діяльності з розкриття та розслідування злочинів висвітлені у наукових дослідженнях В. П. Бахіна, Р. С. Бєлкіна, Г. І. Грамовича, І. А. Ієрусалимова, А. В. Іщенка, Н. С. Карпова, М. І. Клименка, В. В. Коваленка, В. С. Кузьмічова, М. В. Салтевського, В. Ю. Шепітька. Загальні принципи використання науково-технічних засобів та даних одержаних шляхом їх використання в кримінальному провадженні досліджено у працях: О. М. Бандурки, О. В. Бауліна, Б. Т. Безлєпкіна, П. Д. Біленчука, В. Г. Гончаренка, Ф. К. Діденка, А. Я. Дубінського, А. В. Іщенка, О. А. Леві, Н. С. Карпова, В. С. Кузьмічова, О. М. Ларіна, З. М. Ломако, П. А. Лупинської, А. О. Ляша, Г. М. Міньковського, М. Г. Несена, В. Т. Нора, Ю. М. Оропая, Е. А. Разумова, М. А. Селіванова, В. М. Тертишника, С. А. Шейфера, В. П. Шибіки, Р. Х. Якупова та ін..

Водночас, стрімкий розвиток інформаційних технологій зумовлює необхідність постійного вдосконалення як законодавства так і методик застосування інформаційних технологій під час досудового розслідування.

Викладене зумовлює необхідність всебічного дослідження використання інформаційних технологій при вилученні доказів під час досудового розслідування. Безсумнівний інтерес становлять питання щодо стану наукової розробленості питань використання інформаційних технологій під час досудового розслідування; правової основи використання; процесуальних та організаційно-тактичних засад застосування інформаційних технологій при вилученні доказів та можливостей використання їх у кримінальному процесуальному доказуванні; залучення працівників оперативних підрозділів, у тому числі, з числа підрозділів кіберполіції та ін.

Метою дослідження є отримання нових результатів у вигляді комплексу наукових положень щодо використання інформаційних технологій при вилученні доказів під час досудового розслідування, виявлення існуючих проблем у даній сфері та розробка науково обґрунтованих підходів щодо можливих шляхів їх подолання.

Поставлена мета зумовлює необхідність вирішення таких основних **завдань**:

- визначити стан наукової розробленості питань використання інформаційних технологій при вилученні доказів;

- розкрити поняття та надати загальну характеристику інформаційних технологій та їх співвідношення зі спеціальними технічними засобами негласного отримання інформації при проведенні негласних слідчих (розшукових) дій;

- узагальнити нормативно-правові акти, які регламентують використання інформаційних технологій при вилученні доказів;

- визначити особливості використання інформаційних технологій при вилученні доказів в рамках застосування заходів забезпечення кримінального провадження та слідчих (розшукових) дій;

- встановити процесуальні, тактичні та організаційні особливості використання інформаційних технологій при вилученні доказів під час проведення негласних слідчих (розшукових) дій.

Об'єктом дослідження виступають кримінальні процесуальні правовідносини, початок, зміна та припинення яких пов’язана з використанням інформаційних технологій при вилученні доказів під час досудового розслідування.

Предметом дослідження є використання інформаційних технологій при вилученні доказів.

Методи дослідження обрані з урахуванням визначеного об’єкту, предмету, меті і задач дослідження та поділяються на загальнонаукові і спеціальні методи пізнання. До загальнонаукових належать методи, використовувані в усіх галузях науки: аналіз, синтез, індукція, дедукція, абстрагування, конкретизація, узагальнення. Серед спеціальних методів пізнання, що використані при дослідженні варто виділити порівняльно-правовий, формально-логічний, формально-юридичний. Зазначені методи

були застосовані для досягнення всебічності, повноти й об’єктивності наукового дослідження.

Нормативною основою дисертаційного дослідження є Конституція України; міжнародно-правові акти; Кримінальний процесуальний кодекс України; рішення Конституційного Суду України, рішення ЄСПЛ, постанови Пленуму Верховного Суду України.

Структура роботи: Робота складається зі вступу, трьох розділів, шести підрозділів, висновку та списку використаних джерел. Загальний обсяг становить 103 аркушів, список використаних джерел (127 найменування).

РОЗДІЛ 1. ХАРАКТЕРИСТИКА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРИ ПРОВЕДЕННІ ДОСУДОВОГО РОЗСЛІДУВАННЯ

1.1. Поняття та загальна характеристика інформаційних технологій які використовуються під час досудового розслідування

Одним із дієвих інструментів результативності розкриття та розслідування кримінальних правопорушень правоохоронними органами України є застосування науково-технічних засобів й подальше використання отриманих результатів у кримінальному судочинстві. Однак, роль і місце спеціальних технічних засобів отримання інформації в діяльності органів досудового розслідування досі залишається дискусійним. Вивчення практики інформаційних технологій при отриманні доказів та наукового обґрунтування необхідності та ефективності їх застосування в діяльності правоохоронних органів дозволяє зробити висновок, що сьогодні немає системного підходу відсутні щодо особливостей використання інформаційних технологій при вилученні доказів під час досудового розслідування.

Перед законодавцем та правоохоронними органами виникає ряд важливих питань щодо застосування у кримінальному провадженні комп’ютерних технологій; використання оперативно-технічних заходів при проведенні НС(Р)Д; завдання і функції оперативно-технічних підрозділів; організація і тактика проведення оперативно-технічних заходів; легалізація матеріалів, отриманих за допомогою інформаційних технологій і їх використання в інтересах кримінального провадження тощо. При цьому використання спеціальних технічних засобів у слідчій діяльності потребує формування чіткої системи науково-обґрунтованих рекомендацій, які б базувалися на результатах практичної діяльності співробітників правоохоронних органів та передовому досвіді використання новітніх засобів та методів проведення досудового розслідування.

Підвищенні ефективності й результативності досудового розслідування, неможливо без використання відповідних технічних засобів. Зокрема це стосується й комп'ютерних технологій, які використовуються при проведенні конкретних НС(Р)Д, адже постійна зміна реалій боротьби зі злочинністю зумовлює безупинний розвиток законодавства.

У світлі сучасних наукових розробок, що покликані забезпечити ефективне використання комп'ютерних технологій мають враховуватись як сучасні базові правові норми національного законодавства України, які фактично стали результатом запровадження міжнародних правових стандартів у даній сфері, так і цінний доробок вітчизняних науковців, які протягом попередніх років працювали над зазначеною проблематикою.

Більшість НС(Р)Д за своїм змістом збігаються з відповідними оперативно-розшуковими заходами й відрізняються від них лише юридичною формою та колом суб'єктів ініціативи [28, с.15; 68, с.273].

Підтримуючи думку М. А. Погорецького та Д. Б. Сергєєву, зазначимо, що НС(Р)Д мають однакову гносеологічну природу, один алгоритм здійснення з однойменними оперативно-розшуковими заходами, передбаченими ст. 8 Закону України «Про оперативно-розшукову діяльність». Вони проводяться із застосуванням тотожних методів пізнання події злочину, в одному режимі таємності [67, с.140].

Вивчення сучасного стану наукових робіт, присвячених окремим проблемам використання науково-технічних засобів у кримінальному провадженні підтверджує тезу про те, що напрями наукових досліджень, є актуальними для предмета нашого дослідження. Різні аспекти використання науково-технічних засобів розглядаються науковцями в достатньо широкому діапазоні кримінально-правових, кримінально-процесуальних, оперативно-розшукових та інших проблем.

Загальнотеоретичні, правові та організаційно-тактичні аспекти використання науково-технічних засобів та інформаційних технологій у діяльності з розкриття та розслідування злочинів висвітлені у наукових

дослідженнях В. П. Бахіна, Р. С. Бєлкіна, Г. І. Грамовича, І. А. Ієрусалимова, А. В. Іщенка, Н. С. Карпова, М. І. Клименка, В. В. Коваленка, В. С. Кузьмічова, М. В. Салтевського, В. Ю. Шепітька. Загальні принципи використання науково-технічних засобів та даних одержаних шляхом їх використання в кримінальному провадженні досліджено у працях: О. М. Бандурки, О. В. Бауліна, Б. Т. Безлєпкіна, П. Д. Біленчука, В. Г. Гончаренка, Ф. К. Діденка, А. Я. Дубінського, А. В. Іщенка, О. А. Леві, Н. С. Карпова, В. С. Кузьмічова, О. М. Ларіна, З. М. Ломако, П. А. Лупинської, А. О. Ляша, Г. М. Міньковського, М. Г. Несена, В. Т. Нора, Ю. М. Оропая, Е. А. Разумова, М. А. Селіванова, В. М. Тертишника, С. А. Шейфера, В. П. Шибіки, Р. Х. Якупова та ін..

Ефективна боротьба зі злочинністю передбачає застосування правоохоронними органами комплексу технічних засобів з метою негласного отримання (збирання) доказів або перевірки вже отриманих доказів у конкретному кримінальному провадженні. Відповідно, повноцінне вивчення порушених нами питань потребує аналізу теоретико-прикладних досліджень, узагальненим предметом яких є порядок та підстави використання інформаційних технологій під час досудового розслідування.

У різні часи проблеми використання технічних засобів у кримінально-процесуальній діяльності, у тому чисті й у сфері нових інформаційних технологій висвітлювали такі вчені, як В.В. Вехов [16], В.В. Крилов [47], О.Г. Волеводз [19], М.С. Вертузаєв [14; 15], П.Д. Біленчук [9], В.О. Голубєв [23], Ю.М. Батурін [4], О.О.Самойленко [100] та інші.

У той же час сьогодні потрібно констатувати принципову зміну правових засад для застосування спеціальних технічних засобів при проведенні НС(Р)Д, що стало наслідком набуття чинності у 2012 році КПК України. Зміст основних законодавчих новацій, що торкаються предмета нашого дослідження, зводиться до наділення слідчого новими повноваженнями, які раніше належали лише оперативним співробітникам та скасування окремих повноважень останніх.

Значний інтерес для нас становить дисертація В. В. Коваленко «Актуальні проблеми застосування науково-технічних засобів спеціалістами при провадженні слідчих дій» (2004 р.), [42] присвяченій застосуванню науково-технічних засобів спеціалістами при провадженні слідчих дій, де автор детально досліджує питання історичного підґрунтя використання науково-технічних засобів у кримінальному судочинстві; поняття і сучасної класифікації науково-технічних засобів, використовуваних у судочинстві; сучасні засади комплексного використання різнопрофільних спеціалістів і науково-технічних засобів при розслідуванні кримінальних правопорушень.

Що стосується наукових досліджень, безпосередньо присвячених проблемам застосування інформаційних технологій при вилученні доказів під час кримінального провадження слід відзначити, що вказану проблематику наразі розроблено лише в окремих наукових дослідженнях.

Так, у науковій публікації О. О. Козенко досліджено питання про застосування спеціальної техніки, засади, сутність і зміст використання спеціальної техніки для здійснення досудового розслідування, оперативно-розшукових і контррозвідувальних заходів. Автор дійшов висновку, що спеціальна техніка – це сукупність технічних засобів, спеціальних пристроїв, речовин і відповідних тактичних прийомів, що використовуються оперативними та слідчими підрозділами та їх співробітниками із суворим дотриманням законодавства під час здійснення оперативно-слідчих заходів з метою запобігання та подальшого розслідування злочинів, кримінальних правопорушень та інших проступків як цивільного, так і адміністративного характеру [43].

Іншу, достатньо ґрунтовну роботу із досліджуваної проблематики підготував В. М. Святченко «Застосування спеціальних технічних засобів як важливий чинник сприяння винесенню обвинувального вироку» де автором наведено види спеціальних технічних засобів, їх застосування, напрями оперативно-службової діяльності, невідповідності діючих норм законодавства в роботі оперативних підрозділів та шляхи їх подолання.

Зокрема, проаналізувавши діяльність підрозділів НП України при використанні оперативно-технічних засобів негласного отримання інформації, автором відзначено, що найпоширенішими можуть бути такі категорії засобів: 1) контролю акустичної інформації – апаратура, яка використовується для організації прихованого акустичного контролю – прослуховування і (або) фіксації мовних повідомлень та інших звуків; до таких засобів належать пристрої, що фіксують та передають інформацію, різні мікрофони, а також інші засоби фіксації акустичної інформації: диктофони, СТЗ з передавання даних по кабелях, аналоговому радіоканалу чи через Інтернет – мережу і таке інше; 2) контролю візуальної інформації – апаратура для прихованого візуального контролю – спостереження і (або) фіксації візуальної інформації у різних умовах освітленості, як у межах, так і поза межами прямої видимості об'єкта спостереження; до таких засобів належать: оптико-механічні, електронно-оптичні прилади і системи спостереження, а також апаратура фіксації візуальної інформації: аналогові та цифрові фото- і відеокамери, інше; 3) контролю телекомунікаційних каналів та вилучення інформації – програмно-технічні засоби, що дозволяють здійснювати приховане перехоплення, пошук, вилучення, модифікацію, знищення і (або) фіксацію повідомлень, переданих за допомогою практично будь-яких технічних каналів зв'язку (телефонних, телеграфних, факсимільних, пейджингових, комп'ютерних Інтернет – мереж, систем радіотелефонного зв'язку тощо); 4) виявлення об'єктів, які представляють оперативний інтерес, – пристрої, що призначені для визначення місця розташування об'єктів [101].

Загалом, слід відзначити, що у зв'язку із запровадженням у КПК України 2012 року НС(Р)Д в Україні на теперішній час немає комплексних наукових досліджень, присвячених розв'язанню проблемам використання інформаційних технологій для вилучення доказів під час досудового розслідування. Таке становище обумовлено, насамперед, стрімким розвитком технічного прогресу та інформаційного простору. На підставі викладеного

можна констатувати недостатню розробленість проблем використання комп'ютерних технологій слідчими та оперативними підрозділами під час досудового розслідування.

Не розробленими на сьогодні є:

- теоретичні засади використання комп'ютерних технологій під час досудового розслідування;

- проблемні питання нормативно-правового регулювання використання комп'ютерних технологій під час досудового розслідування;

- проблеми процесуального оформлення та використання комп'ютерних технологій у доказуванні;

- питання удосконалення інформаційно-аналітичного забезпечення слідчої діяльності щодо використання комп'ютерних технологій під час досудового розслідування.

Підсумовуючи наведене у цьому підрозділі, можна зробити висновок, що, сучасні теоретичні та практичні засади використання комп'ютерних технологій для вилучення доказів під час досудового розслідування не достатньою мірою досліджені.

Таким чином, проблеми використання інформаційних технологій для вилучення доказів і їх використання у доказуванні можуть бути вирішені за умови вироблення єдиного підходу до зміни, вдосконалення та уніфікації законодавства; визначення вимог до відомостей, отриманих з використанням комп'ютерних технологій; визначення ролі і місця комп'ютерних технологій в доказовому забезпеченні кримінального процесу, діяльності органів досудового розслідування та суду; вироблення принципів їх застосування, що забезпечують охорону державних та суспільних інтересів при неухильному.

Як свідчить практика, наразі діяльність правоохоронних органів з розкриття та розслідування злочинів здійснюється в умовах зростаючої інформаційно-технічної протидії з боку злочинних формувань [63, с.9]. Зусилля органів досудового розслідування нерідко не дають результатів з причини того, що кримінальні елементи за допомогою новітніх технічних

засобів негласного отримання інформації легко отримують необхідні відомості про конкретну направленість діяльності правоохоронних органів і без особливих труднощів і небезпеки паралізують їх роботу. Таким чином, по суті, та боротьба, яку ведуть працівники правоохоронних органів з кримінальним світом – це насамперед боротьба за інформацію, де виграє той, хто зможе найбільш ефективно отримати та використати свою інформацію. Внаслідок цього, на передній план виходить проблема використання науково-технічних засобів з метою виявлення, збирання, фіксації, дослідження й використання фактичних даних щодо обставин кримінального правопорушення при проведенні досудового розслідування як один із визначних факторів підвищення ефективності діяльності з розкриття та розслідування злочинів.

Розслідування та розкриття злочинів, особливо тих, що вчиняються з використанням комп'ютерів, комп'ютерних мереж і комп'ютерної інформації, неможливе без застосування та використання комп’ютерних технологій. Це пов’язано з необхідністю відшукування, фіксування, вилучення та збирання доказів в електронній формі. Також комп’ютерні технології широко використовуються для проведення негласних слідчих(розшукових) дій.

Крім того, до наукового вивчення та прикладного дослідження проблеми використання комп’ютерних технологій під час проведення негласних слідчих (розшукових) дій та їх процесуального оформлення безпосередньо спонукає чинний КПК України, адже він не містить переліку або визначення тих чи інших технічних засобів, які законодавчо обов’язкові або рекомендовані до використання під час проведення НС(Р)Д, та не деталізує окремі аспекти процесуального оформлення за результатами їх проведення. Під час проведення будь-яких негласних слідчих (розшукових) дій на практиці фактично використовуються або технічні пристрої та засоби, в тому сенсі, в якому вони вживаються у КПК та відомчих наказах, проте визначення поняття комп’ютерних технологій або інформаційних технологій в законодавстві відсутнє, що викликає ускладнення під час їх використання,

особливо сучасні новітні інформаційні технології у вигляді обчислювальної техніки та програмного забезпечення.

Термінологічно, у літературі використовуються такі поняття, як «інформаційно-аналітичне забезпечення», «інформаційно-аналітична робота». При цьому, автори наукових праць не дають розгорнутих визначень цих понять. У зв'язку з цим, досить часто у літературі поняття «інформаційно-аналітичного забезпечення» підмінює поняття «інформаційного забезпечення» та використовується у його значенні [65]. В більшості джерел інформаційну систему розуміють досить вузько — як сукупність технічних засобів, які служать для накопичення, зберігання, обробки і передачі інформації [97]. До визначення інформаційної системи іноді включають компоненти системи, а також сфери діяльності, в яких ця система використовується. Інформаційні технології – це сукупність методів, інформаційних процесів із використанням засобів обчислювальної техніки, що забезпечують високу швидкість оброблення даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця розташування [39].

За допомогою комп'ютерної техніки не тільки раціоналізуються інформаційні процеси, але й упроваджуються комп'ютеризовані системи підтримки прийняття слідчими, експертами, оперативними співробітниками, суддями відповідних рішень [40, с.54].

Сфера Big, яка полягала в опрацюванні Data передбачає використання особливостей апаратних засобів, зокрема комп'ютерних мереж та архітектурних особливостей сучасних мікропроцесорних систем; системного програмного забезпечення: операційних систем, утиліт та засобів програмування. Реалізація програмного забезпечення має здійснюватись з урахування особливостей структур даних та алгоритмів: часової та просторової складностей. Усіма цими навичками повинен володіти дата-інеженер [33].

Тож поняття, зміст і підстави застосування комп'ютерних технологій, що використовуються під час проведення досудового розслідування мають бути чітко врегульовані юридично.

Втім, такий підхід, своєю чергою, вимагає чіткого структурування як понятійного апарату, так і власне спеціальних технічних засобів негласного отримання інформації, розроблення та впровадження тактико-технічних і нормативно-правових засад їх застосування в діяльності правоохоронних органів. Отже, саме стандартизація термінології та класифікація засобів, які визначатимуть джерела доказів, на нашу думку, дозволить підвищити ефективність та оптимізувати використання спеціальних технічних засобів негласного отримання інформації, дасть можливість нормативно регламентувати їх застосування у процесуальній діяльності органів досудового розслідування [114, с. 8-14].

Автори підручника «Юридичне, технічне та інформаційно-аналітичне забезпечення оперативно-розшукової діяльності» вказують: «Оперативна техніка – це система спеціально розроблених або запозичених з інших областей технічних засобів і науково обґрунтованих прийомів їх правомірного (переважно негласного) використання для вирішення завдань оперативно-розшукової діяльності у властивій їй формах і методах» [112, с. 168]. Так, професор В. Г. Гончаренко вказує, що в слідчій роботі можуть використовуватись лише науково-обґрунтовані засоби і методи, які пройшли необхідну практичну перевірку. Такі науково-технічні засоби можливо використовувати лише за умови дотримання принципу законності, їх використання повинно в повній мірі відповідати загальновизнаним у суспільстві правилам моралі і етики, бути доцільним взагалі, а також доцільним у конкретних умовах проведення тієї чи іншої слідчої дії [24, с. 13].

Ретельний аналіз нормативно-правових актів, що визначають питання використання комп'ютерних технологій правоохоронними органами показує, що це питання є досить невизначеним.

У нормативних актах, що затверджені МВС України найбільше поширення має термін «спеціальна техніка». Тут можна використовуються такі терміни, як «спеціальна техніка, призначена для правоохоронних органів», «спеціальна техніка, призначена для негласного отримання інформації», «спеціальна техніка», у перелік якої включається оперативна, криміналістична, організаційна та інша техніка [6., с. 16]. Наприклад, у ст. 2 ЗУ «Про оперативно-розшукову діяльність» визначено, що під час здійснення оперативно-розшукової діяльності застосовується система гласних і негласних пошукових, розвідувальних та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів [91].

Зміст поняття «спеціальні технічні засоби» визначається і в інших підзаконних актах, які безпосередньо не відносяться до діяльності правоохоронних органів. Відповідно до абз. 10 п. 3 Ліцензійних умов провадження господарської діяльності, пов'язаної з розробленням, виготовленням, постачанням спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації, затверджених постановою Кабінету Міністрів України від 22 вересня 2016 року № 669, спеціальні технічні засоби для зняття інформації з каналів зв'язку та інші технічні засоби негласного отримання інформації - технічні, апаратно-програмні, програмні та інші засоби, які відповідають критеріям належності технічних засобів негласного отримання інформації, що мають технічну забезпеченість для негласного отримання (прийому, обробки, реєстрації та/або передачі) інформації, призначені для використання у скритний спосіб, характерний для оперативно-розшукової, контррозвідувальної або розвідувальної діяльності. Це визначення дає можливість для надмірно широкого розуміння терміну "спеціальні технічні засоби негласного отримання інформації [31].

У науковій літературі, при всій розмаїтості понять щодо визначення засобів, які використовуються правоохоронними органами у кримінальному

провадженні, найбільше поширення одержав термін «спеціальна техніка» і похідні від нього (наприклад, «спеціальні технічні засоби», «оперативно-технічні засоби»). Ці терміни в основному вживаються у наукових дослідженнях, навчальній літературі, законодавчих і нормативних актах, що відносяться до відомств, які здійснюють правоохоронну діяльність. Тобто проглядається ухил убік визначення науково-технічних засобів, що використовуються у ході оперативно-розшукової діяльності, розкритті й розслідуванні злочинів [7].

Доречно буде зазначити, що до технічних засобів негласного отримання інформації можна віднести і програмні засоби негласного зняття інформації. Так, аналізуючи стан злочинності у сфері інформаційних технологій І. Ф. Хараберюш виділив програмні та програмно-технічні засоби, які відрізняються від традиційних оперативно-технічних засобів [114, с. 22].

Варто зазначити, кожна з новітніх технологій окрім ознак мобільних телефонів має також ознаки комп’ютерів, що робить їх вразливими не лише для суто технічних засобів негласного зняття інформації, а й для суто програмних засобів, які можуть діяти на основі цілком законного і загально доступного зразка комп’ютерної техніки, що в свою чергу, значно збільшує небезпеку порушення прав людини шляхом втручання у роботу мобільного пристрою не лише як мобільного телефону, а і як комп’ютерної системи. Ця обставина, в свою чергу, вимагає виділення програмних засобів негласного зняття інформації в окремий вид засобів зняття інформації з каналів зв’язку не технічного, а суто програмного характеру, і формулювання окремого визначення таких засобів [122, с. 85].

Здійснений аналіз використання науково-технічних засобів в правоохоронній діяльності, дає змогу дійти висновку, що доцільним є використання терміну «спеціальна техніка», під яким розуміється сукупність технічних, програмно-технічних та програмних засобів, пристроїв, автоматизованих систем, речовин та науково обґрунтованих способів і

тактичних прийомів їх використання правоохоронними органами із суворим дотриманням принципу законності для протидії злочинності [113].

Враховуючи вищевикладене, на наш погляд, під спеціальними технічними засобами слід розуміти апаратні, програмні та апаратно-програмні засоби, програмне забезпечення призначені для негласного отримання інформації у прихований спосіб та придатні для здійснення оперативно-розшукових заходів та негласних слідчих (розшукових) дій.

Важливим аспектом у процесі отримання доказової інформації в ході проведення НС(Р)Д є проблема допустимості застосування відповідних технічних засобів негласного отримання інформації.

Для виконання завдань кримінального провадження, використання СТЗ негласного отримання інформації при проведенні НС(Р)Д повинно здійснюватися відповідно до законодавства. При цьому мають бути всебічно забезпечені гарантії прав, свобод і інтересів громадян та юридичних осіб, що гарантуються Конституцією України [6, с.54].

Отже, виникнення розглядуваної проблеми пов’язане з розвитком сучасних комп’ютерних технологій, впровадженням у широкий вжиток новітніх технічних пристроїв, що змінили і продовжують змінювати спосіб і характер використання спеціальних технічних засобів отримання доказової інформації у кримінальному провадженні. А сучасні можливості комп’ютерних технологій дозволяють отримати більш широке коло фактичних даних у кримінальному провадженні шляхом негласного отримання інформації.

Комп’ютерні технології, які спеціально пристосовані та/або взагалі відповідають вимогам, що визначають можливість їх використання для вирішення завдань оперативно-розшукової та кримінально-процесуальної діяльності у властивих їм формах та методах, можуть бути віднесені до спеціальних технічних засобів. Тобто технічні засоби негласного отримання інформації, що були виготовлені не для потреб правоохоронних органів, але

відповідають зазначеним вимогам, можуть бути віднесені до спеціальних технічних засобів [53].

1.2 Нормативно-правова регламентація інформаційних технологій які використовуються під час досудового розслідування.

Законність правовідносин, що пов’язані із застосуванням спеціальних технічних засобів негласного отримання інформації, безпосередньо пов’язана із забезпеченням конституційно закріплених основних прав і свобод людини та громадянина через гарантування кожному охорони приватного життя, особистої і сімейної таємниці, захисту честі й гідності особи (ст. ст. 28, 29 Конституції України), недоторканності житла (ст. 30 Конституції України), таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31 Конституції України), через заборону втручання в особисте і сімейне життя людини, крім випадків, передбачених Конституцією України, не допущення збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини (ст. 32 Конституції України) [45]. Особливо треба підкреслити реалізацію конституційного принципу законності, що є базовим у всій діяльності правоохоронних органів. Цими спеціальними нормами Конституції України встановлені межі роботи з інформацією, які дублюються в нормах Закону України «Про інформацію» [87].

Окремі обмеження деяких прав і свобод (під час зняття інформації з каналів зв’язку, негласне проникнення у житлові приміщення тощо) повинні носити виключний та тимчасовий характер. Вони можуть застосовуватися лише за рішенням суду у відношенні особи, у діяльності якої наявні ознаки тяжкого або особливо тяжкого злочину, у випадках, передбачених законодавством України, з метою захисту прав і свобод інших осіб, забезпечення безпеки держави. Забороняється застосування технічних засобів, психотропних, хімічних та інших речовин, які пригнічують волю або спричиняють шкоду здоров’ю або навколишньому середовищу [45].

Сьогодні спеціальні технічні засоби застосовуються на всіх етапах розслідування злочинів, починаючи зі збору інформації про подію, пошуку матеріальних слідів і їхніх відображень. В. І. Галаган, досліджуючи використання слідчим інформації при провадженні досудового розслідування, зупиняється на новітніх досягненнях науки, які з успіхом можуть використовуватись слідчим в своїй діяльності (АІПС, ЕОМ для провадження окремих експертиз, генна дактилоскопія, засоби відео- та звукозапису тощо) [22, с. 19-23]. Тим самим підкреслюється важлива роль спеціальної техніки у процесуальній діяльності правоохоронних органів [114, с. 10].

Зважаючи на те, що високі інформаційні технології за своїм функціональним призначенням спрямовані на обслуговування інформаційних процесів, існує необхідність аналізу окремих аспектів правового регулювання інформаційних відносин в Україні. Процеси глобалізації та інформатизації, які набувають всесвітніх масштабів, й призвели до належної реакції зі сторони міжнародної спільноти, яка знайшла своє вираження у міжнародно-правових актах, спрямованих на врегулювання основних положень протікання зазначених процесів. До ключових документів, прийнятих міжнародним співтовариством у сфері інформатизації, відносяться: Окінавська хартія глобального інформаційного суспільства, Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру; І Директива 95/46/ЄС Європейського Парламенту та Ради Європи «Про захист м фізичних осіб при обробці персональних даних і про вільне переміщення таких даних», Угода про співробітництво в галузі інформації та інші документи.

Зважаючи на специфіку сфери правового регулювання слід звернути увагу на Конвенцію про кіберзлочинність. Передумовою, що детермінувала прийняття Конвенції, стала експансія кримінальних структур у сферу високих інформаційних технологій та їх використання для здійснення злочинної діяльності. Так, у преамбулі Конвенції зазначено, що держави —

члени Ради Європи та інші держави, які підписали Конвенцію, стурбовані ризиком того, що комп'ютерні мережі та електронна інформація можуть також використовуватись для вчинення кримінальних правопорушень, і того, що докази, пов'язані з такими правопорушеннями, можуть зберігатись і передаватись такими мережами. У Конвенції визначені окремі інноваційні положення процедурного права, спрямовані на забезпечення інтересів кримінального судочинства [117, с. 669].

У Конвенції чітко окреслено поняття «інформація про користувача послуг», під якою розуміється будь-яка інформація у формі комп'ютерних даних чи в іншій формі, яка знаходиться у постачальника послуг, належить користувачам його послуг, не є даними про рух даних або власне даними змісту інформації та за допомогою якої можна встановити: - тип комунікаційної послуги, яка використовувалась, її технічні положення і період користування послугою; - особистість користувача послуг, поштову або географічну адресу, телефони та інший номер доступу, інформацію про рахунки і платежі, яку можна отримати за допомогою угоди або домовленості про постачання послуг. Розглянута Конвенція встановлює досить широке коло повноважень правоохоронних органів щодо протидії інноваційним формам злочинної діяльності. Значну увагу приділено визначенню обов'язків постачальників Інтернет-послуг щодо співпраці з правоохоронними органами. Проте національне законодавство України сьогодні не приведено у відповідність з стандартом, передбаченим Конвенцією.

Загальна допустимість технічного засобу передбачає, по-перше, їх наукову спроможність, а, по-друге, відповідність результатів застосування цих засобів принципам гуманізму та демократії системи права. Зовнішнім проявом наукової спроможності засобу є точність, вірогідність результатів їх застосування при проведенні негласних слідчих (розшукових) дій. Засоби, які відносять до числа науково спроможних, при застосуванні їх в процесі збирання доказової інформації дають правильну, не викривлену уяву, що

відповідає об’єктивній дійсності. Іншими словами, наукова спроможність забезпечується науковою розробленістю і визнанням цього засобу. Вірогідність отриманих в результаті їх застосування результатів передбачає отримання кожного разу однакових результатів в типових умовах [115, с.112].

Запровадження інституту НС(Р)Д є закономірністю побудови Європейської моделі кримінального процесу та розвідувальної (оперативно-розшукової) діяльності [121, с.290].

Аналізуючи КПК України та міжвідомчі нормативні акти, що регламентують порядок використання технічних засобів щодо виявлення, розкриття і розслідування злочинів, можна зустріти різні термінологічні сполучення, які визначають технічні засоби, що використовуються в правоохоронній діяльності. У деяких документах, що відносяться до діяльності оперативних підрозділів, використовуються поняття, як «спеціальна техніка для відео-документування», «спеціальна техніка для розмноження оперативної інформації», «спеціальна техніка фіксації і передачі інформації», «спеціальна криміналістична техніка», «спецобладнання», «спеціальне обладнання», «засоби спецтехніки по боротьбі зі злочинністю» тощо. Зустрічаються також нормативно-правові акти, у яких одночасно використовують два чи більше із зазначених вище термінів, частіше без відповідних коментарів і роз'яснень, що порушує логіко-смислову структуру тексту.

Ретельний аналіз законодавства показує, що поняття спеціальних технічних засобів, використовуваних у кримінальному провадженні, з погляду нормативних актів, що регламентують діяльність правоохоронних органів, є досить невизначеним. При всій розмаїтості понять, що визначають технічні засоби, які використовуються правоохоронними органами, стосовно сфери кримінального провадження найбільше поширення одержав термін «спеціальна техніка» і похідні від нього (наприклад, «спеціальні технічні засоби», «оперативно-технічні засоби»).

Безсумнівно, правову основу використання спеціальних технічних засобів під час проведення НС(Р)Д становлять Конституція України, Закони України «Про Національну поліцію», «Про оперативно-розшукову діяльність», «Про організаційно-правові основи боротьби з організованою злочинністю», «Про заходи протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та зловживанню ними», «Про прокуратуру», «Про державну таємницю», «Про інформацію», Кримінальний кодекс України, Кримінальний процесуальний кодекс України, інші законодавчі акти, міжнародні договори України, а також установчі акти та правила міжнародних правоохоронних організацій, членом яких є Україна.

Так, аналізуючи норми КПК України, приходимо до висновку, що КПК України, регламентуючи використання технічних засобів, у ст. 273 «Засоби, що використовуються під час проведення негласних слідчих (розшукових) дій», встановлює, що уповноважені оперативні підрозділи, виконуючи доручення слідчого, прокурора, можуть використовувати наявні у них оперативно-технічні засоби, якщо такі відповідають вимогам цього кодексу щодо засобів, які використовуються при проведенні негласних слідчих (розшукових) дій. При цьому зазначається, що для цілей ст. 273 КПК України допускається виготовлення та використання спеціально виготовлених речей і документів, створення та використання спеціально утворених підприємств, установ, організацій. Одночасно з цим у інших статтях глави 21 КПК України неодноразово згадується про застосування інших засобів, зокрема технічних, проте не розкривається їх зміст.

Так, ч. 2. ст. 252 передбачає, що проведення НС(Р)Д може фіксуватися за допомогою *технічних та інших засобів.* У ч. 1 ст. 256 встановлюється, що протоколи щодо проведення НС(Р)Д, аудіо- або відеозаписи, фотознімки, інші результати, здобуті за допомогою *застосування технічних засобів*, вилучені під час їх проведення речі та документи або їх копії можуть використовуватися в доказуванні на тих самих підставах, що і результати проведення інших слідчих (розшукових) дій під час досудового

розслідування. Ст. 265 КПК України передбачає, що фіксація та збереження інформації, отриманої з телекомунікаційних мереж за допомогою *технічних засобів* і внаслідок зняття відомостей з електронних інформаційних систем», ст. 266 – «Дослідження інформації, отриманої при застосуванні *технічних засобів*». У ст. 267 КПК України зазначається, що слідчий має право обстежити публічно недоступні місця, житло чи інше володіння особи шляхом таємного проникнення в них, у т. ч. з використанням *технічних засобів*. Одним із завдань такого проникнення визначено встановлення *технічних засобів* аудіо-, відеоконтролю особи. У ч. 1 ст. 268 КПК України передбачено, що установлення місцезнаходження радіоелектронного засобу є НС(Р)Д, яка полягає в застосуванні *технічних засобів* для локалізації місцезнаходження радіоелектронного засобу. Ч. 1 ст. 269 КПК України передбачає можливість застосування для спостереження за особою, річчю або місцем відеозапису, фотографування, *спеціальних технічних засобів* для спостереження. У деяких статтях глави 21 КПК України вжито відмінні від наведених вище терміни: «*спеціальні імітаційні засоби*» (п. 2 ч. 7 ст. 271 КПК України) «*спеціальні несправжні (імітаційні) засоби*» (п. 2 ч. 3 ст. 272 КПК України).

Крім того, деякі аспекти застосування спеціальних технічних засобів визначаються у відомчих інструкціях прийнятих МВС. Так, Інструкція про організацію проведення НС(Р)Д та використання їх результатів у кримінальному провадженні визначає загальні засади та єдині вимоги до організації проведення негласних слідчих (розшукових) дій слідчими органів досудового розслідування або за їх дорученням чи дорученням прокурора уповноваженими оперативними підрозділами, а також використання їх результатів у кримінальному провадженні [79].

Крім того, деякі аспекти застосування спеціальних технічних засобів визначаються у відомчих інструкціях МВС з обмеженим доступом.

На сьогоднішній день**,** визначення спеціальних технічних засобів негласного отримання інформації наведене лише у Постанові КМУ від 22

вересня 2016 р. № 669 «Деякі питання щодо спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації», якою визначено критерії належності спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації; перелік спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації, а також суб'єкти уповноважені на провадження господарської діяльності, пов'язаної з розробленням, виготовленням, постачанням спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації.

Відповідно до Переліку спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації, затвердженого Постановою від 22 вересня 2016 р. № 669, до таких засобів відносяться: засоби для негласного аудіо-, відеоконтролю та спостереження за особою, річчю або місцем; засоби для негласного отримання інформації про місцезнаходження та/або переміщення особи, транспортних засобів чи іншого володіння особи, зокрема для негласного установлення місцезнаходження радіоелектронного засобу зв'язку; засоби для негласного обстеження кореспонденції, предметів, матеріальних носіїв інформації; засоби для негласного проникнення або обстеження публічно недоступних місць, житла чи іншого володіння особи; засоби для негласного зняття інформації з телекомунікаційних мереж; засоби для негласного зняття інформації з електронних інформаційних систем [31].

Подібне визначення спеціальних технічних засобів негласного отримання інформації міститься у наказі Служби безпеки України від 12 серпня 2005 року № 440 «Про затвердження Зводу відомостей, що становлять державну таємницю»: спеціальні технічні засоби – технічні засоби, устаткування, апаратура, прилади, пристрої, програмне забезпечення,

препарати та інші вироби, призначені (спеціально розроблені, виготовлені, запрограмовані або пристосовані) для негласного отримання інформації [78].

Окремі положення що визначають зміст спеціальних технічних заходів негласного отримання інформації визначено у Законах:

- Про Національну програму інформатизації від 04.02.1998 р. № 74/98-ВР [89], однією з головних завдань якої є забезпечення інформаційної безпеки держави; Закон України «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання» від 20.02.2003 р. № 549-IV [75]. Цим законом визначено, поняття товарів подвійного використання і саме до нього відсилає СБУ для визначення критеріїв віднесення виробу до СТЗ;

- Закон України «Про ліцензування видів господарської діяльності» від 02.03.2015 р. № 222-VIII, яким встановлено, що ліцензуванню підлягає діяльність, пов'язана з розробленням, виготовленням, постачанням спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації (критерії належності та перелік технічних засобів негласного отримання інформації визначаються Кабінетом Міністрів України за поданням Служби безпеки України) [88].

- Правовий режим отримання інформації, яка знаходиться в операторів та провайдерів регламентовано законами України «Про телекомунікації» від 18 листопада 2011 року [93], «Про радіочастотний ресурс України» від 1 червня 2000 року [92], «Про інформацію» від 2 жовтня 1992 року [87], Правилами надання та отримання телекомунікаційних послуг, затвердженими постановою Кабінету Міністрів України від 11 квітня 2012 року № 295 [85], та іншими нормативно-правовими актами. Резолюціями Ради Європи від 17 січня 1995 року «Про законне перехоплення телекомунікацій» [77] та від 20 червня 2001 року «Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та

послуг» [90] визначено, що правоохоронні органи потребують постійного моніторингу перехоплення телекомунікацій у режимі реального часу.

Істотне значення щодо нормативного регулювання використання технічних засобів у кримінальному провадженні має і низка підзаконних нормативних актів, передусім постанов Верховної Ради України, указів і розпоряджень Президента України, постанов Кабінету Міністрів України. А саме:

- Правилами надання та отримання телекомунікаційних послуг, затверджених Постановою КМУ від 11 квітня 2012 р. № 295 [85].

- Положенням про порядок розроблення, виготовлення, реалізації та придбання спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації, затвердженого Постановою КМУ від 27 жовтня 2001 р. №1450 [69], визначено замовників, виконавців та державних замовників розроблення, виготовлення та придбання СТЗ можуть бути: СБУ, розвідувальні органи, Національна поліція, Національне антикорупційне бюро, Державна податкова адміністрація, Держкомкордон, Управління державної охорони, Мін'юст, а також Міноборони в межах, визначених законодавством.

Окремі питання використання спеціальних технічних заходів негласного отримання інформації врегульовано у: Постанові КМУ від 05.08.2015 р. № 609 «Про затвердження переліку органів ліцензування та визнання такими, що втратили чинність, деяких постанов Кабінету Міністрів України» [81]; Порядку здійснення державного контролю за міжнародними передачами товарів військового призначення, затвердженого Постановою Кабінету Міністрів України від 20 листопада 2003 р. № 1807 [84]; Постанові КМУ від 24.07.2019 № 671 «Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності, пов'язаної з розробленням, виготовленням, постачанням спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації, що підлягає ліцензуванню, і

визначається періодичність проведення планових заходів державного нагляду (контролю) Службою безпеки» [80]**;**

- Постанові Кабінету Міністрів України від 16.01.2019 №28 «Про внесення змін до Ліцензійних умов провадження господарської діяльності, пов'язаної з розробленням, виготовленням, постачанням спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації» [73].

- Постанові Кабінету Міністрів України від 3 вересня 2014 р. № 411 «Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України» [83].

Якщо розглядати в хронології за останні 15 років, посилена роль щодо контролю процесу негласного збирання інформації на загально-державному рівні визначається і наступними Указами Президента України:

- «Про впорядкування виготовлення, придбання та застосування технічних засобів для зняття інформації з каналів зв'язку» від 13.04.2001 р. № 256/2001 згідно з яким реалізацію державної політики з розроблення, виготовлення, реалізації та придбання спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного одержання інформації та забезпечення державного контролю і координації діяльності державних органів у цій сфері здійснює Служба безпеки України [74].

- «Про додержання прав людини під час проведення оперативно-технічних заходів» від 16.01.2006 р. № 1556 згідно з яким Службі безпеки України приписано підвищити рівень роботи з виявлення, запобігання та припинення фактів придбання чи використання спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного одержання інформації суб'єктами, яким не надано права на проведення оперативно-розшукової діяльності [76].

Серед відомчих нормативних актів слід виділити:

- Наказ Служби безпеки України від 23.12.2020 № 383 «Про затвердження Зводу відомостей, що становлять державну таємницю»:

спеціальні технічні засоби – технічні засоби, устаткування, апаратура, прилади, пристрої, програмне забезпечення, препарати та інші вироби, призначені (спеціально розроблені, виготовлені, запрограмовані або пристосовані) для негласного отримання інформації [78].

- Спільний наказ Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування України. Загальні технічні вимоги» від 04.09.2018 року № 1519/533 [61]. В якому визначено загальні технічні вимоги до технічних засобів для здійснення уповноваженими органами оперативно-розшукових заходів та НС(Р)Д у телекомунікаційних мережах загального користування України в порядку, визначеному законодавством України.

- Загальна методика віднесення об'єктів до спеціальних технічних засобів негласного отримання інформації (ДСК) затверджена внутрішнім документом СБУ від 02.03.2011 р., . реєстраційний код 17.0.01 [58].

- Лист СБУ від 04.06.2009 р. № 18/1462 «Щодо висновків про належність (неналежність) товарів до спеціальних технічних засобів», яким визначено перелік установ та органів Служби безпеки України, що уповноважені надавати висновки (погодження) про належність (неналежність) товарів до спеціальних технічних засобів [124].

Варто також зауважити, що відомості щодо окремих спеціальних технічних засобів негласного отримання інформації містять державну таємницю або службову інформацію та не можуть бути включені до відкритого списку. Ми погоджуємося з думкою Б. І. Бараненка про те, що само по собі створення законодавчої бази застосування спеціальних технічних засобів не вирішить поставлених питань, а тому потрібна, перш за все, чітка діюча система організаційних, методичних і практичних дій щодо повної реалізації відповідних норм права [3, с. 23-24].

У будь якому разі, застосування комп’ютерних технологій при проведенні НС(Р)Д вважається правомірним, якщо воно прямо передбачене або рекомендоване законом, іншими нормативними актами, або не суперечить закону за своєю сутністю. На законодавчому рівні необхідно визначити загальні принципи допустимості застосування таких засобів, до яких відносяться: законність, тобто наявність достатніх підстав й приводів для їх застосування, їх відповідність за характером й функціональними можливостями вимогам міжнародних правових актів; наукова обґрунтованість застосовуваних науково-технічних засобів й методів, достовірність отриманих результатів; об’єктивна доцільність проведення слідчих дій; економічність науково-технічних засобів; їх безпечність для життя і здоров'я громадян, відповідність морально-етичним вимогам [25, с.101].

З означеного можемо констатувати, що правова база використання комп’ютерних технологій при проведенні НС(Р)Д не повною мірою відповідає вимогам забезпечення прав і свобод людини. Адже зміст поняття комп’ютерних технологій не визначається жодним законом, а трактується на підзаконному рівні, що не відповідає принципу правової визначеності, за яким обмеження основних прав людини і громадянина та втілення цих обмежень на практиці допустиме лише за умови забезпечення передбачуваності застосування правових норм, встановлених такими обмеженнями.

Вважаєм необхідним закріплення в КПК України поняття «комп’ютерних технологій» як сукупність технічних, програмно-технічних та програмних засобів, пристроїв, автоматизованих систем та науково-обґрунтованих способів і тактичних прийомів прихованого їх використання спеціально пристосованих для вирішення завдань кримінально-процесуальної діяльності що використовуються уповноваженими особами при проведенні НС(Р)Д для негласного отримання інформації та

відповідають вимогам, що визначають можливість їх використання із суворим дотриманням принципу законності.

РОЗДІЛ 2. ПОРЯДОК ВИЛУЧЕННЯ ДОКАЗІВ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРИ ЗАСТОСУВАННІ ЗАХОДІВ ЗАБЕЗПЕЧЕННЯ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ ТА ПІД ЧАС ПРОВАДЖЕННЯ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

2.1. Порядок вилучення доказів з використання інформаційних технологій при застосування заходів забезпечення кримінального провадження

Одним із найросповсюдженіших способів віручення доказів під час досудового розслідування є застосування такого заходу забезпечення кримінального провадження як «Тимчасове вилучення майна».

Однією із найважливіших гарантій забезпечення прав людини при застосуванні тимчасового вилучення майна є наявність визначених КПК України підстав застосування даного заходу. Кожна процесуальна дія, а тим більше та, що забезпечується державним примусом, має проводитись тільки за наявності певних визначених підстав. Саме встановлення підстав провадження процесуальних дій обмежує суб'єктивний підхід до прийняття рішення про їх проведення, забезпечує перевірку їх законності та обґрунтованості [20, с.502].

Проте, до теперішнього часу як в теорії так і в практичній діяльності не склалося єдиної думки щодо поняття, змісту, мети та функцій тимчасового вилучення майна, як заходу забезпечення кримінального провадження. На неоднозначність та проблемність такого заходу забезпечення кримінального провадження вказує і той факт, що за роки дії Кримінального процесуального кодексу України в Главу 16, яка регулює тимчасове вилучення майна, неодноразово вносились зміни, і доволі суттєві, зокрема Закони України: №222-VII від 18.04.2013, №191-VIII від 12.02.2015, №394-VIII від 13.05.2015, № 2213-VIII від 16.11.2017. Адже глава 16 складається лише з трьох статей.

З метою якісного дослідження сутності та організаційно-тактичних особливостей застосування тимчасового вилучення майна цілком доцільним вбачається розділити об’єкт дослідження на декілька етапів, а саме:

1) визначити юридичну природу такого заходу забезпечення кримінального провадження як тимчасове вилучення майна;

2) проаналізувати проблеми, що виникають під час застосування тимчасового вилучення майна на практиці;

3) установити шляхи подальшого реформування такого заходу забезпечення кримінального провадження на законодавчому та правозастосовчому рівні.

Перш за все, потрібно вказати, що тимчасове вилучення майна є одним із видів заходів забезпечення кримінального провадження відповідно ч. 2 ст. 131 КПК. Цей факт викликає певні труднощі в розумінні його природи.

На теперішній час, як і раніше, законодавець не дає прямого визначення поняття заходів забезпечення кримінального провадження. Однак вчені процесуалісти, усвідомлюючи необхідність визначення такого поняття, на підставі діючих норм, формують свої поняття таких заходів.

Так Шило О.Г. визначає, що заходи забезпечення кримінального провадження – це передбаченні КПК заходи примусового характеру, які застосовуються при наявності підстав та в порядку, встановленому законом, з метою запобігання і подолання негативних обставин, що перешкоджають або можуть перешкоджати вирішенню завдань кримінального провадження, забезпеченню його дієвості [51, с.367].

В. М. Малахов і М. О. Пешков визначають їх, як передбачені кримінальним процесуальним законодавством процесуальні засоби примусового характеру, які застосовуються в сфері кримінального провадження уповноваженими на те особами і державними органами, стосовно підозрюваних, обвинувачених, свідків для попередження і припинення їхніх протиправних дій з метою успішного розслідування і судового розгляду кримінального провадження [29, с.228].

М. Є. Громова формулює заходи забезпечення кримінального провадження як встановлену кримінальним процесуальним законом система заходів примусового характеру, що застосовується з метою досягнення дієвості та виконання завдань кримінального провадження.

Варто зазначити, що Л. Д. Удалова під заходами забезпечення кримінального провадження розуміє – передбаченні кримінальним процесуальним законом процесуальні засоби державно-правового примусу, що застосовуються уповноваженими на те органами (посадовими особами), які здійснюють кримінальне провадження, у чітко визначеному законом порядку стосовно осіб які залучаються до кримінально-процесуальної діяльності, з метою досягнення дієвості кримінального провадження (для запобігання та припинення неправомірних дій, забезпечення виявлення та закріплення доказів тощо) [50, с.164].

Усі наведені визначення майже тотожні за винятком пропозиції Л. Д. Удалової, яка розширила своє визначення фразою «забезпечення виявлення та закріплення доказів». Як вважає С. М. Смоков, з чим ми погоджуємось, означене визначення більше відноситься до примусових заходів кримінального провадження, ніж до заходів забезпечення кримінального провадження [103, с.53].

Таким чином, переважна більшість науковців сприймає заходи забезпечення кримінального провадження як інструмент впливу на учасників процесу з метою забезпечення останніми правомірної поведінки та забезпечення дієвості кримінального провадження.

Однак, згідно ч. 2 ст. 167 КПК України, тимчасово вилученим може бути майно у вигляді речей, документів, грошей тощо, щодо яких є достатні підстави вважати, що вони:

1) підшукані, виготовлені, пристосовані чи використані як засоби чи знаряддя вчинення кримінального правопорушення та (або) зберегли на собі його сліди;

2) призначалися (використовувалися) для схиляння особи до вчинення кримінального правопорушення, фінансування та / або матеріального забезпечення кримінального правопорушення або винагороди за його вчинення;

3) є предметом кримінального правопорушення, у тому числі пов'язаного з їх незаконним обігом;

4) одержані внаслідок вчинення кримінального правопорушення та/або є доходами від них, а також майно, в яке їх було повністю або частково перетворено.

В свою чергу відповідно частина 1 цієї ж статті, зазначено, що тимчасове вилучення майна – це фактичне позбавлення підозрюваного або осіб, у володінні яких перебуває зазначене у частині другій цієї статті майно, можливості володіти, користуватися та розпоряджатися певним майном до вирішення питання про арешт майна або його повернення.

Отже, тимчасове вилучення майна – це дія, яка характеризується вилученням речей і документів, які мають безпосереднє відношення до обставин, що мають значення для кримінального провадження. Іншими словами, можна стверджувати, що такий захід забезпечення кримінального провадження як тимчасове вилучення майна є ні чим іншим як засобом збирання доказів.

Однак варто зазначити щодо певної невизначеності правової природи «Тимчасового вилучення майна», є те, що законодавець визначаючи таку дію, як окремий вид заходів забезпечення кримінального провадження, не наділив останню самостійною процедурою. Так, відповідно до статті 168 КПК України тимчасове вилучення майна здійснюється під час затримання особи, обшуку та огляду, тобто тимчасове вилучення майна проводиться в рамках зазначених процесуальних дій, не маючи власної форми фіксації, а використовуючи протоколи обшуку, огляду, чи затримання. Виникає питання: «Яким чином застосовувати захід впливу без процедури його застосування, і в чому складається такий вплив?»

Також варто зазначити і таку особливість «Тимчасового вилучення майна» є те, що всі заходи забезпечення кримінального провадження, крім тимчасового вилучення майна, мають напрям дії на конкретного учасника кримінального провадження, або особу, яка в подальшому буде залучена до участі в кримінальному провадженні. Тимчасове вилучення майна не обов'язково має напрям дії на конкретну особу. Тимчасово вилучення майна не має суворого направлення на конкретного суб'єкта, з метою забезпечення дієвості кримінального провадження, а охоплює все майно, яке попадає в поле зору особи, що здійснює слідчу (розшукову) дію [55, с.55].

Як вбачається з норм кримінального процесуального кодексу України, такий захід забезпечення кримінального провадження як тимчасове вилучення майна не передбачає самостійної процесуальної дії, а здійснюється в рамках інших процесуальних дій, а саме: при проведенні обшуку; при проведенні огляду; при затриманні особи у порядку, передбаченому статтями 207, 208, КПК України. При цьому, поділяючи думку Ю.М. Мірошниченко, тимчасово вилученими вважаються:

- під час затримання всі речі, документи, гроші тощо;

- під час обшуку – речі та документи, які не входять до переліку, щодо якого прямо надано дозвіл на їх відшукання в ухвалі про дозвіл на проведення обшуку, та не відносяться до предметів, які вилучені законом з обігу;

- під час огляду – речі та документи, що не належать до предметів, які вилучені з обігу [59, с.312].

З точки зору слідчої практики стосовно пошукових (розшукових) заходів зазначається тенденція, що діяльність у даному випадку включає в себе: а) проникнення на місце (об'єкт) пошуку; б) пошукові дії; в) вилучення виявлених об'єктів; г) документальне оформлення вилучення. Зазначене зумовлює виділення різних елементів у процесуальному змісті діяльності з

вилучення майна, і подає наочний приклад її реалізації стосовно конкретних ситуацій з вилучення майна [26].

Відтак, можна стверджувати, що вилучення є елементом процесуальної дії, заходу забезпечення кримінального провадження (затримання, тимчасовий доступ до речей та документів), слідчої (розшукової) дії (огляд, обшук), а не самостійною процесуальною дією. Наприклад, при здійсненні обшуку, вилучення є інструментом досягнення цілі такої дії. Під час обшуку може бути вилучено три категорії об'єктів:

- об'єкти, які зазначені в ухвалі суду на обшук;
- об'єкти, які заборонені законом в обігу;
- об'єкти, як за переконанням особи, що здійснює обшук, мають значення для кримінального провадження.

До всіх вищезазначених об'єктів застосовується такий елемент процесуальної дії, як вилучення, при чому до всіх в однаковій мірі. Тобто при виявлені предметів, які за переконанням особи, що здійснює обшук, мають значення для кримінального провадження, застосовується все той же механізм «вилучення», що і до предмету, вилученого з обігу, чи зазначеного в ухвалі суду на обшук. Вилучення такого предмету, речі, документу (майна), не передбачає окремої процедури, відмінної від вилучення решти предметів. Тому на нашу думку, норми, зазначені в статтях 167, 168, в ч. 7 ст. 236, ч. 7 ст. 237 КПК України, визначають критерії класифікації об'єкту, як тимчасового вилученого майна, а не встановлюють окремої процедури вилучення у випадку виявлення майна, яке особа, що здійснює процесуальну дію вважає важливим для кримінального провадження, однак яке не зазначене в ухвалі суду та не заборонне законом в обігу.

Що стосується вилучення доказів з застосуванням інформаційних технологій, варто заначити наступне.

Неоднозначними, з нашої точки зору, є зміни, які були внесенні до статті 168 КПК України згідно Законом України № 191-VIII від 12.02.2015

[140], згідно якого частину другу зазначеної статті було доповнено абзацом другим такого змісту: «тимчасове вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку для вивчення фізичних властивостей, які мають значення для кримінального провадження, здійснюється лише у разі, якщо вони безпосередньо зазначені в ухвалі суду».

Вказане формулювання протирічить саме собі. Так, виходячи з вищезазначеного аналізу норм, що регулюють порядок тимчасового вилучення майна, можна стверджувати, що чинний КПК України прирівнює затримання особи, а також проведення огляду та обшуку, до тимчасового вилучення майна, яке було вилучене без дозволу слідчого судді, або суду. Виходячи із вказаних змін, можна зробити висновок, що мобільний термінал систем зв'язку, у випадку зазначення його в ухвалі суду може підлягати тимчасовому вилученню. Однак, оскільки тимчасове вилучення майна відповідно до ст. 168 КПК України можливе лише під час затримання, огляду, або обшуку, і лише для проведення обшуку видається ухвала слідчого судді, або суду, в якій зазначається яке майно підлягає вилученню, то під словами ухвала суду, законодавець мав на увазі ухвалу суду про проведення обшуку. Але відповідно ч. 7 ст. 236 КПК, речі і документи, щодо яких прямо надано дозвіл на відшукання, тимчасово вилученим майном не являються. Таким чином, окремі зміни містять істотні протиріччя.

В подальшому згідно Закону України № 2213-VIII від 16.11.2017р. [72], частину другу статті 168 КПК України було доповнено абзацами третім та четвертим, а саме:

«Забороняється тимчасове вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку, крім випадків, коли їх надання разом з інформацією, що на них міститься, є необхідною умовою проведення експертного дослідження, або якщо такі об'єкти отримані в результаті вчинення кримінального правопорушення чи є засобом або знаряддям його вчинення, а також якщо доступ до них обмежується їх

власником, володільцем або утримувачем чи пов'язаний з подоланням системи логічного захисту.

У разі необхідності слідчий чи прокурор здійснює копіювання інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах. Копіювання такої інформації здійснюється із залученням спеціаліста».

Аналізуючи доповнення, вважаємо, що абзац третій ч. 2 ст. 168 КПК України визначив загальну заборону тимчасового вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку, та зазначив особливі випадки можливого тимчасового вилучення зазначеного майна. На нашу думку, вказана норма повністю нівелює суперечливу норму, зазначену в абзаці другому ч. 2 ст. 168 КПК України, в зв'язку з чим, вважаємо необхідним її виключення.

Також варто зазначити прогресивність норми (абз. 4 ч. 2 ст. 168 КПК України), щодо можливості копіювання інформації, яка міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах. Однак, необхідно акцентувати увагу і на деяких нюансах вказаної норми. Виходячи з аналізу означених норм, та підстав їх розроблення, вважаємо, що за задумом законодавця до інформаційних (автоматизованих) систем, телекомунікаційних системах, інформаційно-телекомунікаційних систем, їх невід'ємних частинах, зазначених в абз 4 ч. 2 ст. 168 КПК України, можна віднести і мобільні термінали систем зв'язку (телефони, смартфони), зазначені в абз. 3 ч. 2 ст. 168 КПК України, оскільки ці норми приймались одним законом, та мають спільну мету.

Мобільний пристрій на даний час є невід'ємним предметом, який не тільки дає можливість спілкування, доступу до інформації, тощо, але й накопичує величезну кількість інформації про свого власника. Дзвінки, коло знайомств, фото, місця перебування, коло інтересів та багато іншого. Не

дивно що правоохоронні органи дуже часто використовують мобільні пристрої для збирання необхідної інформації про особу. Основний спосіб здобути необхідну інформацію, це отримати доступ до мобільного пристрою та аналіз даних, які містяться в мобільному пристрої. Здебільшого такий доступ можливо здійснити під час затримання (особистого обшуку), огляду або обшуку в рамках тимчасового вилучення майна, оскільки безперечно мобільний пристрій відноситься до категорії майна.

Однак, розвиток науково-технічного прогресу, на даний час, дозволяє отримати доступ до необхідної інформації в мобільному пристрої, не здійснюючи тимчасове вилучення майна з подальшим накладенням арешту на майно, а маючи в своєму розпорядженні мобільний пристрій, лише на декілька хвилин в рамках проведення затримання, огляду чи обшуку.

Одним з пристроїв, які можуть здійснювати копіювання інформації, яка знаходиться на мобільному пристрої є XRY (виробництва компанії MicroSystemation, Швеція). Програмно-апаратний комплекс призначений для проведення захищеного вилучення цифрових даних з різноманітних мобільних пристроїв, таких як смартфони, GPS-навігатори, 3G-модеми, портативні аудіоплеєри, планшетні комп'ютери. В результаті дослідження телефонів створюються захищені від несанкціонованого доступу звіти, які можна вивести на друк або записати на компакт-диск. Функція експорту XRY забезпечує можливість створення звітів в наступних форматах: html, xml, xlsx, xls, docx, doc та gpx. Комплекс XRY дозволяє вилучати дані з численних програмних додатків смартфонів. З його допомогою можна вилучити дані викликів IP-телефонії, картографічну інформацію GPS та журнали засобів оперативного пересилання повідомлень [18, с.34-35].

Звичайно, в рамках розслідування кримінальних правопорушень при тимчасовому вилученні мобільних пристроїв, особу, яка здійснила таке вилучення, перш за все цікавить саме інформація, яка знаходиться на мобільному пристрої, а не сам пристрій. Отже відпадає необхідність в подальшому звертатись до слідчого судді з клопотанням про накладення

арешту на мобільний пристрій, з метою отримання можливості аналізу та використання як доказу інформації що знаходилась на мобільному пристрої.

Однак, виникає питання чи буде доказ на підставі отриманої шляхом копіювання інформації з мобільного пристрою допустимим, якщо слідчий не отримав дозволу суду на арешт джерела цієї інформації, як підтвердження законності її отримання? Вказане питання є дискусійним та надзвичайно актуальним. На нашу думку, якщо в кримінальному провадженні як доказ буде використовуватись інформація з мобільного пристрою, то і вказаний мобільний пристрій повинен знаходитись у фактичному, законному володінні сторони обвинувачення. Таким чином мобільний пристрій повинен бути вилучений та визнаний речовим доказом.

В подальшому, після вилучення, уповноважена службова особа зобов'язана забезпечити схоронність тимчасово вилученого майна. Процедура його збереження визначена Інструкцією про порядок вилучення, обліку, збереження та передачі речових доказів у кримінальних справах, цінностей та іншого майна органами дізнання, досудового слідства і суду [86].

Фактично, тимчасово вилучене майно є таким протягом 72 годин, у подальшому на нього або накладається арешт шляхом звернення до слідчого судді з клопотанням про накладення арешту, або відається особі, в якої вилучалось зазначене майно.

2.2. Порядок вилучення доказів з використанням інформаційних технологій під час провадження слідчих (розшукових) дій

Глава 20 КПК України, що присвячена слідчим (розшуковим) діям, вперше на законодавчому рівні дає їх визначення. Так, слідчі (розшукові) дії – це дії, спрямовані на отримання (збирання) доказів, а також перевірку вже отриманих доказів у конкретному кримінальному провадженні (ч. 1 ст. 223). До переліку слідчих (розшукових) дій законодавцем віднесено: допит (ст.ст. 225-227 КПК України); пред'явлення особи для впізнання (ст. 228 КПК України); пред'явлення речей для впізнання (ст. 229 КПК України); пред'явлення трупа для впізнання (ст. 230 КПК України); проникнення до житла чи іншого володіння особи (ст. 233 КПК України); обшук (ст. 234 КПК України); огляд (ст. 237 КПК України); огляд трупа (ст. 238 КПК України); слідчий експеримент (ст. 240 КПК України); освідування особи (ст. 241 КПК України); проведення експертизи (ст.ст. 242-245 КПК України).

Аналіз Глави 20 КПК України, яка містить в собі перелік та порядок застосування слідчих (розшукових) дій, дозволяє стверджувати, що слідчими (розшуковими) діями, процесуальний порядок проведення яких передбачає вилучення речей, документів (майна), є обшук та огляд. Зокрема, з огляду на норми ч. 2 ст. 235, ч. ч. 5 і 7 ст. 236 КПК України, під час проведення обшуку вилученню підлягають:

1) речі, які вказані в ухвалі слідчого судді про дозвіл на обшук і для виявлення яких проводиться дана слідча (розшукова) дія;

2) речі, вилучені законом з обігу, незалежно від їх відношення до кримінального провадження;

3) речі, що не входять до переліку, щодо якого прямо надано дозвіл на відшукання в ухвалі про дозвіл на проведення обшуку та не відносяться до предметів, які вилучені законом з обігу;

4) речі, які мають значення для кримінального провадження та вилучені під час особистого обшуку осіб, які перебувають у приміщенні під час проведення обшуку.

Під час проведення огляду, згідно з ч. 5 ст. 237 КПК України, вилученню підлягають:

1) речі, які мають значення для кримінального провадження;

2) речі, вилучені законом з обігу [48].

Так С. О. Шейфер в своїх працях визначав процесуальну сутність слідчої дії як «комплекс регламентованих кримінально-процесуальним законом і здійснюваних слідчим (судом) пошукових, пізнавальних і засвідчуючих операцій, що відповідає особливостям слідів певного виду і пристосованих до ефективного виявлення, сприйняття та закріплення доказової інформації, що міститься в них» [119, с.10-11].

Як зазначив О. П. Рижаков, ознаками слідчих (розшукових) дій є:

1) спрямованість на одержання або перевірку доказів з метою встановлення обставин, що мають значення для розслідування злочину;

2) пізнавальний характер;

3) примусовий характер;

4) провадження тільки уповноваженою на те особою;

5) детальне закріплення провадження в КПК – наявність самостійної, деталізованої процедури проведення;

6) обмеження конституційних прав та інтересів громадян [98, с.10].

З позиції ефективного розслідування зауважимо, що як в минулому, так і в теперішній час, обшук є однією з найбільш ризикованих і в той же час однією з найбільш плідних слідчих (розшукових) дій, що включає і вилучення майна. Адже майже жодне розслідування не може обійтися без обшуку по тій простій причині, що саме обшук передбачає дії слідчого щодо пошуку або збору речових доказів [10, с.16; 5, с.180].

Згідно статистичних даних в Україні щомісяця проводиться близько 4500 обшуків і кількість громадян, і кількість громадян, які стикаються з такою процесуальною дією є значною [27, с.4].

Незважаючи на цей факт, у науці кримінального процесу досі не вироблено єдиного розуміння обшуку. А. Р. Ратінов, наприклад, визначає обшук, як слідчу дію, змістом якої є примусове обстеження приміщень і споруд, ділянок місцевості, окремих громадян з метою відшукання і вилучення предметів, що мають значення для справи, а також виявлення розшукуваних осіб» [94, с.7].

В свою чергу І. Ф. Пантелєєв дає таке визначення: «Обшук – слідча дія, що полягає в примусовому обстеженні приміщень, місцевості й інших об'єктів, а також окремих громадян з метою виявлення та вилучення знарядь злочинів, предметів і цінностей, здобутих злочинним шляхом, а також інших предметів і документів, що мають значення для розслідування» [49, с.331].

В той же час Р. С. Бєлкін зазначає, що «обшук – це слідча дія, що полягає у відшуканні об'єктів, що мають значення для встановлення істини по справі, – знарядь злочину, предметів і цінностей, здобутих злочинним шляхом, а також інших предметів і документів, які можуть мати значення для справи. Може проводитися для виявлення розшукуваних осіб, трупів» [8, с.346].

О. А. Луценко під обшуком розумів: примусове обстеження приміщень, ділянок місцевості, окремих громадян, їх одягу і речей з метою виявлення і вилучення джерел доказової і орієнтуючої інформації (знарядь злочину, предметів і цінностей або інших речовин, які здобуті злочинним шляхом або можуть мати значення для справи), а також виявлення розшукуваних осіб і трупів або відомостей про їх місцезнаходження [56, с.11-12].

А. В. Бабін визначав обшук як слідчу дію, що полягає у відшуканні та вилученні предметів і документів, які мають доказове значення по кримінальній справі, виявлення трупів або живих осіб, а також грошей і

цінностей, набутих злочинним шляхом, у приміщеннях, інших місцях або вулицях, де, за наявними даними, вони заховані [2, с.408].

З. З. Зінатуллін під обшуком розумів процесуальну дію, що застосовується особами, які розслідують кримінальну справу, для відшукання прихованих предметів і осіб, а під виїмкою – вилучення певних предметів і документів, що мають значення для справи, і якщо точно відомо, де і в кого вони знаходяться. На відміну від обшуку виїмка завжди "спрямована на вилучення таких предметів, індивідуальні ознаки яких, а також їх місцезнаходження відомі особі, яка провадить виїмку [38, с.99].

А. Ф. Волобуєв зазначає, що обшук слідча дія, що полягає в примусовому обстеженні приміщень, місцевості, транспортних засобів, окремих громадян з метою відшукання і вилучення об'єктів, які мають значення для встановлення істини у справі, а також виявлення розшукуваних осіб [21, с.175].

Також варто відзначити і розмаїття поглядів, щодо мети обшуку. У філософії мета розуміється як один з елементів поведінки і свідомої діяльності людини, що характеризує передбачення в мисленні результату діяльності і шляхів його реалізації за допомогою певних засобів. Мета виступає як спосіб інтеграції різних дій людини в деяку систему, як одна з форм детермінації людської діяльності, як очікуваний, планований результат» [111].

Відносно обшуку, А. Т. Валєєв зазначає, що можна говорити про існування певної ієрархії мети обшуку і про розподіл їх на кінцеві цілі, що мають більш узагальнений характер, і проміжні, які отримали у дослідників найменування «завдання обшуку» [13, с.14].

Звідси, основною кінцевою метою обшуку є:

1) отримання доказів;

2) створення умов для відшкодування матеріального збитку, заподіяного злочином;

3) вилучення предметів, заборонених до цивільного обороту;

4) виявлення розшукуваних осіб і трупів.

Б. М. Шавер до мети обшуку відносить виявлення і вилучення об'єктів злочину, знарядь злочину, інших предметів, що зберігають на собі сліди або свідчать про злочинну діяльність їх власника; документів і листування; вилучених з цивільного обороту предметів [17, с.155].

Є. М. Ліфшиц вважав, що метою обшуку є: а) виявлення доказів та інших предметів, що можуть мати істотне значення для справи; б) виявлення злочинця, що ховається; в) виявлення майна з метою відшкодування шкоди, завданої злочином [54, с.7].

При визначенні мети обшуку вченими, з одного боку, вказують на об'єкти пошуку ті, що вилучаються, а з іншого – на інформацію, що міститься в них. Але, аналіз вітчизняного українського законодавства дозволяє нам визначити, що мета обшуку спрямована на виявлення та фіксацію відомостей про обставини вчинення кримінального правопорушення, відшукання знаряддя кримінального правопорушення або майна, яке було здобуте в результаті його вчинення, а також встановлення місцезнаходження розшукуваних осіб. Проте, в жодному випадку не вказано на вилучення, як мету. Разом з тим, у ч. 7 ст. 236 КПК України законодавцем визначено, що під час обшуку слідчий, прокурор має право оглядати і вилучати речі і документи, які мають значення для кримінального провадження. В тій же нормі законодавець вказує, що вилучені речі і документи, які не входять до переліку, згідно якому прямо надано дозвіл на відшукання в ухвалі про дозвіл на проведення обшуку, та не відносяться до предметів, які вилучені законом з обігу, вважаються тимчасово вилученим майном.

Одною з основних відмінностей обшуку від огляду полягає в меті їх застосування. Так в обшуку вона більш конкретна, але значно вужче за мету огляду, в ході якого акцентується увага на всебічне дослідження, детальну фіксацію як обстановки, довколишнього середовища, так і об'єкта, що оглядається, можливо, з подальшим його вилученням.

В ході дослідження нами встановлено, що обшук – один із самостійних і найскладніших інститутів процесуального права, який належить до системи слідчих дій та який пройшов до волі тривалий шлях становлення й розвитку, однак, з огляду на КПК України в новій редакції, його продовжують поповнювати новітніми ідеями, підходами, концепціями, удосконалюють і розвивають з урахуванням досвіду міжнародного співтовариства та вітчизняних напрацювань [91].

Головними завданнями обшуку С. Ф. Денесюк визначив:

1) вилучення предметів, що мають доказове значення, якими є:

а) знаряддя й засоби злочину (зброя, знаряддя злому, пристосування для тілесних ушкоджень тощо);

б) об'єкти злочинних дій (викрадене майно, гроші та інші цінності);

в) предмети зі слідами злочину або пристосування, використовувані для його приховування (одяг зі слідами крові, обладнання схованки тощо);

г) трупи розшукуваних осіб;

ґ) майно, гроші, інші цінності, нажиті злочинним шляхом;

д) інші предмети й документи, які можуть мати значення для справи (листи, різні записи, фотознімки тощо);

2) виявлення розшукуваних осіб, зокрема дезертирів, а також матеріалів, що характеризують їх особу та полегшують розшук;

3) відшукання майна, яким можна забезпечити відшкодування матеріальної шкоди та можливу конфіскацію. Відшукуються не лише власне цінності, а й матеріали, які вказують на місця їх зберігання: листування й записи про знаходження майна у родичів і знайомих, квитанції ломбардів тощо, а також предмети, що підтверджують наявність у цієї особи розшукуваного майна (товарні ярлики, фабричні паспорти, деталі шуканого приладу тощо) [30, с.62-63].

Відповідно до ст. 237 КПК України з метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення

слідчий, прокурор проводять огляд місцевості, приміщення, речей та документів.

Зазначена слідча дія дає змогу встановити великий обсяг доказів, які належать до складу злочину (об'єкта, об'єктивної сторони, суб'єкта та суб'єктивної сторони), однак потребує застосування певних тактичних прийомів і засобів криміналістичної техніки.

Для проведення огляду місця події під час здійснення процесуального керівництва та розслідування злочинів, вчинених з використанням електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку, до складу слідчо-оперативної групи (далі – СОГ) можуть залучатися:

– слідчий, прокурор, який спеціалізується на розслідуванні (процесуальному керівництві) кримінальних правопорушень цієї категорії;

– співробітники оперативних підрозділів органів внутрішніх справ України, Служби безпеки України, Державної фіскальної служби України тощо;

– поняті (враховуючи, що в багатьох випадках зазначені злочини вчиняються у співучасті із співробітниками установи, на території якої вчинено злочин, необхідно відмовитися від їх допомоги в якості понятих. Натомість запросити осіб, які розуміються на комп'ютерній техніці. Це не допустить розголошення відомостей досудового розслідування, і надалі, за необхідності, зазначені особи зможуть пояснити в суді перебіг слідчої (розшукової) дії та її результати);

– спеціаліст-криміналіст, що знає особливості роботи зі слідами злочинів цієї категорії;

– спеціаліст по роботі з банківським комп'ютерним обладнанням у сфері мережевих технологій (за наявності на місці події периферійного обладнання віддаленого доступу або локальної комп'ютерної мережі);

– спеціаліст із систем зв'язку (за умови використання для дистанційної передачі даних каналів електрозв'язку);

– інші категорії спеціалістів (інженери-електрики, спеціалісти супутникових систем зв'язку, оператори стільникових, пейджингових, інтернет-мереж).

Після прибуття на місце події члени СОГ з'ясовують обставини вчинення кримінального правопорушення, встановлюють свідків, прикмети осіб, які вчинили кримінальне правопорушення, та ймовірні шляхи їх відходу. У разі необхідності вживають заходів для переслідування транспортних засобів, що використовувалися злочинцями.

Під час огляду місця події в установленому КПК України порядку фіксуються відомості щодо обставин учинення кримінального правопорушення, вилучаються речі та документи, які мають значення для кримінального провадження, та речі обмеженого доступу, в тому числі матеріальні об'єкти, придатні для з'ясування обставин, що підлягають доказуванню. Забезпечується їх належне зберігання з метою подальшого направлення для проведення експертного дослідження.

Прокурорам (процесуальним керівникам) слід мати на увазі, що огляд місця події може проводитися до внесення відомостей про вчинення злочину до ЄРДР. У таких випадках відповідно до ч. 2 ст. 168 КПК України тимчасове вилучення електронних інформаційних систем або їхніх частин, мобільних терміналів, систем зв'язку для вивчення фізичних властивостей, які мають значення для кримінального провадження, не здійснюється.

У разі необхідності вилучення таких систем потрібно у порядку ст. 160 КПК України звернутися до слідчого судді з клопотанням про надання тимчасового доступу до речей і документів.

Під час огляду та описування слідів комп'ютерного (мережевого) обладнання та місця події варто звернути увагу на:

– знаряддя вчинення злочинів у сфері комп'ютерної інформації, які поділяються за характером доступу на безпосередні та опосередковані (віддалені).

До знарядь безпосереднього доступу можна віднести носіїв комп'ютерної інформації (USB-флеш-накопичувачі, лазерні диски, дискети, касети з магнітною стрічкою для стримера), різноманітне периферійне устаткування (друкувальний пристрій, CD-ROM-накопичувач, стример, дисководи), а також електронні ключі, особисті ідентифікаційні коди тощо.

До знарядь опосередкованого (віддаленого) доступу належать насамперед мережеве устаткування, а також засоби доступу до віддалених мереж (модеми, прилади телефонного та супутникового зв'язку);

– застосовані способи доступу до комп'ютерної інформації, які також можна класифікувати на безпосередні та опосередковані.

При реалізації способів безпосереднього доступу інформація знищується, блокується, модифікується, копіюється, а також може бути порушена робота ЕОМ, комп'ютерної системи або мережі шляхом передачі відповідних команд із комп'ютера, на якому інформація знаходиться. Безпосередній доступ можуть здійснювати особи, які працюють з інформацією, а також особи, котрі спеціально проникають у закриті зони та приміщення, де провадиться обробка інформації. Іноді злочинець з метою вилучення інформації, залишеної користувачами після роботи ЕОМ, обстежує робочі місця програмістів у пошуках чорнових записів, роздруківок, ділового листування («прибирає сміття») або здійснює перегляд і відновлення стертих програм.

При реалізації способів опосередкованого (віддаленого) доступу до комп'ютерної інформації відбувається: підключення до лінії зв'язку законного користувача (наприклад, до телефонної лінії) і одержання таким чином доступу до його системи; проникнення в чужі інформаційні мережі шляхом автоматичного перенабору абонентських номерів з подальшим з'єднанням із тим або іншим комп'ютером. Перенабір здійснюється доти, доки на іншому кінці лінії не «відізветься» чужий комп'ютер.

Під час огляду *банкомата* слід приділити увагу його технічному стану, виявити всі можливі пошкодження (як на самому терміналі, так і на кабелях,

що з'єднують його з банківською установою), технічні пристрої, що не передбачені конструкцією банкомату, або сліди їх кріплення, сторонні предмети (накладки, скімери та ін.), вилучити з нього платіжні картки, касові стрічки, виписки, блок пам'яті, відеозапис або фотознімки.

Огляд банківської платіжної картки відбувається за тими ж правилами, що й огляд паперових документів, за винятком дослідження вмісту магнітної смуги (електронного мікропроцесора), що проводиться за допомогою відповідної експертизи чи іншими способами. При візуальному огляді картки обов'язково звертається увага на її стан, наявність пошкоджень, розмір, колір та товщину пластика.

У протоколі описується як лицьовий, так і зворотний бік картки. В описанні лицьового боку мають бути зазначені такі дані: назва платіжної системи, торговий знак якої зображено на картці; назва банку-емітента; номер картки; ім'я держателя картки; дата, до якої вона дійсна; голограма та її стан; додаткові реквізити (наприклад, фотокартка, якщо є). При огляді зворотного боку описується стан паперової стрічки для підпису, наявність підпису держателя і захисного коду та стан магнітної смуги. Необхідно дотримуватись запобіжних заходів, щоб уникнути ушкодження картки і знищення на ній слідів пальців рук.

Огляд сліпів (чеків, квитанцій) як носіїв інформації про використання банківських платіжних карток при здійсненні безготівкових розрахунків, вилучених у затриманих, у банках-емітентах, у сервісних підприємствах торгівлі та послуг, проводиться за участю відповідних фахівців за загальними правилами криміналістичного огляду документів з дотриманням правил обігу з документами, що є речовими доказами. У процесі огляду сліпа (квитанції) фіксується номер картки; код і координати пункту обслуговування; сума вартості товару (послуги); дата операції; підпис власника картки та продавця (касира). Слід зауважити про необхідність ретельного упакування вилучених карток, сліпів (чеків, квитанцій), щоб унеможливити несанкціонований доступ до них і зберегти для наступного експертного дослідження.

При огляді, вилученні та упакуванні накладок на банкомати застосовуються загальні принципи, тактика та методи огляду місця пригоди, але з урахуванням низки специфічних умов. Слід пам'ятати, що первинна інформація, яку можна отримати власне на місці виявлення, безпосередньо зумовить вибір проведення певних оперативно-розшукових заходів, а надалі – і слідчих дій. Так, під час огляду на місці виявлення за можливості встановлюються конструкційні особливості пристрою, що дає змогу з'ясувати, чи в накладці реалізовано принцип передачі інформації на відстань, чи пристрій має вбудований накопичувач інформації. У разі встановлення факту передачі інформації на відстані вирішується питання про спосіб: якщо використано радіосигнал, то можна припустити знаходження приймача цього сигналу в безпосередній близькості, відповідно, поруч можуть знаходитись наглядачі за накладкою. Якщо використано GSM-сигнал, то за номером SIM-картки можна визначити момент її активації у конкретному апараті, історію та географію її попередньої роботи, перелік абонентів.

Під час огляду слід дотримуватися таких специфічних умов:

– не обробляти безпосередньо на місці виявлення пристрої магнітними порошками: використання їх і магнітних пензлів може пошкодити електронні складові та знищити ті сліди, які доцільно та ефективніше було б виявляти в лабораторних умовах (на внутрішньому боці банкомата можуть бути сліди пальців рук та інші сліди біологічного походження осіб, які збирали накладку як пристрій);

– не вимикати електроживлення пристрою та механічно не роз'єднувати електричні ланцюги, не від'єднувати частини (крім випадків огляду SIM-карток);

– з метою запобігання обміну інформації між накладкою на банкомат та іншими пристроями по безпровідному зв'язку – за можливості поміщати об'єкти до пакетів, контейнерів чи інших пристроїв, що блокують (екранують) сигнал;

– упаковувати пристрої таким чином, щоб не допустити пошкодження, відокремлення частин, роз'єднання електричних ланцюгів та приклеювання матеріалу упаковки до накладки.

Звертаємо особливу увагу, що при вилученні комп'ютерного (мережевого) обладнання необхідно обов'язково встановити та врахувати наслідки, які спричинить відсутність зазначених технічних засобів.

Відповідно до ст. 234 КПК України обшук проводиться на підставі ухвали слідчого судді з метою виявлення та фіксації відомостей про обставини вчинення кримінального правопорушення, відшукання знаряддя кримінального правопорушення або майна, яке було здобуте в результаті його вчинення, а також встановлення місцезнаходження розшукуваних осіб.

Під час підготовки або погодження клопотання про проведення обшуку прокурору (процесуальному керівнику) слід мати на увазі, що фактичною підставою для проведення вказаної слідчої дії є наявність достатніх відомостей, що вказують на можливість досягнення його мети. До них, зокрема, можна віднести достатні відомості про те, що знаряддя кримінального правопорушення або майно (речі й цінності), здобуті в результаті його вчинення, а також інші предмети та документи, які мають значення для розкриття правопорушення чи забезпечення цивільного позову, відомості про обставини вчинення кримінального правопорушення знаходяться у певному приміщенні або місці чи в якої-небудь особи.

Положення ч. 6 ст. 236 КПК України дає право слідчому, прокурору примусово проникати до приміщення, обстежувати його та встановлені на ЕОМ, що знаходяться в цьому приміщенні, програми, файли тощо.

Будь-яка слідча (розшукова) дія результативна лише за умов її попередньої підготовки. Підготовка до обшуку під час розслідування зазначених злочинів складається з двох стадій.

1. До виїзду на місце слідчому та прокурору (процесуальному керівнику) необхідно:

– з урахуванням слідчої ситуації, що склалася, намітити коло осіб, які візьмуть участь у слідчій (розшуковій) дії. Окрім учасників СОГ (прокурора, слідчого, співробітника Департаменту захисту економіки Національної поліції України, спеціаліста-криміналіста), залучаються спеціалісти з комп'ютерних технологій, представники юридичних осіб або потерпілий;

– запросити понятих. Бажано запрошувати таких осіб, які мають достатній рівень знань у галузі комп'ютерних технологій. Якщо немає можливості залучити кваліфікованих понятих, то дії слідчого (спеціаліста) з дослідження ЕОМ чи комп'ютерної інформації повинні пояснюватися. Це необхідно на випадок допиту понятих у суді як свідків;

– підготувати відповідну комп'ютерну техніку, програмне забезпечення, що буде використовуватися для зчитування та збереження вилученої інформації. Традиційно відповідні технічні засоби застосовують ІТ-спеціалісти, але це не знімає відповідальності зі слідчого (прокурора) за їх наявність і комплектність;

– пояснити мету проведення слідчої (розшукової) дії та завдання, що стоять перед її учасниками, їх права та обов'язки, а також необхідні заходи обережності під час пересування на місці обшуку або роботи зі слідами тощо.

2. Після прибуття на місце проведення обшуку слідчий, прокурор повинен:

– видалити з місця проведення слідчої (розшукової) дії сторонніх осіб та забезпечити його охорону, якщо це не було зроблено раніше. Обов'язковій охороні підлягають: територія місця події, затриманий, ЕОМ, у якій було виявлено сліди злочину, сервер, пункти вимкнення живлення, якщо техніка знаходиться у ввімкненому стані, тощо;

– виключити можливість вчинення сторонніми особами будь-яких дій з комп'ютерною технікою, їх користування іншими технічними засобами, що можуть за допомогою бездротових технологій вносити зміни в інформацію (видаляти її);

– допитати як свідків потерпілого (заявника), інших осіб про те, що відбулося, зміни, які були внесені в обстановку, дії осіб до прибуття СОГ, види та технологічні операції, під час яких було виявлено ознаки злочину, та ін.;

– дати доручення учасникам СОГ на встановлення свідків, виявлення слідів, їх фіксацію тощо.

Пошук слідів комп'ютерного злочину необхідно розпочинати з виявлення мережевих підключень засобів комп'ютерної техніки, що знаходяться на місці події і в яких виявлені сліди злочину, та дослідження інформації, що пов'язана з цими підключеннями. З цією метою, опираючись на інформацію, що міститься в записах підключень, слід визначити наступну точку пошуку слідів аж до встановлення ЕОМ, яка є предметом злочинного посягання і засобом вчинення злочину.

У результаті пошук може привести до ЕОМ, які є кінцевими точками маршруту. Всі сліди на точках маршруту фіксуються, за потреби досліджуються та вилучаються фахівцем.

Слід зауважити, що спробу протиправного доступу, вчинену одним несанкціонованим користувачем, можна легко виявити. Тому подібний «електронний злам» здійснюється з декількох робочих місць: в означений час понад десять персональних комп'ютерів одночасно роблять спробу несанкціонованого доступу. При цьому кілька «атакуючих» комп'ютерів відсікаються системою захисту, а інші – отримують потрібний доступ. Один із тих комп'ютерів, що «прорвалися», блокує систему статистики мережі, яка фіксує всі спроби доступу. В результаті цього інші комп'ютери не можуть бути виявлені та зафіксовані. Частина з них приступає до «зламу» потрібного сектора мережі, а інші – займаються фіктивними операціями з метою дезорганізації роботи підприємства, організації, закладу і приховування злочину.

Варто звернути увагу процесуальних керівників на те, що відповідно до ст.ст. 159, 168, 236 КПК України тимчасове вилучення електронних

інформаційних систем або їх частин, мобільних терміналів систем зв’язку для вивчення фізичних властивостей, які мають значення для кримінального провадження, здійснюється лише у разі, якщо вони безпосередньо зазначені в ухвалі суду.

РОЗДІЛ 3 ЗАСАДИ ВИЛУЧЕННЯ ДОКАЗІВ З ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПІД ЧАС ПРОВЕДЕННЯ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИ) ДІЙ

3.1.Використання інформаційних технологій при проведенні негласних слідчих (розшукови) дій

Проблеми використання комп'ютерних технологій під час проведення негласних слідчих (розшукових) дій та їх процесуального оформлення потребують наукового вивчення та прикладного дослідження, адже чинний КПК України не містить переліку або визначення технічних засобів (у тому числі й комп'ютерних технологій), які законодавчо обов'язкові або рекомендовані до використання під час проведення НС(Р)Д, та не деталізує окремі аспекти процесуального оформлення за результатами їх проведення. Погоджуючись з думкою Д. М. Цехана щодо впровадження у практичну діяльність оперативних підрозділів високих інформаційних технологій, зазначимо, що це суттєво модифікувало процес отримання оперативно-розшукової інформації та, як наслідок, спричинило «технізацію» всієї ОРД, а також призвело до: 1) якісної модифікації окремих засобів ОРД; 2) появи нових суб'єктів ОРД (оперативно-технічних підрозділів) та модифікації діяльності інших; 3) того, що техніка стала обов'язковою складовою проведення найефективніших оперативно-розшукових заходів. [116, с. 71–72], що, на нашу думку, відноситься і до проведення негласних слідчих (розшукових) дій.

Під час проведення будь-яких НС(Р)Д на практиці фактично використовуються або технічні пристрої та засоби, або інформаційні технології, які викликають ускладнення під час використання у кримінальному повадженні, особливо сучасні новітні інформаційні

технології у вигляді обчислювальної техніки та програмного забезпечення [126, с. 87].

Якщо проведення таких НС(Р)Д, які не пов'язані із втручанням у приватне спілкування, наприклад аудіо-, відеоконтроль особи чи місця, обстеження публічно недоступних місць, житла чи іншого володіння особи не викликає особливих складнощів, то залежно захищеності каналу передачі даних використання злочинцем спеціального, програмного чи апаратного забезпечення обчислювальної техніки може суттєво ускладнити або унеможливити проведення досудового розслідування. Це, зокрема, стосується НС(Р)Д пов'язаних із втручанням у приватне спілкування, таких як зняття інформації з транспортних телекомунікаційних мереж, зняття інформації з електронних інформаційних систем. Тому виникає необхідність наукового вивчення та прикладного дослідження у галузях інформаційних та комп'ютерних технологій.

Загальні положення втручання у приватне спілкування визначено у ст. 258 КПК України, у ч.3 вказаної норми зазначено, що спілкуванням є передання інформації у будь-якій формі від однієї особи до іншої безпосередньо або за допомогою засобів зв'язку будь-якого типу. Спілкування є приватним, якщо інформація передається та зберігається за таких фізичних чи юридичних умов, при яких учасники спілкування можуть розраховувати на захист інформації від втручання інших осіб. При цьому втручанням у приватне спілкування є доступ до змісту спілкування за умов, якщо учасники спілкування мають достатні підстави вважати, що спілкування є приватним.

Достатніми для здійснення під час досудового розслідування втручання у приватне спілкування приводами можна вважати: отримання слідчим, прокурором у передбаченому законом порядку даних про те, що інформація, яка складатиме зміст приватного спілкування, з певним рівнем ймовірності може містити відомості про обставини, які мають значення для кримінального провадження; дані про те, що можливість отримання

відомостей про зміст приватного спілкування може бути забезпечена тільки шляхом проведення негласних слідчих (розшукових) дій, які допускають втручання у приватне спілкування [93, с. 39].

Відповідно до ч.4 ст. 258 КПК України, досліджуючи «втручання у приватне спілкування», маємо виділити такі НС(Р)Д:

1) аудіо- відео контроль особи;

2) арешт, огляд і виїмка кореспонденції;

3) зняття інформації з транспортних телекомунікаційних мереж;

4) зняття інформації з електронних інформаційних систем.

При проведенні НС(Р)Д пов’язаних із втручанням у приватне спілкування застосування комп’ютерних технологій, як і буд-яких науково-технічних засобів передбачає дотримання загальних тактичних рекомендацій. По-перше, в кожному конкретному випадку виникає необхідність вибору лише доцільних для даної ситуації технічних засобів. Такий вибір зумовлений метою й характером здійснюваної НС(Р)Д, особливостями об’єктів, для виявлення, фіксації або дослідження яких необхідним є застосування комп’ютерних технологій, їх придатністю для вирішення специфічних завдань конкретних НС(Р)Д. По-друге, комп’ютерні технології, що застосовуються при проведенні НС(Р)Д, не повинні змінювати якості досліджуваних об'єктів. По-третє, такі комп’ютерні технології доцільно використовувати з іншими технічними засобами комплексно, що надасть можливість встановлювати особливості об’єктів, підвищує вірогідність виявлення різноманітних слідів і предметів, а також надійність фіксації їх якостей.

Ефективність застосування комп’ютерних технологій може бути досягнута лише за умов технічної досконалості засобів, прийомів і методів в проведенні цих дій, а також шляхом розробки цілісної технології їх практичного застосування. Іншими словами, до технічних засобів збирання доказової інформації негласним шляхом можна віднести: засоби для негласного отримання й реєстрації акустичної інформації; візуального

спостереження й документування; прослуховування телефонних розмов, електронного перехоплення й реєстрації інформації із технічних каналів зв’язку; контролю поштових повідомлень й відправлень; дослідження предметів і документів; обстеження приміщень, транспортних засобів та інших об’єктів; отримання інформації з технічних засобів її збереження, оброки, передачі; технічних засобів ідентифікації особи.

Наприклад, така НС(Р)Д як електронне перехоплення й реєстрація інформації з технічних каналів зв’язку передбачає вчинення сукупності дій з отримання відомостей, необхідних для вирішення конкретних задач кримінального провадження й їх фіксації шляхом зняття науково-технічними засобами характеристик електромагнітних та інших фізичних полів, що виникають при передачі інформації мережами електричного зв'язку, в роботі комп'ютерних мереж, баз даних, телекомунікаційних інформаційних систем, що призначені для збирання, обробки, накопичення, збереження, пошуку й розповсюдження інформації [25, с.99].

Узагальнення практики проведення та організації НС(Р)Д, дає підстави стверджувати, що застосування сучасних інформаційних, комп’ютерних та телекомунікаційних технологій в слідчій діяльності дозволяє інтегрувати й опрацьовувати величезну кількість даних про конкретні криміногенні об’єкти, що містяться у відкритих джерелах інформації та спеціалізованих автоматизованих інформаційних системах, отримуючи при цьому нові знання про способи їх взаємодії та взаємозв’язки.

Зняття інформації з транспортних телекомунікаційних мереж для контролю та фіксації інформації, що передається через Інтернет й інші мережі передачі даних, може здійснюватися за відповідними ідентифікаційними ознаками: адресою електронної пошти у форматі «ім'я поштової скриньки @домен. домен верхнього рівня» (наприклад, info@ssu.gov.ua); адресою в мережі передання даних із комутацією пакетів, у т. ч. IP-адреса для мережі Інтернету у форматі «ххх.ххх.ххх.ххх» (наприклад,

008.011.015.130); апаратною адресою (MAC-адресою) пристрою, приєднаного до мережевого середовища [62, с. 80].

Слід зазначити, що із введенням в дію КПК України значно ускладнилася процедура отримання інформації від провайдерів телекомунікаційних послуг. Якщо раніше отримання такої інформації здійснювалося на підставі положень про «Конвенцію про кіберзлочинність» і Закону України «Про міліцію», то зараз така інформація віднесена до категорії документів, що містять охоронювану законом таємницю. А в розумінні статті 505 Цивільного кодексу України така інформація становить комерційну таємницю, яка є одним із об'єктів інтелектуальної власності. Тому, правоохоронні органи позбавлені можливості оперативно і своєчасно отримувати необхідну інформацію через запити правоохоронних органів.

При цьому, система прослуховування телефонних переговорів та установка прослуховуючого обладнання операторами мобільного та стаціонарного зв'язку в Україні вже давно стало однією з умов отримання права на проведення такої діяльності. Провайдерами встановлюється обладнання спецслужб для прослуховування телефонних переговорів. Ця вимога передбачена в ч. 4 ст. 39 закону «Про телекомунікації». Норма зобов'язує операторів телекомунікацій за власні кошти встановлювати в своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових та розвідувальних заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових та розвідувальних заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення [93]. За недотримання цієї вимоги (що може бути встановлено перевіркою Національної комісії, що здійснює державне регулювання у сфері зв`язку та інформатизації на посадову особу оператора телекомунікацій може бути накладено адміністративне стягнення за ст. 145 КУпАП «Порушення умов і правил, що регламентують діяльність у сфері телекомунікацій та користування радіочастотним ресурсом України,

передбачену ліцензіями, дозволами» у вигляді штрафу. При цьому досі залишається відкритим головне питання: хто контролює законність прослуховування телефонних переговорів та інтернет-трафіку у разі проведення НС(Р)Д правоохоронними органами? Адже коли комп'ютерна техніка для прослуховування встановлюється за домовленістю, ніхто, крім співробітників самої спецслужби, не знає, наскільки законно здійснюється прослуховування. Якщо говорити про зняття інформації без ухвали слідчого судді, то контроль законності залежить від типу включення обладнання й від можливості оператора контролювати видиму законність подібних сеансів. Згідно з українським законодавством, у оператора немає можливості знати про законність і правильність мотивації проведення такої дії у кримінальному провадженні.

Загалом, зняття інформації з транспортних телекомунікаційних мереж (каналів зв'язку), безперечно, сьогодні є ефективним способом отримання доказів у кримінальному провадженні. Водночас, задля належного виконання завдань щодо виявлення, попередження та припинення злочинів необхідне повноцінне функціональне отримання як слідчої, так і оперативної інформації, що надає можливість правоохоронним органам вирішувати, який вид зняття інформації необхідно проводити, залежно від конкретної практичної ситуації, [120, с. 45].

Вибір конкретних засобів, форм та методів реалізації будь-якої НС(Р)Д, в тому числі, і зняття інформації з електронних інформаційних систем, здійснюється ініціатором її проведення, з урахуванням дотримання конституційних прав і процесуальних норм, які зачіпають інтереси об'єкта розробки. Слід зазначити, що зазначені вимоги обґрунтованості та законності поширюються на НС(Р)Д, які проводяться за допомогою віддаленого доступу до інформаційних систем, який набув широкого поширення у зв'язку з появою численних систем так званих «Батьківського контролю».

Проте, функціонал численних програм «батьківського контролю» (за результатами опитувань оперативних працівників) включає в себе повний

набір сервісів, найбільш використовуваних в оперативно-розшукової діяльності. Так, наприклад, програма «батьківського контролю» FlexiSPY, при установці на смартфон з будь-якою операційною системою дозволяє, як мінімум, здійснити: контроль і запис стільникових дзвінків; контроль білінгу; контроль і запис VOIP-телефонії; контроль і запис оточення; перехоплення, блокування та підміну СМС повідомлення; перехоплення E-mail; обхід блокування телефону, екрану, додатків; контроль та стеження за місцем розташування по GPS; спостереження на змістом чатів WhatsApp, Facebook, Viber, Skype, Telegram, Tinder, Instagram; копіювання мультимедіа-файлів, включаючи відео-, фото- і аудіо-файли; отримання знімків з фронтальної і тилової камер; віддалене управління перезавантаженням і запуском додатків за допомогою СМС-команд; контроль та запис (логування) Інтернет-активності.

Важливо відзначити, що функціонування будь-яких електронних інформаційних систем включає в себе завдання захисту від зміни або знищення магнітного носія інформації (так званий жорсткий диск - HDD), або твердотільного носія інформації (флеш-пам'ять або SSD), на якому розташовані як мінімум чотири важливих класи інформації: завантажувальний запис (MBR), таблиця розміщення файлів (FAT, NTFS, EXT і т.п.), файли операційної системи та призначені для користувача програми і дані. Відповідно вбудовані носії інформаційних систем, файли програм як правило «прив'язані» і до операційної системи, і до місця запису даних та призначені лише для користувача дані доступні для прямого копіювання засобами OS без втрати цілісності. У зв'язку з цим, при необхідності отримання точної копії носія користуються або способом стороннього завантаження з побітовим копіюванням вбудованих носіїв інформації в так званий файл-образ на відчужуваному носії, або (за можливості) витягують носії і використовують спеціальні дублікатори - пристрої побітового клонування носіїв.

Сучасні реалії нашого життя доводять, що практично кожна особа залишає за собою електронний слід інформації (наприклад, у Великобританії загальна кількість баз даних, де громадяни можуть залишити електронний слід, у 2001 році становила близько трьохсот, сьогодні ця цифра значно більша) [127]. Правоохоронні органи зарубіжних країн широко використовують автоматизовані інформаційно-пошукові системи, які дозволяють значно оптимізувати розкриття та розслідування злочинів, учинених членами організованих угруповань. Наприклад, представляє значний інтерес досвід спецслужб США в розробці і застосуванні систем «Oasis» (ЦРУ) і «Magic Lantern» (ФБР), які уможливлюють не тільки контролювати інформаційний обмін злочинних співтовариств, але і «зламувати» комп'ютери підозрюваних, упроваджувати в них «трояни» (програми-віруси, що дозволяють відстежувати інформацію у цьому комп'ютері) тощо [108].

В рамках нашого дослідження варто звернути увагу на те, що в умовах реформування правоохоронної системи України суттєвим кроком на шляху до створення сучасної інформаційно-аналітичної бази протидії злочинності стало створення, відповідно до наказу Голови Національної поліції України від 07.11.2017 № 1150, Управління кримінального аналізу. Вказаний структурний підрозділ є спеціально уповноваженим щодо проведення, організації та координації інформаційно-пошукової та аналітичної роботи, спрямованої на збір, оцінку, аналіз та реалізацію інформації шляхом надання її уповноваженим органам (підрозділам) для вжиття заходів відповідно до їх компетенції, оцінювання ризиків, а також використання її для забезпечення виконання функцій, покладених на поліцію [83].

Слід зауважити, що на теперішній час в Україні актуальним стає питання щодо запровадження у системі кримінального аналізу новітніх технологій з програмними продуктам (I2, Maltego, Palantir, Big Data, Watsons тощо) та спільної інтегрованої моделі аналізу ризиків (CIRAM), які широко використовуються правоохоронними органами країн Європейського Союзу

З одного боку КПК містить прямі вказівки на необхідність проведення відповідних НС(Р)Д, а з іншого – забороняє співробітникам оперативних підрозділів здійснювати процесуальні дії за власною ініціативою та звертатись з клопотанням до слідчого судді або прокурора, що, в свою чергу, знижує ефективність боротьби зі злочинами у сфері суспільної моралі, яким властива висока латентність. А тому, виникає сумнів щодо ефективності процесуалізації деяких ОРЗ у НС(Р)Д. Фактично, майже весь процес досудового розслідування сьогодні побудовано не лише на законодавчій базі, а більшою мірою на особистих стосунках, що ставить під сумнів ефективність роботи загалом [123].

При проведенні такої негласної слідчої (розшукової) дії як обстеження публічно недоступних місць, житла, іншого володіння особи необхідними будуть науково-технічні засоби пошукового характеру, які негласно застосовуються для виявлення матеріальних носіїв інформації ознак злочину.

Під час негласного обстеження допускаються застосування технічних засобів, що є вимушеним захисним заходом суспільства і держави в боротьбі зі злочинністю [107, с.147].

Слід підкреслити, що проникнення в житло чи інше володіння в змісті частини другої статті 30 Конституції можливе виключно на підставі судового рішення у порядку, визначеному в розділі 21, зокрема у статті 267 КПК України. Для того, щоб суд надав дозвіл на вчинення такої процесуальної дії, мають бути вагомі підстави для отримання важливих відомостей щодо злочину, що готується, чи про скоєний злочин. Із цього приводу В. Тертишник зазначає, що не зважаючи на легітимність негласного проникнення оперативного працівника в житло людини, воно може мати тільки характер негласних розвідувальних та контррозвідувальних оперативно-розшукових заходів і не може бути засобом отримання доказів [106, с. 76].

С. С. Кудінов справедливо зазначає, що підготовча діяльність пов’язана в першу чергу з обранням найбільш сприятливих умов для проведення

НС(Р)Д (час, місце), підготовкою або виготовленням технічних, імітаційних засобів, визначенням кола учасників, їх підбором та інструктажем. Використання спеціальних знань під час проведення може полягати у їх використанні або врахуванні безпосередньо шляхом вчинення конкретних дій, застосування тактичних прийомів проведення тощо. Наприклад розкриття та запечатування спеціалістом кореспонденції, здійснення візуального спостереження [46, с. 158]. Відтак необхідно враховувати специфіку проведення саме цієї НС(Р)Д уже на підготовчому етапі, у тому числі, при залученні відповідних спеціалістів, з урахуванням вимог до законності обмеження права на недоторканість житла чи іншого володіння особи.

До основних вимог законності використання комп'ютерних технологій при проведенні НС(Р)Д у світлі гарантій недоторканності житла та іншого володіння особи належать:

а) підставами для проникнення з метою недопустимості свавільного проникнення у житло та інше володіння особи є суспільна необхідність у демократичному суспільстві, яка випливає із природи тяжких та особливо тяжких злочинів, оцінка яким дається судом у світлі обставин конкретної справи;

б) необхідною умовою для проведення цих процесуальних дій є обґрунтоване судове рішення, на підставі якого правоохоронні органи можуть здійснювати проникнення в житло та інше володіння особи з метою одержання інформації, проведення огляду та обшуку з метою одержання відомостей про тяжкі та особливо тяжкі злочини;

в) втручання має здійснюватися у невідкладних випадках, коли вичерпано інші можливості одержання інформації з метою захисту суспільних інтересів;

г) у разі застосування комп'ютерних технологій при проникненні у житло чи інше володіння особи вона може відстоювати свої права специфічним чином. Ця особа може зробити запит до прокуратури стосовно

того, чи мало місце проникнення в її житло чи інше володіння та на якій юридичній підставі, та вимагати інформацію, яка отримана при проведенні НС(Р)Д. У разі незадовільних дій прокуратури, можливе оскарження дій чи бездіяльності органів прокуратури та органів, що здійснюють оперативно-розшукову діяльність та негласні слідчі дії.

У справі «Волох проти України» Європейський суд з прав людини констатував, що в національному законодавстві має існувати засіб правового захисту від свавільного втручання державних органів у права, гарантовані пунктом 1 статті 8 Конвенції (право на повагу до особистого та сімейного життя). Ризик такої свавільності є особливо очевидним в умовах, коли повноваження виконавчої влади здійснюються таємно [96].

При проведенні спостереження за особою, річчю або місцем можуть використовуватись новітні інтелектуальні моделі поліцейської діяльності, керованої аналітикою яким є аналітичний продукт ІТ-додатку «Інтелектуальна система кримінального аналізу у режимі реального часу» (R.I.C.A.S.) [64, с.112]. Система RICAS розроблена для відображення та аналізу даних та інформації, які містяться в системі «АРМОР» та в інших базах даних, і є інструментом, який забезпечує швидке прийняття рішень. Додаток доступний у публічному та обмеженому режимі. Останній доступний лише підрозділам поліції, за допомогою використанням VPN-з'єднання за протоколом шифрування SSL.

Пошук (вибірка) необхідної інформації здійснюється за допомогою декількох опцій шляхом індексації зі всього контенту системи RICAS, що забезпечує швидкий та точний пошук інформації для аналізу.

Зазначимо, що у країнах Європейського Союзу, США та інших розвинених країнах світу використання можливостей кримінального аналізу є обов'язковим для всіх правоохоронних органів. З усіх існуючих методик аналізу оперативної інформації, прийнятих на озброєння правоохоронними органами більшості розвинених країн світу, найбільш часто використовуються програмні продукти і2 і ANACAPA [37, с, 20].

При розгляді справи «Фрідл проти Австрії» виникло питання про правомірність втручання у приватне життя особи шляхом знімання демонстрації, яка проходила в громадському місці і в ній брав участь заявник. Однак Комісія, яка ухвалювала попередній висновок у справі, підкреслила, що заявник добровільно брав участь у демонстрації, яка проводилася у публічному місці, оскільки фотографування велося виключно з метою фіксації ситуації у день події [36].

Проте визнається втручанням у приватне життя встановлення приладу стеження за рухом особи на базі GPS в автомобілі, яким користувалася особа, підозрювана в терористичній діяльності, та її гаданий замовник (справа «Узун проти Німеччини»). Втручання у приватне життя полягало в тому, що існувало «систематичне збирання та зберігання даних щодо конкретних осіб органами безпеки, навіть без використання методів таємного спостереження» [96].

На сьогодні існують різноманітні методи використання сучасних, у тому числі, й інформаційних, технологій з метою збору інформації, що використовуються при проведенні НС(Р)Д комплексно або окремо.

Одним з таких є інформаційно-аналітична діяльність – сукупність інформаційних процесів (збір, пошук, переробка інформації), необхідних для якісного та ефективного процесу управління. На даний час інформаційно-аналітична діяльність в органах Національної поліції України знаходиться на етапі розвитку, але слід відмітити, що впровадження системи ILP (з англ. Intelligence Led Policing – «поліцейська діяльність, керована розвідувальною аналітикою») в органах досудового розслідування відбувається дуже повільно. [34, с. 36]. Для успішного виконання завдань Інформаційно-аналітичної діяльності поліція у своїй діяльності використовує спеціалізовані аналітичні програмні продукти, такі як IBM i2 Analyst’s Notebook, MindManager та Power BI тощо.

Доповнювати аналітичну діяльність при проведенні НС(Р)Д повинна кримінальна розвідка, як частина кримінального аналізу, що надасть

можливість отримати доступ до джерел інформації та слідів злочину, до яких немає вільного доступу або відсутня можливість отримати такий доступ у гласний спосіб [57].

Головною метою кримінального аналізу є зміцнення механізмів попередження, виявлення, документування та розслідування кримінальних правопорушень, а також налагодження механізмів моніторингу криміногенної ситуації, обміну інформацією на державному, регіональному та міжнародному рівнях стосовно тенденцій та ризиків у цій сфері [60, с.445].

Іншим методом використання сучасних технологій з метою збору інформації при проведенні НС(Р)Д є розвідка відкритих джерел. Розвідка на основі відкритих джерел, яку ще називають Open source intelligence (OSINT) – одна з розвідувальних програм. Включає в себе пошук, вибір та збір інформації, отриманої із загальнодоступних джерел, а також її аналіз. У розвідувальному співтоваристві термін «відкритий» вказує на загальнодоступність джерела (на відміну від секретних джерел та джерел з обмеженим використанням), він не пов'язаний з поняттям open source (відкрите програмне забезпечення) або public intelligence (громадська розвідка).

Специфічна категорія технічних та людських ресурсів, джерела інформації і методи їх збору – все це відрізняє OSINT від інших видів розвідки. До переваг OSINT, на відміну від інших видів розвідки, відносять доступність джерел інформації, обсяг джерел інформації, різносторонність, оперативність отримання, легкість подальшого використання і вартість отримання [125, с.127].

У наш час, в умовах стрімкого розвитку інформаційних технологій, постійного збільшення обсягу інформаційних ресурсів, постають задачі швидкого та коректного пошуку потрібної інформації [70]. Найбільш ефективним напрямком інформаційного пошуку в мережі Інтернет для підрозділів Національної поліції є оперативний моніторинг інформаційних ресурсів, що представляє систему спостереження за станом кримінальних

процесів або відомостей про такі процеси, що містяться в мережі Інтернет з використанням засобів та методів оперативно-розшукової діяльності для їх подальшого аналізу з метою протидії злочинності [41, с. 77].

Наступним методом використання сучасних технологій з метою збору інформації при проведенні НС(Р)Д є технології Face Recognition та TouchID з'явилися порівняно нещодавно. Face Recognition (система розпізнавання облич) – це технологія, яка здатна ідентифікувати особу на цифровому зображенні або відеокадрі. Зараз технологія Face Recognition використовується у різних сферах життя суспільства. Що стосується технології TouchID, то вона ґрунтується на способі ідентифікації особи за слідами відбитків пальців рук.

Хоча вказані технології і є передовими, але все ж їхні можливості обмежені, як правовими механізмами, що унеможливлюють незаконне проникнення в особисте життя людини, так і техніко-матеріальними, що проявляються в обмеженій кількості. Обмеження права на особисте життя людини може здійснюватися і для пошуку та ідентифікації злочинців, що і використовують у своїй практиці правоохоронні органи, проте таке обмеження повинно бути співрозмірними поставленим цілям кримінального судочинства. Однак зараз таке використання обмежене автономними технічними системами, які виконують конкретні цілі Face Recognition та TouchID та використовуються у смартфонах, як правило, для ідентифікації власника [32, с.7].

У силу сучасних тенденцій трансформації розуміння приватності у зв'язку із застосуванням сучасних засобів стеження, які не потребують проникнення в житло чи засоби комунікації особи тощо, формальні процедури, пов'язані із судовим контролем, часто не можуть служити надійною гарантією недоторканності особистого та сімейного життя, зокрема, його комунікаційного аспекту. Оскільки здійснювані на практиці заходи таємного спостереження за обміном інформацією є закритими для їх ретельного аналізу з боку осіб, яких це стосується, або з боку громадськості

загалом, надання правової дискреції органам виконавчої влади у вигляді необмежених повноважень було б несумісним із принципом верховенства права. Отже, закон має з достатньою чіткістю визначати межі такої дискреції, наданої правоохоронним органам, і порядок її здійснення, з урахуванням законної мети даного заходу, щоб забезпечити особі належний захист від свавільного втручання (п. 49) [96].

Враховуючи невеликий досвід діяльності слідчих і оперативних підрозділів правоохоронних органів використання комп'ютерних технологій при проведенні НС(Р)Д у сфері розкриття та розслідування злочинів та з метою удосконалення досудового розслідування чинного кримінального процесуального законодавства, вважаємо за доцільне запропонувати продовжити напрацьовувати дослідження й теоретичні методики та рекомендації для практики щодо удосконалення збору та процесуального закріплення доказів під час використання комп'ютерних технологій при проведенні НС(Р)Д, а також з метою підвищення ефективності протидії, запобігання, моніторингу злочинів створити при підрозділах НП сектори аналітичної і технічної розвідки, із забезпеченням їх потужними комп'ютерними та іншими сучасними інформаційно-технічними засобами.

3.2. Процесуальне оформлення та використання результатів негласних слідчих (розшукових) дій проведених з викоримстанням інформаційних технологій у доказуванні.

Важливим під час досудового розслідування є детальне фіксування фактів протиправної діяльності осіб підозрюваних у вчиненні злочину, а також підтверджених фактів їх злочинної діяльності під час застосування відповідних технічних засобів та комп'ютерних технологій. З цією метою, під час складання протоколу повинні бути враховані умови щодо детального фіксування отриманої інформації в протоколі та відповідних додатках. Для цього необхідно, по-перше, здійснити оформлення необхідних документів, що підтверджують правові підстави, окреслюють коло суб'єктів та умови фіксування даних відповідно до вимог чинного законодавства України. По-друге, при фіксуванні необхідно уникнути можливих фізичних дефектів відповідного носія та забезпечити максимально високу якість фіксації для можливого подальшого експертного дослідження такої інформації. По-третє, залучати спеціалістів, здатних кваліфіковано поводитися з технічними засобами та програмним забезпеченням, і згодом підтвердити технічну можливість та факт отримання таких відомостей у судовому засіданні [118 с. 258].

Фіксування є важливим етапом в роботі з доказами та має на меті: по-перше, надати результатам розслідування значення судового доказу; по-друге, щоб особи, які не брали участь у процесуальній дії, зокрема, склад суду, могли наочно уявити собі обстановку на місці її проведення, отримати будь-яку точну довідку про події, що відбувалися та їх зміст. Ці завдання в ході розслідування можна вирішувати лише використовуючи різні науково-технічні засоби та складаючи відповідні процесуальні документи [12]. Безумовно, обов'язковою умовою правомірного застосування науково-технічних засобів і методів для фіксації ходу й результатів розслідування є документальне оформлення факту й обставин їх застосування, а також

отриманих при цьому даних [25, с.100]. Процесуальне оформлення результатів використання комп'ютерних технологій під час проведення негласних слідчих (розшукових) дій є кінцевим етапом їх проведення слідчим або виконання доручення слідчого працівниками оперативного підрозділу. Вказане потребує процесуального оформлення отриманих результатів згідно з вимогами чинного КПК України для вирішення питання, чи будуть вони визнані доказами у кримінальному провадженні.

Відповідно до ч.1 ст. 84 КПК України, доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому КПК України порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. Тобто, відповідно до ч. 1 ст. 84 КПК України, фактичні дані, які отримані не в порядку передбаченому Кримінальним процесуальним кодексом України**,** доказами в кримінальному провадженні в принципі бути не можуть. Відповідно до ч.1 ст. 86 КПК України, доказ визнається допустимим, якщо він отриманий у порядку, встановленому КПК [48].

Таким чином, положеннями ч.1 ст. 84 та ч.1 ст. 86 КПК України встановлено, що доказ є доказом і може бути визнаний допустимим, лише в тому випадку, коли він отриманий виключно в порядку, передбаченому положеннями КПК України**.** В інших випадках, доказ не може бути визнаний доказом та не може бути визнаний допустимим. Відповідно ж до ч.2 ст. 86 КПК України, недопустимий доказ не може бути використаний при прийнятті процесуальних рішень, на нього не може посилатися суд при ухваленні судового рішення**.** Судам необхідно звертати особливу увагу на порядок отримання доказів слідчим та прокурором під час досудового розслідування та ретельно з'ясовувати, чи в порядку, передбаченому положеннями КПК України, отриманий той чи інший доказ в кримінальному провадженні.

Для подальшого дослідження питань допустимості доказів отриманих в результаті досудового розслідування, необхідно враховуватися низку положень чинного КПК України, зокрема:

1) ст. 103 КПК України «Форми фіксування кримінального провадження», у якій зазначено, що процесуальні дії під час кримінального провадження можуть фіксуватися в таких формах: а) протокол; б) запис за допомогою технічних засобів; в) журнал судового засідання;

2) ч. 2 ст. 105 КПК України «Додатки до протоколів», у якій зазначено, що додатками до протоколу можуть бути: а) спеціально виготовлені копії, зразки об'єктів, речей і документів; б) письмові пояснення спеціалістів, які брали участь у проведенні відповідної процесуальної дії; в) стенограма, аудіо-, відеозапис процесуальної дії; г) фото-таблиці, схеми, зліпки, носії комп'ютерної інформації та інші матеріали, які пояснюють зміст протоколу;

3) ч. 1 ст. 252 КПК України «Фіксація ходу і результатів негласних слідчих (розшукових) дій», у якій зазначено, що фіксація ходу і результатів негласних слідчих (розшукових) дій повинна відповідати загальним процесуальним правилам фіксації кримінального провадження, положеннями, передбаченим КПК України. За результатами проведення негласної слідчої (розшукової) дії складається протокол, до якого в разі необхідності додаються додатки. Відомості про осіб, які проводили негласні слідчі (розшукові) дії або були залучені до їх проведення, у разі здійснення щодо них заходів безпеки можуть зазначатися із забезпеченням конфіденційності даних про таку особу в порядку, визначеному чинним законодавством;

4) ч. 1 ст. 256 КПК України «Використання результатів негласних слідчих (розшукових) дій у доказуванні», у якій зазначено, що протоколи щодо проведення негласних слідчих (розшукових) дій, аудіо- або відеозаписи, фотознімки, інші результати, здобуті за допомогою застосування технічних засобів, вилучені під час їх проведення речі і документи або їх копії можуть використовуватися у доказуванні на тих самих

підставах, що і результати проведення інших слідчих (розшукових) дій під час досудового розслідування;

5) ст. 259 КПК України «Збереження інформації», у якій зазначено, що якщо прокурор має намір використати під час судового розгляду як доказ інформацію, отриману внаслідок втручання у приватне спілкування, або певний її фрагмент, він зобов'язаний забезпечити збереження всієї інформації. Враховуючи викладене, слід зазначити, що не менш важливим за отримання, в ході проведення НС(Р)Д, процесуально значимої інформації, є обізнане, своєчасне процесуальне оформлення отриманих результатів та закріплення їх як доказів [126, с. 87].

Слід зазначити, що крім стандартних процесуальних реквізитів, які необхідно заповнити під час складання протоколу, при використанні комп'ютерних технологій, в ньому необхідно фіксувати такі відомості про використання технічних засобів і пристроїв, обчислювальної техніки та програмного забезпечення. При цьому слід враховувати, що відповідно до ч.1 ст. 107 КПК України, рішення про фіксацію процесуальної дії за допомогою технічних засобів під час досудового розслідування приймає особа, яка проводить відповідну процесуальну дію**.**

Вважаємо що при використанні комп'ютерних технологій при проведенні НС(Р)Д в протоколі необхідно зазначати: 1) точну назву технічного засобу, пристрою, обчислювальної техніки або програмного забезпечення мовою виробника; 2) серійний номер комп'ютерної програми, пристрою, обчислювальної техніки або програмного забезпечення; 3) наявний стан зношеності або будь-яких дефектів зовнішнього вигляду чи у роботі використаного технічного засобу, пристрою, обчислювальної техніки, програмного забезпечення (визначається зовнішнім візуальним оглядом слідчого чи оперативного працівника); 4) умови, у яких було використано технічний засіб, пристрій, обчислювальну техніку або програмне забезпечення, а також дату й точний час; 5) всю інформацію в цифровому вигляді, яка представляє процесуальний або оперативний інтерес незалежно

від того, на якому носії вона знаходиться, бажано оглянути в присутності спеціаліста й понятих, після чого скопіювати її на матеріальний носій, який повинен бути долучений до протоколу проведення НС(Р)Д незалежно від того, чи долучається до цього ж протоколу оригінальний носій скопійованої інформації [35, с. 303]; 6) у процесі копіювання цифрової інформації з носія на носій, наприклад, під час огляду жорсткого диску комп'ютера, необхідно користуватись програмним забезпеченням для побітового копіювання інформації (наприклад, програми «SMART», «NED», «FTK»,«dd» тощо), а після копіювання до протоколу проведення НС(Р)Д необхідно обов'язково додати копію програмного засобу, яким це копіювання було здійснено. Використання вказаних та інших вимог положень чинного КПК України слугуватиме більш ефективному застосуванню новітніх технологій у досудовому розслідуванні, зокрема під час проведення негласних слідчих (розшукових) дій, а також під час їх оформлення як слідчими, так і працівниками оперативних підрозділів, що виконують такі дії за їх дорученням. Однак окреслені питання потребують окремого дослідження або наукового вивчення [126, с. 87].

Під час проведення НС(Р)Д слідчим та працівниками оперативних підрозділів особливу увагу слід звертати не лише на методи їх проведення, а й оформлення отриманих внаслідок НС(Р)Д даних у відповідних протоколах. Саме на оформлення протоколів про хід і результати НС(Р)Д під час судового розгляду звертається увага. Відповідно до ч.1 ст. 252 КПК України, фіксація ходу і результатів НС(Р)Д повинна відповідати загальним правилам фіксації кримінального провадження**,** передбаченим КПК. За результатами проведення НС(Р)Д складається протокол, до якого в разі необхідності долучаються додатки. Таким чином, положення ч. 1 ст. 252 КПК України відсилає до загальних правил фіксування кримінального провадження, які визначено у главі 5 КПК України. Відповідно до ч.1 ст. 104 КПК України, у випадках, передбачених КПК України, хід і результати проведення процесуальної дії фіксуються в протоколі. Отже, відповідно до ч.1 ст. 252 та

ч.1 ст. 104 КПК України, за результатами проведення негласних слідчих (розшукових) дій, обов'язково складається протокол про хід та результати даної процесуальної дії. Слід наголосити, що в протоколі проведення НС(Р)Д повинно бути зафіксовано хід даної процесуальної дії. Разом із тим, на практиці під час складання протоколу фіксуються результати НС(Р)Д і залишається поза увагою фіксування в протоколі НС(Р)Д ходу даної процесуальної дії.

Тобто, співробітники правоохоронних органів не відображають весь перебіг НС(Р)Д, обмежившись відображенням лише отриманих під час НС(Р)Д результатів [53].

Таким чином, на для визнання протоколу НС(Р)Д, як доказу в кримінальному провадженні, повинні бути враховані положення ч.1 ст. 252 та ч.1 ст. 104 КПК України, що вимагають, аби в протоколі був зафіксований і хід, і результати НС(Р)Д.

Наявність підстав і умов застосування технічних засобів. Інформація, отримана в результаті проведення НС(Р)Д з використанням комп'ютерних технологій і є доказом у кримінальному провадженні, повинна бути обов'язково відображена у відповідному протоколі. У протоколі повинні бути вказані: технічні характеристики використаної апаратури, її справність; зафіксовані події та факти в динаміці, відомості про загальні умови застосування технічних засобів; спосіб упаковки та опечатування отриманих носіїв інформації, а також місце та умови їх зберігання в подальшому. В протилежному випадку, як справедливо зазначає Е. А. Доля, може бути ускладнено встановлення дійсного змісту інформації, відображеної на носіях, до неї можуть бути внесені зміни, що тягне неможливість адекватного сприйняття даних (в тому числі й шляхом проведення відповідної експертизи), більш того, внаслідок незворотних змін інформація буде загублена [35, с.100-102].

Основним функціональним призначенням НС(Р)Д в системі кримінального процесу України є забезпечення оптимальних шляхів

використання у кримінально-процесуальному провадженні інформації, здобутої із використанням негласних сил та засобів, якими послуговується оперативно-розшукова діяльність [99, с. 299]. Тому, надалі потрібно приділити увагу дослідженню окремих питань використання результатів НС(Р)Д у доказуванні. Відповідно до ч.1 ст. 256 КПК протоколи щодо проведення НС(Р)Д, аудіо- або відеозаписи, фотознімки, інші результати, здобуті за допомогою застосування технічних засобів, вилучені під час їх проведення речі і документи або їх копії можуть використовуватися в доказуванні на тих самих підставах, що і результати проведення інших слідчих (розшукових) дій під час досудового розслідування [48]. Отже, результати НС(Р)Д використовуються при доказуванні на тих самих підставах, що й результати проведення інших слідчих (розшукових) дій. Але, на жаль, сьогодні, використання результатів НС(Р)Д з використанням комп'ютерних технологій у доказуванні бажає кращого. Адже, слабка результативність використання результатів у доказуванні, пов'язана з неналежним процесуальним закріпленням проведення НС(Р)Д; неякісним процесуальним оформлення результатів НС(Р)Д; порушенням прав, свобод та законних інтересів осіб під час проведення НС(Р)Д; невідповідністю результатів НС(Р)Д вимогам допустимості, належності й достовірності тощо; громіздкістю процедури їх розсекречення, що потребує часу в реальних умовах його процесуальної обмеженості; неможливістю чи недоцільністю розсекречення результатів НС(Р)Д з урахуванням форм і методів їх проведення; невизнанням судом результатів НС(Р)Д допустимими, належними, достовірними доказами, а сукупності наданих доказів, отриманих за результатами НС(Р)Д, – достатніми для прийняття судового рішення. [102, с. 105].

Для використання комп'ютерних технологій під час проведення НС(Р)Д, повинні бути законні підстави як правові, так і фактичні. Правовими підставами є сукупність передбачених кримінально-процесуальним законом умов, що дають право на використання комп'ютерних технологій під час

проведення НС(Р)Д. Фактичними підставами є факт правопорушення (фактично вчиненого суспільно небезпечного діяння). Наявність таких підстав є гарантією дотримання законності в їхньому проведенні та подальшого використання результатів проведених НС(Р)Д у доказуванні. Разом із тим правові підстави використання комп'ютерних технологій при проведенні НС(Р)Д недостатньо чітко визначені в чинному КПК України. З метою запобігання зловживанню безпідставним проведенням НС(Р)Д, зокрема, порушення права людини на приватне спілкування, необхідно закріпити в КПК України чіткий перелік підстав їхнього використання, що, своєю чергою, забезпечить дотримання вимог чинного законодавства щодо конституційних прав і свобод громадян, які допускаються Конституцією України, за необхідного тимчасового обмеження їх.

Ми погоджуємось з поглядом О. В. Соколова, який зазначив що доцільно на слідчого, прокурора покласти обов'язок в ході досудового розслідування злочинів, з метою ідентифікації особи ініціювати проведення судово-технічних експертиз, за результатами яких підтверджувати наступне: 1) файли, які містяться на матеріальних носіях інформації, створені завдяки технічним засобам, що вказані у протоколі відповідної НС(Р)Д; 2) аудіо та відеофайли не містять ознак монтажу; 3) голос, зафіксований у ході НС(Р)Д, належить підозрюваному; 4) на відеоматеріалах, отриманих в результаті проведення НС(Р)Д, зображений підозрюваний тощо [105, с.125].

З урахуванням прийнятих в Україні нормативних актів доцільно розширити поняття доказів, а також визначити, що є електронним доказом, критерії допустимості та достовірності. Зростаюча ступінь витонченості злочинної діяльності викликає ще більші труднощі, пов'язані з виявленням електронних доказів, застосуванням зловмисниками методів заплутування, необхідністю аналізу великих обсягів даних і отриманням даних від постачальників послуг. Транснаціональний та транскордонний характер злочинності, специфіка утворення електронних слідів поза юрисдикцією держави зумовлюють необхідність розвитку міжнародного співробітництва,

формування уніфікованого міжнародного законодавства щодо використання електронних доказів у кримінальному судочинстві [1, с. 228].

Д. М. Цехан під «цифровими доказами» розуміє фактичні дані, що представлені у цифровій (дискретній) формі та зафіксовані на будь-якому типі носія та після обробки ЕОМ стають доступними для сприйняття людиною. При цьому, обов'язковою ознакою цифрового доказу є конвергентність, під якою розуміється здатність одиничного доказу входити у сукупність інших доказів і набувати у зв'язку з цим доказового значення. Проте, цифровий об'єкт, який є нематеріальним, не має відповідних якісних фізичних характеристик, має специфічну процедуру та середовище створення, здатний до копіювання та переміщення без втрати характеристик, сприймається людиною лише після обробки ЕОМ та виведення інформації на відповідний технічний пристрій (монітор), неможливо визнати матеріальним об'єктом і, як наслідок, речовим доказом чи традиційним документом. У даному випадку необхідно оцінювати власне інформацію, а не матеріальний об'єкт на якому вона зафіксована. У кримінальному процесі електронний доказ повинен відповідати вимогам відносності і допустимості [118 с. 256]. У зв'язку з цим, особливої уваги потребує процедура фіксації цифрової інформації та забезпечення її доказового значення. Ключовим чинником у цьому випадку є коректна фіксація інформації, яка може здійснюватись автоматично за допомогою спеціального програмного забезпечення та за участю відповідного суб'єкта (експерта, спеціаліста).

Стосовно використання електронних документів у доказуванні ОП ККС ВС у своєму рішенні від 10 вересня 2020 року, справа № 51-1704км20 вказує, що ототожнення електронного доказу як засобу доказування та матеріального носія такого документа є безпідставним, оскільки характерною рисою електронного документа є відсутність жорсткої прив`язки до конкретного матеріального носія [71].

Ототожнення електронного доказу як засобу доказування та матеріального носія такого документа є безпідставним, оскільки характерною

рисою електронного документа є відсутність жорсткої прив`язки до конкретного матеріального носія.

Відповідно до ст. 7 Закону України «Про електронні документи та електронний документообіг» від 22 травня 2003 року № 851-IVу випадку зберігання інформації на кількох електронних носіях кожний з електронних примірників вважається оригіналом електронного документа.

Матеріальний носій - лише спосіб збереження інформації, який має значення тільки коли електронний документ виступає речовим доказом. Головною особливістю електронного документа є відсутність жорсткої прив`язки до конкретного матеріального носія. Один і той же електронний документ (відеозапис) може існувати на різних носіях. Всі ідентичні за своїм змістом примірники електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом та датою створення. Питання ідентифікації електронного документа як оригіналу можуть бути вирішені уповноваженою особою, яка його створила (за допомогою спеціальних програм порахувати контрольну суму файлу або каталогу з файлами - CRC-сума, hash-сума), або за наявності відповідних підстав шляхом проведення спеціальних досліджень.

Долучений слідчим до матеріалів провадження в якості речового доказу DVD-R диск з відеозаписом обставин події був виготовлений у зв`язку із необхідністю надання інформації, яка має значення у кримінальному провадженні та є самостійним джерелом доказу похідним від інформації, що зберігається на комп`ютері в електронному вигляді у виді файлів.

Таким чином, записаний на оптичний диск - носій інформації електронний файл у вигляді відеозапису є оригіналом (відображенням) електронного документу. Суд першої інстанції за результатами оцінки доказів у порядку, передбаченому ст. 94 КПК, оцінюючи вказані протоколи НС(Р)Д, зважив на наявність у матеріалах провадження клопотань про надання дозволу на їх проведення та ухвал Апеляційного суду про надання

дозволу на проведення НРСД, які є підставою для їх проведення, обґрунтовано зазначив, що НС(Р)Д були здійснені з додержанням вимог статей 246-257 цього Кодексу, є належними і допустимими доказами [71].

Існує необхідність нормативного закріплення категорії «цифрового доказу».

Сьогодні можна говорити про низький рівень підготовки слідчих до роботи із програмно-технічними комплексами та складними програмними технологіями. Як зазначають вчені, з боку слідчих та працівників оперативних підрозділів було б самовпевнено розраховувати на власні сили у цій галузі [109, с.119].

В цілому, слідчий може самостійно застосовувати у своїй діяльності спеціальні знання та науково-технічні засоби, адже відповідно до положень ст.ст. 40, 246, 252, 266 КПК України слідчий під час безпосереднього проведення ним НС(Р)Д може самостійно застосовувати спеціальні знання та науково-технічні засоби, якщо він вважає, що достатньо ними володіє для вирішення конкретних питань [52, с. 156].

Враховуючи положення чинного КПК України, можна виокремити три процесуальні форми використання спеціальних знань під час досудового розслідування:

1) залучення спеціаліста для надання письмової консультації;

2) залучення спеціаліста для надання безпосередньої технічної допомоги під час процесуальних дій;

3) залучення експерта для проведення судової експертизи й виконання обов’язків судового експерта [100, с.292].

Як свідчать матеріали слідчої практики, в абсолютній більшості проваджень пояснення надають штатні працівники кіберполіції, які є фахівцями з інформаційних технологій або електроніки й телекомунікацій, і в процесуальному статусі спеціаліста були залучені під час проведення огляду процесуальних дій. У письмовому поясненні такий спеціаліст описує методи так званого експрес-аналізу (процес встановлення фактичних даних, що

мають значення для конкретного факту правопорушення); методи вилучення (копіювання) та збереження нетрадиційних (цифрових) слідів злочину.

Спеціаліст може залучатися під час проведення процесуальних дій, пов'язаних з дослідженням інформації, отриманої при проведенні НС(Р)Д з використанням комп'ютерних технологій. В таких випадках, відбувається огляд документів слідчим за участю спеціаліста носіїв інформації з вивченням змісту зафіксованої в них інформації. Адже законодавець до документів відносить і матеріали фотозйомки, звукозапису, відеозапису, носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії, що прямо передбачено частиною другою ст. 99 КПК України. Негласність способу отримання таких технічних носіїв інформації (USB-флеш-накопи́чувач, диск) зумовлює потребу проведення негласної слідчої (розшукової) дії для їх огляду й вивчення змісту, що охоплюється поняттям дослідження [44, с. 169].

Виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації здійснюється в строки, установлені законодавством, має вигляд спеціальної, таємної операції, тактика та методи проведення якої визначаються чинним законодавством.

Виконання спеціального завдання в кіберпросторі, дає можливість залучити до його виконання штатного працівника кіберполіції та значно зменшує обсяг застосування заходів безпеки до такої особи.

З іншого боку, такі дії повинні бути виконані виключно в правовому полі, і не повинні бути розтлумачені як провокація злочину. Для визначення провокації злочину ЄСПЛ встановив, зокрема, такі критерії: чи були дії правоохоронних органів активними, чи мало місце з їх боку спонукання особи до вчинення злочину, наприклад, прояв ініціативи у контактах з особою, повторні пропозиції, незважаючи на початкову відмову особи, наполегливі нагадування, підвищення ціни вище середньої; чи був би скоєний злочин без втручання правоохоронних органів; вагомість причин проведення оперативної закупівлі, чи були у правоохоронних органів

об’єктивні дані про те, що особа була втягнута у злочинну діяльність і ймовірність вчинення нею злочину була суттєвою. Висновок про наявність провокації злочину без перевірки зазначених обставин та надання їм оцінки є необґрунтованим [66].

Етап дослідження інформації, отриманої при застосуванні комп’ютерних технологій під час проведення слідчих та негласних слідчих (розшукових) дій також передбачає необхідність активного застосування спеціальних знань. Відповідно до положень ч.1 ст. 266 КПК України таке дослідження може здійснюватися шляхом: 1) вивчення змісту отриманої інформації безпосередньо слідчим самостійно або із залученням відповідних фахівців; 2) проведення досліджень отриманих відомостей та об’єктів у рамках відповідних судових експертиз.

У ході перевірки інформації, отриманої при застосуванні комп’ютерних технологій, має бути встановлено: а) автентичність даних, зафіксованих на носіях інформації [110, с. 65]; б) місце, дата та час отримання відповідних даних; в) учасники подій.

Спеціаліст може залучатись до виконання зазначених дій для надання консультації або технічної допомоги слідчому.

При цьому допомого полягає в:

- описі характеристик носіїв інформації, технічних засобів її фіксації, комп’ютерних технологій за допомогою яких була відтворена наявна на них інформація;

- експлуатації технічних засобів: підборі та налаштуванні необхідного технічного обладнання; створенні умов для відтворення зафіксованої на носіях інформації (відео-та фонограми); забезпеченні можливостей для розшифрування інформації; повторного її перегляду, прослуховування; перегляду в сповільненому режимі або в збільшеному вигляді; відтворенні в повному обсязі або відповідної частини інформації, що має значення для досудового розслідування із зазначенням змісту розмов осіб, звуків, рухів, дій, що пов’язані з протиправною діяльністю яка документувалася тощо;

- з’ясуванні відомостей, що містяться у відео-та фонограмах, на відповідних носіях інформації, належній оцінці їх змісту;

- використанні можливостей: ідентифікаційно-пошукових та діагностично-пошукових систем і мультимедійних технологій очищення та синтезу аудіо-, відеоінформації, відновлення в разі їх часткового пошкодження; сучасних комп’ютерних технологій та спеціальних програмних комплексів для усунення звукових перешкод, вилучення необхідної інформації з аудіо- та відеозаписів; ідентифікації осіб за сукупністю ознак (за голосом); комп’ютерних систем розпізнавання мовлення (перетворення звуку в текст) при складанні стенограм розмов осіб та фіксуванні послідовності вчинюваних ними дій, що в подальшому полегшить процес оперування доказами за рахунок можливості в будь-який момент часу без допомоги технічних засобів ознайомитися зі змістом процесуальної дії;

- забезпеченні умов збереження цілісності інформації та носіїв, на яких вона зафіксована [12, с.53].

ВИСНОВКИ

В результаті дослідження використання інформаційних технологій при вилучення майна під час досудового розслідування проаналізовано нормативне забезпечення порядку застосування інформаційних технологій, акцентовано увагу на проблемних аспектах, та неврегульованості деяких норм, а також запропоновано шляхи удосконалення чинного законодавства. Основними результатами роботи слід зазначити наступне.

На сьогодні стан розробленості теоретичних та організаційно-тактичних основ використання інформаційних технологій при вилученні доказів під час досудового розслідування свідчить про відсутність сучасного комплексного системного підходу у цьому напрямку з урахуванням новітньої моделі діяльності оперативних і слідчих підрозділів. Крім того, з нашої точки зору не достатньою досліджено використання інформаційних технологій під час розслідування кримінальних правопорушень; відсутня конкретизація суб'єктів-виконавців та видів злочинів відносно, яких під час кримінального провадження можуть використовуватися інформаційні технології, як різновид спеціальних технічних засобів; відсутній перелік комп'ютерних технологій.

Вищезазначене свідчить про необхідність створення науково-практичних рекомендацій з питань боротьби зі злочинністю спрямованих на:

- визначення сучасних теоретичних засад кримінально-процесуальної діяльності щодо використання інформаційних технологій, з урахуванням особливостей сучасного стану реформування кримінально-процесуального законодавства;
- вирішення нормативно-правових питань (визначення формальних та матеріальних підстав та умов використання інформаційних технологій, удосконалення інформаційно-аналітичного забезпечення діяльності підрозділів, що здійснюють досудове розслідування, визначення мети та загальних принципів використання інформаційних технологій);

- удосконалення організаційно-тактичних основ застосування інформаційних технологій під час досудового розслідування.

За цільовим призначенням комп'ютерні технології при досудовому розслідуванні є різновидом технічних засобів, що використовуються у правоохоронній діяльності. При цьому лише технічні засоби негласного отримання інформації, які спеціально пристосовані та/або взагалі відповідають вимогам, що визначають можливість їх використання для вирішення завдань оперативно-розшукової та кримінально-процесуальної діяльності у властивих їм формах та методах, можуть бути віднесені до спеціальних технічних засобів. Тобто технічні засоби негласного отримання інформації, що були виготовлені не для потреб правоохоронних органів, але відповідають зазначеним вимогам, можуть бути віднесені до спеціальних технічних засобів.

У законодавстві України, що регулює застосування технічних засобів у сфері кримінального судочинства, не сформувалася однозначна понятійна система, яка визначає призначення, види і класифікацію інформаційних технологій, що використовуються при виявленні, розкритті та розслідуванні злочинів.

Використанню інформаційних технологій при вилученні доказів під час досудового розслідування притаманні їх специфічні ознаки: юридичний характер; здійснення виключно державою; правоохоронна спрямованість; негласна форма проведення; обмеження переважно сферою боротьби зі злочинністю; наявність триєдиної мети, якою є захист людини – суспільства – держави.

Відсутність єдиного розуміння сутності комп'ютерних технологій, що застосовуються в сфері кримінального судочинства, невизначеність їх правового статусу та порядку використання у кримінальному провадженні тягне за собою не тільки неясність нормативно-правових формулювань, а й негативно позначається на якості досудового розслідування та судового розгляду.

З метою удосконалення нормативного регулювання порядку застосування комп'ютерних технологій під час проведення НС(Р)Д пропонується:

- окремо виділити і законодавчо закріпити поняття комп'ютерних технологій, як різновиду спеціальних технічних засобів негласного отримання інформації шляхом внесення змін у закони України;

- визначити вимогу, що під час отримання даних із застосуванням спеціальних технічних засобів негласного отримання інформації правоохоронним органам приймати заходи щодо охорони та нерозголошення інформації, отриманої за їх допомогою.

Перспективним є подальше впровадження концепції правоохоронної діяльності, керованої аналітикою, відповідно до якої задля інкорпорування аналітичної розвідувальної інформації у сферу кримінального провадження, у тому числі, для ефективного використання інформайційних технологій при здійсненні досудового розслідування, запропоновано створення секторів аналітичної та технічної розвідки.

При застосуванні інформаційних технологій під час проведення негласних слідчих (розшукових) дій не повинні змінювати якості досліджуваних об'єктів.

Інформаційні технології доцільно використовувати з іншими технічними засобами комплексно, що надасть можливість встановлювати особливості об'єктів, підвищує вірогідність виявлення різноманітних слідів і предметів, а також надійність фіксації їх якостей.

Потребує визначення та закрпілення процедура ліцензування комп'ютерних програм, що використовують у сфері комп'ютерних технологій в Україні. У разі створення відповідної правової бази необхідною умовою використання будь-якої комп'ютерної програми стане її сертифікація, а відповідно, і контроль держави за її використанням.

Необхідним є створення багатоступеневої системи контролю за здійсненням НС(Р)Д та використання при цьому науково-технічних засобів та комп'ютерних технологій.

Загальна принципова допустимість застосування технічних засобів визначається вимогами законності, повноти, об'єктивності та всебічності кримінального судочинства.

Електронні (цифрові) докази містять доказову інформацію та можуть підтверджувати або спростовувати належність і допустимість інших доказів у кримінальному провадженні.

Необхідним є внесення змін до КПК України у частині визначення поняття електронного (цифрового) доказу, вимог до його належності, допустимості та достовірності, закріплення процесуальних джерел електронних (цифрових) доказів.

Умовами фіксації, закріплення та використання доказової інформації, отриманої за допомогою інформаційних технологій (в тому числі цифрових) як при проведенні НС(Р)Д так і при здійсненні досудового розслідування в цілому є: наявність підстав і умов застосування технічних засобів; правильне процесуальне та технічне оформлення отриманих результатів.

Належне використання комп'ютерних технологій в ході проведення НС(Р)Д під час досудового розслідування полягає в обов'язковому залученні слідчим, прокурором у взаємодії з оперативним підрозділом спеціалістів, які мають навички використання комп'ютерних технологій, технічних засобів аудіо- та відеоконтролю тощо з метою отримання інформації, яка може бути використана як доказ, після перевірки та оцінки на предмет належності, допустимості, достовірності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ахтирська Н.М. Міжнародний досвід використання цифрової інформації у кримінальному судочинстві. *Юридичний науковий електронний журнал*. 2019. № 4. С.221-229.
2. Бабин А. В. Содержание обыска. Учебные записки: Сборник научных трудов юрид. фак-та Оренбургского гос. ун-та. Вып. 3. Оренбург : Издат. Центр ОГАУ, 2006. 408 с.,
3. Бараненко Б.І., Бочковий О.В., Гусєва К.А. Негласні слідчі (розшукові) дії та особливості їх проведення оперативними підрозділами органів внутрішніх справ: навч. посіб. Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2014. 416 с.
4. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность. М.: Юрид.література, 1999. 158 с.
5. Бразоль Б. Л. Очерки по следственной части : История. Практика. Петроград, 1916. 180 с.
6. Безруков Д. В. Використання оперативно-технічних засобів щодо протидії злочинам проти власності підрозділами карного розшуку: дис. … канд. юрид. наук: 12.00.09. Кривий Ріг. 2015. 229 с.
7. Безруков Д.В., Хараберюш І.Ф. Особливості використання матеріалів, отриманих засобами спеціальної техніки у досудовому розслідуванні органами внутрішніх справ за новим кримінальним процесуальним законом. *Проблеми правознавства та правоохоронної діяльності: Збірник наукових праць Донецького юридичного інституту МВС України*. 2013. № 1. С. 96-104.
8. Белкин Р. С. Общая теория советской криминалистики. Саратов: Изд-во Саратовского университета, 1986. 677 с
9. Біленчук П.Д., Зубань М.А. Комп’ютерні злочини: соціально-правовий і кримінолого-криміналістичні аспекти: навчальний посібник . К.: Українська академія внутрішніх справ, 1994. 72 с.; Комп’ютерна злочинність: навчальний посібник / [Біленчук П.Д.,Романюк Б.В., Цимбалюк В.С. та ін.]. К.: Атіка, 2002. 240 с.
10. Благодир А. А. Застосування примусу під час провадження слідчих дій : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, НУВС. 2009. 20 с., с.16;
11. Бондар В.С., Кривонос М.В. Використання спеціальних знань під час проведення негласних слідчих (розшукових) дій у розслідуванні

злочинів у сфері обігу наркотичних засобів *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2016. № 3.

12. Бондар В.С., Кривонос М.В. Використання спеціальних знань під час проведення негласних слідчих (розшукових) дій у розслідуванні злочинів у сфері обігу наркотичних засобів *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2016. № 3. С 40-45.
13. Валеев А. Т. Тактика обыска и выемки при производстве расследования преступлений, совершенных в учреждениях уголовно-исполнительной системы (научные и организационно-правовые основы) : автореф. дис. ... к.ю.н. 12.00.09. Москва, 2006. 14 с.
14. Вертузаєв М.С. Попов А.Ф.Проблеми боротьби із злочинами в сфері комп'ютерної інформації. *Інформаційні технології та захист інформації*. 1998. № 1. С. 4-14.;
15. Вертузаєв М.С., Ільницький А.Ю., Юрченко О.М. Класифікація способів здійснення злочинів з використанням пластикових платіжних засобів. *Вісник Університету внутрішніх справ. Спецвипуск*. 1999. № 1. С. 130-142.
16. Вехов Б.В. Компьютерные преступления: Способы совершения и раскрытия. М.: Право и закон, 1996. 182 с.], В.В. Крилов [Крылов В.В. Информационные компьютерные преступления. М.:ИНФРА М, 1997. 285 с.
17. Винберг А. И, Шавер Б. М. Криминалистика. Москва : Изд-во «Юридическая литература», 1949. 155 с.
18. Виявлення, фіксація та вилучення криміналістично значущої інформації з мобільних пристроїв під час розслідування кримінальних правопорушень / А.В. Холостенко, Д.С. Афонін, К.Ю. Ісмайлов, Д.В. Лісніченко, О.І. Постол. Одеса: Одеський державний університет внутрішніх справ, 2018. 38 с.
19. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: ООО «Юрлитформ», 2002. 496 с.
20. Волобуєв А.Ф., М.В. Даньшин та ін.; Криміналістика : підручник : у 2 т. Т. 1 / за заг. ред. А.Ф. Волобуєва та ін., Харківський національний університет внутрішніх справ. Харків, 2017. 384 с.
21. Волобуєв А.Ф., М.В. Даньшин та ін.; Криміналістика : підручник : у 2 т. Т. 1 / за заг. ред. А.Ф. Волобуєва та ін., Харківський національний університет внутрішніх справ. Харків, 2017. 384 с.

22. Галаган В.И. Использование следователем информации на первоначальном етапе расследования: автореф. дисс. на соиск. ученой степени канд. юрид. наук: спец. 12.00.09. К., 1992. 24 с.
23. Голубєв В.О. Теоретико правові питання кваліфікації злочинів у сфері використання електронно-обчислювальних машин. *Проблеми правознавства та правоохоронної діяльності.* Донецьк: ДІВС, 2002. № 2. С. 176-183.
24. Гончаренко В.И. Научно-технические средства в следственной практике. К. , 1984. 78 с.
25. Гора І. Проблеми використання науково-технічних засобів і методів в ході проведення негласних слідчих (розшукових) дій. Історико-правовий часопис. 2017. №2 (10). С.98-102.
26. Горошко В. В. Порядок здійснення тимчасового вилучення майна під час провадження окремих слідчих (розшукових) дій. *Електронне наукове фахове видання «Юридичний науковий електронний журнал» Запорізького національного університету* Сер.: Юриспруденція. Вип. № 5. Запоріжжя 2015. (Депонований рукопис).
27. *Горошко В. В.* Тимчасове вилучення майна (кримінальний процесуальний аспект): дис. ... канд. юрид. наук. 12.00.09. Одеса, 2018. 243 с.
28. Грібов М. Л. Засоби, що використовуються під час проведення негласних слідчих (розшукових) дій. *Бюлетень міністерства юстиції України*. 2014. С.152-158, с.15;
29. Гумін О. М. Система заходів забезпечення кримінального провадження за новим кримінальним процесуальним кодексом України. *Науковий вісник Національної академії внутрішніх справ*. 2013. Вип. №1. С. 228.
30. Денисюк С. Ф. Шепитько В. Ю. Обыск в системе следственных действий. (Тактико-криминалистический анализ) : науч.-практ. пособие. Харьков : Консум, 1999. 159 с.
31. Деякі питання щодо спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації: Постанова Кабінету Міністрів України від 22.09.2016 р. № 669. URL: https://zakon.rada.gov.ua/laws/show/669 2016 п#n158 (дата звернення 12.02.2022).
32. Дикий О. В. Можливості використання технологій face recognition та touchid: кримінологічний аспект. *Кібербезпека в сучасному світі :* матеріали всеукраїнської наук.-практ конференції (м. Одеса, 29

лист.а 2019 р.). Одеса : Видавничий дім «Гельветика», 2019. С.5-12.

33. Діденко В. М. Технології опрацювання bigdata у спеціалізованих комп'ютерних системах на базі платформи hadoop: автореф. дипломної роботи на здобуття освітнього ступеня «магістр». Тернопіль. 2018. URL: http://elartu.tntu.edu.ua/bitstream/lib/26912/1/Автореферат%20Діденко%20В.М..pdf (дата звернення 21.03.2022).
34. Довідник керівника поліції: поліцейська діяльність, керована розвідувальною аналітикою / О.Є. Користін та ін.; за заг. ред. М.Г. Вербенського. Київ : «Видавництво Людмила», 2019. 120 с.
35. Доля Е. А. Формирование доказательств на основе результатов оперативно-розыскной деятельности : монография. М. : Проспект, 2009. 357 с.
36. Доповідь комісії Європейського суду з прав людини: CASE OF FRIEDL v. AUSTRIA (Application no. 15225/89) URL:http://hudoc.echr.coe.int//eng?i=001 57917. (дата звернення 21.02.2022).
37. Заєць О. М Інститут аналітичного супроводження досудового розслідування кримінального провадження в Україні: сучасний стан і перспективи розвитку. *Вісник кримінального судочинства*. 2016. № 4. С.17-26.
38. Зинатуллин З. З. Уголовно-процессуальное принуждение и его эффективность. Казань : Изд-во Казанского ун-та. 1981. 99 с.
39. Інформаційні технології. Вікіпедія. URL : https://uk.wikipedia.org/wiki (дата звернення 21.03.2022)
40. Іщенко П.П. Інформаційне забезпечення слідчої діяльності : [наук.-практ. пос.]; під ред. Є.П. Іщенко. М.: Юрлитинформ, 2011. 168 с.
41. Карташов И.И., Постолов С.А. Информационные ресурсы сети Интернет как источник оперативно-розыскной информации о состоянии оперативной обстановки. *Вісник Луганського університету внутрішніх справ імені Е.О. Дідоренка. Спеціальний випуск*. 2011. № 2. Частина 2. С. 75-81.
42. Коваленко В.В. Актуальні проблеми застосування науково-технічних засобів спеціалістами при провадженні слідчих дій : дис. ... канд. юрид. наук : 12.00.09. Луганськ, 2004. 253 с.
43. Козенко О.О. Спеціальна техніка під час проведення досудового розслідування, оперативно-розшукових і контррозвідувальних

заходів. *Науковий вісник Ужгородського національного університету. Серія Право*. 2016. Випуск 38. Том 2. С.110-114.

44. Колесник Ю.В. Слідчі та негласні слідчі (розшукові) дії як криміналістичні засоби діяльності слідчого в досудовому розслідуванні: дис. … канд. юрид. наук: спец. 12.00.09. К., 2016. 253 с.
45. Конституція України : Закон України від 28.06.1996 р. № 254к/96 ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141
46. Корнієнко М.В., Тертишник В.М. Доктринальні проблеми інституту негласних слідчих (розшукових) дій URL: http://sd vp.info/2016/doktrinalniproblemi institutu neglasnih slidchih rozshukovih dij/ (дата звернення 01.02.2022)
47. Крылов В.В. Информационные компьютерные преступления. М.:ИНФРА М, 1997. 285 с.
48. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012р. №4651-VI: (станом на 11.02.2022р.) URL: https://zakon.rada.gov.ua/go/4651-17 (дата звернення: 11.02.2022).
49. Криминалистика / Ашмарта Е. М.; Викторова Е. Н.; Викторова Л. Н.; Лазари А. С. ; Любичев С. Г. и др.; под ред. д-ра юрид. наук, проф. В.А. Образцова. Москва: Юрист, 1995. 760 с.
50. Кримінальний процес : підручник / За заг. ред. Коваленка В. В., Удалової Л. Д., Письменного Д. П. Київ : «Центр учбової літератури», 2013. 544 с.
51. Кримінальний процесуальний кодекс України Науково-практичний коментар Т.1; за заг. ред. В. Я. Тація та інших Харків «Право», 2012. 367 с.
52. Кудінов С. С. Використання спеціальних знань під час проведення негласних слідчих (розшукових) дій. *Вісник Академії адвокатури України*. 2014. Т. 11. № 3. С. 154-161.
53. Леонов А. Особливості проведення негласних слідчих (розшукових) дій під час досудового розслідування кримінальних проваджень. *Закон і Бізнес*. URL:https://zib.com.ua/ua/136530osoblivosti_provedennya_nsrd_v_kriminalnomu_provadzhenni.html(дата звернення 21.02.2022)
54. Лісніченко Д. В. Деякі процесуальні особливості вилучення майна під час здійснення окремих слідчих (розшукових) дій. *Південноукраїнський правничий часопис.* 2019. №3. С. 44-45.
55. Лісніченко Д. В. Тимчасове вилучення майна як особливий захід забезпечення кримінального провадження. *Процесуальні та*

психологічні аспекти досудового розслідування : матеріали всеукраїнської науково-практичної конференції. 7 листопада 2014 р. Одеса: ОДУВС, 2014. С.54-55.

56. Луценко О.А. Тактика проведения обыска и выемки: учебно-практическое пособие: Изд-во Рост. ун-та, 2003., С. 11-12.
57. Мельник Д. Перспективи нормативно правового врегулювання зняття інформації з телекомунікаційних мереж та електронних інформаційних систем у новому КПК України. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* 2012. 2(24) URL: https://ela.kpi.ua/bitstream/123456789/8587/1/24_p34.pdf(дата звернення 21.02.2022)
58. Методика проведення судових експертиз, яка розроблена Українським науково-дослідним інститутом спеціальної техніки та судових експертиз: наказ СБУ від 02.03.2011 р. реєстраційний код 17.0.01 (ДСК).
59. Мирошниченко Ю. М. Проблемні питання тимчасового вилучення майна за новим кримінальним процесуальним законом. *Порівняльно-аналітичне право.* 2013. Вип. №3. С. 310-312.
60. Мовчан А.В. Поняття та сутність аналітичної розвідки як особливої форми інформаційно-аналітичної роботи в ОРД. *Науковий вісник Львівського державного університету внутрішніх справ.* 2012. № 3. С.443-453.
61. Наказ Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 04.09.2018 р. № 1519/533. URL: https://ssu.gov.ua/uploads/p_140_70438355.pdf(дата звернення 12.02.2022)
62. Негласні слідчі (розшукові) дії. Коментар до глави 21 Кримінального процесуального кодексу України [кол. авт.; за заг. ред. Є.Д. Скулиша]. К. : Наук. вид. центр НА СБУ, 2012. 132 с,
63. Орлов Ю. Ю. Технічна сторона (основа) оперативно-розшукової діяльності. *Спеціальна техніка у правоохоронній діяльності : матеріали III міжнар. наук. практ. конфер., (Україна. Київ, 25 26 жовт. 2007 року)* [ред. кол. : О. М. Джужа, О. В. Рибальський, Ю. Ю. Орлов та ін.]. К., 2007. С. 9-12.
64. Основи кримінального аналізу : посібник з елементами тренінгу / О.Є. Користін , С.В. Албул, А.В. Холостенко, О.М. Заєць та ін. Одеса : ОДУВС, 2016. 112 с.

65. Основи оперативно-розшукової діяльності в Україні : навч. посіб. Одеса : ОДУВС, 2020. 400 с.
66. Пленум Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ: Постанова №6 від 03.06.2016р. URL: https://forum.antiraid.com.ua/topic/8666 . (дата звернення 09.03.2022).
67. Погорецький М. А. Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі : монографія. Харків : Арсіс, 2007. 576 с.
68. Погорецький М. А., Сергєєва Д. Б. Негласні слідчі (розшукові) дії та оперативно-розшукові заходи: поняття, сутність і співвідношення. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2014. № 2. С. 137-141.
69. Положення про порядок розроблення, виготовлення, реалізації та придбання спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації: Постанова Кабінету Міністрів України від 27.10.01 р. № 1450 https://zakon.rada.gov.ua/laws/show/1450 2001 п (дата звернення 02.04.2021)
70. Полянко А. Особенности поисковой системы Google Site seo.ru поисковая оптимизация и интернет маркетинг. к URL: http://siteseo.ru/info/seostati/GoogleMSNYa/40/.(дата звернення 21.02.2022).
71. Постанова ОП ККС ВС від 10 вересня 2020 року, справа № 51-1704км20. URL: https://reyestr.court.gov.ua/Review/91722819. (дата звернення 21.03.2022).
72. Про внесення змін до деяких законодавчих актів щодо забезпечення дотримання прав учасників кримінального провадження та інших осіб правоохоронними органами під час здійснення досудового розслідування : Закон України від 16.11.2017р. №2213-VIII. URL: https://zakon.rada.gov.ua/laws/show/2213-19#n51 (дата звернення: 20.02.2022).
73. Про внесення змін до Ліцензійних умов провадження господарської діяльності, пов'язаної з розробленням, виготовленням, постачанням спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації: Постанова Кабінету Міністрів України від 16.01.2019 №28. URL: https://ssu.gov.ua/ua/pages/115 (дата звернення 12.02.2022).

74. Про впорядкування виготовлення, придбання та застосування технічних засобів для зняття інформації з каналів зв'язку: Указ Президента України від 13.04.2001 р. № 256/2001. URL: https://zakon.rada.gov.ua/laws/show/256/2001(дата звернення 12.02.2022).
75. Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання: Закон України від 20.02.2003 № 549 IV. URL: https://zakon.rada.gov.ua/laws/show/549 15 (дата звернення 12.02.2022).
76. Про додержання прав людини під час проведення оперативно-технічних заходів: Указ Президента України від 16.01.2006 р. № 1556. URL: http://zakon3.rada.gov.ua/laws/show/1556/2005 (дата звернення 12.02.2022).
77. Про законне перехоплення телекомунікацій: Резолюція Ради Європи від 17 січня 1995 року. URL: http://zakon3.rada.gov.ua/laws/ show/994_235(дата звернення 12.02.2022).
78. Про затвердження Зводу відомостей, що становлять державну таємницю: Наказ Служби безпеки України від 23.12.2020 № 383. URL: http:// https://zakon.rada.gov.ua/laws/show/z0052 21#Text. (дата звернення 23.02.2022).
79. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ ГП України, МВС України, СБ України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16 листоп. 2012 р. №114/1042/516/1199/936/1687/5. URL: https://zakon2.rada.gov.ua/laws/show/ v0114900 12. . (дата звернення 23.02.2022).
80. Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності, пов’язаної з розробленням, виготовленням, постачанням спеціальних технічних засобів для зняття інформації з каналів зв’язку та інших технічних засобів негласного отримання інформації, що підлягає ліцензуванню, і визначається періодичність проведення планових заходів державного нагляду (контролю) Службою безпеки Постанова Кабінету Міністрів України від 24.07.2019 № 671. URL: https://ssu.gov.ua/ua/pages/115(дата звернення 12.02.2020).

81. Про затвердження переліку органів ліцензування та визнання такими, що втратили чинність, деяких постанов Кабінету Міністрів України: Постанова КМУ від 05.08.2015 р. № 609 URL: https://ssu.gov.ua/ua/pages/115 (дата звернення 12.02.2020).
82. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України від 3 вересня 2014 р. № 411 Постанова КМУ. URL: https://zakon.rada.gov.ua/laws/show/411 2014.
83. Про затвердження Положення про Управління кримінального аналізу Національної поліції України: наказ Національної поліції України від 07.11.2017 № 1150 URL: https://zakon.rada.gov.ua/laws/show/86 2004 п. (дата звернення 12.04.2020).
84. Про затвердження Порядку здійснення державного контролю за міжнародними передачами товарів військового призначення: Постанова Кабінету Міністрів України від 20 листопада 2003 р. № 1807. URL: https://zakon.rada.gov.ua/laws/show/1807 2003 п(дата звернення 12.02.2020).
85. Про затвердження Правил надання та отримання телекомунікаційних послуг: постанова Кабінету Міністрів України від 11 квітня 2012 року № 295. URL: https://zakon.rada.gov.ua/laws/show/295 2012 п(дата звернення 12.02.2020).
86. Про затвердження та введення у дію Інструкції про порядок вилучення, обліку, збереження та передачі речових доказів у кримінальних справах, цінностей та іншого майна органами дізнання, досудового слідства і суду : наказ Генеральної прокуратури України від 27.08.2010р. № 51/401/649/471/23/125 URL**:** https://zakon.rada.gov.ua/go/v0051900-10 (дата звернення: 27.02.2022).
87. Про інформацію: Закон України від 2 жовтня 1992 року № 2657 XII. URL: http://zakon3.rada.gov.ua/laws/show/2657 12 (дата звернення 12.02.2022).
88. Про ліцензування видів господарської діяльності: Закон України від 02.03.2015 р. № № 222 VIII**.** URL: https://zakon.rada.gov.ua/laws/show/222 19. (дата звернення 23.02.2022)
89. Про Національну програму інформатизації: Закон України від 04.02.1998 № 74/98 ВР. URL:

https://zakon.rada.gov.ua/laws/show/74/98 вр/card2#Card(дата звернення 12.02.2022).

90. Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг: Резолюція Ради Європи від 20 червня 2001 року. URL: http://zakon3.rada.gov.ua/laws/show/994_234(дата звернення 12.02.2022).
91. Про оперативно-розшукову діяльності : Закон України від 18.02.1992 р. станом на 02.04.2022р. URL: https://zakon.rada.gov.ua/go/2135-12 (дата звернення: 02.04.2022).
92. Про радіочастотний ресурс України: Закон України від 1 червня 2000 року № 1770-III. URL: http://zakon3.rada.gov.ua/laws/show/1770 14(дата звернення 12.02.2022).
93. Про телекомунікації: Закон України від 18 листопада 2003 року № 1280 IV. URL: http://zakon2.rada.gov.ua/laws/show/1280 15(дата звернення 12.02.2022)
94. Ратинов А. Р. Обыск и выемка / Под ред. проф. А. И. Винберга. Москва: Госюриздат, 1961. 217 с.
95. Рішення Європейського суду з прав людини у справі: CASE OF UZUN v. GERMANY (Application no. 35623/05) Judgment 2 September 2010 URL:http://hudoc.echr.coe.int/eng?i=001 100293 . (дата звернення 23.02.2022).
96. Рішення Європейського суду з прав людини у справі: CASE OF VOLOKHY v. UKRAINE (Application no. 23543/02) Judgment 2 November 2006 URL:http://hudoc.echr.coe.int/eng?i=001 77837 . (дата звернення 23.02.2022).
97. Романов А.Л., Одинцов Б.Е. Компьютеризация аудиторской деятельности: Учеб.пособие. М.: Аудит: ЮНИТИ, 1996. 270 с.
98. Рыжаков А. П. Следственные действия и иные способы собирания доказательств. Москва : Филинъ, 1997. 336 с.
99. Сало О. М. Реалізація повноважень керівником органу досудового розслідування при проведенні негласних слідчих (розшукових) дій. Дис. канд. юрид. наук (доктора філософії):12.00.09. Університет державної фіскальної служби України, Ірпінь, 2018. 254 с.
100. Самойленко О.А. Основи методики розслідування злочинів, вчинених у кіберпросторі. Монографія; за заг.ред. А.Ф, Волобуєва. Одеса: ТЕС, 2020. 372 с.
101. Святченко В.М. Застосування спеціальних технічних засобів як важливий чинник сприяння винесенню обвинувального вироку.

Сучасна спеціальна техніка. 2017. 1(48). http://elar.naiau.kiev.ua/bitstream/123456789/6604/1/спецтехника%20№%201%201 108%202017_p031 040.pdf(дата звернення 23.04.2020)

102. Сергеева Д.Б. Результати негласних слідчих (розшукових) дій: проблемні аспекти визначення. *Право і громадянське суспільство*. 2014. № 1 (6). С. 97-106.
103. Смоков С. М. Запобіжні заходи та кримінально-процесуальні гарантії їх застосування : навчальний посібник. Одеса : ОДУВС. 134 с.
104. Снігєрьов О.П., Голубєв В.О.Проблеми класифікації злочинів у сфері комп'ютерної інформації. *Вісник Університету внутрішніх справ*. Х., 1999. № 5. С. 25-28.
105. Соколов О.В. Виконання оперативними підрозділами доручень слідчого, прокурора про проведення негласних слідчих (розшукових) дій: дис…канд.. юрид. 12.00.09/ Національний юридичний університет імені Ярослава Мудрого. Харків, 2019. 240 с.
106. Тертишник В.М. Верховенство права та забезпечення встановлення істини в кримінальному процесі України : монографія. Дніпропетровськ: Ліра ЛТД, 2009. 404 с.
107. Толпиго Д.М. Особливості обстеження публічно недоступних місць, житла чи іншого володіння особи. *Правова держава*. 2015. №19. С.147-154.
108. Уваров В. Г. Зняття інформації з технічних каналів зв'язку. *Зовнішня торгівля: економіка, фінанси, право*. 2013. № 2. С. 177-181. URL: http://nbuv.gov.ua/UJRN/uazt_2013_2_28. (дата звернення 23.04.2020), с. 940
109. Федотов Н. Н. Форензика компьютерная криминалистика. М.: Юрид. мир, 2007. 360 с.
110. Федюнин А. Е. Процессуальные правила и критерии допустимости доказательств, полученных при раскрытии и расследовании преступлений с использованием технических средств. *Актуальные проблемы раскрытия и расследования преступлений :* межвуз. сб. науч. тр. Красноярск, 2005. Вып. 7. С. 60-68.
111. Философский энциклопедический словарь. Москва, 1989. 731 с.. Мета – це ідеальне, уявне передбачення результату якої-небудь діяльності [Новий тлумачний словник української мови : у 3 т. / уклад. В. В. Яременко, О. М. Сліпушко. Київ : АКОНІТ, 2003. Т. 1. 2003. 928 с.

112. Халиков А. Н., Яковец Е. Н., Журавленко Н. И. Юридическое, техническое и информационно аналитическое обеспечение оперативно-розыскной деятельности : учеб.пособие / под ред. А. Н. Халикова. Москва : Юрлитинформ, 2010. 472 с.
113. Хараберюш І.Ф. Протидія злочинності засобами спеціальної техніки: концептуальний підхід: монографія. Донецьк: Вид-во «Ноулідж», 2011. 362 с.
114. Хараберюш І.Ф. Спеціальна техніка в органах внутрішніх справ: Загальна частина : навчальний посібник; ДЮІ МВС України [4 е вид., перероб. і доп]. Донецьк: Донецький юридичний інститут МВС України, 2013. 284 с.
115. Ходанович В. О. Використання науково-технічних засобів в ході проведення негласних слідчих (розшукових) дій. *Вісник Академії адвокатури України.*Том 13. 2(36). 2016. С.111-118,
116. Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ : монографія. Одеса : Юрид. літ., 2011. 214 с.
117. Цехан Д. М. Правове регулювання мережі Інтернет як передумова її декриміналізації. *Актуальні проблеми держави і права : збірник наук. праць.* Вип. 65. Одеса : Юрид. л ра, 2012. С. 668-676.
118. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування *Науковий вісник Міжнародного гуманітарного університету.* Юриспруденція. 2013. Вип. 5. С. 256-260. URL: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2013_5_58. (дата звернення 13.02.2022),
119. Шейфер С. А. Следственные действия. Основания, процессуальный порядок и доказательственное значение. Москва: Издательство «Юрлитинформ», 2004., С. 10-11.
120. Шерудило В.О. Процесуальний порядок проведення негласних слідчих (розшукових) дій, пов'язаних з втручанням у приватне спілкування: дис… кандид.юрид. наук (доктор філософії) 12.00.09 (081 Право)/ Національна академія внутрішніх справ, Київ, 2018. 264 с.
121. Шинкаренко І.І. Проблеми удосконалення правового регулювання організації спостереження за особою, місцем та річчю під час кримінального провадження. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2017. №1. С.289-295.
122. Шитий С., Огороднікова І. Особливості порушення прав людини шляхом незаконного використання програмних засобів негласного

зняття інформації. *Наукові записки Інституту законодавства Верховної Ради України.* 2017. № 1.С. 82-92.

123. Шраго А.О. Нормативно правові аспекти забезпечення виявлення та розслідування збуту і розповсюдження порнографії у мережі інтернет: *Інформаційно-аналітичне забезпечення діяльності підрозділів кримінальної поліції*: збірник наукових статей за матеріалами доповідей Всеукраїнського наук.-практ.семінару 23 бер. 2018 р. Львів: ЛьвДУВС, 2018. URL:https://www.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/23_03_2018.pdf. (дата звернення 23.02.2022)
124. Щодо висновків про належність (неналежність) товарів до спеціальних технічних засобів: Лист СБУ від 04.06.2009 р. № 18/1462 URL:http://search.ligazakon.ua/l_doc2.nsf/link1/MUS10261.html. (дата звернення 03.03.2020)
125. Щурат Т.Г., Смук А.О. Деякі аспекти розвідки з відкритих джерел інформації (OSINT). *Оперативно-розшукова діяльність Національної поліції: проблеми теорії та практики* : матеріали Всеукр. наук. практ. конф. (Дніпро, 20жовт. 2017 р.) : у 2 х ч. Дніпро : Дніпроп. держ. ун т внутр. справ, 2017. Ч. 1. С. 126-128.
126. Юхно О. О. Особливості використання інформаційних технологій під час проведення негласних слідчих (розшукових) дій та їх процесуальне оформлення. *Вісник ХНУВС*. 2016. № 2 (73). С.86-95.
127. Police. 2001. September. P. 24-27.