Мотлях О.І.

Методика розслідування комп'ютерних злочинів

Монографія

КИЇВ - 2010 р.

Рецензенти:

Клименко Н.І. – доктор юридичних наук, професор Київського національного університету ім. Тараса Шевченка;

Біленчук П.Д. – кандидат юридичних наук, професор Київського національного університету внутрішніх справ.

Мотлях О.І.

Методика розслідування комп'ютерних злочинів. Монографія / О.І. Мотлях. – К.: Видавництво «Освіта України» 2010. – 236 с.

У монографії детально викладено зміст методики розслідування злочинів, передбачених розділом XVI КК України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

Використано матеріали слідчої і судової практики, сформульовані пропозиції щодо протидії злочинам з використанням комп'ютерних технологій.

Монографічний матеріал може бути використаним: у навчальному процесі, практичній та науковій діяльності.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

КК …….....…..Кримінальний кодекс

КПК …….....……Кримінально-процесуальний кодекс

АС …….....……. Автоматизовані системи

ЕОМ …….....…… Електронно-обчислювальні машини

ПЕОМ ……...……. Програмні електронно-обчислювальні машини

ЗЕОТ ……...……Засоби електронно-обчислювальної техніки

ЗКТ……....…… Засоби комп'ютерної техніки

ОРД ……...…….Оперативно-розшукова діяльність

ОРЗ ……...……Оперативно-розшукові заходи

СД ……...…….Слідчі дії

ДТСУ ……...…….Державний стандарт України

МВС ……...…….Міністерство внутрішніх справ

СБУ ……...……Служба безпеки України

ДПА ……...……...Державна податкова адміністрація

НДІСЕ….…….... Науково-дослідний інститут судових експертиз

ДСБЕЗ ……....….Досудове слідство безпеки економічної злочинності

УБОЗ ……...…….Управління по боротьбі з організованою злочинністю

УБЕЗ ……...……Управління по боротьбі з економічною злочинністю

ІНТЕРНЕТ ……...……Глобальна комп'ютерна мережа INTERNET

НДЦ …….....…… Науково-дослідний центр

ВСТУП

Подальший розвиток сучасних INTERNET – технологій, удосконалення виробництва і розширення сфери застосування комп'ютерної техніки дали можливість зародження специфічного, складного виду злочинних діянь, де комп'ютерне оснащення та електронна інформація є об'єктом протиправного посягання. Поряд з позитивними здобутками інформатизація супроводжується побічним, негативним явищем криміногенного характеру, до якого відносять злочини у сфері електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку або ж «комп'ютерну злочинність» (скорочена назва цього виду злочинів) [28]. На сучасному етапі технологізації суспільства: обробки та обміну інформацією за допомогою міжнародної глобальної мережі INTERNET, відбуваються негативні процеси – перехід від простої поодинокої комп'ютерної злочинності до організованої – складної. Спостерігається динаміка злиття такої злочинності з міжнародним криміналітетом, що несе у собі відповідну загрозу суспільству в цілому. Слід зазначити, що така транскордонність ускладнює можливості розкриття та розслідування цієї категорії злочинів працівниками правоохоронних органів різних держав. У більшості документів, прийнятих на міжнародному рівні, зазначається, що для ефективної боротьби проти «кіберзлочинності» необхідне більш широке, оперативне і налагоджене міжнародне співробітництво [73]. У червні 2001 р. Європейським комітетом разом з комітетом експертів у дослідженні проблем злочинності був розроблений проект Конвенції про кіберзлочинність. У листопаді того самого року Конвенція була затверджена комітетом міністрів Ради Європи і підписана 35 державами, які взяли на себе зобов'язання здійснювати погоджену політику боротьби зі злочинністю у цій сфері.

Україна відповідно до Європейської Конвенції, розробила «Концепцію стратегії і тактики боротьби з комп'ютерною злочинністю», де чітко визначила основні питання, що мають бути вирішеними для інформаційного простору

держави у цілому. Крім того, був прийнятий новий Кримінальний кодекс, який набув чинності з 01.04.2001 р. Він містить окремий розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку», у якому попередньо містилися три статті, якими регулювалися злочини у сфері з використанням комп'ютерних технологій, а саме: 361, 362 і 363, замість однієї ст. 198^1 Кримінального кодексу України 1960 р. Однак життєві реалії змусили законодавця змінити і доповнити зазначений вище розділ, отже згідно Закону № 2289-IV від 23.12.2004р. він містить шість статей: 361, 361^1, 361^2, 362, 363, 363^1 Кримінального кодексу України. Внесено до ст. 1 Закону України «Про боротьбу з тероризмом» від 20.04.2003 р. поняття технологічного тероризму як злочинів, що здійснюються з терористичною метою із застосуванням комп'ютерних систем та комунікаційних мереж для виведення з ладу небезпечних об'єктів, які прямо чи опосередковано створили загрозу виникнення надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру [202, с. 5]. У ст. 7 Закону України «Про основи національної безпеки України» від 19.06.2003 р. серед загроз її національним інтересам і національній безпеці в інформаційній сфері йдеться про комп'ютерну злочинність та комп'ютерний тероризм [202, с. 6]. Розроблено й інші нормативно-правові документи, які покликані сприяти співпраці, протидії і запобіганню такого феномену, однак, як виявляється, цього замало для ефективної боротьби з комп'ютерною злочинністю особливо на нинішньому етапі бурхливого розвитку технологізації суспільства.

Статистичні дані свідчать про досить високий відсоток таких правопорушень у загальному спектрі злочинності, а їх кількість, як і складність, цілеспрямовано просуваються вперед. Підтвердженням тому є проведений у м. Запоріжжі перший український міжнародний з'їзд «хакерів» під назвою «Хак-Форум 2000», а пізніше і в інших містах України. Такі дані напрацьованих матеріалів показали, що «хакерський» рух в Україні стрімко

розвивається і певною мірою обганяє у своєму розвитку інші країни колишнього СРСР [4, с. 40 – 41]. До переліку негативних чинників розповсюдження цієї категорії злочинів можна віднести:

1. Низький рівень контролю за тиражуванням та розповсюдженням програмної комп'ютерної продукції.

2. Високу латентність злочинів. Лише 10 – 15 % комп'ютерних злочинів стають відомими [5, с. 101 – 103]. На думку більшості суб'єктів віктимології розголошення про такий злочин може зашкодити їх подальшій репутації, тому доволі часто комп'ютерні жертви потерпають вагомими збитками заради збереження власного престижу.

3. Недостатність теоретичних знань і практичних навичок розслідування злочинів у сфері комп'ютерних технологій практичними працівниками правоохоронних органів, неможливість доведення до суду порушених кримінальних справ цієї категорії.

За офіційними даними у Росії за останніх п'ять років (1997 – 2001) зареєстровано: 2432 злочини, пов'язані з неправомірним доступом до комп'ютерної інформації (ст. 272 КК РФ), 579 – з створенням, використанням і розповсюдженням шкідливих носіїв для ЕОМ (ст. 273 КК РФ) і 175 – з порушенням правил експлуатації ЕОМ, систем ЕОМ чи їх мереж (ст. 274 КК РФ). Співробітниками підрозділів по боротьбі зі злочинами цієї категорії виявлено осіб, що скоїли дані злочини: 1111 – за ст. 272 КК РФ, 316 – за ст. 273 КК РФ та 92 – за ст. 274 КК РФ [6, с. 799]. Зокрема за 1999 р. до суду було направлено 83 кримінальні справи пов'язані з комп'ютерною злочинністю, із 282 зареєстрованих таких злочинів. У 2000 р. – 274 справи з 800 порушених. У той час в Україні, за даними Верховного суду України, у 1997 р. було порушено 15 кримінальних справ за ст. 198^1 Кримінального кодексу України 1960 р., проте не розкрито протягом року жодного. За чотири місяці 2001 р. – зареєстровано лише 16 злочинів, передбачених ст. 361, 362 і 363 КК України, а впродовж 2002 р. – 30. На січень 2003 р. набрали чинності вироки лише двох кримінальних справ, передбачених ст. 363 КК, і одна

кримінальна справа про злочин, передбачений ст. 361 КК України [202, с. 9]. За даними інформаційних технологій МВС України за шість місяців 2004 р. зареєстровано 36 злочинів, з них розслідувано (розкрито) – 18. У той час інше джерело констатує такі дані: «Дослідженням встановлено, що правоохоронними органами з 1994 р. щорічно в Україні офіційно реєструється до десяти злочинів, що вчинюються з використанням комп'ютерних технологій. Вони приховані від офіційної статистики. За експертними оцінками, рівень латентності комп'ютерної злочинності становить 90 – 95 %» [51, с. 107]. За даними МВС України в період 2005 – 2008 р.р. в загальному по Україні зареєстровано – 2545 злочинів, пов'язаних з використанням комп'ютерних технологій.

Виходячи з викладених вище даних, можна дійти висновку про актуальність порушеної проблематики питання, зокрема її криміналістичного аспекту. Безперечно, цей феномен злочинності не залишається поза увагою вчених. Значний вклад у вивчення, розслідування та протидії цим злочинам зробили такі провідні науковці-фахівці: Т.В. Аверьянова, Б.В. Андрєєв, Ю.М. Батурін, Р.С. Белкін, П.Д. Біленчук, О.А. Баранов, В.Б. Вехов, М.С. Вертузаєв, Т.В. Варфоломеєва, О.Г. Волєводз, В.О. Голубєв, В.А. Губанов, В.Г. Гончаренко, Ю.В. Гаврилін, М.В. Гуцалюк, В.Д. Гавловський, В.Ю. Гайкович, А.М. Жодзишський, А.В. Іщенко, В.В. Крилов, В.А. Колесник, В.Є. Козлов, Р.А. Калюжний, М.І. Камлик, О.І. Котляревський, В.Б. Міщенко, В.І. Оборський, П.Н. Пак, Б.В. Романюк, О.Р. Россінська, М.В. Салтевський, Н.А.Селіванов, А.В. Селюк, І.О. Саакянц, О.І. Усов, В.П. Хорст, В.С. Цимбалюк та ін.

Разом з тим, незважаючи на теоретичну та практичну значущість опублікованих праць, наукових досліджень вони в неповній мірі відображають питання, пов'язані з методикою розкриття та розслідування комп'ютерних злочинів. У зв'язку з цим пропонується монографічне видання, яке містить в собі розробки і рекомендації направлені на краще теоретичне сприйняття студентами-юристами вищих навчальних закладів України змісту проблеми та

надання практичної допомоги спеціалістам правоохоронних органів від діяльності яких залежить забезпечення результативності розслідування такої категорії злочинів.

Метою і завданням підготовки цього видання – є поглиблений аналіз і подальший розвиток існуючих теоретичних та практичних напрацювань вітчизняних спеціалістів і зарубіжних у сфері розслідування злочинів, пов'язаних з використанням комп'ютерних технологій. На основі вивчення та дослідження різних точок зору фахівців цього напряму буде розкрито і проаналізовано різні підходи науковців до формування дискусійних питань, що стосуються актуальних проблем зазначеної злочинності.

Таким чином – реалізація мети обумовила необхідність вирішити основні завдання:

- формування криміналістичної характеристики комп'ютерних злочинів;
- визначення організації і змісту планування початкового та подальшого етапів розслідування цих злочинів;
- дослідження типових слідчих ситуацій, що складаються при вчиненні таких злочинів;
- розробка правил і змісту висунення та перевірки криміналістичних версій злочинів з використанням комп'ютерних технологій;
- встановлення особливостей проведення слідчих дій у злочинах зазначеної категорії;
- визначення можливостей комп'ютерно-технічної експертизи.

РОДІЛ 1. ОКРЕМІ ГАЛУЗЕВО-ПРАВОВІ ХАРАКТЕРИСТИКИ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

1.1. Кримінологічна характеристика злочинів, пов'язаних з використанням комп'ютерних технологій

Третє тисячоліття, на думку вчених-дослідників злочинів у сфері з використанням INTERNET-технологій, – це період повного розквіту комп'ютеризації на нашій планеті. Піввіковий термін від створення перших ЕОМ до сучасності свідчить про надзвичайно швидкий хід розвитку технічних інформаційних засобів. Сьогодні практично не існує виду людської діяльності, де у тій чи іншій формі не використовувалася б обчислювальна техніка (комп'ютери) [164, с. 1]. Масова комп'ютеризація витіснила з обігу застарілі технології отримання, обробки та передачі інформації, значно розширила діапазон бачення та трактування деяких понять у погляді на життя і спілкуванні між народами, прискорила потік обміну електронною інформацією у питаннях, що стосуються військово-промислового комплексу, стратегічного, екологічного, торговельного за допомогою глобальної всесвітньої мережі INTERNET. Оперуючи цим поняттям, слід зазначити, що: «INTERNET – це просторово-розподільна глобальна мережа комп'ютерної техніки і інформаційної інфраструктури користувачів, яка дозволяє здійснити операції по обміну інформацією та послугами з метою задоволення потреб фізичних та юридичних осіб, державних органів і інших суб'єктів, забезпечувати їх контакти у режимі реального часу, мережі, функціонування якої регулюється технічними стандартами, правилами етики, а також міжнародними нормами і національним правом, орієнтованими на захист прав людини, забезпечення належної безпеки держави, суспільства, особистості» [85, с. 8]. Комп'ютеризація стала невід'ємною частиною нашого буття. Але разом з тим вона перетворилася на камінь спотикання для суспільства у цілому, а саме – новоявленим феноменом комп'ютерної злочинності [149, с. 57].

Переважна частина державного, комерційного, приватного сектора та окремих громадян потерпає від нападів на свої інформаційні банки даних з різного боку «білокомірцевих злочинців» (у подальшому по тексту як одна з форм звертання до осіб, що скоюють злочини у сфері комп'ютерних технологій). У комп'ютерних мережах відбуваються різнотипні збої та перекручування електронної (машинної) інформації, викачування та викрадення окремих блоків інформаційних сайтів. Запускається безліч комп'ютерних програм-паразитів (вірусів), парадоксів, двійників, що у кінцевому результаті дезорганізує технологічний, фінансовий, інформаційний та інші виробничі потоки. Статистичні дані говорять самі за себе: у США середня сума збитків від одного фізичного пограбування банку становить 3,2 тис. доларів.; від одного шахрайства – 23 тис. доларів., від однієї комп'ютерної крадіжки – 500 тис. доларів [17]. Щорічний економічний збиток від комп'ютерної злочинності наприкінці 90-х років минулого століття наблизився до 100 млрд. доларів [94, с. 29]. Стосовно направленості вчинення злочинцями протиправних дій, то за даними американських вчених Д. Срауба та К. Видома, 11 % комп'ютерних посягань спрямовані на крадіжку обладнання, приблизно п'ята частина – на програми; близько 3/5 – на інформацію і близько 13 % – на послуги. Переважна більшість посягань спрямована на інформацію-програми і даних від загальної кількості випадків [82]. Разом з тим, слід зазначити, що ідеологія «хакерів» (один з різновидів комп'ютерних злочинців), полягає у постійному пошуку нових, неосвоєних вершин злочинної сфери. Особливий інтерес вони виявляють до стратегії військово-промислового комплексу. Скажімо, у збройних силах США з 1998 р. запровадили програму створення єдиної системи електронної торгівлі, в рамках якої передбачається впорядкувати процес закупівлі озброєння і предметів матеріально-технічного постачання військ через INTERNET. З метою успішної її реалізації в Агентстві збройних сил США створили управління електронної комерції. Система електронної торгівлі діє за принципом INTERNET-порталу, який поєднує сайти видів збройних сил і

комерційних фірм-виробників. Ця система надто зацікавила «хакерів», і вони почали приділяти їй більше уваги, як інформаційним системам Пентагону разом узятим. Для прикладу у 1999 р. зареєстровано майже 22 тис. спроб проникнення і зняття інформації з систем електронної торгівлі, а в 2000 р. їх кількість зросла до 27 тис. [65, с. 133]. За даними Інституту комп'ютерної безпеки (Computer Security Institute), у другій половині 2002 р. число хакерських атак збільшилося на 33 % порівняно з аналогічним періодом 2001 р. [74, с. 114].

Англійський віце-президент групи страхових компаній Вільям Барр оприлюднив такі факти:

- 90 % організацій виявляють порушення інформаційних систем щороку;
- 80 % з них підтверджують фінансові збитки;
- тільки один вірус MIMOA призвів до збитку у понад 1,8 млрд. фунтів стерлінгів;
- у жовтні 2002 р. кібератака протягом 1 год. вивела з ладу 9 з 13 головних комп'ютерів, які управляють глобальним рухом у мережі Інтернет;
- щороку викрадається приватної інформації на суму понад 38 млрд. фунтів стерлінгів [75, с. 61].

За оцінкою незалежного журналу п'яти континентів «Ділові люди», фірми в країнах з розвинутою ринковою економікою щорічно витрачають 15–20 % чистого прибутку на боротьбу з промисловим шпіонажем [150, с. 40]. Продемонстровані статистичні дані констатують невпинний розвиток цього виду злочинів. І головна проблема динаміки розповсюдження цього феномену полягає у тому, що комп'ютерна злочинність як складова загальної злочинності, набирає своїх обертів, інтерпретується до характеру транснаціональних злочинів. Фахівці відзначають, що ці злочини загрожують економічним основам держав та світовій економічній системі [42, с. 7]. Тому одним із аспектів їх запобігання є стратегія міжнародної боротьби з

потенційною загрозою злочинів, пов'язаних з кібернетичними технологіями. (Кібернетика – це наука про загальні закони отримання, зберігання, передачі і перетворення інформації у складних керуючих системах) [146, с. 49]. Таким чином, далі по тексту «кібернетичні технології» розуміти як ті, до системи яких входять комп'ютери та їх носії. Одну з таких Стратегій було продемонстровано у Лондоні 2002 р., де проходив перший Міжнародний конгрес «E-CRIME CONGRESS 2002», присвячений проблемі електронної злочинності за ініціативи Національного центру по боротьбі зі злочинами у сфері високих технологій. 400 делегатів з усього світу взяли участь у його проведенні, у тому числі і з Росії. В основу цього заходу було покладено стратегію «Project Trawler», розроблену Асоціацією поліцейських офіцерів (ACPO) та робочою групою з питань комп'ютерної злочинності й опублікованою Національним бюро кримінальних розслідувань (NCIS) у 1999 р. На виконання Стратегії з державного бюджету було виділено 25 млн. фунтів на 3 роки, 10 млн. з яких – на розвиток відділів на місцях, та 15 млн. – на створення Національного центру по боротьбі зі злочинами у сфері високих технологій [75, с. 61].

Оприлюднені статистичні дані в черговий раз показують, що зазначений різновид злочинних діянь з використанням сучасних комп'ютерних технологій становить у світі великомасштабну загрозу для усіх сфер людського буття. І вона існуватиме доти, поки людство перебуватиме взаємозв'язку з електронними комп'ютерними системами. Але це жодною мірою не означає, що ми закликаємо до бойкоту INTERNET – систем, а разом з тим і всіх кібернетичних технологій. Як зазначили дослідники сучасності І.Л. Бачило і С.І. Семилєтов: «Проблеми INTERNET, як нового інформаційного середовища, що отримали організаційно-технічне оформлення, – безмежні, разом з тим вони формують для кожної країни і її правової системи свої пріоритети» [23, с. 91]. Основне завдання всіх держав-учасниць Європейської Конвенції про кіберзлочинність, полягає у співпраці, протидії та запобіганні цим злочинам. У зв'язку з цим, доцільним є, проаналізувати реальний стан

речей даного напряму злочинності та застосування відповідних кроків у їх протидії на прикладі своєї держави України.

Відповідно до законів України: «Про інформацію» від 02.10.1992 р., «Про оперативно-розшукову діяльність» від 18.02.1992 р., «Про організаційно-правових основах боротьби з організованою злочинністю» від 30.06.1993 р., «Про захист інформації в автоматизованих системах» від 05.06.1994 р., а також вступу України до Європейського співтовариства і підписання Європейської Конвенції про кіберзлочинність, від 23.12.2001 р. у Будапешті, яка набула чинності з 01.07.2004 р., яку станом на червень 2005 р. підписали 42 країни в тому числі й Україна, з них 11 держав її ратифікували. Того ж таки 2005 р. Україна підписала Додатковий договір до Конвенції про кіберзлочинність щодо криміналізації передавання комп'ютерними системами матеріалів расистського чи ксенофобського характеру, що був чинним від 28.01.2003 р., внесення парламентом змін до Концепції національної безпеки України і прийняття оновленого варіанту Закону «Про основи національної безпеки України» від 19.06.2003 р., прийняття Закону України «Про захист інформації в автоматизованих системах», що був оприлюднений 31.05.2005р. і набрав чинності з 01.01.2006 р. тощо, наша держава поступово набирає обертів і упорядковує законодавчу базу до світових стандартів. Однак слід зазначити, що питання протидії злочинності, пов'язаної з використанням комп'ютерних технологій для України є наразі досить актуальними. Тому тішити себе тим, що наша держава не дуже потерпає від втручання комп'ютерних злочинців у сфери життєдіяльності країни – неправильно. Це не означає, що вітчизняні «хакери» та їх закордонні спільники не контролюють соціальний, економічний, політичний рівні розвитку держави, вони, як вибухівка уповільненої дії, можуть у будь-який час заявити про себе. Прикладом тому може служити вірусна атака обчислювальної мережі Генеральної дирекції ВАТ «Укртелеком» у 2001 р., в оперативному віданні якої знаходиться близько 700 комп'ютерів, а також десятки серверів. У результаті тимчасового відключення комп'ютерів від INTERNET та виведення з ладу системи

корпоративної пошти, компанії було нанесено збитків майже на 1 млн. грн. [76]. Цей протиправний факт вкотре підтверджує загальносвітову тенденцію до розширення меж злочинців у реалізації своїх протиправних дій. Так, у Сінгапурі затримали п'ятьох наших співвітчизників, яких звинуватили у використанні підроблених карток для оплати товарів і послуг. Вони зробили кілька несанкціонованих оплат через комерційний банк «Фінанси і кредит», скориставшись українськими кредитними картками. У результаті спільних дій українських та сінгапурських правоохоронців шахраї були виявлені та заарештовані. Визнаним є факт існування в Україні і організованих хакерських груп, в яких простежується зв'язок злочинного елементу з тероризмом. Підтвердженням тому є випадок з INTERNET-технологіями, який стався у січні 2004 р. До Одеського міжнародного аеропорту надійшов телефонний дзвінок від невідомого з настирливою пропозицією увійти в мережу електронної адреси і ознайомитися з наступними даними. У вимозі «хакера»містилася інформація терористичного характеру з погрозою знищення одного з пасажирських літаків у випадку невиконання деяких умов інформаційного і фінансового аспекту. За цим фактом було порушено кримінальну справу за статтею «тероризм». Після ретельної перевірки електронних адрес, правоохоронці встановили ймовірне місце передачі інформації. Їм виявилося INTERNET-кафе м. Одеси. У ході проведення оперативно-розшукових та організаційно-тактичних заходів було встановлено осіб-злочинців і за короткий проміжок часу затримано комп'ютерних терористів. Розкриття цього злочину набуло резонансного характеру, як і розкриття у 1999 р. спорідненого злочину, що відбувся у Вінницькому обласному управлінні Національного банку України, де з рахунків резервного фонду було викрадено 80,4 млн. грн., якими намагалися заволодіти гр. К. та гр. Р. за рахунок підроблених електронних документів. Вказані суб'єкти перевели кошти з одного банку в інший і мали на меті їх конвертувати, але дії злочинців були зупинені. Суд визнав громадян К. і Р. винними у розкраданні державного майна в особливо великих розмірах (ст. 86-1 КК України 1960 р.),

та повторній підробці документів, які видаються державною установою (ч. 3 ст. 194 КК України 1960 р.) [11]. Успіх позитивного розслідування цих двох кримінальних справ можна віднести до розряду найбільших досягнень діяльності правоохоронних органів у цьому спектрі злочинності. Однак, це не привід для заспокоєння. Тенденція збільшення зазначених злочинів в Україні повторює світову – щорічне зростання вдвічі-тричі (тільки у 2002 р., за даними Департаменту інформаційних технологій МВС України, було виявлено 681 злочин, вчинений у сфері з використанням комп'ютерних технологій) [77, с. 121 – 126]. А з моменту прийняття та набрання чинності нового Кримінального кодексу України, по лінії боротьби зі злочинами цієї категорії, в Україні порушено понад 40 кримінальних справ, з яких більшість не має аналогів у світовій практиці [94, с. 32]. Набагато інформативнішою є статистика МВС України, що сформована з урахуванням чинного законодавства передбачених ст. ст. 361-363 КК України. Зокрема:

у 2001 р. було зареєстровано 16 злочинів, (їх питома вага у загальній кількості злочинів становила 0,0031 %);

у 2002 р. зазначений показник становив 30 злочинів (0,0066 %);

у 2003 р. – 74 злочини (0,013 %);

у 2004 р. – 53 злочини (0,01 %) [155, с.8].

Наступні роки позначилися різким підвищенням показників зазначеної категорії злочинів. Відповідно до статистичних даних МВС України в загальному по Україні у:

2005 р. їх кількість становила – 615 зареєстрованих злочинів;

2006 р. – 583 злочини, що на 5,2 % менше у порівнянні з попереднім роком;

2007 р. – 656 злочинів на 12,5 % більше від минулорічних;

2008 р. – 691 комп'ютерний злочин на 5,3 % у сторону збільшення.

На думку іноземних спеціалістів, – це викликане тим, що:

- високий потенціал і професійний рівень українських «хакерів», про який так часто говорять представники зарубіжних спецслужб;

- політична нестабільність суспільства [13, с. 31].

Ці та інші фактори впливають на динаміку скоєння злочинів у сфері з використанням комп'ютерних технологій. Єдиним шляхом до поліпшення цієї ситуації є плідна співпраця причетних структур як державного, так і міжнародного рівнів, які покликані вести боротьбу з зазначеним злочинним явищем. У зв'язку з цим слушними є точки зору науковців про доцільність створення високопрофесійних, фахових підрозділів у структурах Служби безпеки України, Міністерства внутрішніх справ, Державній податковій адміністрації. Як позитивне слід відзначити діяльність Управління по боротьбі зі злочинами у сфері комп'ютерних технологій, створене у структурі МВС України у 2001 р. Вони, як і Міжвідомчий НДЦ з проблем боротьби з організованою злочинністю при Президентові України, накопичують світовий досвід розкриття, розслідування, протидії і запобігання комп'ютерній злочинності і перетворюють отримані знання на практичні рекомендації відповідним структурам нашої держави.

Одним з таких важливих документів є «Концепція реформування законодавства України у сфері суспільних інформаційних відносин», в якій визначені основоположні напрями стратегії і тактики боротьби з організованою злочинністю і корупцією. Для захисту інтересів держави в комп'ютерній інформаційній сфері діє «Концепція національної безпеки України», яка функціонує і постійно удосконалюється з урахуванням виникнення нових загроз системи захисту електронної інформації. Реалізація державної політики в галузі захисту державних інформаційних ресурсів у мережах обміну даними, криптографічного і технічного захисту Указом Президента № 1120 від 06.10.2000 р. покладена на Департамент спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України (ДСТСЗІ СБУ) [165].

Подальші кроки протидії кіберзлочинності знайшли своє відображення в Указах Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі в Україні», від 31.07.2000 р.

№ 928/ 2000; «Про деякі заходи щодо захисту державних інформаційних ресурсів у межах передачі даних» від 24.09 2001 р., № 891/2001р.; «Про рішення Ради національної безпеки і оборони України» від 31.10.2001 р.; «Про заходи щодо вдосконалення державної політики та забезпечення інформаційної безпеки України» від 06.12.2001 р., № 1193/2001, яка передбачила створення Міжвідомчого центру з питань боротьби з комп'ютерною злочинністю (МЦПБКЗ) [75, с. 63]. Ця структура покликана бути координуючою організацією і виступати генератором подальшої стратегії вивчення та протидії зазначеної категорії злочинів на державному і міжнародному рівнях. У зв'язку з необхідністю посилення боротьби з організованою злочинністю і корупцією, Президентом України підписано Указ «Про невідкладні додаткові заходи щодо посилення боротьби з організованою злочинністю і корупцією» від 06.02.2003 р. У ньому (п. 9) одним з пріоритетних завдань Міністерства внутрішніх справ і Служби безпеки України є удосконалення взаємодії правоохоронних органів з Міжнародною організацією кримінальної поліції (Інтерпол) у боротьбі з організованою злочинністю та посилення ролі і відповідальності співробітників Національного бюро Інтерполу за виконання покладених на них обов'язків. Значна роль відводиться в документі питанням розкриття і розслідування злочинів у сфері комп'ютерних технологій та оформленню запитів через канали Інтерполу про ці злочини, що мають міжнародний характер [160, с. 135 – 136].

Підсумовуючи викладене вище, доходимо висновку, що незважаючи на окремі проблемні питання економічного, політичного, правового характеру, які нині є в Україні, протидія комп'ютерній злочинності є дієвою. Правоохоронцями приділяється значна увага питанню оптимального поєднання правових і профілактичних заходів, розробці та впровадженню кримінального законодавства і застосуванню інших норм, покликаних регулювати і встановлювати відповідальність за злочини з використанням комп'ютерних технологій.

1.2. Кримінально-правова характеристика комп'ютерних злочинів (в контексті окремих зауважень до попередньої редакції статей 361-363 КК України)

Важливе місце при дослідженні злочинів з використанням комп'ютерних технологій у науковій літературі відводиться питанням кримінально-правової характеристики. Однак більшість науковців зосереджують свою увагу лише на загальній констатації кримінальної відповідальності за вчинення злочинів у цій сфері, не звертаючи при тому увагу на окремі прогалини які існують у викладенні змісту розділу. Так, як уже вище зазначалося**,** у чинному Кримінальному кодексі України подано окремий Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку», який мав початковий виклад у трьох статтях: 361, 362 і 363 замість однієї статті 198^1 Кримінального кодексу України 1960 року, та реалії життя змусили законодавця переглянути зміст названих статей і внести суттєві корективи у зазначений вище розділ і нині він містить шість статей, які регулюють злочини у сфері з використанням комп'ютерних технологій, а саме: 361, 361^1, 361^2, 362, 363, 363^1 Кримінального кодексу України. З одного боку такі зміни несуть в собі позитивні аспекти, тобто відбулося розмежування злочинів, що відносяться до злочинів даної категорії. З іншого – не зовсім кваліфікований, виважений підхід законодавців до цих злочинів внесли певну плутанину у підходах щодо кваліфікації дій злочинців та їх протиправних дій, пов'язаних з використанням комп'ютерних технологій. На окремих таких аспектах і хотілося б зупинитися.

Перш за все, доречним буде провести деякі порівняння з попередньо діючими нормами, які потребували додаткового розгляду та тлумачення як у формулюванні відповідних статей, так і їх внутрішнього викладу змісту. У свою чергу, слід зазначити, що згадані три статті чинного Кримінального кодексу створили можливість реального притягнення до кримінальної

відповідальності осіб, які винні у вчиненні комп'ютерних злочинів [179, с. 41]. Разом з тим, вони мали деякі неузгоджені питання, що потребували уточнень та доповнень. Зокрема, дослідниками наголошувалося, на неточностях формулювання диспозицій статей 361, 362 і 363, що вносило певні суперечності при кваліфікації злочинів цієї категорії. Автор, також, у своїх наукових працях відстоював точку зору гнучкого механізму змін та доповнень новими статтями відповідно до вчинених злочинцями протиправних дій з використанням комп'ютерних технологій. Однією з таких пропозицій було додатково внесення нової четвертої статті до розділу XVI Кримінального кодексу України. Таку позицію автора поділяли і інші дослідники, зокрема В.О. Голубєв, який пропонував подати його у такій редакції: «Порушення порядку обігу технічних засобів та програмного забезпечення, призначеного для отримання несанкціонованого доступу до комп'ютерів, автоматизованих систем та комп'ютерних мереж» [66, с. 1 – 4]. Практичне відображення вона знайшла у змісті ст. 363^1 та частково у ст. 361^1 КК України. Такі зміни були продиктовані необхідністю законодавчої неврегульованості відповідальності осіб за умисне розповсюдження програмних і технічних засобів, які використовуються з метою вчинення несанкціонованого доступу до електронно-обчислювальних машин, їх систем та комп'ютерних мереж, включаючи комп'ютерні віруси, оскільки такі діяння не лише сприяють вчиненню інших злочинів, пов'язаних з несанкціонованим доступом до електронно-обчислювальних машин, систем чи мереж, а й можуть спровокувати їх вчинення [179, с. 41].

Наступним, не менш важливим. неврегульованим аспектом були недоліки законодавства України у трактуванні понятійного апарату злочинів, що відносяться до цієї категорії. На думку вітчизняних науковців В.Д. Гавловського, Б.В. Романюка, В.С. Цимбалюка, їх сутність полягала у наступному: «...по-перше, різні закони і підзаконні акти, які регулюють суспільні відносини, об'єктом яких є інформація, приймалися у різні часи без належного узгодження понятійного апарату… Термінологічні неточності та

різне тлумачення близьких за формою і змістом понять та категорій призвели до їх неоднозначного розуміння і застосування на практиці, що викликало соціальну ентропію (невизначеність). Це у свою чергу породжувало соціальні конфлікти в інформаційних правовідносинах і правовий хаос. По-друге, велика кількість законів та підзаконних актів у сфері інформаційних відносин ускладнювала їх пошук, аналіз та узгодження для практичного застосування, насамперед, працівниками правоохоронних органів у боротьбі з комп'ютерною злочинністю, а особливо такою, що має ознаки організованої. Це призвело до зниження рівня виявлення, розкриття та доведення до суду кримінальних справ про такі злочини в Україні» [52].

Певні непорозуміння виникали при тлумаченні поняття злочину, в якому фігурувала комп'ютерна інформація, адже серед дослідників відсутній єдиний підхід щодо трактування цієї категорії. Автор, у свою чергу, відстоював позицію тих науковців, які вважали, що розв'язання таких питань необхідно починати з аналізу ключового для цих злочинів поняття – комп'ютерної інформації, тобто даних про навколишній світ та процеси, що в ньому відбуваються, які представлені у формі даних, зафіксованих в електронному вигляді [2, с. 12]. Інформація (від лат. informatio – роз'яснення, викладення) спочатку трактувалася як відомості, що передаються людьми усним, письмовим або іншим шляхом… На сучасному етапі «…інформація – це одне з основних понять кібернетики» [195, с. 498]. Але окремі вчені цієї думки не поділяли і намагалися ототожнювати її з поняттям комп'ютерної злочинності в основі якої є електронна інформація на яку, тим чи іншим чином здійснюється вплив сторонньою особою – це неправильно. Комп'ютерна інформація – це текстова, графічна чи будь-яка інша інформація (дані), яка існує в електронному вигляді, зберігається на відповідних носіях і може створюватись, змінюватись чи використовуватись за допомогою АЕОМ [156, с. 903]. Особливістю її організації є те, що вона сконцентрована в окремому файлі, програмі або іншій базі даних, які мають свої ідентифікаційні атрибути, котрі відносяться до предмета зазначеного посягання [182, с. 800].

Тоді як комп'ютерна злочинність – суспільно небезпечна діяльність чи бездіяльність, яка здійснюється з використанням сучасних інформаційних технологій і засобів комп'ютерної техніки з метою нанесення збитку майновим або громадським інтересам держави, підприємств, відомств, кооперативів, громадським організаціям і громадянам, а також правам особи [31, с. 6]. Особливістю цих злочинів є те, що комп'ютер у них може виступати одночасно як предмет посягання і як знаряддя вчинення злочину [100, с. 75]. Таким чином, про тотожність цих понять не може йти мова. Фахівці у свою чергу аргументують тим, що до змісту цього аспекту входить втручання в сферу чужих інтересів за допомогою комп'ютера: доступ до операційної системи, крадіжка інформації, спостереження або зміна в комп'ютерній мережі, використання комп'ютера для доступу до інших комп'ютерних машин, систем. Це, безперечно так, але використання комп'ютера для доступу до інших комп'ютерних систем не може бути злочином, якщо не несе порушення будь-яких чи будь-чиїх прав.

Характерною рисою комп'ютерної злочинності є зв'язок з інформаційною діяльністю, що базується на використанні інформаційних комп'ютерних технологій. А тому злочинні посягання на суспільні відносини, що базуються на використанні АЕОМ (комп'ютерів), систем та комп'ютерних мереж, спрямовані насамперед на погіршення інформаційної безпеки соціальних систем або об'єктів. Побутують й інші точки зору, зокрема висловлювання одного з провідних фахівців у цій сфері – Ю.М. Батуріна. Суть його теорії базується на тому, що комп'ютерної злочинності, з юридичної точки зору, взагалі не існує, але багато традиційних видів злочинів модернізуються за рахунок втягування в них обчислювальної техніки, тому найправильніше говорити про комп'ютерні аспекти злочинів [23, с. 129]. З даною висловленою автором точкою зору можна погодитися, і правильно буде говорити про злочини у сфері електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, але враховуючи, що скоєння всієї категорії злочинів відбувається з використанням комп'ютерів, їх мереж,

електронно-програмного забезпечення, де в основі є ЕОМ та їх комп'ютерні технології – думається, що вживання терміна комп'ютерна злочинність, як скорочена форма, а не тотожність понять, не може вважатися помилкою. Підтвердженням тому є позиція Д.О. Янішевського, який наголошує: «Використання терміна «комп'ютерний злочин», не є точним. Він характеризує спосіб та засіб здійснення злочину, а не його об'єкт (інформаційні відносини у суспільстві). Злочини, в яких об'єктом злочинного посягання виступає безпосередньо комп'ютер (технічні засоби), не відрізняються від злочинів, де об'єктом є будь-яке інше майно. Тому термін «комп'ютерні злочини» може використовуватися як зручне скорочення» [216, с. 119]. У свою чергу, Р.А. Калюжний стверджує, що до комп'ютерної злочинності належать протизаконні дії, за яких електронна обробка інформації є знаряддям їх скоєння або ж їх засобом [95, с. 14]. Найбільш виваженою та обґрунтованою є точка зору тих вчених, які до комп'ютерних злочинів відносять протизаконні дії у сфері електронно-обчислювальних машин (комп'ютерів), систем комп'ютерних мереж і мереж електрозв'язку і лише у тому разі, коли вони здійснили знищення, блокування, модифікацію або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їх мережі. Таку позицію відстоюють: Т.В. Аверьянова, Р.С. Бєлкін, П.Д. Біленчук, О.А. Баранов, В.Г. Гончаренко, В.Д. Курушин, В.В. Крилов, Н.А. Селіванов, М.І. Шилан та ін. Хотілося б сподіватися, що саме цієї позиції дотримувався і законодавець при формуванні зазначених статей чинного Кримінального кодексу України. Отже, автор доходить висновку, що буде правильним таке трактування, де під комп'ютерною злочинністю розуміється передбачена кримінальним законом суспільно небезпечна дія (бездіяльність), що посягає на право власників чи користувачів комп'ютерних інформаційних технологій своєчасно отримувати та обмінюватися належною їм достовірною інформацією, а також відповідними комп'ютерними програмними засобами та їх захистом від несанкціонованого інформаційного впливу з боку різної категорії комп'ютерних злочинців.

Правового уточнення потребували й окремі питання структури складу злочину з використанням комп'ютерних технологій. Як зазначав Ф.Г. Бурчак: «…склад злочину є єдиною підставою обґрунтування кримінальної відповідальності, служить законодавчим еталоном для кваліфікації злочинів і являє собою дієвий інструмент відмежування одного злочину від іншого» [39, с. 29]. Стисло прокоментуємо кожен з них.

Об'єкт комп'ютерного злочину. Цьому структурному елементу у теорії кримінального права відводиться чільне місце і він розглядається в сукупності з предметом злочину. Науково обґрунтована класифікація об'єктів злочину дозволяє правильно визначити місце конкретного об'єкта в загальній системі суспільних відносин, що є визначальним для точної кваліфікації злочинів [137, с. 94 – 100]. Аналізуючи об'єкт комп'ютерних злочинів, слід зазначити, що він різний залежно від диспозицій статей вказаного вище розділу. При його кваліфікації ми виходимо з загальновизнаного науковцями підходу, підтриманого та покладеного в основу кодифікації кримінального законодавства України, вітчизняними вченими-криміналістами В.Я. Тацієм та М.Й. Крижановським. Його суть полягає у введенні поняття загального, родового (видового) та безпосереднього об'єкта злочину, але при цьому вважається, що лише віднесені до того чи іншого родового об'єкта характеристики досить суттєво впливають на відповідну кваліфікацію злочинів. У свою чергу В.М. Кудрявцев зазначав, що під кваліфікацією розуміють встановлення і юридичне закріплення точної відповідності між ознаками заподіяного діяння та ознаками складу злочину, передбаченими кримінально-правовою нормою [117, с. 5].

а) Загальний об'єкт

До загального об'єкту комп'ютерного злочину відносимо сукупність суспільних відносин, які охороняються кримінальним законодавством. Тільки суспільні відносини як цілісна система, а не будь-які їх складові частини можуть бути визнані об'єктом злочину [200, с. 114]. Побутує думка, що глобалізаційні процеси, пов'язані з розвитком комп'ютерних технологій,

досить суттєво вплинули на розвиток суспільних відносин, навіть породили їх нові форми. І це вірно. Поява ЕОМ (комп'ютерних) технологій зорієнтувала суспільство на перехід від постіндустріального розвитку до вищої фази людського буття – інформаційного. Характерною рисою переходу до нової фази стало збільшення частки «внесків» у ВНП сфери інформаційних послуг (виробництво засобів створення електронних інформаційних продуктів, створення власно електронно-інформаційних продуктів та надання їх користувачам тощо). За оцінками експертів у США сьогодні ця частка становить більше 10 %, що перевищує частку інших галузей промисловості, у тому числі автомобільну та металургійну [19].

Загальновідомо, що інформаційне суспільство – це необхідність, продиктована часом. Таким чином, інформаційні відносини та інформаційна безпека мають досить важливе значення сукупності суспільних відносин сучасного типу держави. А тому розгляд загального об'єкта злочину закономірно визначає сукупність суспільних відносин, пов'язаних з забезпеченням інформаційної безпеки особи, суспільства та держави.

б) Родовий (видовий) об'єкт комп'ютерного злочину

Під родовим (видовим) об'єктом комп'ютерного злочину розуміємо суспільні відносини, що складаються у сфері несанкціонованого використання інформаційних комп'ютерних технологій, спрямованих на протиправне розповсюдження та обмін чужою електронною інформацією. В.Я. Тацій подає це як елемент суспільних відносин, що охороняється кримінальним законом, на який здійснюється безпосередній вплив і якому насамперед заподіюється шкода [205, с. 133 – 134]. Особливу суспільну небезпеку становить для громадянина та держави, а саме:

- досить інтенсивно і у масовому порядку майже у всіх сферах людської життєдіяльності застосовуються технологічні процеси з використанням комп'ютерних технологій;

- злочини, віднесені до цієї категорії, мають досить високий коефіцієнт застосування протиправних інтелектуальних зусиль, що суттєво позначається на великомасштабності нанесеного збитку;
- обмеження доступу широкого кола осіб користувачів до спеціальних знань та техніки, що використовувалися для скоєння та шифрування комп'ютерного злочину.

в) Безпосередній об'єкт комп'ютерного злочину

Безпосереднім об'єктом будь-якого злочину, у тому числі й комп'ютерного, є те, на що конкретно спрямований злочин. Як зазначила Н.Ф.Кузнєцова, «…без об'єкта злочину немає і злочину» [118]. У сфері зазначеної категорії злочинів несанкціоновані дії спрямовані на:

- порушення функціонування автоматизованих систем;
- порушення цілісності інформації в автоматизованих системах;
- доступ та використання інформації в автоматизованих системах.

Цей об'єкт діяльності має неординарний протиправний характер, а тому і нанесені збитки носитимуть різну тяжкість. Наприклад, порушення функціонування автоматизованих систем, у подальшому (АС), неминуче призведе до:

- повного або часткового фізичного знищення основного або додаткового обладнання АС;
- повного або часткового виведення зі складу різних елементів АС;
- порушення логіки роботи програмних засобів і самої АС;
- блокування надходження або передачі АС;
- повної чи часткової втрати інформації.

Порушення цілісності інформації в автоматизованих системах призведе до:

- перекручення або знищення даних, що може відбутися на будь-якому з етапів їх збирання, зберігання, обробки та передачі;
- перекручення або знищення програмних засобів, що можуть відбутися в процесі роботи, а також при його зберіганні чи передачі.

Несанкціонований доступ та використання інформації в автоматизованих системах означає:

- доступ до даних та програмних засобів куди надходить, де зберігається та опрацьовується або передається в автоматизовані системи інформація з порушенням встановлених правил доступу до механізмів;
- неправомірне використання даних та програмних засобів куди надходить, де зберігається та опрацьовується або передається в автоматизовані системи інформація з нанесенням збитку власнику чи користувачу цих засобів [18, с. 5 – 7].

Отже, викладені вище об'єкти комп'ютерного злочину тією чи іншою мірою викличуть порушення прав власників та добросовісних користувачів, а також їх програмних систем.

Предмет злочину

За загальновизнаним поняттям – це елемент об'єкту злочинного посягання, впливаючи на який злочинець порушує або намагається порушити суспільні відносини [119, с. 138]. Переносячи акцент на нетрадиційні види злочинів, слід прокоментувати наступне. Як було зазначено у попередній редакції ст. 361 КК України (науково-практичного коментаря Кримінального кодексу України), за загальною редакцією М.О. Потебенька та В.Г. Гончаренка предметом злочину є:

- електронно-обчислювальні машини (ЕОМ);
- програмні матеріали, що забезпечують нормальне функціонування ЕОМ;
- системи ЕОМ та комп'ютерні мережі [157, с. 721].

Дещо інший зміст має предмет злочину у науково-практичному коментарі до Кримінального кодексу України за редакцією С.С. Яценка – це:

- автоматизовані електронно-обчислювальні машини;
- системи АЕОМ або автоматизовані системи;
- комп'ютерні системи;

- носії комп’ютерної інформації;
- комп’ютерні віруси;
- комп’ютерна інформація;
- програмні та технічні засоби, призначені для незаконного проникнення до автоматизованих електронно-обчислювальних машин, їх системи;
- комп’ютерні мережі [158, с. 783–784].

У той час в аналогічному коментарі за редакцією М.І. Мельника та М.І. Хавронюка (датований від 5 квітня 2001 року):

- автоматизовані електронно-обчислювальні машини (комп’ютери, АЕОМ), у тому числі персональні;
- їх системи;
- комп’ютерні мережі, а також ст. 362 КК України – комп’ютерна інформація [156, с. 902–905].

Згодом той же авторський колектив за редакцією М.І. Мельника та М.І. Хавронюка датованій 2007 роком предметом злочину визначає:

для статті 361

- електронно-обчислювальні машини (комп’ютери);
- автоматизовані системи;
- комп’ютерні мережі;
- мережі електрозв’язку.

Для статті 361-1:

Шкідливі програмні та технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ, АС, комп’ютерних мереж чи мереж електрозв’язку.

Для статті 361-2: інформацію з обмеженим доступом, яка зберігається в ЕОМ, АС, комп’ютерних мережах або носіях такої інформації, тобто комп’ютерна інформація з обмеженим доступом. А для статті 362 –

- інформація, яка обробляється на відповідних носіях в ЕОМ, АС, комп'ютерних мережах або зберігається на відповідних носіях;
- комп'ютерна інформація, що не призначена для відкритого доступу і вільного користування, тобто комп'ютерна інформація з обмеженим доступом або комп'ютерна інформація, доступ до якої є платним [159, с. 943-950].

А у науково-практичному коментарі до Кримінального кодексу України за загальною редакцією В.В. Сташиса та В.Я. Тація предметом злочину є:

Для статті 361

- електоронно-обчислювальна машина (ЕОМ) комп'ютер;
- автоматизовані системи (АС);
- комп'ютерні мережі (мережа ЕОМ);
- мережі електорозв'язку;
- комп'ютерна інформація;
- інформація, що передається мережами електрозв'язку (телекомунікаційними мережами).

Для статті 361-1 – шкідливі програмні та технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж, мереж електрозв'язку.

Для статті 361-2 – інформація з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства.

Для статей 362 і 363 предмет злочину визначений нормами статті 361 КК України [160, с. 964-978].

Виходячи зі змісту викладеного вище, доходимо висновку, що існують між авторами окремі розбіжності стосовно визначення складових предмета злочину. Зазвичай, кожна з запропонованих точок зору має право на існування, якщо вона достатньо науково обґрунтована. Однак, що стосується предмета злочину комп'ютерної інформації, то є розбіжності, які потребують уточнення.

Слід зауважити, що деякі дослідники не вважали альтернативним предметом злочину комп'ютерну інформацію, яка була зазначена в ст. 361 КК України як предмет, на перекручення або знищення якого спрямовані дії злочинця [180, с. 24]. Як подано у ДСТУ 2226-93, «…комп'ютерна інформація є предметом віртуальним, тобто умовним, фізично відсутнім, але за допомогою спеціальних методів наданим у розпорядження» [83]. У той час О.Н. Радутний наголошував, що сьогодні реалії вимагають визнати у подальшому предметом злочину речі або інші явища об'єктивного світу (інформація, енергія тощо), з певними властивостями яких кримінальний закон пов'язує наявність у діянні особи складу конкретного злочину [177, с. 10]. У свою чергу В.С. Комісаров трактував комп'ютерну інформацію як відомості про осіб, предмети, факти, події і явища обмеженого доступу або необмеженого характеру, які знаходяться в ЕОМ, системах ЕОМ або їх мережах [105]. На думку автора, слушним у цьому аспекті було твердження Д. С. Азарова. Він зазначав: «Не важко помітити, що існують такі злочини, при вчиненні яких комп'ютерна інформація в одних випадках може бути лише предметом, в інших – лише знаряддям» [3, с. 66].

У зв'язку із внесенням змін законодавцем до Розділу XVI, комп'ютерній інформації приділено особливу увагу і вона має виклад у трьох статтях 361, 361^2 та 362 КК України, але при тому є розбіжності, що стосуються предмету злочину. А саме: перша редакція Розділу XVI у статтях 361-363 КК України предметом злочину визначала комп'ютерну інформацію, нова ж редакція Закону України № 2289-IV від 23.12.2004 р. акцентує увагу на інформації при тому слово «комп'ютерна» пропущено і незрозуміло з яких міркувань. Таким чином виходить, що предметом злочину за статтями 361 є просто інформація; 361^2 – інформація з обмеженим доступом, яка зберігається в ЕОМ, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створена і захищена відповідно до чинного законодавства; 362 – інформація, яка обробляється в ЕОМ, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації. Така позиція

законодавця ускладнила систему понятійного апарату, бо поняття просто «інформація» може містити в собі будь-яку інформацію непов'язану з використанням комп'ютерних інформаційних даних в тому числі використання комп'ютерної електронної інформації та інформації в мережах електрозв'язку. Все це викликало плутанину та розширення меж складів злочинів, що відносяться до даної категорії. Слушною у цьому питанні є позиція А.А. Музики та Д.С. Азарова: «Невдала спроба об'єднати у ст. 361 КК одним терміном ознаки предмета злочину у сфері комп'ютерної інформації та предмета злочину у сфері телекомунікацій зайвий раз свідчить про неприпустимість встановлення відповідальності за ці посягання в одній кримінально-правовій нормі.

Варто також зазначити, що у ст. ст. 361^2 і 362 ознаки інформації описані суперечливо. Очевидно, що законодавець розрізняє поняття «інформація, яка зберігається в ЕОМ, автоматизованих системах, комп'ютерних мережах або носіях такої інформації» та «інформація, яка оброблюється в ЕОМ, автоматизованих системах, комп'ютерних мережах». Внаслідок розмежування цих двох понять предметом злочину, передбаченого ст. 361^2 КК, не може бути інформація (з обмеженим доступом), яка оброблюється в ЕОМ, автоматизованих системах, комп'ютерних мережах. Окрім цього, предметом жодного із злочинів, передбачених ст. ст. 361^2 і 362 КК, не може виступати інформація, що передається мережами електрозв'язку» [155, с. 69].

Об'єктивна сторона складу злочину

Досліджуючи об'єктивну сторону злочинів, пов'язаних з використанням комп'ютерних технологій зупинимося лише на окремих аспектах розбіжностей, що існували раніше у кримінальному праві. Виходячи із першої редакції ст. 361 КК України, об'єктивна сторона злочину проявлялася у формі: 1) незаконного втручання у роботу АЕОМ, їх систем чи комп'ютерних мереж, що призвело до перекручення чи знищення комп'ютерної інформації або носіїв

такої інформації; 2) розповсюдження комп'ютерного вірусу. У цьому питанні законодавцю не слід було б їх подавати їх в одній нормі. Як підкреслюють вітчизняні фахівці М.С. Вертузаєв, В.О. Голубєв, О.І. Котляревський, О.М. Юрченко: «…незрозумілою лишається ідея законодавця об'єднати однією статтею такі різні за рівнем суспільної небезпечності дії, як «втручання в роботу АС» та «розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в АС» [199, с. 19]. Така позиція видається нам правильною. У оновленій редакції ці норми мають виклад у двох статтях 361 та 361^1 КК України, що на думку багатьох дослідників це дасть можливість уникнути плутанини.

Далі звертаємо увагу на ще недавно діючу окрему ознаку ч. 1 ст. 361 КК України, а саме: «…перекручення чи знищення комп'ютерної інформації». У трактуванні між дослідниками виникали деякі розбіжності щодо змісту цього поняття. За визначенням А.М. Ришелюка, це будь-яка зміна такої інформації, за відсутності можливості відновити ті її фрагменти, які зазнали змін, у їх первісному вигляді [156, с. 903]. У той час Д.С.Азаров наполягав, що перекручення комп'ютерної інформації слід вважати модифікацією останньої, у тому числі її часткове знищення [4, с. 71]. Проте, існували й інші точки зору вчених на цей предмет. Виваженим є науковий підхід В.Г. Гончаренка, який зазначив, що «…під перекрученням інформації слід розуміти зміну її змісту по суті, порушення цілісності, в тому числі і вилучення (знищення) окремих фрагментів» [157, с. 723].

Така позиція є вірною, разом з тим, при формулюванні альтернативного наслідку при перекрученні комп'ютерної інформації слід звернути увагу на те, що будь-яка несанкціонована зміна даних – це втрата цілісного початкового змісту інформації. Однак може існувати варіант відновлення перекрученої (видозміненої) комп'ютерної інформації до первісного вигляду. Якщо ж виключена така можливість, то не про модифікацію потрібно вести полеміку, а про знищення інформаційних комп'ютерних даних, які несуть у собі заподіяння і нанесення матеріальної шкоди потерпілій стороні. У цьому сенсі

слід наголосити на обов'язковій ознаці злочину – причинному зв'язку між злочинним діянням (дією чи бездіяльністю) і суспільно небезпечними наслідками. Досить змістовно виклав своє бачення у цьому аспекті М.І. Панов. Він зазначив: «…причинний зв'язок – це об'єктивно існуючий зв'язок між діянням – дією чи бездіяльністю (причиною) – і суспільно небезпечними наслідками (наслідком), коли дія або бездіяльність викликає (породжує) настання суспільно небезпечного наслідку» [167, с. 108].

У новій редакції ч.1 ст.361 КК України законодавець уже уникнув допущених прогалин і за акцентував «… що призвело до витоку, втрати, підробки, блокування інформації…».

Суб'єкт злочину

Згідно з визначенням законодавцем суб'єктом злочину є фізична осудна особа, яка вчинила злочин у віці, з якого може настати кримінальна відповідальність (ч. 1 ст. 18 КК України). (Детальний розгляд суб'єкта злочину викладений за текстом у параграфі 1.3. Криміналістична характеристика комп'ютерних злочинів).

У цьому параграфі проведемо паралелі у поглядах суб'єкта злочину між законодавцем та іншими дослідниками. Отже, як зазначено у науково-практичному коментарі КК України, за редакцією М.І. Мельника та М.І. Хавронюка, у колишніх статтях 361 і 362 суб'єкт злочину загальний, а у ст. 363 – спеціальний. Тобто, виходячи з кваліфікації цих статей, суб'єкти, що вчиняють протиправні дії, різні за статусом. У той самий час мають спільне – відповідальності за скоєне підлягають осудні фізичні особи, яким до вчинення злочину виповнилось 16 років. Однак доволі часто у матеріалах юридичної літератури зустрічаються окремі припущення авторів про перенесення спеціального суб'єкта зі ст. 363 на ст. 361 і 362 КК України. Проаналізуємо, наскільки це є виправданим. Так, наприклад, П.П. Андрушко наголошує, що суб'єктом злочину зазначених статей є особа, яка досягла 16-річного віку, у тому числі й особи з персоналу «АЕОМ, їх систем та комп'ютерних мереж». І далі продовжує автор: «…суб'єктами злочину у формі розповсюдження

комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в АЕОМ, їх системи та комп'ютерні мережі і здатних спричинити перекручення або знищення комп'ютерної інформації чи її носіїв, можуть бути розробники таких програм і технічних засобів, їх виготовлювачі, зокрема, виробники (розробники) програм з комп'ютерними вірусами, так звані «технопацюки», «хакери» та ін.» [158, с. 142; с. 104]. Інші дослідники О.П. Снігерьов і О.І. Сергач не поділяють суб'єктів злочину за відповідністю до статей і акцентують, що це особа, яка має доступ до комп'ютерної системи (програміст, оператор ЕОМ, налаштовувач обладнання, користувачі), так і сторонній громадянин [196, с. 85]. Науково-обґрунтоване бачення є у твердженні В.Г. Гончаренка. Вчений розмежував юридичні склади ст. 361 КК України і запропонував такий виклад: «…суб'єктом цих злочинів може бути будь-яка фізична осудна особа, що досягла 16-річного віку. Насамперед, це ті особи, яких власник або уповноважена ним особа чи розпорядник АС призначили обслуговувати АС, а також і сторонні особи. Що ж до розповсюдників комп'ютерного вірусу, то ними насамперед є розробники програмних і технічних засобів проникнення до АС (хакери), здатні спричинити перекручення або знищення комп'ютерної інформації чи її носіїв, виробники цих програм і засобів, а також, звичайно, й інші особи» [157, с. 724]. Розглядаючи загальний суб'єкт початкового варіанту ст. 361 і 362 КК України, вбачаємо перенесення акценту на спеціальний суб'єкт. Але останній, у свою чергу, – це особа, яка, окрім наявності осудності та досягнення віку кримінальної відповідальності, наділена спеціальними ознаками, закріпленими нормою права і виробничими стосунками. Тобто, йдеться про спеціалістів у своїй сфері, фахівців інформаційних комп'ютерних технологій як внутрішніх (співробітників компанії), так і зовнішніх (сторонніх осіб) «профі» вищого ґатунку.

У новій редакції зазначеного Розділу XVI враховані такі розбіжності й у ст. 362 та 363 КК України суб'єкт спеціальний, а в інших – загальний.

Суб'єктивна сторона складу злочину

Особлива увага у структурі складу комп'ютерного злочину приділяється суб'єктивній стороні. Саме вона розкриває внутрішній бік психологічного відношення суб'єкта до скоєного ним суспільно небезпечного діяння та відповідних шкідливих чи небезпечних наслідків матеріального характеру. Встановлює у певній формі вину, а також факультативні ознаки злочину: мету і мотиви протиправної дії особи. (Детальний розгляд суб'єктивної сторони складу злочину викладений за текстом у параграфі 1.3. Криміналістична характеристика комп'ютерних злочинів).

У цьому сенсі автор, як і у попередніх структурних елементах складу злочину, сконцентрує увагу лише на окремих розбіжностях, що траплялися у трактуваннях науковців цього питання.

Своєрідною плутаниною у поглядах вчених було у дослідженні форми вини скоєного злочину з використанням комп'ютерних технологій, зокрема у колишній редакції ст. 361 КК України «Незаконне втручання в роботу АЕОМ, їх систем чи комп'ютерних мереж». Так, наприклад, зустрічалися у правовій літературі твердження авторів, які вбачали у діях злочинців не прямий умисел, а необережну вину. Тобто вони відстоювали позиції, що особи, які незаконно втручалися в роботу чужого програмного забезпечення, маніпулювали електронною інформацією чи здійснили її модифікацію або знищення, викрадення при тому не мали прямого умислу – нонсенс.

Таке бачення дослідників суттєво ускладнювало тлумачення і застосування кримінально-правових норм цієї статті. До того ж, зазначене могло б призвести до надмірної криміналізації, наприклад: злочином мали б визнаватися необережні зміни, знищення або блокування інформації, яка оброблюється в ЕОМ, автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї [155, с. 79]. Про вчинений злочин слід говорити тоді, коли суб'єкт обов'язково усвідомлював суспільно небезпечний характер свого діяння, передбачав шкідливі чи небезпечні наслідки і бажав їх настання. Досить влучно з цього приводу зауважив П.С. Матишевський: «Ознаки

прямого умислу, що вказані у ч. 2 ст. 24 КК України, характерні для так званих матеріальних злочинів (злочинів з матеріальним складом), необхідною умовою яких є настання певних суспільно небезпечних наслідків, передбачених законом, і наявність причинного зв'язку між діянням особи і наслідками, що настали. Тому, при вчиненні цих злочинів винний передбачає не тільки суспільно небезпечні наслідки свого діяння, а й у загальних рисах – розвиток причинного зв'язку між діянням, що вчинюється, і злочинним наслідком, що настає» [143, с. 24].

Винятки становлять категорії осіб, що страждають новим видом психічних захворювань – інформаційно-комп'ютерними фобіями [32, с. 15]. Коли суб'єкт раніше на достатньому професійному рівні освоїв комп'ютерні технології, але з тих чи інших причин захворів на один з різновидів «комп'ютерної хвороби» й під час вчинення злочину не усвідомлював у своїх діях злочинного умислу і настання відповідних наслідків.

Аналогічної ситуації стосувалося і «Розповсюдження комп'ютерного вірусу» тієї самої статті. Нелогічно було б стверджувати, що особа, яка розробила комп'ютерний вірус, не передбачала прямого умислу своїх дій. Навіть якщо припустити, що вірус був написаний «початківцем-любителем» чи «жартівником». Дія шкідливої програми адресувалась певному суб'єктові, і незалежно з яких мотивів, тобто, у своїй основі злочинець простежував прямий умисел і, відповідно, передбачав хоча б мінімальні наслідки скоєного. Ю.В. Голік доводить, що «випадкові злочинці» можуть вчинювати «невипадкові злочини», але в цьому випадку суспільна небезпечність таких злочинів буде порівняно невеликою. Це стає відомим при вчиненні мотивів суспільно небезпечних діянь, які вчинюються випадковими злочинцями [71, с. 132]. Про непрямий умисел можемо стверджувати, коли особа усвідомлювала суспільно небезпечний характер свого діяння (дії або бездіяльності), передбачала його суспільно небезпечні наслідки і хоча і не бажала, але свідомо припускала їх настання (ч. 3 ст. 24 КК України). Для прикладу: суб'єкт, що перебував у трудових відносинах з роботодавцем,

володів даними у межах своїх функціональних обов'язків про виток конфіденційної комп'ютерної інформації з підприємства, але не вважав за потрібне сповіщати про це представників адміністрації установи, хоча і знав про настання можливих суспільно небезпечних наслідків та ін.

Ці та інші суттєві прогалини врахувала нова редакція Розділу XVI Закону України №2289-IV від 23.12.2004 р. У науково-практичних коментарях Кримінального кодексу України за редакціями М.І. Мельника, М.І. Хавронюка; за загальною редакцією В.В. Сташиса, В.Я. Тація та ін. чітко визначено форми вини суб'єкта злочину, що тим самим унеможливлює допущення плутанини та неправильного трактування відповідної норми зазначеного вище розділу дослідниками права та практичних працівників правоохоронних органів України, які уповноважені законом здійснювати розслідування злочинів у тому числі й комп'ютерних.

1.2. Криміналістична характеристика комп'ютерних злочинів

Одним з найважливіших завдань розвитку криміналістики було і залишається розширення та поглиблення дослідження теоретичних проблем науки, котрі стосуються як загальних, так і окремих розділів, у тому числі й криміналістичної методики злочинів. Криміналістика за історично короткий час пройшла шлях від науково-технічної дисципліни, яка виконувала суто допоміжні практичні завдання під час розслідування різних подій, до методологічно зрілої системи знань, розвинутими пізнавальними, інформаційними і прогностичними (апофеоз науки!) функціями [63, с. 41]. На сучасному етапі виникнення нового виду злочинності вона обумовлює необхідність перегляду даних теорії та практики, а також уточнення і доповнення традиційних рішень додатковими.

Актуальним залишається підхід до вивчення та розробки криміналістичної характеристики окремих видів злочинів, особливо, що стосується злочинів, що розглядаються. О.М. Глотов у праці «Деякі проблеми

попереднього наслідку в зв’язку з науково-технічною революцією», яка вийшла друком у 1972 р. зазначав: «…не можна виключати можливість появи нових видів злочинів» [72].

Ця точка зору є слушною і правильною, оскільки розвиток суспільних відносин обумовлює появу нових різновидів злочинів. Підтвердженням тому є розробка та впровадження в людську життєдіяльність комп’ютерних технологій, що відповідно викликали появу злочинності цього виду. У зв’язку з цим вчені-криміналісти досить активно включилися до процесу вивчення та вироблення нових методик, що сприяють розслідуванню, розкриттю та протидії високотехнологічної злочинності. Запропоновано нові наукові теорії та вчення. Використано при цьому практику вітчизняних та зарубіжних правоохоронних органів тощо.

Однак, цього недостатньо для твердження, що правоохоронні органи підготовлені до цілковито повного, відпрацьованого розкриття комп’ютерних злочинів. Здебільшого фахівці-криміналісти акцентують свою увагу на окремих аспектах тактичних особливостей таких злочинів, вирішенні деяких проблемних питань методики їх розслідування. Автор, даного монографічного дослідження, в свою чергу, ставить за мету проаналізувати структуру окремих криміналістичних методик розслідування цієї категорій злочинів, виробити практичні рекомендації, які б були дієвим механізмом у роботі слідчого при розгляді питань, пов’язаних зі злочинами у сфері комп’ютерних технологій. Тому дотримуємося позиції тих науковців, які вважають, що основними елементами структури окремих криміналістичних методик мають бути:

- криміналістична характеристика цих злочинів;
- типові ситуації та програми з метою виявлення ознак злочину та стадії порушення кримінальних справ;
- типові слідчі ситуації початкового та наступного етапів і програм розслідування;
- особливості тактики окремих слідчих дій, проведення інших заходів тощо [86, с. 69].

У теорії науки криміналістики, чільне місце відводиться визначенню понять і системи елементів криміналістичної характеристики злочинів. Саме поняття криміналістичної характеристики, то воно відносно нове, дискусійне та належним чином неопрацьоване. Одним з перших застосував таке визначення А.М. Колесниченко. Він зазначив, що до числа найсуттєвіших положень загальних для всіх часткових методик відноситься: «…загальна криміналістична характеристика даного виду злочину». А тому, як наголошує далі автор, «злочини мають і загальні риси криміналістичного характеру» [103, с. 8–9]. Це трактування було по-різному сприйняте вченими, а тому не знайшло належної підтримки. Більш розгорнута система була запропонована Л.А. Сєргєєвим, а саме: спосіб скоєння злочину, умови, за яких здійснюються злочини та особливості обстановки; обставини, пов'язані з безпосередніми об'єктами злочинних посягань, з суб'єктами та суб'єктивною стороною злочину; злочинні зв'язки конкретного виду з іншими злочинами та окремими діями, що не є кримінально покарані, але мають схожість з даними злочинами за деякими об'єктивними ознаками; зв'язками між зазначеними групами обставин [192]. Своє бачення в цьому аспекті було подане С.І. Винокуровим. Він під криміналістичною характеристикою злочину пропонував розуміти науково розроблену систему його найбільш істотних, типових криміналістичних рис, ознак, властивостей, відносин, що слугують орієнтиром у з'ясуванні характеру, механізму та умов утворення слідів (матеріальних та ідеальних) конкретного злочину, визначенні кола об'єктів, у яких вони (сліди) могли утворитися, а також у вирішенні слідчих завдань, пов'язаних з вибором напряму розслідування, встановленням сукупності обставин, що мають значення для справи, планування, висування і перевірки слідчих версій та інше [46, с. 101].

За теорією М.П. Яблокова, зміст криміналістичної характеристики зводиться до трьох елементів: криміналістичні риси способу скоєння злочинів, типові слідчі ситуації та характер інформації, що підлягає виявленню [214, с. 38]. Тоді як І.Ф. Герасимов наголошував, що криміналістична

характеристика є сукупністю даних про загальні, типові ознаки, обставини та інші характерні риси конкретно визначеного виду злочинних діянь, які мають важливе організаційне і тактичне значення для розкриття цього виду злочину [56, с. 96]. Трактування окремих вчених зводилося до перенесення акценту з опису ознак криміналістичної характеристики на розкриття механізму злочину. Такої думки дотримувалися В.О. Образцов і В.Г. Танасевич. Вони зазначають, що криміналістична характеристика – це система об'єктивних даних про механізм злочинного діяння, типових відображуваних і ті, які відображують об'єкти і взаємодіють у процесі вчинення злочину, про особливості та джерела формованої ними фактичної інформації, що має значення для вирішення завдань кримінального судочинства шляхом застосування обумовлених криміналістичних засобів, прийомів і методів [185, с. 266].

Досить виважену наукову позицію відстоює В.П. Бахін. На його думку, до змісту криміналістичної характеристики, як практичного інструменту розслідування, а не наукової категорії криміналістики, повинні бути віднесені тільки ті елементи, котрі відрізняються чіткою розшуковою спрямованістю [15, с. 14]. У той час А.О. Фокіна констатує: «Чи правомірно говорити про криміналістичну характеристику злочину? Безумовно, оскільки конкретний злочин-одиниця сукупності, так званого виду (роду) злочину…. Криміналістична характеристика роду (виду) злочину – лише результат аналізу множинності одиничних злочинів» [207, с. 18]. Своє бачення цієї проблематики обґрунтовували також: А.Н. Басалаєв, П.Д. Біленчук, А.Н. Васильєв, Л.Г. Видонов, І.А. Возгрін, В.Г. Гончаренко, В.А. Гуняєв, В.Ф. Єрмолович, Є.І. Зуєв, А.В. Іщенко, В.А. Колесник, Г.А. Кушнір, І.Ф. Пантєлєєв, В.Л. Подпалий, М.В. Салтевський, Є.В. Циплєнкова, Н.Г. Шурухнов та ін. Досить своєрідну наукову класифікацію запропонував Р.С. Бєлкін. Він в кілька етапів підходив до аналізу криміналістичної характеристики, уточнюючи та доповнюючи самого себе. На його думку, криміналістична характеристика окремого виду злочину повинна включати:

характеристику вихідної інформації; системи даних про спосіб скоєння та приховування злочину, а також типових наслідків його застосування; особи злочинця та ймовірних мотивів і мети злочину; особи-жертви злочину; деяких обставин скоєння злочину (часу, місця, обстановки) [26, с. 179].

Не знайшла цілковито повної підтримки і ця точка зору вчених-криміналістів. Одним із суперечливих аспектів залишається питання доцільності у структурі елементів криміналістичної характеристики вихідних даних про злочинне діяння, яке слугує підставою для порушення кримінальної справи або застосування іншого передбаченого законом кримінально-процесуального рішення по суті того або іншого матеріалу з ознаками злочину. Зокрема, проти цієї теорії виступає В.Ф. Єрмолович, який доводить, що «…у криміналістичну характеристику злочинів… недоцільно включати: вихідні дані про злочинну діяльність; типові слідчі ситуації тощо…». Разом з тим він наголошує: «…варто погодитися з тими авторами, які, на нашу думку, правильно включають до змісту криміналістичних характеристик злочинів наступі дані: механізм злочину; умови місця і часу скоєння злочину; обставини і умови, що сприяють скоєнню злочинів;…» [84, с. 27].

На нашу думку, точка зору В.Ф. Єрмоловича та його однодумців заслуговує на увагу. Криміналістична характеристика злочинів формується із змісту типової слідчої ситуації, яка склалася, а тому відображати вона має систематизований опис типових криміналістично-значущих ознак, при тому не всіх, а основних. Однак у цьому сенсі слід прислухатися до думки В.Г.Гончаренка, науковець вважає, що: «…розділяти їх на першорядні і другорядні немає підстав» [59, с. 7]. Криміналістична характеристика – це інформаційна модель, що становить собою сукупність істотних, стійких якісно-кількісних систем опису типових ознак конкретного виду (групи) злочинів. Відповідно опису мають підлягати лише типові ознаки, що є притаманними конкретному виду чи групі злочинів. Таким чином, найбільш доцільними елементами криміналістичної характеристики мають бути:

- предмет безпосереднього злочинного посягання;

- деякі обставини скоєння злочину (місце, час, обстановка, умови).
- способи вчинення та можливого приховування злочинів;
- слідова картина цих злочинів;
- особа злочинця та особа потерпілого;
- мета і мотиви вчинення злочину.

Отже, ми розглядаємо криміналістичну характеристику як одну з найімовірніших моделей орієнтованої інформації, яка служить для конкретизації чітко виражених цілей, а також направлень розслідування кримінальної справи. Її зміст охоплює особливості елементів предмета доказування, що є характерними для розслідування конкретної категорії злочинів. Структура зазначених елементів визначає не лише загальний перелік типової інформації про осіб, способи скоєння та приховування злочинів, а й місце, час, мету і мотиви. Разом з тим, вона вказує на зв'язки між цими обставинами. Така сукупність даних повинна розглядатися у певному взаємозв'язку та взаємозалежності як єдине ціле. Досліджуючи цілісність системи підходів, В.Г. Афанасьєв зазначав: «…сукупність об'єктів, взаємодія яких обумовлює наявність нових інтеграційних якостей, невластивих вірним її частинам, компонентам. У цьому, насамперед і полягає відмінність цілісної системи від простої сумарної системи, сукупності, конгломерату, суміші, наприклад, купи зерна, каміння або скупчення мінералів у земних шарах, властивості яких є простою сумою відповідних властивостей складових частин» [12, с. 240]. Таким чином, відповідний набір елементів перетворюється на зв'язане ціле, де кожний елемент взаємодіє з іншими, і поодинокі властивості системи, незважаючи на свою відносну самостійність, не можуть бути зрозумілі без урахування всіх у сукупності. Саме у такому вигляді, на думку автора, елементи криміналістичної характеристики можуть слугувати основоположним засобом визначення найефективніших шляхів розслідування комп'ютерних злочинів.

Більш детально проаналізуємо викладені елементи криміналістичної характеристики відповідно до запропонованого вище переліку.

1.3.1. Предмет безпосереднього злочинного посягання

Даний елемент криміналістичної характеристики злочинів носить конструктивну ознаку, оскільки мова йде про злочини, що скоюють особи з використанням саме комп'ютерних технологій. Виходячи із видової класифікації – це можуть бути комп'ютерні злочини у будь-якій сфері людської життєдіяльності і різної галузевої спрямованості. Найбільш поширеними вони є: у сфері економіки, зокрема банківській, кредитно-фінансовій; військовій галузі, у тому числі стратегічних військових сферах; міжнародних трансграничних, глобалізаційних сферах; державотворчому процесі та ін.

Предмет безпосереднього злочинного посягання завжди різний, він прямо пропорційний реалізації поставленої особою мети вчиненої протиправної дії. Це може бути комп'ютерний:

- тероризм, піратство, хуліганство, вандалізм, торгівля людьми, зброєю, наркотичними і психотропними речовинами;
- економічне та промислове шпигунство, шахрайство, у тому числі з банківськими рахунками, саботаж;
- підробка платіжних електронних документів, пластикових магнітних карток, крадіжка коштів;
- виготовлення та розповсюдження несанкціонованих комп'ютерних програм (вірусів), поширення дитячої порнографії, азартні ігри;
- спуфінг, крадіжка машинного часу через INTERNET, незаконне заволодіння комп'ютерною інформацію, що містить таємний чи конфіденційний характер та ін.

Предметом таких посягань виступатиме саме посягання, здійснене особою, яке становитиме суспільно небезпечне, винне діяння і матиме усі ознаки складу злочину.

Основним змістом цього елементу виступатимуть речі матеріального світу і предмети, у тому числі й інтелектуального характеру, індивідуальної

державної чи приватної власності, які становлять собою конкретно визначену матеріальну цінність.

1.3.2. Деякі обставини скоєння злочину (місце, час, обстановка, умови)

При визначенні тактики розслідування зазначених вище злочинів, важливе значення відіграють дані про місце, час обстановку та умови вчинення протиправної дії. У науці криміналістиці ці складові сприймаються як система різного роду взаємодіючих між собою до і у момент здійснення злочину об'єктів, явищ і процесів, що характеризують місце, час, речові, природнокліматичні, виробничі, побутові та інші умови навколишнього середовища, а також інші умови об'єктивної реальності, що визначають можливості, умови й інші обставини скоєння злочину [215, с. 18]. Особливістю комп'ютерних злочинів є те, що на них фактично не здійснюють вплив природокліматичні фактори. Місце, час та інші умови протиправних дій визначаються суб'єктивними, об'єктивними та іншими параметрами. Від них деякою мірою залежить вибір способу впливу на машинну (комп'ютерну) інформацію операційної системи. Одночасно обстановка скоєння злочину може знаходитися у взаємодії із особою та способом скоєння злочину. Бо, як відомо, вибір способу вчинення протиправних дій залежить від самої особи, враховуючи при цьому саму обстановку, в якій буде скоєно злочин. Як зазначав І.Н. Якимов: «Уважне, вдумливе вивчення обстановки, ніби то вводить в атмосферу значимості, яка закінчується на оточуючому, і не скільки бачену, скільки ту, що відчуваємо та про яку догадуємося» [217, с. 75]. Отже, спосіб неправомірного втручання в роботу автоматизованих комп'ютерних систем визначатиметься найбільш характерними складовими конкретної обстановки:

- місцем і часом дії злочинця (злочинців);
- особливостями комп'ютеризації суб'єкта господарювання;
- особливостями організації інформаційної безпеки;

- можливостями порушення цілісності комп'ютерної інформації безпосередньої участі людини;
- рівнем кваліфікації спеціалістів, що забезпечують захист інформації, а також адміністрування комп'ютерів та їх мереж [98, с. 168].

З точки зору розслідування таких злочинів особливий інтерес фахівців викликає інформація про ймовірне місце скоєння злочину. Як засвідчує практика, місце звідки було скоєно злочин (місце, де виконувалися дії об'єктивної сторони складу злочину) та місце настання шкідливих наслідків (місце, де наступив результат протиправної дії) можуть не співпадати. Але, при безпосередньому доступі, місце, де було скоєно злочин та місце настання негативних наслідків, в основному співпадають. Це викликане насамперед тим, що переважну кількість несанкціонованих дій вчиняють саме внутрішні користувачі, а також обслуговуючий установу чи конкретну операційну систему персонал. А, отже, якщо неправомірний доступ здійснюється одночасно з кількох комп'ютерів, то кількість місць, де було скоєно злочин, відповідає кількості задіяних при цьому комп'ютерів [53, с. 29]. Тому при розслідуванні справ, пов'язаних з доступом до комп'ютерної інформації, може бути не одне, а кілька місць, а саме:

- місце безпосередньої обробки і постійного збереження інформації;
- місце безпосереднього використання технічних засобів для неправомірного доступу до комп'ютерної інформації;
- місце зберігання інформації на машинних носіях;
- місце безпосереднього використання результатів неправомірного доступу до комп'ютерної інформації [34, с. 179].

Не слід забувати ще про одну суттєву особливість комп'ютерних злочинів – для них відсутнє територіальне (просторове) обмеження. Тобто, злочин може виходити за рамки однієї держави. Але, незважаючи на віртуальність у використанні комп'ютерних технологій, злочин є реальним і важко розслідуваним. Складність полягає у відтворенні слідової картини злочину, визначенні конкретного місця та часу вчинення протиправної дії.

Слід зазначити, що ще на стадії підготовчих дій злочинці, з моменту виникнення свого замислу, чітко вивчають обстановку та умови, в якій їм доведеться діяти. Збирають інформацію про об'єкт посягання; вивчають системи захисту, якими забезпечене комп'ютерне устаткування; реальний час несанкціонованого втручання в роботу комп'ютерних технологій, пам'ятаючи при цьому, що час не завжди пропорційний способу скоєння злочину.

Досить дискусійним серед фахівців-криміналістів залишається питання вибору місця, часу та умов реалізації злочинцем своїх намірів. Для злочинів даної категорії таким місцем може бути:

- адміністративні та службові приміщення різного типу суб'єктів господарювання (підприємств, організацій, компаній, фірм тощо), які використовують у своїй виробничій діяльності операційні комп'ютерні системи та їх периферійні устаткування;
- власні та орендовані житлові приміщення(офіси, квартири, кімнати та інше), в яких встановлені комп'ютери (комп'ютер), що забезпечені виходом до всесвітньої мережевої системи INTERNET;
- приміщення комунальної власності або ж споріднені з ними (цокольні, напівпідвальні чи ті, що примикають до житлових будинків приміщення), котрі на правах власності чи оренди можуть використовуватися під комп'ютерні клуби, INTERNET-кафе тощо.

Як показує практика, до поля зору злочинного елементу здебільшого потрапляють ті суб'єкти підприємницької діяльності, в яких є порушення виробничого процесу або не відлагоджений механізм захисту комп'ютерної інформації чи здійснений неправильний кадровий підбір спеціалістів. За таких умов, вчинення комп'ютерного злочину буде безпроблемним як зовнішнім, так і внутрішнім користувачам. До числа таких суб'єктів слід віднести:

- підприємства, організації, заклади, фірми, компанії з розширеною та бюрократизованою організаційною структурою, в якій діють сконцентровані повноваження влади і відсутня будь-яка чи будь-чия конкретна відповідальність;

- суб'єкти підприємницької діяльності, що мають високі темпи розвитку, за якими відстають функції управління. У деяких випадках самі керівники не знають, як провести ті чи інші організаційно-управлінські заходи, щоб позбавитися несанкціонованого доступу до комп'ютерної інформації;
- структури, де з огляду на різні обставини існує неналежний морально-психологічний клімат, що в остаточному підсумку впливає на розбіжність поглядів членів колективу і насамперед – керівного складу.

Стосовно часу скоєння комп'ютерного злочину, то слід наголосити, що він є конкретно визначеним:

- у період інтенсивної роботи операційних комп'ютерних систем конкретної установи;
- під час профілактичних заходів комп'ютерної системи, а також перезавантаження чи зчитування програм;
- у святкові, вихідні дні та нічні години тощо.

За допомогою комп'ютерних програм загальносистемного призначення можна встановити поточний час роботи комп'ютерної системи. Це дозволяє за відповідною командою вивести на екран дисплею комп'ютера інформацію про день, години, хвилини та секунди виконання тієї або іншої операції [67, с. 101]. За даними емпіричного дослідження У.А. Мусаєвої, час скоєння комп'ютерних злочинів становив такі показники залежно від системи допуску та розповсюдження технічних носіїв інформації:

- при безпосередньому доступі до комп'ютерної інформації, системи ЕОМ або їх мережі: у денний час – 39 %, за аналізом матеріалів кримінальних справ; у вечірній час – 8,6 %; нічний – 2,9 %; у 2,9 % час скоєння злочину не встановлений;
- при опосередкованому доступі до комп'ютерної інформації або системи ЕОМ: у вечірню пору – 11,4 % вивчених випадків; у денний

час – 8,6 %; нічний – 2,9 %; в 5,75% – час скоєння злочину не встановлений;

- при розповсюдженні технічних носіїв інформації, що містять шкідливі програми: у денний час – 15,7 % досліджених випадків; вечірнього часу – 2,9 % [154, с. 9].

Продемонстровані дані мають умовні показники і можуть змінюватися залежно від багатьох факторів, включаючи суб'єктивний. При цьому слід зважити на те, що елемент місця та часу має властивість видозмінення залежно від самої типології осіб-злочинців.

1.3.3. Способи вчинення та можливого приховування злочинів

Серед елементів криміналістичної характеристики чільне місце посідає спосіб вчинення та приховування комп'ютерних злочинів. Він несе у собі вагоме смислове навантаження як у теоретичному, так і у практичному сенсі. Аналіз відтворення способів скоєння злочинів взаємопов'язаний з результатом типових наслідків застосування того чи іншого способу та ймовірними слідами, залишеними злочинцем на місці вчинення протиправних дій.

Одним із новаторів структуризації способу умисного злочину, була Е.Д. Куранова. Вона запропонувала даний елемент розглядати як комплекс дій з підготовки, скоєння та приховування злочину, визначення винними відповідно до визначеної мети, а також тими умовами, в яких реалізувався злочинний замисел [120, с. 165 – 167]. Цю думку розширили, доповнили такі радянські вчені-криміналісти І.Ф. Герасимов, Г.Г. Зуйков, І.Ф. Пантелєєв та ін. Вони зосередили увагу на відносній стійкості способів скоєння окремих видів злочинів, а також на їх прямих залежностях відносно ступеня детермінованості з різними факторами. Сприймаючи спосіб як комплекс (систему) об'єктивно та суб'єктивно детермінованих дій з підготовки, здійснення, приховування злочину, що відповідає злочинному задуму і досягненню мети.

Точка зору авторів є слушною, але потребує уточнень. У цьому сенсі більш виваженою є позиція В.Б. Вехова, який під способами у криміналістичному значенні розуміє: «… об'єктивно та суб'єктивно обумовлену систему поведінки суб'єкта до, в момент та після скоєння злочину, котрий залишає по собі різного роду характерні сліди, які дозволяють за допомогою криміналістичних прийомів та засобів отримати картину баченого про подію, що відбулася, своєрідність злочинної поведінки правопорушника, його окремих особистих даних, а відповідно визначити найбільш оптимальні методи вирішення завдань розслідування злочинів» [44, с. 49].

Стосовно характеристики способів вчинення комп'ютерних злочинів, то досить слушні трактування навколо цього аспекту були запропоновані дослідниками: Ю.М. Батуріним, П.Д. Біленчуком, В.Б. Веховим, А.М. Жодзишським, В.В. Криловим, В.Ю. Рогозиним, Н.О. Селівановим та ін. Своєрідний підхід запропонував Ю.М. Батурін. Він систематизував способи комп'ютерних злочинів у п'ять груп, взявши за основу метод використання злочинцями конкретних дій по доступу до засобів комп'ютерної техніки. А саме:

- вилучення засобів комп'ютерної техніки;
- перехоплення інформації;
- несанкціонований доступ до засобів комп'ютерної техніки;
- маніпуляція даними і керуючими командами;
- комплексні методи [22].

Перелічені способи на достатньому рівні і досить детально були проаналізовані науковцями-криміналістами, але, незважаючи на обґрунтованість змісту цих способів вони мають суттєві зауваження, зокрема:

1. Автор та його однодумці класифікують не способи скоєння комп'ютерних злочинів, а способи протиправних дій, що тим чи іншим чином пов'язані з комп'ютерними технологіями.
2. Поданий вище перелік способів скоєння комп'ютерних злочинів відтворює не повний характеристику навіть і основних ознак.

Як зазначав Р.С. Бєлкін: «Голе описання способу скоєння злочину не досягає мети, його необхідно проводити або від слідів застосування цього способу з тим, щоб за ними розкривати механізм злочину, або до слідів застосування даного способу, щоб знаючи його, зуміти виявити докази скоєного злочину й встановити особу злочинця» [25, с. 314].

Способи скоєння комп'ютерних злочинів та його окремих видів мають поділятися на три групи:

- способи безпосереднього доступу до комп'ютерних технологій (операційної системи) та комп'ютерної інформації;
- способи видаленого (опосередкованого) доступу;
- способи виготовлення, розповсюдження на технічних носіях шкідливих програм для ЕОМ.

Способи безпосереднього доступу до комп'ютерних технологій (операційної системи) та комп'ютерної інформації, пов'язані з діями злочинців по знищенню, блокуванню, копіюванню комп'ютерної інформації. Можливий варіант порушення роботи іншого комп'ютерного устаткування чи комп'ютерної мережі шляхом видачі відповідних команд з комп'ютера, у пам'яті якого є розроблений план протиправних дій. Зазначений спосіб має найбільш розповсюджений характер застосування у злочинах, пов'язаних з «білокомірцевою злочинністю». Серед цієї категорії злочинів першість посідають особи, що безпосередньо задіяні у виробничому процесі: програмісти, інженери, оператори та ін.

Способи видаленого (опосередкованого) доступу до комп'ютерної інформації знаходиться не в прямому зв'язку з іншим комп'ютером (мережевим сервером) і наявною на ньому інформацією. Такий зв'язок може бути здійснений лише за допомогою локальних мереж або ж глобальних систем типу INTERNET. Сюди можна віднести:

- підключення до лінії зв'язку законного користувача, а також забезпечення доступу до його телекомунікаційної системи;

- проникнення в чужі інформаційні мережі шляхом автоматичного підбору абонентських номерів з подальшим приєднанням до інших комп'ютерних систем;
- проникнення в іншу комп'ютерну мережу під виглядом законного користувача, використавши при цьому чужі коди та паролі [53, с. 18–21].

Способи виготовлення, розповсюдження на технічних носіях шкідливих програм для ЕОМ. Сюди відносимо створення (написання) несанкціонованих, вірусних програм, які призводять до шкідливих та небезпечних наслідків. Різновид та кількість таких комп'ютерних програм обчислюється десятками тисяч варіантів, і вони модифікуються залежно від категорії осіб, які їх створюють і на який суб'єкт вони розраховані. Стосовно способу написання цих протиправних програм, то їх теж налічується досить велика кількість і їх можна скомпонувати в кілька груп за місцем виготовлення:

1. Створення шкідливої комп'ютерної програми здійснюється на одному з робочих місць автоматизованої інформаційної системи в організації або на ПЕОМ, що є власністю зловмисника.
2. Створення шкідливої програми може здійснюватися поза сферою безпосередньої діяльності комп'ютерної системи, для впливу на яку вона призначена.
3. Шкідлива комп'ютерна програма створюється шляхом внесення змін до існуючої комп'ютерної програми [178, с. 46 – 47].

Розповсюдження програм-вірусів здійснюється, здебільшого, шляхом інформаційного обміну даними каналами INTERNET, або ж через лазерні комп'ютерні диски чи гнучкі дискети. Виявлення зазначених несанкціонованих програм можна шляхом:

а) оперативно-розшукових заходів;

б) аудиторської перевірки;

в) фінансово-бухгалтерської перевірки;

г) інших джерел доказового значення (журналів обліку, протоколів слідчих дій, окремих документів-програм, матеріальних слідів).

Не менш шкідливим та складним є спосіб виготовлення на технічних носіях піратських програм для користувачів операційних комп'ютерних систем. Такі протиправні програми виготовляються в основному на лазерних дисках за умови кустарного виробництва. Їх продаж здійснюється торговцями підпільного програмного забезпечення в малолюдних або ж багатолюдних місцях: метрополітені, ринках, комп'ютерних клубах, у місцях проводження часу молоді, окрім спеціально відведеної торговельної мережі. Шкідливість та небезпечність цієї продукції полягає в наступному:

- під виглядом власної програми продається чужа, викрадена у розробника, продукція;
- підпільна продукція придбана за здешевлену ціну ніж ліцензована, може містити в собі не ту інформацію, на яку розраховував покупець, а тому законодавчо позбавлений права захисту споживача;
- інформація на диску підпільного виготовлення може мати зміст скеровування до дії по зламуванню кодів, паролів операційних систем, а також програм по блокуванню, маніпуляції, підміни даних тощо;
- під виглядом різнопланових ігор може містити: порнографічну інформацію, насилля, вандалізм, расову дискримінацію тощо, не виключаючи при цьому прихованих вірусів, що проявлять себе у подальшому.

Важливу роль у виборі правильної тактики слідчого по збиранню інформації розшукового характеру відіграють знання способу приховування того чи іншого злочину цієї категорії. Він завжди знаходиться у взаємозв'язку з іншими структурними елементами і, безпосередньо, розглядається на одній паралелі зі способом скоєння злочину. Одним з перших сформулював поняття способу приховування злочину Б.В. Лисиченко. Він запропонував цей елемент розглядати як «…комплекс дій, спрямований на приховування злочину з

метою уникнути відповідальності за скоєне» [139, с. 48]. Більш розгорнуто виклав свою точку зору В.П. Лавров: «Спосіб приховування злочину – це комплекс (сукупність) умисних дій злочинця та інших осіб, направлених на протидію встановлення компетентними органами обставин, що мають значення для розкриття і розслідування злочинів» [135, с. 39].На думку Р.С. Бєлкіна, – це діяльність (елемент злочинної діяльності), спрямований на перешкоджання розслідування шляхом приховування, знищення, маскування або підроблення слідів злочину і злочинця та їх носіїв [27, с. 130]. Таке визначення може стосуватися будь-якої категорії злочинів, у тому числі й комп'ютерних. Своє бачення в цьому аспекті запропонував Ю.В. Гаврилін. Він зазначив, що сутність способу приховування злочину зводиться до відтворення обстановки, яка передувала злочину, тобто знищенню залишених слідів (слідів пальців рук, слідів взуття, мікрочасток тощо) [53, с. 27]. Спосіб приховування комп'ютерного злочину може розглядатися у контексті з способами протидії розслідуванню справ про злочин. Одночасно другий слугує складовим елементом способу здійснення злочину або ж є самостійною системою дій. Його можна визначити як таку діяльність злочинців і пов'язаних з ними осіб, що заважають і ускладнюють роботу правоохоронних органів у розкритті та розслідуванні конкретних злочинів. Протидія розслідуванню – це умисна діяльність, яку спрямовано на будь-яку перешкоду процесу розслідування злочинної діяльності і встановлення істини [87, с. 29]. Але враховуючи, що способи приховування охоплюють більш широке поняття і несуть у собі основне інформаційне навантаження, детальніше зупинимося саме на них. Способи приховування комп'ютерних злочинів мають деяку відмінність від «традиційних». Зокрема, комп'ютерні злочинці деякою мірою легковажно відносяться до способів приховування своєї злочинної діяльності, мотивуючи це наступним:

- основу своїх практичних знань та здібностей у керуванні INTERN0ET-технологіями ставлять вище за знання фахівців правоохоронних органів у цій сфері;

- впевнені, що ті чи інші залишені ними сліди мають тимчасовий характер або ж як такі, що взагалі відсутні;
- мала ймовірність у системі доказування у відшуканні тих речових доказів, що б аргументовано доводили доказове значення.

Ці аспекти притаманні лише комп'ютерним злочинам. У цілому, зазначений спосіб скоєння та приховування комп'ютерних злочинів зберігає сформовану структуру, що й «традиційні». І.М. Лузгін акцентував: «…це – ситуаційно повторюване явище, детермінованих низкою суб'єктивних та об'єктивних факторів, де найважливішим з них є умисел і пов'язані з ними мета і мотиви » [141, с. 17–18]. Отже, можемо стверджувати, що злочинець разом із способом скоєння протиправних дій вкладає, як один з складових елементу, спосіб його приховування, з метою уникнення від покарання, однак не завжди це йому вдається. Доречною у цьому сенсі є думка В.М. Карагодіна: «Всі сліди злочину виявляються внаслідок того, що суб'єкт, реалізовуючи спосіб приховування не придав їм особливого значення» [99, с. 24]. При цьому слід чітко усвідомити, що спосіб приховування – це загальнозбудована модель, за якої злочинний елемент знаходить свій індивідуальний шлях її реалізації. Існує у криміналістиці багато класифікацій способів приховування злочинів, але найбільш вдалою, у випадку з комп'ютерними злочинами є визначена Р.С. Бєлкіним. Автор пропонує розглядати це через такі групи:

- приховування злочину шляхом знищення інформації або її носіїв;
- приховування злочину шляхом маскування інформації або її носіїв;
- приховування злочину шляхом підробки інформації або її носіїв;
- змішані способи (інсценування) [25, с. 364].

Запропонований перелік є виваженим та ґрунтовним, але не вичерпним. Його можна доповнити й іншими способами приховування злочинів безпосереднього доступу до інформаційних технологій. А саме:

- відновлення нормальної роботи операційної системи та окремих програм;

- маскування, підроблення та приховування технічних носіїв з викраденою комп'ютерною інформацією, а також самої інформації;
- маскування зовнішності тощо.

Розглянуті вище способи приховування злочинів можуть використовуватися при розслідуванні протиправних дій у цій сфері. Але при цьому слід врахувати причинно-наслідкові зв'язки з конкретними процесами і матеріальними об'єктами та їх ознаками й іншими носіями інформації, які мають відношення до справи.

1.3.4. Слідова картина злочинів

Скоєння особою протиправних дій, пов'язаних з використанням комп'ютерних технологій спричиняє виникнення певної кількості слідів у тому числі і специфічних, притаманних лише зазначеній категорії злочинів. Використання цих інформаційних даних при розслідуванні злочинів є необхідною умовою забезпечення всебічного, повного й об'єктивного дослідження обставин справи. Д.О. Турчин писав: «Використання слідів з метою розкриття злочину згодом стало найбільш надійним методом боротьби із злочинністю з боку державних органів, тому законодавці різних країн закріплюють у правових нормах поняття «слід» як обов'язкову умову під час доказування деяких видів злочинів» [204, с. 7]. Під такою системою розуміємо інформаційні дані про місцезнаходження слідів, їх видовій характеристиці, та засобах, що дають можливість їх виявлення, фіксацію, вилучення і збереження з метою подальшого дослідження. За С.М. Потаповим, це: «…сліди-відображення на матеріальних предметах ознак явищ, які причинно пов'язані з розслідуваною подією» [170, с. 30].

У юридичній літературі поділ слідів визначають як матеріальні та ідеальні, які у свою чергу відображають дві сторони: інформаційну і доказову. Стосовно інформаційного боку слідів виваженою є точка зору В.Я. Колдіна, який зазначив: «сліди злочину в широкому розумінні, тобто різноманітні зміни обстановки в результаті злочину, і утворюють ту інформацію, яка може бути використана для встановлення об'єктів, пов'язаних з розслідуванням подій»

[110, с. 131]. Сліди у вузькому значенні – це матеріальні утворення, що відображують зовнішню будову взаємодіючих об'єктів (відбиття поверхневої будови одного предмета на іншому), тобто сліди-копії. Вони можуть бути об'ємними або площинними [183, с. 141 – 148]. Переносячи акцент дослідження на комп'ютерні злочини, слід зазначити, що матеріальні сліди цих злочинів мають опосередкований характер, адже їх присутність не завжди має яскраво виражений характер, а тому часто-густо відсутні дані про місце, звідки було вчинено злочин, але відоме місце настання протиправних наслідків. Проте це не означає, що матеріальних слідів немає взагалі. Насамперед вони залишаються на ЕОМ (комп'ютерних) магнітних носіях інформації і відображають зміни даних інформації, що зберігається (порівняно з вихідним станом). Йдеться про сліди модифікації баз даних, програм, текстових файлів на твердих дисках, дискетах, магнітних стрічках, лазерних і магнітооптичних дисках [210, с. 65]. Таким чином, про їх наявність можемо говорити лише як про нонвербальну інформацію події, яка утворилася в процесі його вчинення, так звану слідову картину злочину.

Встановити механізм вчинення протиправної дії, як один з варіантів, можна за умови сприяння працюючого з комп'ютерними системами персоналу в установі, де відбувся злочин, та й то не завжди. Здебільшого може йтися не про матеріальні, а про ідеальні сліди відображення. Адміністрація володіє інформацією про всіх працівників структури, систем допуску, контролю та персонального складу, допущеного до роботи з комп'ютерними мережами. Оперує даними про нештатні ситуації функціонування обчислювальної техніки та технологічних управлінських процесах, що в кінцевому результаті спрямує слідство на правильний шлях розслідування справи. Таким чином, слідову картину злочину можна розглядати як сукупність абстрагованої інформації про типові матеріальні й ідеальні сліди-ознаки та умови скоєння суб'єктом протиправних дій з використанням комп'ютерних технологій. Разом з тим, слід наголосити, слідові картину утворюють обставини і сліди події злочину. Виявлення їх, аналіз, встановлення причинних зв'язків дозволяють побудувати

картину події, сформувати уявні або дійсні моделі злочину, механізм його вчинення. Дослідження таких слідів і речових доказів може вказати на особу злочинця, потерпілого та обставини події, виявити негативні обставини, сліди приховування злочину [177, с. 395].

1. *«Слідова картина» незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку*

Має досить розповсюджений характер і супроводжується дією у вигляді несанкціонованого втручання в роботу ЕОМ (комп'ютерів) та іншого автоматизованого, операційного науково-технічного оснащення чи мереж електрозв'язку, що призводить до перекручення, спотворення процесу обробки електронних даних або знищенням комп'ютерної інформації чи її носіїв, витоку, підробки та порушення встановленого порядку маршрутизації інформації. Відповідною слідовою картиною злочинів цієї категорії є зміни, що відбулися у самій системі, окремому файлі, документі тощо. Зокрема:

- знищення, модифікація чи заміна каталогів, файлів тощо;
- зміна первинних даних каталогів і файлів, дати та часу їх створення;
- зміну розміру документа;
- появи нових даних, заставок, картинок та ін.;
- не спрацювання або уповільнення роботи окремо взятої програми;
- порушення послідовності їх функціонування тощо.

Відповідно до залишених злочинцем слідів можна встановити час і спосіб вчинення протиправної дії; внутрішньо чи зовнішньо відбулися несанкціоновані дії; локальною чи периферійно. Шляхом перегляду електронних журналів реєстрації доступу до операційної комп'ютерної системи встановити ймовірне місце звідки було вчинено злочин. Залежно від того, чи співпадає місце скоєння злочину з місцем настання шкідливих або ж небезпечних наслідків, можемо говорити про присутність матеріальних та ідеальних слідів відображення.

2. «Слідова картина» створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут

Наявність такої слідової картини характеризується наступними альтернативними діями у вигляді:

- створення шкідливих програм чи технічних засобів, призначених для несанкціонованого втручання в роботу ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку;
- розповсюдження таких програмних чи технічних засобів;
- збут вказаних програмних чи технічних засобів.

За умови встановлення такої слідової картини злочину, необхідно звернути увагу на те, що являє собою шкідлива програма чи технічний засіб. Які його властивості і якості. Адже мова йде про комп'ютерні програми, засоби, віруси, які здатні під дією активованих комп'ютерних мереж адаптуватися до іншого комп'ютерного середовища чи мережі електрозв'язку. Такі паразитичні програми керуються прихованими інструкціями, командами до несанкціонованої дії за сприятливої умови або часового фактору. Вони можуть виражатися у вигляді певних символів, кодів, цифр, схем, малюнків, ігор тощо. Необережне чи питливе звернення користувача до перелічених даних викликає запуск замаскованої шкідливої, в тому числі і небезпечної програми. Вона в свою чергу здатна на між файлове і каталогове курсування по всі операційній комп'ютерній системі, шляхом маршрутизації здійснювати свої приховані копії, а разом з тим виконувати дії по зміні, знищенню, пошкодженню, блокуванню електронної інформації, у тому числі й тієї, яка передається каналами мереж електрозв'язку.

Виготовлення та збут зазначених вище програм має свою конкретно направлену мету і виражається у прямому умислі суб'єкта злочину. А саме у:

- несанкціонованому втручанні в роботу ЕОМ, АС, комп'ютерних мереж чи мереж електрозв'язку;
- застосуванні шкідливих програм чи технічних засобів за призначенням;

- отриманні бажаного результату дії шляхом збуту шкідливих чи небезпечних, спеціально-створених технічних засобів, програм тощо.

3. «Слідова картина» несанкціонованого збуту або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації

У цьому випадку йдеться про сліди-відображення, які вказують на те, що протиправна дія відбулася з комп'ютерною інформацією, яка містилася на електронних носіях, тобто жорстких магнітних дисках, що є частиною системного устаткування (блоку) електронно-обчислювальних машин, шляхом впливу на її через спеціальні технічні пристрої, а також з використанням інших носіїв електронної інформації, зокрема: флеш-дисків, оптичних (компакт-дисків), магнітних дисків (дискет) та ін. Це інформаційні дані автоматизованих систем, відповідних комп'ютеризованих систем, які містять в собі конфіденційну у тому числі і таємну інформацію. До переліку конфіденційної інформації віднесено:

- відомості, які перебувають на електронних носіях автоматизованих систем ЕОМ (комп'ютерів) і знаходяться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб;
- відомості громадян, а також юридичних осіб, які віднесені до категорії конфіденційної інформації і на власний розсуд визначають систему захисту такої інформації та осіб, які мають режим доступу до неї;
- деякі відомості держави, які перебувають у користуванні органів державної влади, муніципальних органів, установ, підприємств, організацій за винятком конфіденційної інформації доступ до якої обмежений законодавством України.

До переліку таємної інформації віднесено:

- відомості, які становлять державну та іншу передбачену законом таємницю (військову, банківську, медичну (лікарську), комерційну тощо);

- будь-яку іншу таємну інформацію, що може завдати шкоди особі, суспільству, державі – режим доступу до таємної інформації, в тому числі і в автоматизованих комп'ютерних системах, встановлюється законом.

Оскільки такі комп'ютерні інформаційні дані мають обмежений доступ користувачів, то вони наділені правом захисту відповідно до чинного законодавства, зокрема: ст.428 Закону України «Про державну таємницю» від 21.09.1999 р., ст.30 Закону України «Про інформацію» від 03.04.2003 р. та ін. нормативно-правових актах.

Характер такої слідової картини злочину буде виражатися у:

- незаконному заволодінні та несанкціонованому розповсюдженні перерахованої вище комп'ютерної інформації без згоди на те власника;
- несанкціонованій передачі права володіти комп'ютерними даними іншій особі, зацікавленій стороні або розголошенні відомостей, що носять характер конфіденційної чи таємної інформації.
- несанкціонованому збуту конфіденційної чи таємної комп'ютерної інформації чи розповсюдження таких даних, що мають обмежений доступ до неї, шляхом оплатної або іншої зацікавленої дії.

4. «Слідова картина» несанкціонованих дій з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчиненої особою, яка має право доступу до неї

Дана слідові картина вчиненого злочину має специфічну направленість, оскільки поєднує в собі два напрямки об'єктивної сторони:

- по-перше, зміну, знищення чи блокування комп'ютерної інформації, яка знаходиться та піддається обробці в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах;
- по-друге, перехоплення, копіювання та витік комп'ютерних інформаційних даних без згоди на те добросовісного власника програмного продукту.

Ще однією особливістю цієї слідової карти події є сам суб'єкт злочину – він спеціальний. Тобто особа, яка перебуває на праві трудових правовідносин

чи договору або інших юридичних підстав, має безпосередній доступ до конкретного програмного забезпечення, чи відповідних комп'ютерних даних, і в силу своїх службових (функціональних) повноважень (обов'язків), може оперувати певною інформацією власника або уповноваженої її особи. Однак, в силу тих, чи інших обставин, здійснює несанкціоновані дії з комп'ютерною інформацією не маючи при тому ні дійсного, ні передбачуваного права на таку діяльність. Здійснюючи такі дії, особа злочинця усвідомлює настання протиправних наслідків але від поставленої перед собою мети не відмовляється. Хоч іноді може імітувати таку діяльність з оброблювальною комп'ютерною інформацією як автоматичний збій ЕОМ (комп'ютерної) системи. Результат такого злочинного несанкціонованого втручання в інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчиненої особою, яка має право доступу до неї, призводить до того, що власник позбавляється цих даних частково, повністю або електронна інформація шляхом її копіювання знаходить свій виток як обов'язковий наслідок цього злочину.

5. «Слідова картина» порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється

Зазначена слідові картина події злочину, як і інші подібні їй, пов'язані використанням комп'ютерних технологій, вирізняється своєю індивідуальністю, і в деякій мірі не повторюваністю. Вона має окремі елементи схожості з попередньо розглянутою слідовою картиною (див.1. «Слідова картина» незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку), але ця схожість є лише зовнішньою ознакою на відміну від внутрішнього її змісту.

Спеціальним є суб'єкт злочину, оскільки він відповідає за експлуатацію ЕОМ, автоматизованих систем, комп'ютерних мереж, мереж електрозв'язку чи повинен здійснювати правила захисту інформації, яка в них обробляється у межах своїх повноважень, але допустив умисно чи необережно протиправність дій, що завдало значну шкоду власникові.

Дана слідові картина злочину характеризуватиметься такими ознаками:

- по-перше, суспільно-небезпечними діяннями (діями чи бездіяльністю) визначеними самою слідовою картиною злочину;
- по-друге, суспільно-небезпечними наслідками у вигляді значної заподіяної шкоди, спричиненої дією чи бездіяльністю
- по-третє, самим причинним зв'язком між суспільно-небезпечними діяннями та суспільно-небезпечними наслідками.

Результатом порушення правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється може бути: викрадення, копіювання, втрата повна чи часткова електронних даних, модифікування, блокування інформації, підробка в тому числі й порушення встановленого порядку її маршрутизації.

Таку слідові картину події злочину можна розглядати з двох позицій. По-перше як:

- халатне ставлення особою до своїх функціональних обов'язків, що виражалося в невиконанні або неналежному виконанні встановлених нормативно-правовими актами вимог (організаційних чи технічних) захисту інформації, що обробляється в автоматизованих системах;
- недостатність знань особи у сфері комп'ютерних технологій, що привело до порушення правил зазначених вище автоматизованих систем і спричинило значну шкоду її власникові;
- підривна діяльність з боку особи, яка б мала належним чином виконувати покладені на неї зобов'язання в межах своїх функціональних обов'язків.

Виходячи з матеріальних та ідеальних слідів-відображень, можна встановити реальну картину того, що відбулося. Зокрема, за місцем, часом і об'ємом настання негативних наслідків; за шкідливістю і небезпечністю даної протиправної дії; за її спрямованістю.

У другому варіанті слідову картину необхідно трактувати як:

- цілеспрямовану протиправну дію особи з чітко вираженою метою (наживою, помстою, заздрістю, самовираженням та ін.);
- цікавістю та допитливістю, що як результат спричинило нанесення значної шкоди або ж небезпечних наслідків її власникові;
- психічною неврівноваженістю, інформаційною блокадою, дратівливістю суб'єкта злочину;
- хуліганських намірів у поєднанні зі зухвальством тощо.

За такої ситуації необхідно системно дослідити наявні сліди протиправності, які прямо чи опосередковано вказують на причетність до злочину тієї чи іншої особи. Дослідженню підлягають: електронні програми реєстрації, доступу, допуску та протоколювання; електронні журнали обліку введення токенів, кодів, паролів; часу початку та завершення роботи; фіксацію конкретного каталогу, файла, програми, з якими проводилася робота і яка саме та ін. Це дасть можливість фахівцям правоохоронних органів за сприяння спеціалістів у сфері комп'ютерних технологій та громадськості швидше зорієнтуватися у напрямі розслідування визначеного такою слідовою картиною події злочину.

6. «Слідова картина» перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку

Така слідові картина злочину має специфічний характер події, що відбулася. Оскільки доволі важко встановити протиправних намірів (фізичних та юридичних) осіб, які за допомогою комп'ютерних мереж, з

використанням електронної пошти, здійснюють розсилку, копіювання повідомлень, що в переважній більшості носять рекламний або інформаційний зміст. Особливістю такої протиправності дій полягає у односторонньому прийнятті рішення провайдерів чи окремих осіб здійснювати електронну передачу даних поза волею та бажанням іншої сторони. Така несанкціонована діяльність осіб, компаній, підприємств, установ тощо, може спричинити до непередбачуваних наслідків об'єктивної сторони, яка виражатиметься у:

- суспільно-небезпечних діях у вигляді масового розповсюдження різного змісту повідомлень каналами мереж електрозв'язку здійсненими певними суб'єктами без попередньої на те згоди адресата, що створює для другої сторони небажані результати;
- суспільно-небезпечних наслідків для власника комп'ютерного програмного забезпечення, оскільки його технічне оснащення виконує дії з порушенням роботи ЕОМ, АС, що виражається у технологічних збоях параметрів процесу обробки, передачі, перекручення чи зміни електронної інформації машинних носіїв, мереж чи мереж електрозв'язку;
- причинним зв'язком викликаним такими діями та протиправними наслідками, які виражаються у припиненні роботи зазначених вище систем чи мереж, що спричиняє значну шкоду її власникові і підпадає під дію злочинного діяння.

За такої слідової картини події доволі важко встановити яка саме інформація, повідомлення, реклама могла викликати порушення чи припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку і чи не містила вона в собі певні паразитичні програми, команди тощо, у зв'язку з її масовим тиражуванням та пересилкою, оскільки не виключений варіант того, що її могли змінити (навмисно чи випадково) під час адресації або вона самомодифікувалася у процесі руху INTERNET-мережею.

1.3.5. Особа злочинця та особа потерпілого

Центральне місце у системі криміналістичної характеристики комп'ютерних злочинів відводиться особі злочинця. Конкретному аналізу підлягають: стать, вік, приналежність, професія, психічні, психологічні, фізичні та інші якості ймовірного злочинця. Для криміналістики першочерговими є дані професійних звичок злочинців, які проявляються у певних способах, методах та прийомах. Дослідження «почерку» злочинця, тобто індивідуальної особливості скоєння злочину, та залишення по собі відповідних слідів.

Необхідно розмежовувати дві категорії суб'єктів, які мають відношення до протиправних дій даного напряму:

- невиявлені або невідомі;
- виявлені або відомі.

Невиявлені або невідомі – це та категорія осіб, що полишає по собі відповідні сліди скоєного, але тимчасово знаходиться поза увагою фахівців правоохоронних органів. Дані про них мають загальний характер. Разом з матеріальними слідами злочинів можливі варіанти присутності й ідеальних слідів, залишених у пам'яті свідків, потерпілих, сторонніх осіб. За цієї умови слід підключати статистичні дані всіх суб'єктів, які мають чи мали відношення до комп'ютерної злочинності. Їх інформація та знання INTERNET - технологій можуть сприяти у розслідуванні кримінальної справи.

Виявлені або відомі – це особи, що здійснили протиправну дію і дані про них відомі правоохоронцям чи іншим особам. Їх діяльність знаходиться у полі зору з метою встановлення поведінки суб'єкта, його зв'язків з іншими суб'єктами. Або ж протиправна дія припинена і особа затримана в якості підозрюваного чи обвинуваченого. Слід відзначити, що особлива увага повинна приділятися вивченню портрета особи злочинця, встановлення з ним психологічного контакту, з метою виявлення можливих співучасників скоєного і встановлення істини по справі. Необхідно створити також сприятливі умови безконфліктного ведення справи, а бо ж спонукати причетних до вчинення злочину осіб до щиросердного зізнання у справі. Досить вдало це зазначили Г.М. Бірюков, Ю.М. Кривонос, М.І. Шилан. Автори

доводять, що: «Характеризуючи осіб, які скоюють комп'ютерні злочини, необхідно вказати на їх основну ознаку, а вона полягає в тому, що такі злочини вчиняє широкий діапазон осіб – від висококваліфікованих спеціалістів до дилетантів» [211, с. 39]. Як показує вітчизняна та зарубіжна практика, в коло злочинців втягнуті особи різного інтелектуального рівня розвитку, різних спеціальностей та професій. Вік осіб, причетних до комп'ютерних злочинів, становить від 15 до 45 років. За матеріалами експертних досліджень визнається, що на момент протиправних дій вік 33 % злочинців не перевищував 20 років; 13 % – були старші 40 років; 54 % мали вік від 20 до 40 років [44, с. 36].

Стосовно інтелектуального розвитку цих осіб, то фахівці подають такі дані:

- 77 % злочинців, які вчинили комп'ютерний злочин, мали середній рівень інтелектуального розвитку, 21 % – вищий від середнього і лише 2 % – нижчий від середнього. При цьому 20 % мали середню освіту, 20 % середню спеціальну і 40 % – вищу [94, с. 369].

Як зазначають далі дослідники, діапазон рівня спеціальної освіти відомих правопорушників достатньо широкий – від мінімальних знань у цій сфері, до високопрофесійних знань своєї справи:

- 52 % злочинців мали спеціальну підготовку в галузі автоматизованої обробки інформації;
- 97 % були службовцями державних установ і організацій, які використовували комп'ютерні системи і інформаційні технології у своїх виробничих процесах;
- 30 % мали безпосереднє відношення до експлуатації засобів комп'ютерної техніки [33, с. 369].

З дослідницької точки зору цікавим є той факт, що з кожної тисячі комп'ютерних злочинів, лише сім вчинені професійними програмістами. В окремих випадках особи вчиняли такі протиправні дії, взагалі не маючи технічного досвіду. Досить цікавим є питання статевої приналежності особи

злочинця. Доля участі чоловіків та жінок у комп'ютерних злочинах наближено має відповідну пропорцію з деяким відсотком переважування на бік сильної статі. Але за критерієм злочинності та агресивності у своїх діях значну перевагу отримують чоловіки. Жіноча злочинність більш продумана, чіткіше спланована, складніша у сприйнятті та розслідуванні. Залежно від напрямів діяльності, вчені-криміналісти здійснювали кілька підходів до визначення типології осіб у такої категорії злочинності. В.В. Крилов згрупував такі категорії:

- особи у групі за попереднім зговором або організованій групі;
- особи, що здійснюють неправомірний доступ до комп'ютерної інформації з використанням свого службового становища;
- особи, що мають доступ до ЕОМ, але здійснюють неправомірний доступ до комп'ютерної інформації або порушують правила експлуатації на ЕОМ;
- особи, які створюють, використовують та розповсюджують шкідливі програми [124, с. 64].

В.Б. Вехов свою увагу зосередив на наступних категоріях комп'ютерних злочинців:

- особи, які вирізняються з-поміж інших злочинців стійким поєднанням професіоналізму в галузі комп'ютерної техніки та програмування з елементами своєрідного фанатизму і винахідливості;
- особи, що страждають новим видом психічних захворювань – інформаційними хворобами чи комп'ютерними фобіями;
- професійні комп'ютерні злочинці з яскраво вираженими корисними цілями [44, с. 31 – 40].

У юридичній літературі дослідники таких осіб визначають як:

- порушники правил користування електронно-обчислювальними машинами;
- «білі комірці»;
- «комп'ютерні шпигуни»;

- «хакери» або «одержимі програмісти» [34].

Найбільш загальноприйнятою залишається класифікація за редакцією В.Б. Вехова. На посиланнях до даного науковця більшість авторів будують свої розробки та публікації. Цієї думки дотримується автор, але при цьому не відкидає точку зору ще одного фахівця у сфері дослідження злочинів з комп'ютерними технологіями Ю.В. Гавриліна. Під категорією злочинних елементів цього напряму він розуміє:

1) осіб, які перебувають у трудових відносинах з підприємством, організацією, закладом, фірмою або компанією, де скоєний злочин (за цими даними, вони становлять більше 55 %), а саме:
   - які безпосередньо займаються обслуговуванням ЕОМ (оператори, програмісти, інженери, персонал, що здійснює технічне обслуговування і ремонт комп'ютерних систем або обслуговуючий персонал комп'ютерної мережі);
   - користувачі ЕОМ, що мають визначену підготовку та вільний доступ до комп'ютерної мережі;
   - адміністративно-управляючий персонал (керівники, бухгалтери, економісти).
2) громадяни, які не перебувають у правовідносинах з підприємством, організацією, закладом, фірмою чи компанією, де скоєно злочин (близько 45 %). Ними можуть бути:
   - особи, що займаються перевіркою фінансово-господарської діяльності підприємства та ін.;
   - користувачі та обслуговуючий персонал ЕОМ інших підприємств, що пов'язані з комп'ютерними мережами підприємства, на якому скоєно злочин;
   - особи, які мають у своєму користуванні комп'ютерну техніку (у тому числі володарі персональних ЕОМ, що отримали доступ до телекомунікаційних комп'ютерних мереж) [53, с. 38].

Подана класифікація не є вичерпною. Її можна доповнювати, видозмінювати, розширювати, з чимось погоджуватися, щось відкидати тощо. Так, наприклад, коло осіб, що скоюють комп'ютерний злочин Ю.В. Гаврилін, більш характеризує не загальну класифікацію суб'єктів, а категорії осіб, які мають доступ до засобів комп'ютерної техніки. Тобто, в полі зору знаходяться внутрішні користувачі програмного забезпечення і обслуговуючий його персонал та зовнішні користувачі, які тим чи іншим чином мають причетність до операційної комп'ютерної системи. При цьому не розглядається інша категорія осіб, що здійснює несанкціонований протиправний доступ до ЕОМ, АС мереж чи мереж зв'язку. Ті ж самі програмісти-любителі, професіонали-хакери і їх різновиди, хворі та психічно-неврівноважені особи тощо. Хоча, деякою мірою можна погодитися з автором, на долю саме внутрішніх злочинців, як свідчить статистика США, припадає близько 80 % всіх злочинів [113, с. 4]. Такої самої думки дотримується і частина російських дослідників. Прикладом можуть служити лише деякі особливості скоєння злочинів у фінансовій сфері:

- більшість злочинців – клерки, проте вищий персонал банку також може скоювати злочини і нанести установі значно більшого збитку, хоча такого роду випадки відбуваються набагато рідше;
- як правило, злочинці використовують свої власні рахунки, на які переводять викрадені суми;
- більшість злочинців не знають, як «відмити» викрадені гроші; вміння скоювати злочин і вміння отримувати гроші – це не одне й те саме;
- комп'ютерні злочини не завжди високотехнологічні, ряд злочинних дій достатньо простий і може бути скоєний обслуговуючим персоналом;
- багато злочинців пояснюють свої дії тим, що вони лише беруть у банка гроші в борг з подальшим їх поверненням, але, як правило, це не відбувається [112, с. 166].

1.3.6. Мета і мотиви вчинення злочину

Корисну інформацію при дослідженні особи злочинця визначають *мотиви та мета* вчинення протиправної дії. Мотив – усвідомлена підстава, обумовлене бажання досягти конкретно визначеної мети. Він тісно пов'язаний з виною, але не співпадає з нею. Впливаючи на свідомість людини, мотив формує спрямованість його волі, обумовлює характер його дії [70, с. 84].

Слід погодитися з позицією окремих вчених, що мотив та мета скоєння злочину пов'язані із соціально-психологічною та криміналістичною характеристиками особи злочинця. Вони входять до групи суб'єктивних факторів і таким чином здійснюють вплив на вибір засобів та прийомів досягнення цілей. А, отже, визначають характер основних дій злочинця, спосіб скоєння злочину, який включає у себе відповідний комплекс вольових дій людини і є головним аспектом будь-якого злочинного посягання. Вони в деяких випадках є необхідною ознакою суб'єктивної сторони умисних комп'ютерних злочинів. Прикладом тому може бути особа злочинця, яка свідомо йшла на здійснення протиправних дій, покладаючи в основу корисний мотив, а також зловживання владою чи службовим становищем, досягаючи мети викраденням ЕОМ (комп'ютерних) даних шляхом несанкціонованого доступу до засобів комп'ютерної техніки. Але однозначно слід зазначити, що мотиви та мета інших злочинів є необхідним елементом суб'єктивної сторони, буде не правильним, оскільки вони є факультативною ознакою кримінально-правової характеристики. Хоча в усіх випадках при розслідуванні цієї категорії злочинів такі елементи повинні бути встановлені відносно ступеня небезпечності вчиненого. Дані про мотиви та мету скоєння комп'ютерного злочину обов'язково будуть використані при висуванні слідчих версій стосовно суб'єкта та суб'єктивної сторони протиправної дії, а також при організації пошуку злочинця. Піддаючи аналізу світову та вітчизняну практику розкриття та розслідування злочинів даної категорії, можна всі мотиви та мету побудувати у такій відповідності:

1) корисливі – на долю яких припадає близько 66 % злочинів (скоюють переважно професіонали вищого ґатунку);
2) політичні –17 % шпигування, злочини спрямовані на підрив фінансової та грошово-кредитної політики, підрив ринкових відносин вчиняють ті самі професіонали;
3) зацікавленість – 7 % (студенти та професійні програмісти);
4) хуліганські наміри – 5 % (хакери та їх різновиди у поєднанні з професіоналами вищого ґатунку;
5) помста – 5 % (професійні злочинці та психічно неврівноважені особи) [114, с. 5 – 10].

Запропонована вище вченими-криміналістами класифікація заслуговує на увагу, однак, хотіли б дещо доповнити та уточнити по окремих позиціях. Аналізуючи корисливі наміри злочинців, слід зазначити, що це найбільш розповсюджена і найскладніша категорія. До її числа входять кілька протиправних напрямів. Скажімо, до сфери комп'ютерних злочинів віднесені діяння, пов'язані з розповсюдженням шкідливих програм. На їх долю припадає близько 20 % всіх злочинів де основою були корисливі наміри. Рідше злочини такого характеру базувалися на отриманні безвідплатного програмного забезпечення 7,1 % або подальшого продажу викраденого програмного забезпечення чи іншої інформації 5,7 %. Певний відсоток злочинців переслідують мету долучитися до всесвітньої мережі INTERNET через канали незаконно здійсненого доступу до системних комунікацій компаній провайдерів, з метою уникнення оплати, за використаний ними інформаційний час. Прикладом тому є кримінальна справа, порушена прокуратурою м. Чернігова у зв'язку із зверненням клієнтів провайдерської компанії ЗАТ «Синет» до Управління по боротьбі з організованою злочинністю УМВС у Чернігівській області. Потерпілими особами виявилися деякі державні, комерційні структури та навчальні заклади. Їх позов базувався на наступному:

- на сервері доступу провайдера є місце зникнення електронної інформації клієнтів;

- провайдер не турбується про захист комп'ютерної інформації своїх клієнтів.

Призначена комп'ютерно-технічна експертиза встановила, що система захисту обліку комп'ютерної інформації на сервері доступу ЗАТ «Синет» має високий захист і не допускає викрадання даних. Однак, ймовірною причиною витоків електронної інформації є програмне забезпечення, встановлене на персональних комп'ютерах абонентів ЗАТ «Синет», а саме, операційна система Microsoft Windows 95, яка немає механізмів захисту файлової системи від несанкціонованого доступу. Під час оперативних заходів було виявлено чотирьох місцевих молодиків, що займалися протиправними діями у системі комп'ютерних мереж. За основу вони брали типові прогалини в операційній систем і та використовували утиліти Back Orifice, а також переобладнали на своїх комп'ютерах ОС Microsoft Windows 98, що дозволило по IP – адресі комп'ютера, який був у з'єднанні з мережею INTERNET, звернутися до власних ресурсів з метою їх включення до процесу. Протиправні дії здійснювалися у нічний та у святкові дні, а рахунки відправлялися на адреси добросовісних користувачів зазначених вище установ. Деснянський районний суд м. Чернігова розглянув кримінальну справу щодо обвинувачених у злочині, передбаченому ч. 2 ст. 198^1 КК України 1960 р. Суми нанесеного збитку становили 248 грн., 317 грн. та 1329 грн. Постановою того самого районного суду від 10.03.2000 р. справу направлено на додаткове розслідування у зв'язку з необхідністю технічної експертизи. Судова колегія у кримінальних справах Чернігівського обласного суду залишила постанову районного суду без змін [10].

Аналіз конкретних кримінальних справ, пов'язаних з комп'ютерними злочинами та теоретичні обґрунтування фахівців цього напряму діяльності, викладені у матеріалах практики, дають можливість виділити наступну мету, яку ставить перед собою протиправний елемент:

- фальсифікація платіжних документів;
- розкрадання як безготівкових, так і готівкових коштів;

- підроблення рахунків та інших платіжних відомостей;
- повторне отримання уже здійснених виплат;
- легалізація злочинних прибутків на завчасно підготовлені інші рахунки;
- незаконні операції з сировинними та паливно-енергетичними ресурсами;
- незаконне отримання кредитів;
- маніпуляції з нерухомістю;
- продаж конфіденційної комп'ютерної інформації;
- розкрадання матеріальних цінностей тощо.

При цьому, як правило, 52 % злочинів пов'язано з розкраданням грошових коштів; 16 % – з руйнацією та знищенням засобів комп'ютерної техніки; 12 % – із підмінюванням вихідних даних; 10 % – з розкраданням інформації та програм; 10 % пов'язані з розкраданням послуг [176, с. 97].

Таким чином автор доходить висновку, що мотив обумовлює мету, а мета визначає дію чи бездіяльність по скоєнню і приховуванню злочину, які знаходять відображення в предметах (об'єктах) і матеріальних слідах. При тому мотив і мета є двома взаємопов'язаними, взаємоуточнюючими та взаємодоповнюючими елементами криміналістичної характеристики у тому числі і комп'ютерних злочинів.

РОЗДІЛ 2 ПОЧАТКОВИЙ ЕТАП РОЗСЛІДУВАННЯ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

2.1. Порушення кримінальної справи та забезпечення оперативно-розшукових заходів розслідування комп'ютерних злочинів

Організаційно-тактичні основи розслідування злочинів – це надзвичайно вагомий, об'ємний і тривалий процес. Він вимагає від слідчого не лише теоретичних знань, практичного досвіду роботи, творчого підходу до конкретної справи, а й професіоналізму. За родом своєї професії і процесуальних функцій слідчий повинен володіти спеціальними знаннями, методами і науково-технічними засобами, необхідними для встановлення обставин, що входять до предмета доказування по справі [171]. На питання, в чому полягають професійно важливі якості слідчого, досить змістовно відповів один з фундаторів науки криміналістики Г. Гросс. Зокрема він вважає, що: «Із всіх положень, які в житті може займати юрист, без сумнівів, положення слідчого – найсвоєрідніше… Слідчий повинен володіти всіма добрими якостями, властивими людині: невпинною старанністю і завзяттям, самовідданістю і твердістю, дотепністю і знаннями людей, освітою, залізним здоров'ям і відомостям з усіх галузей знань – це само собою. А ще йому притаманні:

- тверда рішучість в характері і в діях. Немає нічого більш шкідливого, ніж повільність, легкодухість і млявість;
- здібність до самовідданої, безумовно чесної праці;
- точність, а не приблизність знань обставин події, що розслідується;
- ґрунтовне знання людини як головного матеріалу попереднього слідства» [78, с. 8 – 9].

Дані характерні ознаки найбільш змістовно відображають сутність особи, на яку покладається відповідальна місія – встановити об'єктивної істину по справі у цілому і зокрема, що стосується розслідування

комп’ютерних злочинів. Ця справа доволі складна для більшості працівників правоохоронних органів, оскільки за характером не зовсім ординарна порівняно з розслідуванням іншої категорії злочинів, хоча в аспекті планування, розробці тактичних прийомів має наближену форму проведення відповідних заходів. А саме: початковий етап розслідування має включати:

- підбір і формування кваліфікованої слідчої групи з можливим залученням спеціалістів у сфері комп’ютерних технологій;
- розробка і складання плану оперативних заходів і слідчих дій;
- визначення, підготування та використання відповідного обладнання, технічного забезпечення, інструментів, аудіо – та відеотехніки;
- підготування необхідного автотранспорту для перевезення технічних засобів, що служать речовими доказами по справі;
- забезпечення збереження засобів комп’ютерної техніки на випадок неможливого вилучення через об’ємну кількість обладнання;
- вибір технічної експертної установи, яка здійснюватиме відповідну експертизу вилучених речових доказів;
- встановлення контакту та отримання, при потребі, кваліфікованих консультацій від програмістів – математиків; інженерів – програмістів; фахівців відповідних установ;
- взаємодія, при потребі, з іншими правоохоронними структурами, підрозділами [151, с. 157 – 160].

До початку проведення оперативних чи слідчих дій необхідно мати певну попередню оперативно-розвідувальну інформацію такого змісту:

- місцезнаходження (місцерозташування) комп’ютерного технічного забезпечення, з якого здійснювався злочин;
- кому і на яких правах належить операційна система, окреме комп’ютерне обладнання? За ким персонально закріплений комп’ютер;
- система доступу, допуску та контролю до засобів комп’ютерних технологій;

- марка, модель комп’ютера; комп’ютерної операційної системи; периферійних пристроїв, засобів зв’язку; інші відомості про систему, яка є об’єктом дослідження;
- стороння інформація, яка сприяла б успішному розслідуванню справи.

Наявна інформація повинна бути терміново і своєчасно передана фахівцеві, щоб той мав час для здійснення відповідних заходів:

- налагодити зв’язки та провести консультації з іншими фахівцями, якщо виникає потреба;
- підготувати план збору необхідної для формування доказів комп’ютерної інформації;
- провести інструктаж слідчої чи оперативно-розшукової групи, що буде виїжджати на конкретну слідчу дію [34, с. 184–185].

М.Я. Сегай доводить, що: «Розслідування злочинів – це опосередковане пізнання, засноване на вивченні тих предметів і слідів, що містять інформацію про об’єкти і події минулого. Результатом розслідування виступає закінчена провадженням кримінальна справа, яка є упорядкованою інформаційною моделлю розслідуваної події» [193, с. 12]. Вивчення практики розслідування злочинів як специфічної діяльності та методики розслідування злочинів як розділу криміналістики дає підстави для роздумів щодо складності та специфічності розслідування злочинів [89, с. 5]. Безперечно, розслідування такої категорії справ – надзвичайно складний і до кінця непізнаний процес. У багатьох аспектах він співпадає з розслідуванням традиційних видів злочинів, але разом з тим має і свої особливості. Зокрема:

- злочини здійснюються з використанням комп’ютерних технологій;
- залишені відповідні сліди злочинцем мають достатньо інтелектуальний характер;
- оригінальність способу вчинення та приховування злочину суб’єктом – злочинцем;

- складнощі доказового характеру щодо встановлення конкретного місця, звідки було вчинено злочин;
- глобалізаційний характер даного напряму злочинності, тобто злочин виходить за рамки однієї держави тощо.

Але, разом з тим, даний феномен злочинності як і «традиційні» види злочинів підпадають під ті ж самі приводами та підставами порушення кримінальних справ. Згідно з ч. 1 ст. 94 КПК України вичерпним переліком приводів до порушення кримінальної справи для всіх видів злочину, у тому числі й комп'ютерних, є:

1) заяви або повідомлення підприємств, установ, організацій, посадових осіб, представників влади, громадськості або окремих громадян;
2) повідомлення представників влади, громадськості або окремих громадян,

   які затримали підозрювану особу на місці вчинення злочину або з речовим доказом;
3) явка з повинною;
4) повідомлення, опубліковані в пресі;
5) безпосереднє виявлення органом дізнання, слідчим, прокурором або судом ознак злочину.

А також ч. 2 ст. 94 КПК України, якою визначаються підстави, що є обов'язковими при порушенні конкретно взятої кримінальної справи [147, с. 189–191]. Слідча практика показує, що повідомлення про скоєний комп'ютерний злочин визначається у такій пропорції:

- повідомлення посадових осіб організацій або їх об'єднань(близько 40 %);
- заяви громадян (понад 35%);
- безпосереднє виявлення органів дізнання, слідчими або прокурором даних, які вказують на ознаки злочину (близько 5 %) [44, с. 37].

Розкриття та розслідування зазначених вище злочинів мають свої особливості у проведенні окремих слідчих дій. Разом з тим, слідчому,

оперативному працівникові, експертові та іншим учасникам кримінального процесу необхідно мати спеціальні знання та навички і вміло їх застосовувати на практиці у злочинах, віднесених до цієї категорії. В.П. Бахін і А.В. Іщенко наголошують: «Сучасні завдання вдосконалення слідчої діяльності ставить перед криміналістикою проблеми: а) інтенсифікації використання наявних засобів, прийомів і методів; б) активізації залучення новітніх досягнень науки й техніки у розкритті, розслідуванні та попередженні злочинів» [90, с. 17].

Ознайомлення з слідчою та судовою практиками засвідчує те, що досить важко фахівцям цього напряму довести розслідуваний ними злочин до логічного завершення. У 14 % кримінальних справ комп'ютерних злочинів в сфері економіки вдається довести вину суб'єкта. В інших 90 % випадках – доказових джерел або ж замало, або ж як такі відсутні, з них 67 % справ, що знаходяться в провадженні, припиняються ще на стадії попереднього слідства [161, с. 12]. Однією з основних причин такого негативного фактора є допущення тактичних помилок, що припускають практичні працівники у ході слідчих дій, особливо на початковому етапі розслідування. Найбільш загальними, але досить значущими помилками є:

- несвоєчасність проведення слідчих дій у злочинах даної категорії або ж ігнорування як таких;
- недостатність досвіду практичних працівників у розслідуванні комп'ютерних злочинів, у зв'язку з слабкою обізнаністю у цій сфері;
- низька результативність проведених слідчих дій через незастосування або ж неправильне використання техніко-криміналістичних засобів та методів, а також тактичних прийомів і оперативно-розшукових заходів.

Доречною у цьому випадку є думка В.К. Лисиченка: «…необхідно врахувати, що на даному етапі ще не всі слідчі можуть успішно користуватись науково-технічними прийомами і засобами» [138]. Ці та інші недоліки спричиняють розвиток негативних наслідків і позначаються на практичному боці встановлення об'єктивної істини в конкретному аспекті справи.

Суттєве значення має підготовка слідчим відповідної групи спеціалістів, які будуть виїжджати на ту чи іншу процесуальну дію. Особлива роль на цьому та інших етапах відводиться оперативним співробітникам, адже розшук може вести як слідчий, так і орган дізнання [116, с. 7]. У свою чергу, орган дізнання – це одна з форм досудового розслідування, для якого законом передбачена можливість проведення комплексу слідчих дій, а не лише огляду місця події, який передбачено законом, як виняток, для протокольної форми досудової підготовки матеріалів [117, с. 40]. Слушною є думка І.І. Приполова: «Орган дізнання і зокрема оперативні апарати, його співробітники при виконанні вказівок, доручень слідчого як суб'єкта правовідносин мають юридичний обов'язок виконувати рекомендовані розшукові дії… Вони спрямовані на встановлення особи чи поповнення інформаційних даних про її можливе місцезнаходження та причини переховування від слідства, суду, про наміри такої особи та ін. Проте здійснювані ними розшукові заходи можуть бути значно ефективними, оскільки оперативники мають кращий потенціал, зважаючи на знання оперативної обстановки та поінформованість на обслуговуваній території» [175, с. 28].

Стан успішного здійснення оперативно-розшукових заходів полягає, насамперед, у тому, що стратегію і тактику виявлення і розкриття протиправних дій вони мають будувати на основі належних знань специфіки комп'ютерних злочинів. З цією метою видані накази Міністерства внутрішніх справ України № 429 від 31.05.2001 р. «Про створення в структурі ДСБЕЗ підрозділів по боротьбі з правопорушенням у сфері інтелектуальної власності та високих технологій» і №737 від 19.08.2001 р. «Про затвердження Типового положення про підрозділи ДСБЕЗ по боротьбі з правопорушеннями у сфері інтелектуальної власності та високих технологій», згідно з якими оперативно-розшукова діяльність здійснюється з урахуванням особливої специфіки зазначених злочинів [159]. Хоча на нинішньому етапі підхід реалізації даних наказів має кілька проблемних аспектів. Першим чинником тому є недостатня підготовка співробітників МВС у цій сфері. Радикально проблема може бути

вирішеною шляхом істотної корекції існуючих планів і програм підготовки студентів різної фахової направленості, у тому числі й спеціальної, вищих навчальних закладів України. Слушними є окремі концептуальні положення даного напряму викладені Г.Ю. Маклаковим та Є.В. Рижковим. Автори зазначають, що з огляду на невідкладність вирішення задачі щодо стабілізації злочинів у сфері, що розглядається, оперативно-розшукова діяльність має базуватися на окремих додаткових принципах, а саме:

- стратегія і тактика ОРД у цій сфері повинна будуватися на основі широкого використання сучасних досягнень науки і техніки;
- на етапі розробки стратегії тактики ОРД у сфері високих технологій гласно і негласно повинні залучатися висококваліфіковані фахівці з інформаційних технологій;
- арсенал оперативної техніки необхідно поповнити сучасними технічними приладами і пристроями (у тому числі комп'ютерними програмами), розробленими й успішно застосовуваними в інформаційно-технологічній сфері народногосподарського комплексу тощо [144, с. 1 – 6].

Без використання найсучасніших технічних засобів в оперативно-розшуковій діяльності не можна досягти бажаного результату. З цією метою працівникам МВС слід використовувати так звані універсальні (різнопланові інформаційно-пошукові системи, електронні редактори тощо) та спеціальні програмні забезпечення (системи контролю за інформаційним програмним забезпеченням та суб'єктами, що контактують з комп'ютерними технологіями). Останні з них мають можливість:

- контролювати процес спроб злому комп'ютерної автоматизованої мережі чи мережі електрозв'язку;
- визначати індивідуальний почерк роботи програміста й ідентифікаційних характеристик розроблених ним програм;
- визначати перелік електронних адрес і INTERNET – сайтів, якими оперував користувач;

- проводити ідентифікацію комп'ютерних систем за слідами застосування на різних матеріальних носіях електронної інформації;
- досліджувати матеріальні носії з метою пошуку заданих інформаційних комп'ютерних даних.

Звичайно, це далеко не повний перелік тих можливостей, що можуть реалізовувати слідчо-оперативні органи в аспекті запобігання та протидії чи розслідуванні комп'ютерної злочинності. Ті ж самі пошукові програмні засоби, не процесуальної форми, необхідно використовувати в ОРД, скажімо, при виявленні об'єктів несанкціонованого втручання в операційну систему або ж застосування пошукових програм у процесуальній формі при проведенні окремих слідчих дій. Зваженого підходу вимагає і тактика використання оперативно-розшукових матеріалів, отриманих за допомогою спеціальних технічних засобів, арсенал яких постійно наповнюється і результати їх застосування у окремих випадках мають вирішальне значення для розкриття злочинів [102, с. 108].

Як правильно відзначає В.Г. Гончаренко: «…це обумовлює можливість використання даних природничих і технічних наук як важливого інструменту пізнання не тільки у процесуальних формах, а й у не процесуальних. Тому способи пізнання за кримінальною справою являють собою систему прийомів і операцій, необхідних для пошуку, виявлення, отримання, закріплення, дослідження фактичних даних (інформації), а також систему операцій по збиранню і використанню допоміжних орієнтуючих даних (наприклад, даних оперативно-розшукової роботи)» [60, с. 105]. Безперечно, ключем до успіху повинні бути скоординовані дії оперативно-розшукових органів у розслідуванні цих злочинів, а не формальна їх участь у досудовому провадженні. Погоджене планування визначає взаємозумовленість і зв'язок між слідчими діями та оперативно-розшуковими заходами. Адже під час оперативно-розшукової діяльності може надійти інформація, що зорієнтує слідчого на необхідність проведення тих або інших слідчих дій. З іншого боку, виникають і такі випадки, коли факти, встановлені в процесі проведення

слідчих дій, викликають необхідність проведення оперативно-розшукових заходів [47, с. 49 – 50].

Вітчизняна та зарубіжна статистика констатують, на практиці зазначений аспект має реальне відображення. Проведене дослідження доводить, що у 78 % випадків у процесі розслідування кримінальних справ про злочини виділеної категорії, спостерігається позитивна тенденція спільного проведення слідчих дій та в 72 % – їх спільне планування за участю слідчого і оперативного співробітника. Проте зміст плану конкретної слідчої дії залишає бажати кращого [130]. Необхідно до плану підготовки та проведення окремої слідчої дії стосовно злочинів з використанням комп'ютерних технологій включити основні складові, що відображатимуть суть конкретного заходу. А саме: мету слідчої дії; питання, які підлягають з'ясуванню чи обставини, що підлягають встановленню; час та місце проведення; коло суб'єктів, котрі будуть задіяні в процесі, а також розподіл між ними ролей; підготовка науково-технічних засобів для виявлення, фіксації та вилучення речових доказів по справі.

Досить важливе значення має підготовка інших учасників слідчо-оперативної групи, що виїжджатимуть на окремо взяту слідчу дію у злочинах зазначеної категорії. Інтелектуальні злочини потребують більш спеціалізованого, виваженого підходу у розумінні суті справи, що знаходиться у проваджені правоохоронних органів. Осередком сформованої групи необхідно, щоб були практичні працівники структур у поєднанні з фахівцями у сфері ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Але останні мають бути не з числа запрошених представників установ, компаній, підприємств, організацій тощо, а саме з штатних працівників правоохоронних органів. Адже навіть чіткі скоординовані вказівки слідчого щодо співпраці з спеціалістами- програмістами, комп'ютерниками, іншими фахівцями цієї сфери не дадуть того ефекту дії, якого б досягли, якщо б мали власний кадровий потенціал. Але це не означає, що слід повністю відкинути кваліфіковану допомогу провідних установ, які спеціалізуються на сучасних комп'ютерних INTERNET-технологіях. Слідчим і оперативним

працівникам необхідно консультуватися і використовувати на практиці знання експертів ЕОМ, АС, комп'ютерних програмістів, операторів, що працюють та обслуговують програмне забезпечення та мережі електрозв'язку, але цілком покладати справу розв'язання проблемних аспектів виявлення, фіксації та вилучення речових доказів по зазначеній справі – є не правильним. Підтвердженням тому виступає проведене соціологічне опитування слідчих криміналістом-дослідником А.В. Касаткіним. За його даними, лише 14 % слідчих працюють на ЕОМ на рівні користувача, а 56 % не знають принципів роботи ЕОМ. З іншого боку, 92 % з числа програмістів вважає, що на сучасному рівні розвитку обчислювальної техніки без участі професіонала знайти «сховану» інформацію вкрай складно, оскільки не виключна загроза знищення пошукової інформації [98, с. 17 – 18].

У цьому сенсі доцільним є створення ще у 2001 р. у структурі ДСБЕЗ підрозділів по боротьбі з правопорушеннями у сфері інтелектуальної власності та комп'ютерних технологій, що паралельно з координаційними консультаційними центрами інших відомчих структур займаються відслідковуванням та вивченням такого виду злочинності в Україні. Забезпечують взаємний обмін інформацією з іншими державами через повновладні міжнародні структури типу Інтерпол тощо. Однак реалії сьогодення вимагають більш активного і зваженого підходу до формування відповідних підрозділів у МВС, СБУ, ДПА України, діяльність яких була б спрямована на спеціалізацію розслідування лише злочинів даної категорії [77, с. 116].

На важливу увагу заслуговує також питання підготовки науково-технічного спорядження для тої чи іншої слідчої дії зазначеної категорії. Виїжджаючи на розслідування «традиційних» видів злочинів слідчо-оперативна група, зазвичай, бере криміналістичний чемодан різної комплектації або ж одорологічну валізу чи спеціальне пошукове та моніторингове обладнання, для більш чіткого та упорядкованого відшукання і відбору слідів протиправних дій. Н.С. Карпов відзначає, що «…застосування

науково-технічних засобів у слідчій діяльності є одним із шляхів досягнення об'єктивної істини, підвищує наочність та впевненість доказів, що розглядаються, сприяє правильному їх засвоєнню та оцінці, розширює можливості у дослідженні доказового матеріалу, підвищує точність фіксації всього перебігу окремих слідчих дій, підвищує культуру розкриття та розслідування злочинів» [93, с. 94]. Злочини зазначеної категорії заслуговують на особливу увагу, тому недостатньо буде використовувати загальновживані технічними засобами, оскільки вони не зовсім відповідають поставленому змісту завдань. Слушною є думка В.Г. Гончаренка: «…Нинішні науково-технічні засоби в основному відповідають середньому рівню технічних і наукових знань визначеної галузі, а нерідко і відстають від неї…. технічні засоби криміналістики можуть відповідати рівню вимог сьогодення лише при умові безперервно широкої розробки, удосконалення і впровадження у практику оригінальних засобів спеціальних для потреб слідчого, використання при цьому найсучасніших досягнень природничих і технічних наук» [58, с. 39].

Таким чином, необхідно паралельно з вказаним комплектом технічного забезпечення слідчого використовувати не так давно запроваджену у практичній діяльності правоохоронних органів, уніфіковану валізу слідчо-оперативної групи, яка б мала спеціально спрямований характер дії і відповідала б поставленим завданням слідства. До цього комплекту входять такі предмети та матеріали:

- переносний портативний комп'ютер типу «Note Book»;
- ручний сканер та портативний принтер;
- радіо-модем або інші засоби зв'язку;
- цифрова відеокамера з вмонтованим всередині цифровим фотоапаратом або ж один цифровий фотоапарат;
- лазерний диск CD-RW, CD-ROM, а також гнучкі дискети — кілька одиниць;
- спеціальний контейнер для вилучених дискет, який би застерігав електронний носій від розмагнічування при транспортуванні;

- індивідуальні файл-пакети з бирками для зберігання вилучених роз'ємів, кабелів, окремих плат тощо;
- липка стрічка, маркери, клей та ін.

Зазначений перелік технічного оснащення комплектації слідчої валізи може бути доповнений та видозмінений залежно від розширення застосування комп'ютерних мереж та їх модернізації. Але суть їх основного призначення, повинна всебічно сприяти слідчому в належному, результативному проведенні процесуальної дії. В.В. Бірюков з цього приводу зазначає, що використання радіо-модема дозволяє здійснювати оперативний зв'язок, підтримувати постійний контакт із керівником слідчого підрозділу, іншими службовцями, а також відправляти для перевірки інформацію стосовно різних об'єктів. Наприклад, відсканувавши сліди рук, виявлені у ході огляду, їх електронні зображення можна миттєво відправити у відповідний підрозділ НДЕКУ для перевірки. При позитивному результаті можна організувати пошук злочинця по «гарячих слідах» [38, с. 140].

Разом з тим слід приділити увагу і загальновживаному науково-технічному спорядженню, що використовується при розслідуванні комп'ютерних злочинів, адже грамотне його застосування для виявлення, фіксації та вилучення інформації, у тому числі й тієї, що знаходиться на магнітних носіях, має доказове значення по справі, що розслідується. Аналіз практики засвідчує, що з-поміж технічних засобів, що використовуються при «традиційних» видах злочинів, найбільш застосованими у інформаційно-технічних – є фотографування близько 40 % випадків та відеозапис 28 %. А також спеціалізоване під комп'ютерну техніку і програмне забезпечення лише в 9 % випадків та пошукового обладнання для виявлення інформації і вплив на неї 2 % [45, с. 30]. Такі невтішні статистичні дані підтверджують, що розслідування комп'ютерних злочинів знаходяться на низькому рівні. І як один з негативних факторів є те, що на проведення процесуальних заходів слідчо-оперативна група виїздить з типовим комплектом технічних засобів, якими не завжди можна досягти бажаних результатів. Відбувається процес зневажання

спеціалізованих, адаптованих до комп'ютерних злочинів технічних устаткувань та пристроїв не з огляду їх відсутності, а з причини браку фахівців у правоохоронних органах яки б могли оперувати належними знаннями у галузі комп'ютерного забезпечення та програмування.

На думку багатьох дослідників, які вивчають зазначені злочини як складне антисоціальне явище, позиції зводяться до єдиного – слід оживити, удосконалити діяльність практичних спеціалістів у підході до цього протиправного феномену. Доречною є думка А.В.Іщенка: «Доцільно підкреслити, що дієвість заходів щодо вдосконалення правоохоронної діяльності залежить не лише від зазначених обставин, а й від оптимального наукового їх забезпечення» [91, с. 8]. А тому, правильним було б, доукомплектувати діючі слідчо-криміналістичні валізи додатковим, необхідним приладдям. А саме: паралельно з дактилоскопічними порошками на феромагнітній основі, якими виявляють пото-жирові сліди людини, ввести хімічні засоби (наприклад, прожарений порошок оксиду цинку) чи продукт після згорання (наприклад, сажа), які не мають магнітних носіїв, що спричиняють процес руйнування електронної інформації на магнітних носіях комп'ютерних програмних устаткувань. Доцільність цього заходу можемо продемонструвати конкретним прикладом, запропонованим О.М. Моїсеєвим: «Під час огляду комп'ютерної техніки при розслідуванні обставин заміни вінчестера з метою крадіжки інформації виникла необхідність вилучення слідів пальців рук на комплектуючих деталях комп'ютера. Приступаючи до обробки поверхонь дактилоскопічними порошками, експерт-криміналіст разом з спеціалістом – електронником експериментально встановили недоцільність використання магнітних порошків, які можуть реагувати на магнітні поля жорсткого диску...» [153, с.83]. Аналогічно доречно було б говорити і про доцільність використання пошукового технічного оснащення, що використовується при проведенні окремих слідчих дій. У цьому сенсі слід сказати про суттєву особливість – пошук схованок з магнітними носіями (дискетами, CD-дисками, флеш-стрічками). Їх відшукання ускладнюється

неможливістю використання металошукачів або рентгенівської установки, оскільки їх застосування може призвести до знищення електронної інформації на носіях. Таким чином, аби не допустити необдуманої втрати інформаційних комп'ютерних даних, слід грамотно підійти до відшукання та вилучення носіїв машинної інформації, які також реагують на вплив електромагнітних полів під дією чого можуть модифікуватися або ж піддатися руйнуванню. З метою подальшої їх придатності для проведення відповідних експертиз необхідно вжити заходів безпеки та застереження, зокрема: використовувати при їх вилученні спеціальні алюмінієві, свинцеві контейнери чи побутову фольгу тощо.

Не менш важливе значення при підготовці до проведення досудових процесуальних заходів з розслідуванням злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку відводиться участі понятих у конкретній слідчій дії. У криміналістичній літературі справедливо наголошується: «В якості понятих слід залучати осіб, які добре розуміються на роботі відповідної обчислювальної техніки» [189, с. 38]. Ця позиція вчених цілком слушна. Згідно з чинним кримінально-процесуальним законодавством (ст. 127 КПК України) зазначені суб'єкти є обов'язковими учасниками слідчих дій у кількості не менше двох осіб. Зважаючи на специфіку розслідуваної категорії злочинів, відповідно і поняті мають бути особливими. До числа таких слід віднести:

- не зацікавлених у кінцевому результаті осіб;
- запрошені як поняті особи повинні мати принаймні загальну уяву про предмет злочину, що досліджується;
- бажано, щоб поняті були хоча б поверхово обізнані із системами і технологіями ЕОМ (комп'ютерів), АС та мереж електрозв'язку.

Але такої позиції дотримуються далеко не всі дослідники та практики. Окремі з них відкидають спеціальну підготовку до слідчої дії понятих, які б мали принаймні мінімальні знання в цих сферах. Підставою до таких

трактувань є власні обмежені пізнання ЕОМ та їх технологій, що викликають певний дискомфорт з боку слідчого відносно учасників даного заходу. У окремих криміналістичних джерелах висловлюється рекомендація щодо залучення службовців того самого підприємства, організації, установи, компанії, фірми, в якому проводиться слідчий огляд, як поняті та інші спеціалісти, за умови, що вони не зацікавлені у кінцевому результаті справи [153, с. 114 – 115]. Така позиція дослідників є передчасна і не виважена. Слушною у цьому питанні є думка В.Ф.Шевченка та С.О. Суслова, які наголошують: «…Не варто залучати спеціалістів інженерно-технічного персоналу того ж підприємства (організації, установи), де вчинено комп'ютерний злочин, оскільки він певною мірою може бути причетним до злочину» [210, с. 71 – 72]. Таке бачення авторів є виправданим. У цьому сенсі необхідно зважити на той факт, що проведення слідчих дій в основному відбувається у ситуації інформаційної невизначеності, тому недоцільно, навіть необдумано брати в якості понятих з числа потерпілих осіб. Серед понятих може виявитися зацікавлений у результаті справи суб'єкт або ж гірше того – сам злочинець. Таким чином, розшукувана особа, вона ж понятий, матиме повну інформацію про результат огляду місця події і, відповідно, допущені слідчими прорахунки, а вони можуть бути, слугуватимуть своєрідним керівництвом до подальшої дії злочинцеві з метою протидіяти слідству.

2.2. Типові слідчі ситуації початкового етапу розслідування комп'ютерних злочинів та їх особливості

Піддаючи аналізу слідчі ситуації у злочинах зазначеної категорії, хочеться хоча б у загальному зупинитися на окремих положеннях формування цього поняття вченими-криміналістами, які внесли свій вклад у методологічну розробку їх структурних елементів. Під слідчою ситуацією в криміналістиці розуміється та чи інша обстановка, яка складається на момент розслідування злочину. Вона може бути розглянута як сукупність інформації про обставини

вчинення злочину, які встановлені, вивчені, оцінені відповідними особами (співробітником оперативного підрозділу, слідчим). Це залежить насамперед від того, що потрібно встановити у ході проведення ОРЗ або досудового слідства; які обставини, що характеризують злочинне діяння, встановлені, з яких джерел отримані тощо [140, с. 79]. Слідча ситуація залежить від об'єктивних та суб'єктивних факторів, які впливають тою чи іншою мірою на сам процес розслідування конкретної кримінальної справи. Це нова категорія криміналістичної тактики, яку сформував в 1967 р. О.Н. Колісниченко [35, с. 263]. Згодом це поняття знайшло своє застосування у працях інших провідних вчених-криміналістів: І.Ф. Герасимова, І.М. Лузгіна, О.Р. Ратинова та ін. Особливих суперечностей між фахівцями це вчення не викликало, хоча дискусії навколо цього питання точаться і сьогодні. Досить цікавою є позиція В.П. Бахіна, який запропонував розглядати слідчі ситуації у «широкому і вузькому значенні цього слова». Суть її полягає у тому, що «у широкому розумінні слідча ситуація являє собою сукупність усіх умов, які впливають на розслідування та визначальні його особливості». У вузькому: «характеристику інформаційних даних, які має слідство на конкретному етапі розслідування» [16, с. 196–197]. У той час А.Г. Філіппов відносить вчення про слідчі ситуації до одного з основних структурних елементів загальних положень методики розслідування окремих видів і груп злочинів, разом з тим пропонує розглядати їх у частковій криміналістичній методиці «порядок, програму, алгоритм дій слідчого… з урахуванням, виникаючих при цьому типових слідчих ситуацій» [206, с. 71–75]. Таку точку зору підтримує І.А. Возгрін, який акцентує, що вчення про слідчу ситуацію є «необхідною і важливою частиною теорії криміналістичної методики розслідування злочинів» [48, с. 24–26]. В.К. Гавло подає слідчу ситуацію як обстановку розслідування, що характеризується сукупністю фактичних даних, які мають суттєве значення для пояснення події, що відбулась [54, с. 40]. І.Ф. Герасимов, Л.Я. Драпкін, Є.П. Іщенко вбачають у слідчій ситуації розумову динамічну модель, яка відображує інформаційно-логічний, тактико-психологічний, тактико-управлінський і організаційно-

структурний стан, що склався по кримінальній справі і характеризує сприятливий чи несприятливий характер процесу розслідування [127, с. 263–265]. І.В. Гора, В.А. Колесник вважають, що слідча ситуація – це сукупність інформаційних, процесуальних, тактичних, психологічних і організаційних умов, за яких на конкретний момент здійснюється розслідування справи [101, с. 114]. Р.С. Бєлкін трактує це поняття, як «…існуюча в даний момент реальність, за умов якої діє слідчий»…«сукупність умов, у яких на даний момент здійснюється розслідування, тобто обстановка, в якій проходить процес розслідування» [1, с. 501]. Такої точки зору дотримується і П.Д. Біленчук. Слідча ситуація, на його думку, – це, з одного боку, об'єктивна реальність (матеріальні та ідеальні джерела), а з другого, – пізнана суб'єктом доказування об'єктивна реальність, яка існує на цей момент [36, с. 106].

Не будемо вдаватися до полеміки, адже позиція кожного із зазначених авторів заслуговує на увагу і окремі розбіжності, які існують у трактуванні науковців ні в якій мірі не зменшують значущість піднятого питання. У кінцевому результаті погляди науковців збігаються в одному: роль слідчих ситуацій слугує планомірній і ефективній організації розслідування і розробки її методики, стосовно окремих видів злочинів і є загально прийнятими. У криміналістиці достатньо уваги приділено вченими цьому питанню. Сформовано класифікації слідчих ситуацій за різними умовами, а саме:

- прості та складні;
- проблемні й конфліктні;
- типові і специфічні;
- закриті та відкриті;
- одноелементні та багатоелементні (комплексні);
- суворого та не суворого суперництва [184, с. 87].

Більш виваженою є наукова точка зору дослідників О.Я. Баєва, В.П. Бахіна, П.Д. Біленчука, А.В. Дулова, М.В. Салтевського, які запропонували іншу класифікацію слідчих ситуацій, складених з урахуванням їх змісту та напряму розслідування. Зокрема:

- сприятливі та несприятливі;
- конфліктні й безконфліктні;
- типові і специфічні (нетипові);
- початкові, проміжні, кінцеві [35, с. 264].

Не вдаючись до описання наведеної вище класифікації слідчих ситуацій, які мають достатній виклад у юридичній літературі, автор погоджується, що це – інформаційна модель, якою оперує суб'єкт доказування на підставі пізнання реальних умов про обставини злочину. Залежно від специфіки протиправної дії злочинця виникають свої закономірності способу, місця скоєння злочину, відповідних слідів тощо. У злочинах з використанням комп'ютерних технологій присутні також індивідуальні закономірності слідчих ситуацій, які мають свій виклад у юридичній науковій та навчальній літературі. У той час конкретні криміналістичні методики розраховані на слідчі ситуації з урахуванням слідчих версій та відповідної послідовності проведення слідчих дій. Це нам дає підстави для визначення і вивчення слідчих ситуацій, тим самим допоможе у подальшому як:

- правильно зорієнтуватися у багатоаспектності фактичного положення тих чи інших обставин у процесі розслідування з метою отримання даних для прийняття стратегічних і тактичних рішень по справі;
- висунути найбільш обґрунтовані слідчі версії і визначити (скоригувати) подальший хід розслідування в найбільш перспективному напрямку;
- спланувати повний перелік слідчих дій і оперативно-розшукових заходів та їх цілеспрямовану черговість з метою об'єктивного розслідування злочину;
- звести до мінімуму число рішень слідчого, що базуються на спробах та можливих помилках [41, с. 134].

Одним з важливих завдань розслідування злочинів цієї категорії є забезпечення постійного контролю за можливим розвитком слідчих ситуацій і застосуванням належних засобів їх регулювання в інтересах слідства [122,

с. 22]. Таким чином, успіх початкового етапу розслідування комп'ютерних злочинів залежить від сукупності факторів та умов, що склалися на відповідний момент досудового провадження справи. Формування слідчої ситуації у злочинах даної категорії відбувається під впливом об'єктивних та суб'єктивних факторів.

До *об'єктивних* – можемо віднести:

- наявність та характер орієнтуючої і доказової інформації, що знаходиться у розпорядженні слідчого на початковому етапі розслідування, а також механізму злочину й умов виникнення слідів на місці злочину;
- інтенсивність процесів зникнення доказів та вплив сторонніх сил на ці фактори;
- використання слідчим та органом дізнання належного кадрового і технічного потенціалу для забезпечення конкретно визначеної слідчої ситуації;
- визначення оцінки вчиненого комп'ютерного злочину та його співвідношення з кримінально-правовими нормами.

До *суб'єктивних* – ті, що мають вплив на формування слідчої ситуації:

- рівень знань та практичного досвіду роботи слідчого з комп'ютерними злочинами;
- уміння оперативно реагувати та приймати тактичне рішення за екстремальних ситуацій при зазначеній категорії злочинів;
- уміння спрямувати хід розслідування справи у правильне русло;
- при допущенні помилок під час проведення слідчих і оперативно-розшукових заходів, уміння не розгубитися та не піддатися сторонньому психологічному впливу;
- досягнення конфіденційності при проведенні попереднього розслідування всіма учасниками досудового провадження.

Сукупність викладених факторів формує індивідуальність слідчої ситуації, її зміст та умови за яких повинен працювати слідчий. На думку

І.Ф. Герасимова, – це компоненти слідчої ситуації [26, с. 93]. До елементів слідчої ситуації входять:

- обставини злочину, відомі на даний момент;
- наявність джерел доказового значення;
- технічна та організаційно значуща інформація;
- сплановані чи вже виконані слідчі та інші заходи;
- заплановані, але ще не реалізовані слідчі та інші заходи;
- невикористані можливості (резерви);
- час, що є у розпорядженні слідчого;
- дані про поведінку осіб, які зацікавлені в кінцевому результаті справи;
- оцінка перерахованих факторів, що в кінцевому результаті визначають характер ситуації [57, с. 7–8].

Всупереч І.Ф. Герасимову свою позицію відстоює В.К. Гавло, який виділяє такі компоненти слідчої ситуації:

- обстановку місця скоєння злочину;
- вплив на цю обстановку обвинуваченої особи та її співучасників;
- поведінку осіб, котрі мають відношення до справи, що розслідується, та окремі судження в даному аспекті свідків, спеціалістів тощо;
- дії слідчого, спрямовані на отримання фактичних даних, їх оцінка при формуванні слідчої ситуації [55, с. 94].

Однак, найбільш виваженою є точка зору Р.С. Бєлкіна який відносять до компонентів слідчої ситуації такі групи:

- психологічного характеру;
- інформаційного характеру стосовно події злочину;
- процесуального й тактичного характеру;
- матеріального і організаційно-технічного характеру [26, с. 94]; [35, с. 264].

На думку автора, саме вони слугують основою для аналізу вивчення слідчих ситуацій. Хоча практично проводити дослідження за запропонованими вище складовими доволі складно, а іноді й просто неможливо через велику кількість варіативності протиправних дій цієї категорії. Здебільшого, на практиці, розгляд криміналістичних методик окремих видів злочинів проводиться за однією, рідше за кількома елементами складових події, що відбулася. Тут потрібно враховувати ще й саму специфіку злочинності, адже вона пов'язана з використанням ЕОМ (комп'ютерами), АС їх мережами чи мережами електрозв'язку, де доволі важко виявити, вилучити та використати джерело доказового значення. Разом з тим пам'ятаємо, що будь-які зміни як зовнішнього, так і внутрішнього впливу на комп'ютерну інформацію можуть мати безповоротні процеси знищення чи модифікації електронних даних. Зрозуміло, що визначення ходу розкриття злочину буде значно ефективним при повному аналізі слідчої ситуації, що склалася на момент розслідування справи, але у випадках недостатності вихідної інформації про злочин використання окремих складових події злочину матиме неабияке значення для ведення кримінальної справи в цілому. Тому при розслідуванні справ, пов'язаних з використанням комп'ютерних технологій, особливо на початковому її етапі, такі отримані дані дадуть можливість слідчому краще зорієнтуватися у визначенні тактики та вибору методики розслідування злочинів цієї категорії.

Дослідники-науковці: Ю.М. Батурін, Р.С. Белкін, В.Б. Вехов, Ю.В. Гаврилін, В.О. Голубєв, В.В. Крилов, В.Є. Козлов, М.В. Салтевський та ін. робили спроби систематизації слідчих ситуацій злочинів, пов'язаних з використанням ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку. Скажімо, В.В. Крилов виділяє три типові слідчі ситуації:

- власник або користувач комп'ютерної мережі (бази даних) власними силами виявив факт незаконного проникнення й інших протиправних дій, знайшов винну особу і заявив про це у правоохоронні органи;

- власник або користувач комп’ютерної мережі (бази даних) інформаційної системи виявив факт незаконного проникнення й інших протиправних дій, але не зміг установити винної особи і заявив про це в правоохоронні органи;
- дані про порушення цілісності (конфіденційності) інформації в інформаційній системі і винну особу стали загальновідомими чи безпосередньо виявлені органом дізнання (наприклад, у ході проведення оперативно-розшукових заходів стосовно іншої справи) [129, с. 621].

Запропонований виклад слідчих ситуацій має наукове підґрунтя і може застосовуватися в слідчій практиці. Разом з тим у ній є певні недоліки, а саме: відсутність інформації про обставини, що становлять інтерес з точки зору розшуку. Р.С. Бєлкін також акцентує на трьох слідчих ситуаціях, у злочинах з рухом комп’ютерної інформації:

- за умов очевидності – характер і його обставини відомі (наприклад, який вірус і яким способом введений в комп’ютерну мережу), і виявлений потерпілим власними силами, злочинець відомий і затриманий (з’явився з каяттям);
- відомий спосіб скоєння, але механізм злочину в повному обсязі незрозумілий, наприклад, відбувся несанкціонований доступ до файлів законного користувача через Інтернет, через слабкі місця у захисті комп’ютерної системи, злочинець відомий, але зник;
- при наявності лише злочинний результат, наприклад, дезорганізація комп’ютерної мережі банку, механізм злочину і злочинець невідомі [1, с. 952].

Позиція науковця слушна, але, має спрощений і узагальнений характер. Враховуючи широкий спектр злочинності цієї категорії, слід більш поглиблено підходити до викладення слідчих ситуацій, особливо початкового етапу розслідування справи. Скажімо як це трактують Ю.В. Гаврилін, А.В. Пушкін, Є.А. Соцков та М.Г. Шурухнов, а саме:

- неправомірний доступ, виявлений при реалізації комп'ютерної інформації незаконним користувачем;
- неправомірний доступ до комп'ютерної інформації, виявлений законним користувачем по записах у «журналі оператора», що автоматично ведеться, в комп'ютері, але особа, що його вчинила не встановлена;
- неправомірний доступ виявлений законним користувачем з фіксацією на своєму ЕОМ даних про особу, що здійснювала перекачування інформації через мережу;
- неправомірний доступ, виявлений оператором, програмістом у результаті того, що злочинець виявлений на місці злочину;
- є відомості про те, що мав місце неправомірний доступ до комп'ютерної інформації [212, с. 126 – 127].

Запропонована систематизація справляє враження наукового підходу окреслення проблемних питань розслідування. У ній в розгорнутій формі подано варіанти слідчих ситуацій, зокрема початкового етапу розслідування комп'ютерних злочинів. Однак, у порядку зауваження автор вбачає таке:

- у змісті формулювання варіантів слідчих ситуацій відсутні чіткі критерії викладень;
- у поданому переліку охоплено не весь спектр слідчих ситуацій, що можуть скластися у розслідуванні злочинів даної категорії, а лише його частина.

Змістовною у даному питанні є позиція В.О. Голубєва, зокрема:

1. Установлене незаконне втручання в роботу ЕОМ (комп'ютерів), систем і комп'ютерних мереж, є сліди, є підозрюваний, і він дає правдиві свідчення.
2. Установлене незаконне втручання в роботу ЕОМ (комп'ютерів), систем і комп'ютерних мереж, є наявні сліди, що прямо вказують на конкретного підозрюваного, але він заперечує свою причетність до вчинення злочину.
3. Установлене незаконне втручання в роботу ЕОМ (комп'ютерів), систем і комп'ютерних мереж, відомі особи, які за своїм службовим становищем

несуть за це відповідальність, але характер їх особистої вини, а також обставини доступу невстановлені.

4. Установлено факт незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж, скоїти який і скористатися результатами якого могли тільки особи з певного кола (за своїм становищем, професійними навичками і знаннями) або відомі особи (фірми, організації), зацікавлені в отриманні цієї інформації [69, с. 126].

Такий підхід автора найбільш науково-обґрунтовано відображає сутність порушеної проблематики. В основу слідчих ситуацій покладено знання вихідної інформації про злочин, що є основоположним при розслідуванні злочинів у тому числі й комп'ютерних. Однак, хотілося б уточнити окремі аспекти, зміст яких зводиться до наступного: виходячи з аналізу вітчизняної та зарубіжної практики у розслідуванні комп'ютерних злочинів, потрібно сказати, що слідчий на початковому етапі розслідування перед тим, як визначити слідчу ситуацію, стикається з певними вихідними даним про скоєне. До змісту цих даних входить інформація про:

- зовнішнє вираження (форму) злочину;
- спосіб доступу до комп'ютерних носіїв та комп'ютерної інформації;
- видову характеристику конкретного злочину;
- суб'єкта злочину.

Прокоментуємо викладене.

1. Про зовнішнє вираження (форму) злочину. Сюди відносимо всі дані про вчинений комп'ютерний злочин, які стали відомі слідчому й іншим учасникам процесу від осіб, які за своїми функціональними обов'язками уповноважені та ті, що мають допуск до даних, які містяться в окремо взятих ЕОМ (комп'ютерах), АС комп'ютерних мереж чи мереж електрозв'язку, а також іншими суб'єктами, що здійснюють внутрішній та зовнішній контроль за діяльністю процесу операційних програмних забезпечень. Це:

- повідомлення про злочин потерпілої сторони та інших суб'єктів;

- виявлення факту злочину в ході кредитно-фінансових, бухгалтерських перевірок та аудиту;
- встановлення факту злочину під час оперативно-розшукових заходів тощо.

Ці вище зазначені дані є підставою для порушення кримінальної справи та призначення відповідної перевірки правоохоронними органами. До зовнішнього вираження (форми) злочину включаємо також дані про предмет злочину. Сюди відносимо:

- викрадення комп'ютерного обладнання його частин, окремих програм;
- порушення роботи операційних автоматизованих комп'ютерних систем чи мереж електрозв'язку і заволодіння чужими комп'ютерними даними чи іншими програмними продуктами;
- знищення, модифікація, блокування інформації та внесення в неї шкідливих чи небезпечних програм, команд тощо, що приводять її до зміни, на відміну від початкового стану або у негодність, тим самим наносять значний збиток власникові програмного продукту.

2. Про спосіб доступу до комп'ютерних носіїв та комп'ютерної інформації. Такими даними слідчий може оперувати виходячи з вихідних даних про злочин, що достовірно стали йому відомі від інших суб'єктів, або ж із результатів проведення огляду місця події, як первинної і обов'язкової слідчої дії. Як свідчить вітчизняна та зарубіжна слідча практика, існує два види доступу до комп'ютерних носіїв і її електронної інформації — безпосередній і віддалений. Перший з них належить здебільшого внутрішнім злочинцям з числа працюючого персоналу, або тих, хто володіють даними про доступ до операційних автоматизованої комп'ютерної системи, мережі чи мережі електрозв'язку. Другий – суб'єктам злочину, що володіють даними про спосіб доступу до зацікавлених комп'ютерних носіїв, програм, файлів, каталогів та ін. зі сторонніх джерел і реалізовують свій злочинний замисел

через мережі телекомунікацій автоматизованих (комп'ютерних) інформаційних систем, мереж чи мереж електрозв'язку.

3. Про видову характеристику конкретного виду злочину. До змісту цих даних входить інформація про типову спрямованість протиправної дії злочинця. У свою чергу, комп'ютерних злочинців поділяють за наступними видовими ознаками, що вчиняють протиправні дії у сфері:

- державній (політичній, економічній, військовій);
- підприємницькій (комерційній) і приватній;
- банківській і бухгалтерській;
- кредитно-фінансовій та ін.

Останній з них найбільш розповсюджений напрям протиправних дій злочинця. «Частіше інших видів інформації (у 58 % випадків комп'ютерних злочинів) виступають предметом злочинного посягання» [173, с. 385–386].

4. Про суб'єкта злочину. Ці дані окремими науковцями визначаються як основоположні при розгляді слідчих ситуацій, що склалися на момент розслідування комп'ютерного злочину. Однак, в процесі дослідження вихідної інформації про подію злочину початкового етапу розслідування, ми не завжди володіємо навіть мінімальними знаннями про ймовірного суб'єкта злочину, тому зосереджувати свою увагу лише на особі злочинця недоцільно. Потрібно встановити взаємозв'язок між всіма складовими злочину, а з них виходити на суб'єкта злочину. Залежно від конкретної слідчої ситуації, що склалася, виділяємо два варіанти даних про осіб, які вчинили протиправні дії: відомі і невідомі.

До першого відносимо дані, з яких випливає, що є відомості про суб'єкта (суб'єктів) злочину, або ж він затриманий з речовими доказами, чи маємо інформацію про його місцеперебування.

Другий варіант, коли відомості про особу-злочинця відсутні. Така ситуація при розслідуванні комп'ютерних злочинів має найбільш розповсюджений характер, і тоді слідчому доводиться працювати з іншими

даними, якими оперують учасники процесу уповноважені законом здійснювати розслідування злочину.

Як приклад можемо розглянути кілька слідчих ситуацій комп'ютерних злочинів, що стосуються впливу на комп'ютерну інформацію.

- *Виявлено факт несанкціонованого втручання в інформацію, що циркулює в банківській чи кредитно-фінансовій сфері, але відсутні дані про спосіб вчинення злочину та причетних до його осіб*

Така слідча ситуація має досить розповсюджений характер адже переважна частина злочинів спрямована саме на цю сферу з метою наживи. За умови виконання таких протиправних дій комп'ютерними злочинцями, на місці вчинення злочину практично відсутні джерела доказового значення, що ускладнює шлях розслідування злочину і виявлення причетних до скоєного осіб.

- *Виявлено факт внесення будь-якого плану змін у комп'ютерну інформацію, при цьому спосіб доступу до баз даних відсутній або ж має опосередкований характер, суб'єкт злочину невідомий*

Як засвідчує практика, третина всіх комп'ютерних злочинів підпадає під цю слідчу ситуацію. Під внесенням змін до комп'ютерної інформації розуміється внесення до бази даних неправдивих свідчень про суб'єктів господарювання, їх професійну діяльність, виробничі відносини, ділові та партнерські стосунки тощо. За відсутності відомостей про суб'єкта злочину, доволі важко встановити мету конкретного виду протиправності.

- *Виявлено факт внесення змін до комп'ютерної інформації, зафіксовано спосіб доступу до баз даних, окремих програм, відома ймовірна особа злочинця*

Зазначена слідча ситуація є достатньо рідкісною як у вітчизняній, так і у світовій практиці і трапляється у 5 % всіх злочинів, що відносяться до категорії дослідження. Такий результат розвитку події стає відомим за умови спрацювання систем захисту та контролю руху інформації окремо взятого

програмного забезпечення або ж отримання даних шляхом повідомлень іншими суб'єктами, що володіють інформацією про предмет злочину.

- *Встановлено факт внесення в програмне забезпечення чи окремі файли шкідливих, небезпечних вірусних програм, спосіб зараження та особа злочинця невідомі*

Слідча ситуація має розповсюджений характер з-поміж всіх видів комп'ютерних злочинів. Досить важко встановити спосіб зараження і мету протиправного діяння суб'єкта, який вчинив цей злочин, характер нанесеного збитку та кількість комп'ютерних систем, що підпали під дію «хакера».

- *Встановлено факт знищення інформації у комп'ютерній мережі, дані про спосіб вчинення та причетних до злочину осіб відсутні*

Зазначена слідча ситуація має місце, коли є підстави вважати, що комп'ютерна інформація була знищена не випадково, а цілеспрямовано. У даному випадку йдеться про конфіденційну чи таємну інформацію, що становить державну чи комерційну таємницю будь-якої установи, організації, підприємства та ін. Метою такої протиправності осіб-злочинців можуть бути: помста, невдоволення, фінансові махінації, конкуренція та ін.

- *Встановлено факт викрадення (заволодіння) комп'ютерною інформацією, при цьому дані про спосіб доступу до інформації та про суб'єкт злочину невідомі*

Слідча ситуація має подібність до попереднього варіанту, коли відбувається викрадення електронної інформації, яка знаходилася в ЕОМ (комп'ютерних) мережах чи в мережах електрозв'язку під час її маршрутизації. Викрадені дані є своєрідним товаром здебільшого з метою наживи.

- *Встановлено факт модифікації баз даних чи маніпуляції інформацією в окремих програмних файлах, дані про спосіб та про ймовірного суб'єкта злочину відомі*

Зазначена слідча ситуація характерна тим, що даний факт злочину несе в собі певні інформаційні дані як про спосіб вчинення, так і про особу, котра цю протиправну дію реалізувала. В основному суб'єкт належить до внутрішніх

користувачів програмного забезпечення і входить до числа працюючого персоналу структури. Дані маніпуляції з електронною інформацією проводяться з метою наживи, шляхом внесення до комп'ютерної бази неправдивих даних та ін.

Запропоновані та частково прокоментовані слідчі ситуації злочинів, що розглядаються, і вони стосуються лише аспекту несанкціонованого впливу на комп'ютерну інформацію, до уваги не взято решту видів злочинів, які вчиняються з використанням автоматизованих (комп'ютерних) програмних забезпечень, мереж чи мереж електрозв'язку. Стосовно інших видів комп'ютерних злочинів, де предметом злочину є викрадення ЕОМ (комп'ютерів), обладнання, окремих їх частин тощо, то, на думку автора, початковий етап розслідування, шляхом визначення слідчої ситуації, що склалася на час розслідування, повинен проводитися відповідно до розслідування « традиційних » видів злочину.

Таким чином, виходячи зі змісту викладеного можемо висунути слідчі версії та кваліфіковано підійти до організації і планування початкового та подальших етапів розслідування справи, визначити доцільність проведення тих чи інших слідчих дій, оперативно-розшукових і тактико-організаційних заходів, а також послідовність їх реалізації.

2.3. Огляд місця події

Першочерговим, основоположним і найбільш розповсюдженим є слідчий огляд (п. 1 ст. 190 КПК України). Це невідкладна слідча дія, що полягає у безпосередньому сприйнятті, дослідженні, оцінці і фіксації дізнавачем (слідчим) обстановки місця події, слідів та об'єктів, які мають відношення до справи, їх ознак, властивостей, станів та взаємозв'язків з метою з'ясування суті події, що сталася, механізму злочину і його обставин, які мають значення для встановлення істини по справі [108, с. 18]. Слідчий огляд являє собою цілеспрямовану діяльність, що має бути належним чином

організована і спланована. Планування і організація слідчої діяльності виступають як тактичні прийоми [185, с. 151].

Огляд місця уособлює єдиний процес, тому він обов'язково повинен бути завчасно продуманий, виважений та підготовлений. Огляд – сама «продуктивна» дія, що дозволяє установити великий обсяг доказів, які відносяться до всіх сторін складу злочину – об'єкту, об'єктивної сторони, суб'єкту та суб'єктивної сторони; найскладнішого, яке потребує застосування певних тактичних прийомів і засобів криміналістичної техніки [40]. Таким чином, слідчий може проводити: огляд місця події, місцевості, приміщень, предметів та документів з метою виявлення та фіксації різних матеріальних об'єктів, а на них слідів, що ймовірно мають відношення до справи, а, також, їхніх ознак, станів тощо. При розслідуванні комп'ютерних злочинів слідчий огляд проводитися на місці:

- збереження й обробки комп'ютерної інформації, підданої злочинному впливу (наприклад, у разі незаконного втручання у роботу ЕОМ (комп'ютерів), їх систем, комп'ютерних мереж і мереж електрозв'язку);
- знаходження комп'ютерного обладнання, яке використовувалося для вчинення злочину (наприклад, у разі виявлення на ньому шкідливої чи небезпечної програмної продукції, що мало місце виходу з неї на інші ЕОМ (комп'ютери), АС та комп'ютерні мережі чи мережі електрозв'язку);
- збереження інформації, отриманої злочинним шляхом (наприклад, у разі заволодіння комп'ютерною інформацією шляхом викрадення, привласнення, вимагання, шахрайства чи зловживання службовим становищем);
- порушення правил експлуатації ЕОМ (комп'ютерів), комп'ютерної системи або мережі;

- настання шкідливих наслідків (знищення, блокування, модифікації, копіювання комп'ютерної інформації, порушення роботи комп'ютера, комп'ютерної системи або мережі [199, с.77 – 78].

Як і при «традиційних» видах злочинів, так і у злочинах з використанням комп'ютерних технологій, слідчі дії здійснюються в три етапи: підготовчий, робочий (дослідний) та заключний. Кожний з них вимагає продуманості, злагодженості та логічної послідовності. Враховуючи специфіку зазначеної категорії злочинів, слід *підготовчий етап* розділити на дві стадії: до виїзду на огляд та дії на місці події до початку робочого етапу.

Перша стадія – до виїзду на місце події. Слідчому необхідно до виїзду на місцевість ознайомитися з матеріалами справи, які були йому надані як вихідна інформація про злочин. У зв'язку з значним обсягом робіт щодо опанування масиву криміналістично-значущої інформації за короткий проміжок часу слідчий здійснює кваліфікований підбір необхідних спеціалістів. З метою оперативності та ефективності підготовчої стадії до виїзду на слідчу дію до справи долучається оперативний працівник, одним із завдань якого буде проведення таких заходів:

- установити місцезнаходження засобів електронно-обчислювальної техніки (у подальшому – ЗЕОТ), програмного забезпечення, комп'ютерної інформації та документів, що використовувалися під час підготовки, здійснення і можливого приховування злочину, а також інших криміналістично-значущих даних, які мали відношення до скоєної протиправної дії;
- при визначенні місця, де знаходяться ЗЕОТ, встановленні програмного забезпечення, за допомогою якого було здійснено комп'ютерний злочин, провести оперативну-розшукову дію з метою: а) виявити її власника чи користувача або осіб, що мають відповідний допуск до її носіїв електронних даних; б) забезпечити слідчо-оперативній групі можливості законних підстав виїмки

комп'ютерного обладнання, програмного продукту чи окремих комп'ютерних даних, що становлять собою інтерес для слідства;

- з'ясувати схематичний план місця (приміщення, ділянки місцевості, де проводитиметься слідча дія), також місцерозташування ЕОМ (комп'ютерів), АС та їх кількість;
- вияснити режим роботи установи, в якій було вчинено злочин, кількісний та персональний склад працюючих з комп'ютерним програмним забезпеченням, осіб які обслуговують (програмують, діагностують, здійснюють захист) автоматизованих комп'ютерних систем, мереж та мереж електрозв'язку тощо.

На підставі отриманих даних про скоєний злочин, слідчий спільно з оперативним працівником складає відповідний план проведення заходів щодо організації та ефективного проведення зазначених дій. Зосереджує увагу на оптимальному варіанті формування слідчо-оперативної групи основного складу, а також тих, хто має сприяти в організації слідчої дії (консультанти, технічні оператори та ін.). Особлива роль у проведенні процесуальних заходів належить спеціалісту-криміналісту (ст. 128-1 КПК України) як особі, що володіє спеціальними знаннями та навичками – це «будь-які професіональні знання, що можуть сприяти виявленню, фіксації та вилученню доказів» [92, с. 8]. Слушну думку висловив М.П. Шаламов: «Факт може стати доказом, коли під час виявлення, закріплення, оцінки дотримуються правил визначених кримінально-процесуальним законодавством» [208, с. 31]. Саме від грамотного, вдумливого, професійного підходу спеціаліста-криміналіста, до виконання поставленої задачі слідчим, залежить результативний бік проведення конкретної слідчої дії. Так, на думку В.О. Снєткова, якщо огляд відбувається без участі спеціаліста-криміналіста, то слідів та інших об'єктів, що мають значення для успішного розслідування злочину, вилучається в 4 рази менше [197, с. 11]. Не менш важливе завдання відводиться відбору осіб, які виконуватимуть функції понятих, а також визначенню та підбору необхідних техніко-криміналістичних засобів, які цілком і повністю

відповідали б тим вимогам, що від них вимагаються. За умови, що це не порушує планів слідчо-оперативної групи, слідчому бажано б зв'язатися з представниками установи, компанії, підприємства, що виступають як потерпіла сторона, з метою отримання від них інформації про системи захисту та контролю мереж і операційних систем. Також одержати й проаналізувати з відповідними фахівцями інформацію про логічні особливості функціонування технічного програмно-операційного оснащення, їх системної співпідпорядкованості, використаннях засобів телекомунікацій та зв'язку, запобігши при цьому неприпустимості руйнації, а найголовніше – уникнути заподіяння будь-яких матеріальних збитків їх законним власникам. Не допустити непоправної помилки – часткового або повного знищення матеріальних слідів відображення, залишених злочинцем на місці вчинення злочину. Для цього необхідно провести чіткий інструктаж всім учасникам слідчої дії.

Друга стадія – по прибуттю на місце події. Діставшись на місце пригоди, слідчо-оперативна група повинна швидко включитися до процесуального заходу, згідно з завчасно розробленим планом дій, пам'ятаючи про основне – необдуманий крок будь-кого з них може призвести до негативних наслідків. Змістовною у цьому питанні є позиція М.В. Салтевського, який достатньо обґрунтовано підійшов до характеристики підготовчого етапу. Він сформулював основне коло завдань, яке повинен вирішити слідчий перед тим, як приступити безпосередньо до зазначеної слідчої дії. Зокрема автор наголошує, що керівник слідчо-оперативної групи у свою чергу має виконати такі дії:

1) У керівника підрозділу, особи, яка несе відповідальність за експлуатацію комп'ютерної техніки чи іншого співробітника організації, установи необхідно відібрати пояснення, а при порушенні кримінальної справи допитати та вияснити такі обставини:

- чи заблоковано приміщення в якому знаходиться комп'ютер, електронною системою допуску чи охоронною сигналізацією і які технічні засоби забезпечення використовувалися при цьому;
- чи встановлені спеціальні засоби у комп'ютері для знищення інформації у випадку спроби несанкціонованого доступу до неї; з'ясувати місце знаходження організації, що встановила цю систему;
- чи потрібен пароль (додатковий пристрій – електронний ключ) для доступу до інформації (окремим задачам, областям даних, тощо), що знаходиться в комп'ютері або окремим її частинам;
- чи з'єднані (підключені) комп'ютери до локальної мережі підприємства (фірми), об'єднання, якою є схема локальної мережі, основні правила її безпечного використання.

2) Якщо комп'ютер під'єднаний до мережі INTERNET, то необхідно вилучити у керівника підприємства кодові дані, в якого здійснюється огляд, і негайно зв'язатися з мережевим адміністратором, провайдером вузла, до якого під'єднане зазначене підприємство (фірма), і за його допомогою здійснити вилучення та збереження електронної інформації, що належить чи яка надійшла на адресу підприємства.

3) Вилучити та вивчити документацію, пов'язану з забезпеченням безпеки комп'ютерної інформації, що є цікавою для слідства. Вилучити протоколи і резервні копії вінчестера. При наявності протоколів можна встановити видалену (стерту) інформацію на вінчестері (магнітному носії) [186, с. 5 – 6].

Запропонований перелік основного аспекту питань, що висувається перед слідчо-оперативною групою, не є вичерпним, а тому може бути видозміненим або ж доповненим залежно від конкретної ситуації. Враховуючи особливості цієї категорії злочинів, доцільно було б доповнити початковий етап огляду місця події додатковими суттєвими заходами. А саме: по прибутті на слідчу дію керівник групи має вжити заходів щодо охорони та забезпечення

цілісності електронної інформації на основних та периферійних запам'ятовуючих пристроях. З цією метою необхідно:

- за сприяння керівника чи представника організації, підприємства, установи тощо, або ж без їх допомоги, пояснити працюючому з комп'ютерним обладнанням персоналу мету цього заходу, щоб уникнути непорозумінь під час проведення слідчого огляду;
- заборонити присутнім на місці проведення слідчого огляду подальше ведення операцій з використанням автоматизованих систем, а також самостійне здійснення відключення ЕОМ (комп'ютерів) від мереж чи мереж електрозв'язку;
- вжити заходів стосовно тимчасового відсторонення працюючого персоналу від їх робочих місць та виконання дій, пов'язаних з використанням ЕОМ (комп'ютерів), систем та комп'ютерних мереж чи мереж електрозв'язку;
- на випадок, якщо перед початком слідчої дії комп'ютерне обладнання або його частина було не в робочому режимі, то не поспішати його вмикати та запускати в дію програмно-операційну систему, а з'ясувати причину відключення її від мережі;
- при наявності у приміщенні, де проводитиметься слідчий огляд, сторонніх предметів, електромагнітних, вибухових, токсичних та інших речовин, забезпечити їх негайне видалення, з метою запобігання непередбачуваних наслідків;
- перед тим як приступити до ходу реалізації процесуального заходу, необхідно ще раз узгодити керівнику слідчо-оперативної групи коло питань з фаховим спеціалістом чи експертом у галузі комп'ютерних технологій на предмет виваженого, професійного підходу до проведення огляду місця події.

Ю.В. Гаврилін зазначав, що слідчому перед початком слідчої дії, пов'язаної з оглядом комп'ютерного устаткування кожного разу слід переконатися в компетентності спеціаліста [53, с. 83]. Ця рекомендація є

обґрунтованою і щоб уникнути будь-якого непрофесіоналізму на стадії реалізації практичних дій, необхідно запрошувати в якості консультантів штатних спеціалістів експертних установ, що займаються проведенням комп'ютерно-технічних експертиз. Таким чином, усі без винятку загальні положення тактики заслуговують на увагу і є вагомими у цілісному сприйнятті злочинності, але особливої зосередженості вимагає саме невідкладність, своєчасність проведення огляду місця події. Будь-яка сфера злочинів не терпить відкладення та перенесення на подальший, невизначений термін цього процесуального заходу, а особливо з використанням ЕОМ (комп'ютерів) систем, комп'ютерних мереж і мереж електрозв'язку. Виходячи з аналізу вітчизняної та зарубіжної практики, констатуємо, що у:

- 70 % випадків час, що пройшов з моменту здійснення злочину (останнього епізоду) до початку огляду місця події, перевищував три місяці;
- 30 % випадків цей термін перевищував шість місяців;
- 34 % – один рік і більше [154, с. 10].

Як зазначають фахівці-практики, верхня межа максимально допустимого часового інтервалу протягом якого має бути проведений огляд місця події, не повинен перевищувати тримісячного терміну з моменту здійснення злочину (останнього епізоду). У іншому випадку дана слідча дія втрачає свій сенс. Прикладом тому є той факт, що підприємства, організації, установи, компанії тощо регламентують процес збереження конфіденційної електронної інформації у максимальний термін три місяці, після чого її знищують. А за чинними правилами ділового обороту між фізичними та юридичними особами термін збереження комп'ютерної інформації, електронних та інших документів, що містяться у комп'ютерних файлах, журналах неповинні перевищувати одного місяця. Стосовно юридичних осіб, які найбільш потерпають від несанкціонованих нападів з боку комп'ютерних злочинців у таких сферах як: банківська, кредитно-фінансова, торгівельна, промислова тощо, то практичним спеціалістам слід враховувати наступні особливості.

Інформаційні, у тому числі електронні, документи, які найбільш цікавлять слідчо-оперативних працівників, а саме: журнали обліку статистичних показників та даних контролю ймовірності інформації, яка опрацьовується у ЗЕОТ; протоколи вечірніх рішень, що являють собою копії дій оператора ЕОМ (комп'ютерів), які мають відображення в паперовому варіанті при обробці інформації по завершенню кожного робочого дня чи зміни, зберігаються лише протягом п'яти-десяти днів, після чого знищуються. Окрім цього, потрібно враховувати ще одну суттєву деталь, комп'ютерна конфіденційна інформація не завжди має документовану, підзвітну форму збереження, відповідно її знищення не потребує жодних протокольних вимог [154, с. 13]. Зважаючи на викладені деталі окремих аспектів справи, наголошуємо, що не врахування зазначених особливостей може призвести до малоефективного або ж взагалі марного огляду місця події скоєного злочину.

Серед фахівців-криміналістів досить спірним питанням залишається кількісний та персональний склад суб'єктів, які мають брати участь в огляді місця події. На даному етапі дослідження проблематики комп'ютерної злочинності відсутні чіткі рекомендації стосовно факультативного складу слідчої групи виділеної справи. Практичні працівники на власний розсуд, залежно від об'єму та складності слідчої дії, вирішують кадрове питання.

Статистичні дані вітчизняного та ближнього зарубіжжя засвідчують, що на огляд місця події виїжджають:

- слідчий та оперативний працівник, у 100 % випадків;
- спеціаліст ЕОМ, у 100 % випадків;
- співробітник відділу боротьби з економічною злочинністю (УБЕЗ), у 80 –85 % випадків;
- експерт-криміналіст, у 50 – 60 % випадків;
- експерт (фахівець у галузі комп'ютерних технологій), у 18–20 % випадків;

- інші суб’єкти (інспектор відділу охорони технічних засобів, представник служби позавідомчої охорони тощо), у 8–10 % випадків [203, с. 12].

Проаналізувавши викладені статистичні дані, можна дійти висновку про те, що слідчо-оперативна група, яка виїздить на огляд місця події злочинів даної категорії, немає свого основного (обов’язкового) складу учасників, що в остаточному підсумку позначається на результативності проведеного заходу. Відношення окремих учасників слідчої дії, має опосередкований характер простої присутності, а не відповідальності за встановлення об’єктивної істини. Це в черговий раз засвідчує, що кістяк формування слідчо-оперативної групи у злочинах з використанням комп’ютерних технологій мають становити підготовлені штатні спеціалісти, на чому наголошувалося вище. При тому, участь сторонніх фахівців у цій сфері, які мають сприяти правоохоронним органам, у повній мірі не відкидається. Беручи до уваги ці обставини, доцільно було б запропонувати таку редакцію методичних рекомендацій щодо формування слідчо-оперативної групи, яка виїздить на огляд місця події.

- слідчий, що спеціалізується на розслідуванні злочинів у сфері комп’ютерних технологій (керівник СОГ);
- оперативні працівники, фахівці у ОРД, що практикують на ЕОМ (комп’ютерній) злочинності, представники: МВС (Управління по боротьбі з організованою злочинністю (УБОЗ) та Управління по боротьбі з економічною злочинністю (УБЕЗ); представники Державної податкової міліції (ДПМ) та Служби безпеки України (СБУ);
- працівники дізнання зазначених вище відомств, спеціалісти по виявленню і розслідуванню злочинів даної категорії;
- експерт-криміналіст, який володіє навичками роботи зі слідами злочинів зазначеної категорії;
- фахівці засобів електронно-обчислювальних машин, штатні співробітники практичних органів: комп’ютерний програміст;

фахівець мережевих технологій (для виявлення периферійного устаткування та локальної комп'ютерної системи); фахівець системи зв'язку (для використання дистанційної передачі даних каналами електрозв'язку).

- поняті (не менше двох) обізнані з засобами ЕОМ (комп'ютерів), з числа сторонніх осіб, які не мають жодних зв'язків з потерпілою стороною, окремим суб'єктом, установою, організацією, компанією тощо.

Робочий (дослідний) етап

Після успішного проведення відповідних заходів підготовчої стадії до здійснення огляду місця події, слідчо-оперативна група має приступити до не менш складного завдання – робочого (дослідного) етапу зазначеної слідчої дії, обов'язковою умовою якого є чітке дотримання норм КПК України. Цю стадію доцільно, як і попередню, також поділити на умовні під етапи. А саме: загальний огляд (статична дія), детальний (динамічна) дія.

До під етапу загального огляду (статичної дії) віднести:

- інструктаж учасників слідчого огляду безпосередньо у самому приміщенні, кімнаті тощо, де проводитиметься огляд місця події;
- розподілення функцій між учасниками, які задіяні у даному заході;
- складання план-схеми місця події; розташування речей-предметів, комп'ютерного технічного оснащення тощо;
- визначити та здійснити прив'язку основних предметів огляду місця події відносно кількох постійних орієнтирів;
- вибрати вихідну точку, з якої буде розпочато слідчу дію. (Зазначимо, способом ексцентричним, концентричним чи фронтальним.);
- провести загальну фіксацію приміщення та розміщеного у ньому технічного комп'ютерного устаткування фото-, відеозасобами.

До предмета розгляду цього питання найбільше пасує точка зору М.В. Салтевського, котрий чітко та лаконічно систематизував роботу слідчо-оперативної групи на даному етапі. Робочий етап огляду починається з

розблокування вхідних дверей у приміщення. Слідчий пропонує спеціалісту, який входить до складу слідчо-оперативної групи, виконати дії, спрямовані на недопущення руйнування зовнішньої електронної інформації, наприклад, за допомогою модемного чи радіозв'язку. Для цього необхідно:

- відсторонити співробітників фірми (підприємства) від комп'ютерних засобів та надати їм можливість розміститися в іншому приміщенні, що виключає доступ до використання будь-яких засобів зв'язку;
- зафіксувати інформацію на екранах працюючих комп'ютерів шляхом фотографування (детальна зйомка) або методом складання креслення;
- скласти схему підключення зовнішніх кабелів до комп'ютерної мережі, а також здійснити їх позначення з метою подальшого безпроблемного зібрання в зворотному процесі;
- найбільш ефективним чином здійснити відключення комп'ютерних засобів від електроживлення (у тому числі від безперебійних джерел) тощо [186, с. 6–7].

Таким чином, виконавши зазначені методичні рекомендації цього підетапу загальної (статичної дії), можна переходити до самого дослідження механізму вчинення злочину.

Детальний (динамічний) під етап.

Відповідно до складеного плану дії, узгодженого з оперативним працівником, слідчо-оперативна група приступає до практичної реалізації заходу, пам'ятаючи, що головними об'єктами є комп'ютерне обладнання, носії інформації та електронні документи, які знаходяться в самій системі. Все це можна розглядати як один комплекс технічних засобів та інформаційних потоків, а також і як окремий самостійний об'єкт, що підлягає дослідженню. Скажімо, комп'ютерне обладнання включає арсенал технічного устаткування (основного та периферійного), у сенсі виготовлення електронної інформації, її обробки, відправлення, переопрацювання, модифікації тощо. Водночас при проведенні слідчої дії необхідно бути максимально уважним в усіх аспектах,

зокрема, в якій залежності знаходиться комп'ютерне обладнання щодо інших технічних пристроїв. Адже воно може мати:

- автономне існування, коли технічне оснащення знаходиться відокремлено від інших систем і має індивідуальну операційну систему;
- у з'єднанні з мережею, коли комп'ютер та його устаткування знаходиться у складі кількох аналогічних чи інших технічних оснащень, об'єднаних системою локального або ж розподіленого сполучень.

Особливу увагу необхідно звертати на локальне з'єднання (об'єднання кількох комп'ютерних систем у межах одного чи кількох приміщень, що становлять єдине ціле) та розподільне (кілька комп'ютерних систем, розкиданих у межах визначеної території (кварталу, району, міста, області тощо), що об'єднані в одну телекомунікаційну систему. З метою належного функціонування зазначеного технічного комплексу та збереження конфіденційної інформації при непередбачуваних випадках, створюються один чи кілька центральних комп'ютерів, так званих серверів, на яких зберігається основна базова електронна інформація, а всі інші мережеві комп'ютери, відносно названих, є робочими станціями. Таким чином, при огляді місця події необхідно виявити, де саме встановлені ці сервери, їх кількість та зміст комп'ютерної інформації, що в них знаходиться. Переглянути файлові сервери, сервери додатків (програм), а також бази серверних даних та ін.; обстежити робочі станції (всі інші відносно серверів комп'ютери та їх периферійні улаштування); мережеві кабельні з'єднання на предмет відповідності встановленим технічним параметрам, правильному послідовному сполученню з іншими операційними системами та відсутності слідів позаштатного підключення сторонніх улаштувань. Під час проведення слідчої дії бажано б від'єднати одну комп'ютерну систему від іншої, що сполучені між собою в локальну мережу, на випадок уникнення ризиків самостійного обміну чи знищення інформації поза волею спеціалістів. При

цьому допускається переміщати предмет (предмети), який піддається обстеженню, досліджувати шляхом розбирання та маніпуляції, якщо є на те у слідства переконання необхідності вчиненої дії. Але це в жодному разі це не повинно виглядати як погром технічних та комунікаційних засобів з боку правоохоронних органів.

Однією з найважливіших умов проведення слідчого огляду є суворе дотримання встановлених правил поводження з комп'ютерною технікою і носіями інформації, технічно грамотне проведення пошуку доказів, потрібної інформації [199, с. 80]. Комп'ютерна техніка є засобом для роботи з інформацією [96, с. 58]. Тому всі учасники огляду місця події мають виконувати чіткі вказівки слідчого без жодних відступів від плану. Результати дослідження та поетапні дії від загального до конкретного фіксувати документально:

- склад комп'ютерного засобу: наявність системного блоку, монітора, клавіатури, принтера, модему, безперебійного джерела електроенергії;
- по розміщенню частин на передній панелі системного блоку визначають наявність та види систем збереження інформації (дисководи), а також влаштувань для зчитування кредитних карток, парольних карт тощо, особливо відмічають наявність невідомих влаштувань. При можливості визначають засоби, що знищують інформацію;
- по розташуванню роз'ємів, які розміщені на задній панелі системного блоку визначають наявність та види вмонтованих улаштувань: мережевої плати, модему, наявність портів послідовного та паралельного каналів, чи були вони підключені до зовнішніх ліній зв'язку[199, с. 84–85].

Особливу цікавість для слідчо-оперативної групи становитиме виявлена електронна інформація, що знаходилася в комп'ютері та на машинних носіях, яка виступає джерелом доказового значення. Вона потребує правильної виїмки

та в подальшому дослідження не за «польових», а за лабораторних умов. Здебільшого такі дані знаходиться на жорстких дисках та змінних носіях електронної інформації, можливий варіант і паперової інформації, за наявності її виявлення у технічних засобах: факсі, принтері, ксероксі тощо. Однак, вагомішу цінність становить знайдена інформація на електронних носіях [7, с. 505], оскільки може направити слідство до відправної установи, що її надіслала, або кому адресувалася. На виявлених носіях також можуть міститися дані про:

- незаконні бухгалтерські та фінансові операції, здійснені у кредитно-фінансовій сфері;
- програми, які відповідають за проведення електронних платежів мережею INTERNET з використанням послуг INTERNET-магазинів і віртуальних фірм, а також списки зроблених перерахувань з чужих рахунків і кредитних карток на рахунки злочинців та їх співучасників;
- відомості про рахунки, кредитні картки потерпілих у вітчизняних та закордонних банках, спеціальне програмне забезпечення, яке дозволяє одержувати реквізити таких рахунків і карток;
- листування учасників злочину, яке стосується організації та вчинення злочину;
- відомості, які становлять державну, комерційну, банківську таємницю, а також порушують авторські та суміжні права;
- порнографічні зображення;
- шкідливі програми;
- інформація про конфіденційні реквізити доступу до системних ресурсів персональних комп'ютерів і нелегального доступу в INTERNET [199, с.79].

Паралельно з дослідженням технічних комп'ютерних засобів не зайвим буде проведення відповідних пошукових заходів на предмет виявлення можливих витоків електронної інформації з обстежуваного приміщення чи конкретної операційної системи. Для цього необхідно застосувати фахівцями

спеціальне оснащення та перевірити ймовірні місця зняття інформаційних даних. Це можуть бути: електроустановча арматура, дверні та віконні пройоми, пожежна і вентиляційна системи, сигналізація, телекомунікаційне устаткування, а також все комп'ютерне обладнання тощо. Доцільно перевірити облікові документи підприємства, де зазначаються дані про осіб, що працюють з ЕОМ (комп'ютерами) та їх програмними забезпеченнями, зокрема: (журнали обліку робочого часу; проведення ремонтних робіт, регламентних та аварійних). Документи поточної діяльності підприємства (накази, розпорядження, договори).

При огляді місця події центральне місце посідають сліди злочинної діяльності. У криміналістиці під цим розуміють матеріальні та ідеальні сліди відображення. У злочинах з використанням комп'ютерних технологій особливу роль відіграють саме матеріальні сліди, адже вони мають неординарні індивідуальні особливості. Останні можуть бути притаманні «традиційним» видам злочинів, а також характерними лише ЕОМ (комп'ютерним). Тому проводячи огляд місця події, перш ніж занурюватися у внутрішній зміст комп'ютерних устаткувань, слід ретельно оглянути зовнішній вигляд предмета дослідження. У процесі роботи програмно-операційної системи на її поверхні осідає природний та побутовий пил (від роздруковуючих пристроїв), який не підлягає щоденному прибиранню, а також накопичується він в інших малодоступних місцях (під монітором, системним блоком, клавіатурою, факсом, принтером, у місцях з'єднання кабелів тощо [199, с. 84]. Отже, не виключено, що під час ймовірних несанкціонованих дій з комп'ютерними системами, особа-злочинець залишила по собі сліди відображення: нашарування, відшарування; невидимі-безбарвні; одорологічні; трасологічні та ін). До слідів внутрішніх відносимо:

- різнотипні зміни у будові комп'ютерного устаткування (наявність позаштатного обладнання, пристроїв розширення оперативної пам'яті, програми для зчитування оптичних дисків, заміна або відсутність мікросхем чи інших комплектуючих);

- будь-який вплив на саму електронну інформацію, що знаходиться всередині машинних носіїв (зміни у файловій системі; шкідливі та небезпечні файлові програми;
- програми-файли зі зверненням до INTERNET- сайтів; програми, що спричиняють копіювання, блокування, модифікацію чи знищення інформації; файлове програмне забезпечення підбору паролів до несанкціонованого доступу в INTERNET та ін.).

У цьому сенсі цікавою є точка зору Т.Е. Кукарникової, яка зазначає, що слід комп'ютерного злочину є будь-яка зміна середовища (файлової системи), пов'язана з подією злочину. Оскільки файлова система є сукупністю особливих інформаційних одиниць-файлів, спеціальних службових таблиць (каталогів, таблиці розділів, завантажувальних записів, таблиць розміщення файлів) і кластерів, ці зміни можуть виражатися в зміні місцеположення і вмісту файлів; зміні формату або характеристик файлів; створенні чи вилученні файлів; зміні вмісту спеціальних службових таблиць та зміні стану кластерів. Дія одного інформаційного об'єкта на інший може бути виявлена між двома відомими станами інформаційного об'єкта — за ознаками зміни змісту формату файлових характеристик та за зміною алгоритму роботи програми [121, с. 12].

Чільне місце у системі слідчої дії посідає огляд документів. (Документ – будь-який важливий діловий папір – В.І. Даль.) [80, с. 458]. Його можна розглядати як самостійну дію, так і разом з оглядом місця події. Для нас більший інтерес становить другий варіант, що стосується окремих аспектів документообігу, пов'язаного зі сферою використання комп'ютерних технологій. Документ – це матеріальний носій інформації (у тому числі і машинний), в якому посадова особа або інший громадянин зафіксували у встановленому порядку зведення про обставини, що мають значення для справи, у письмовій, фотографічній або ж іншій формі з метою їх збереження і подальшого використання [97, с.26]. Функціональною характеристикою будь-якого документа є його властивість зберігати і передавати інформацію у часі і

просторі про події, факти, права і обов'язки [194, с. 79]. Аналіз спеціальних криміналістичних джерел засвідчує, що дослідження документів, які мають відношення до справи, слугують вагомим аргументом при розслідуванні злочинів даної категорії. Це ті документи, в яких є криміналістично-значуща інформація про обставини протиправних дій та їх суб'єктів. Як відзначив О.Р. Михайленко: «Документ буде законним лише тоді, коли він відповідає названим вимогам, є істинним, правдивим, безсумнівним» [148, с. 29]. Зокрема, з електронного чи письмового документа можемо виявити ознаки комп'ютерних злочинів, визначити способи їх підготовки, вчинення та приховування, основні сліди протиправної діяльності. Вивчення таких документів допоможе слідчому і оперативному співробітнику висунути обґрунтовані версії, намітити невідкладні слідчі дії й оперативно-розшукові заходи тощо, але при цьому слід пам'ятати, що доказами по справі, яка розслідується можуть бути лише оригінали документів, а саме:

- документи, що регламентують і визначають порядок виконання конкретної виробничої діяльності; повноваження та обов'язки конкретних осіб, контрольні функції;
- документи, що регламентують і визначають порядок застосування ЗЕОТ та електронного документообігу, контроль за їх здійсненням;
- документи, що регламентують категорію і тактико-технічні характеристики ЗЕОТ, комп'ютерної інформації та їх засобів захисту в конкретній виробничій операції;
- робоча документація конкретного ЗЕОТ та засобів його захисту (наприклад, журнал оператора, обліку роботи ЗЕОТ, його програмного забезпечення; журнал обліку збійних ситуацій; технічний паспорт; журнал ремонту і технічного обслуговування; інструкція з експлуатації та здійснення окремих операцій; протоколи дій оператора; протоколи обліку роботи користувачів мережі тощо);

- документи, що фіксують питання дотримання технічного процесу, який включає в себе конкретну виробничу операцію, належного виконання правил роботи і техніки безпеки на кожному ЗЕОТ;
- документи, що стосуються особового складу, фіксують прийом та звільнення з роботи осіб, заохочення та стягнення, підвищення кваліфікації та навчання кадрів тощо.

Особливе зацікавлення слідства викликають документи виконані на машинних носіях (електронні документи), адже їх створення здійснювалося за допомогою комп'ютерних технологій. Під електронним цифровим документом розуміють виділену перетворювальну форму організаційно структурованої та ідентифікаційної інформації з реквізитами, сформульованої і виконаної за допомогою програмних операційних систем ЕОМ (комп'ютерів) або інших апаратних засобів, у вигляді іменного запису файлу (файлів) у цифровому коді з атрибутами (ім'я, дата, об'єм); в оперативній пам'яті чи на різного роду матеріальних носіях, які входять до системи цих засобів (магнітний диск, CD-ROM, флеш карта тощо) [194, с. 84]. У них відображені вихідні, первісні джерела тих, хто їх створював та кому вони адресувалися. Цей шлях передачі документа можна прослідкувати, використавши канали (мережі) електрозв'язку автоматичних пристроїв, що реєструють електронну інформацію у процесі її надходження чи маршрутизації. Це можливо здійснити при перегляді документів, що знаходяться в оперативній пам'яті ЗЕОТ та на машинних носіях інформації, переважно у їх складних формах. Будь-який електронний документ виконаний у такому варіанті має містити такі реквізити:

- місцезнаходження організації, яка виконала цей документ або ж поштову чи мережеву адресу;
- найменування документа та дату його виготовлення;
- ідентифікаційний код особи, відповідальної за правильність виготовлення документа або ж того, хто його затвердив. Можливий варіант реєстрації цих даних автоматичними засобами, що виключають можливість несанкціонованого використання підміни

даних та гарантують дійсність електронного документа (наприклад, використання електронного цифрового підпису) тощо.

Отже, при проведенні слідчого огляду та дослідженні документа (документів) на місці події, слід використовувати необхідні знання науково-технічних засобів та, за потреби, практичні навички фахівців у сфері комп'ютерних технологій. Фіксація документів, що оглядаються, повинна здійснюватися з дотриманням загальних вимог, які висуваються до виявлених речових доказів, що мають відношення до аспекту розслідування. Оригінали документів підлягають вилученню з подальшим їх доданням до матеріалів справи.

Заключний етап огляду місця події

Цей етап, на думку багатьох практиків, є найбільш об'ємним та складним, адже потребує фіксації ходу результатів слідчого огляду. Він включає:

- оформлення протоколу проведення слідчої дії;
- упакування виявлених та вилучених слідів і предметів;
- завершення роботи над складанням планів, схем, креслень приміщень та розташування в них технічних устаткувань;
- виправлення неточностей та прогалин, які були допущені з тих чи інших причин слідчо-оперативною групою в ході огляду місця події;
- врахування можливих зауважень з боку всіх учасників слідчої дії тощо.

У протоколі мають бути зафіксовані та відображені всі дії у такій послідовності, в якій вони відбувалися в ході слідчого огляду. Як вказував І.Ф. Крилов: «Усі засоби одержують своє доказове значення за умови, якщо застосування їх знайшло відображення у протоколі. У такий спосіб він акумулює доказову силу всіх інших засобів і способів фіксації» [126, с. 126]. Отже, особа уповноважена слідчим, повинна уважно та грамотно без незрозумілих умовних позначень та скорочень записувати всі дані, що їй

коментували відповідні спеціалісти, під чітким керівництвом старшого групи. Фіксувати поетапно від загального до детального:

- назву предмета дослідження, марку, модель, серію, заводський та інвентарний номер, пломби, позначення, зовнішній стан, колір; якщо виявлені на ньому «традиційні» сліди (дактилоскопічні, одорологічні, трасологічні тощо), здійснювати описання за встановленою формою для такого виду слідів;
- місце розташування об'єкта дослідження відносно інших комп'ютерних устаткувань та приміщення в цілому;
- детальне описання того, де було виявлено ймовірне знаряддя вчинення злочину, яке саме або ж інше джерело доказів та ймовірний його носій.
- Останніми, у свою чергу, можуть бути: переносні комп'ютери «Note Book» та їх модифікації; системні блоки, точніше інформація на їх жорстких дисках; принтери і сканери, в яких при розпізнанні та друкуванні можлива фіксація інформації за рахунок вмонтованих плат пам'яті; модем; машинні носії знімного типу (магнітні стрічки, лазерні компакт-диски, гнучкі дискети).

Обов'язково у протоколі огляду місця події необхідно відобразити, в якому стані перебувала та чи інша комп'ютерна система до початку проведення слідчої дії. Якщо ж технічне устаткування мало робочий режим, то слід у процесуальному документі зафіксувати, яку саме операцію воно здійснювало. Як уже зазначалося вище, має бути проведена фото-, відеозйомка чи цифровий запис інформації, яка є на екрані монітора та прилеглих до нього програмних засобів, а паралельно з тим обов'язково здійснена графічна фіксація детального дослідження баченого. У випадку виявлення не працюючого комп'ютерного забезпечення, не слід самостійно здійснювати будь-які операції до вияснення обставин справи по даному устаткуванню. Уповноважений працівник організації, в якій проводиться слідча дія, повинен проінформувати слідчого на предмет не використання

даного технічного обладнання. Старший слідчо-оперативної групи за погодженням з іншими спеціалістами, задіяними у цьому процесі або ж одноособово вправі вирішувати питання чи здійснювати детальне дослідження не працюючої комп'ютерної системи, чи зупинитися на фіксації загального виду за тими ж правилами, які застосовуються до працюючої системи.

Насамкінець – це підготовка до виїмки намічених апаратних засобів, які містять у собі шкідливі, небезпечні програми чи електронну інформацію, що спричинили збитки або значну шкоду власнику, користувачу програмних забезпечень. На цьому етапі старшому слідчо-оперативної групи слід зважливо підійти до даної дії. Визначити:

- кількість того, що потребує експертного дослідження;
- об'єм габаритних розмірів технічного обладнання;
- відповідну наявність готовності до їх упакування згідно з тими вимогами, що висуваються для такого виду оснащення;
- транспортні можливості для їх перевезення;
- відповідне місце, куди саме воно має бути звезене з подальшим відправленням до експертної установи.

Для цього необхідно:

- вивести комп'ютерне обладнання з робочого режиму;
- відключити від нього мережеве чи автономне живлення;
- від'єднати від комп'ютера та периферійного устаткування з'єднувальні кабелі локальної чи (віддаленої) системи з обов'язковою фіксацією порядку їх відокремлення;
- відділити одне від одного технічне устаткування комп'ютерної програмно-операційної системи для подальшого індивідуального упакування у відповідні екрановані контейнери, коробки, паперові пакети, чисті аркуші паперу, окрім поліетиленових пакетів тощо.

Під час демонтажу апаратних засобів, у послідовному порядку від'єднання окремих комплектуючих системи необхідно дотримуватися таких загальних рекомендацій:

- на кожному вилученому технічному обладнанні має бути проставлений порядковий номер, прикріплений липкою стрічкою аркуш паперу (або папір який має липку основу) з обов'язковою поміткою дати, підписом слідчого, спеціаліста (спеціалістів), понятих, власника (уповноваженої особи) чи користувача;
- місця роз'ємів технічних комп'ютерних засобів повинні мати наклейку, щоб до них не могли приєднувати інше устаткування без відповідного на те дозволу слідчого. Аналогічна процедура проводиться з кабелями, які з'єднують між собою програмно-операційну систему (обидва кінці роз'ємів заклеюють липкою стрічкою або ж намащують краї бокових стінок клеєм та обгортають місце з'єднання папером, що виключає стороннє приєднання);
- всі наявні місця кнопок включення, гнізд, роз'ємів пломбуються і підписуються всіма учасниками слідчої дії. Та ж сама процедура проводиться із у пакувальними прилаштуваннями. При цьому пояснювальні написи можуть зазначатися лише на окремих додатках і прикріплюватися шнурівкою до тієї ж упаковки;
- за умови габаритності, великої кількості чи інших неприпустимих варіантів вилучення засобів комп'ютерного устаткування (коли комп'ютер є сервером чи робочою станцією всієї системи), після їх детального дослідження необхідно опломбувати місця підключень та відключень до системи, а також опломбувати і саме приміщення, в якому вони розташовані. Вжити заходів щодо від'єднання електроживлення устаткування або ж залишити ввімкненим за умови лише прийому електронних інформаційних даних та ін.

Здійснюючи огляд місця події не зайвим буде актуалізувати слідчому, а також слідчо-оперативній групі на предмет того, що слід вжити заходів, аби виявлена, зібрана та вилучена електронна інформація не була втрачена через некваліфіковані дії будь-кого з учасників даного заходу:

- по-перше, неприпустимо підносити до вилучених об’єктів криміналістичної ідентифікації, які можуть у подальшому виявитися вагомими джерелами доказового значення, будь-які предмети, що містять у собі руйнівний вплив на електромагнітні носії інформації;
- по-друге, категорично заборонено до електромагнітного носія будь-що: приклеювати, прикріпляти, робити в ньому отвори, помітки, надписи, підписи, печатки та ін.;
- по-третє, небезпечно на етапі «польового» дослідження здійснювати розбирання системного блоку для вилучення з нього жорсткого диску для подальшого дослідження за лабораторних умов. За умови, якщо система облаштована спеціальними засобами захисту від стороннього втручання і вчасно не отримала запрограмованого коду доступу, спрацьовує програма самознищення інформації;
- по-четверте, важливо пам’ятати, що неприпустимо неохайно поводитися з вилученими носіями електронної інформації: складати (скидати) в одну купу предмети дослідження; гнути, кидати, стукати лазерними компакт-дисками та дискетами; торкатися магнітної поверхні диска; піддавати носії прямому впливу сонячних променів тощо.

2.4. Окремі аспекти допиту осіб у злочинах, пов’язаних з використанням комп’ютерних технологій

Основними тактичними завданнями допиту є: виявлення елементів складу злочину, встановлення обставин, місця і часу вчинення значущих для слідства дій, способу й мотивів їх вчинення, визначення предмета злочинного посягання, розміру причинених збитків, встановлення інших свідків та осіб, причетних до скоєння злочину. Допит можна визначити як слідчу дію, змістом якої є особисте спілкування слідчого з допитуваним з метою отримання у

нього даних про обставини, які підлягають доказуванню по кримінальній справі [131, с. 314].

У чинному Кримінально-процесуальному кодексі України досить чітко регламентовано порядок підготовки та проведення допиту, права й обов'язки особи, яка проводить цю дію, а також особи, що підлягає допитові. В юридичній літературі зазначеному аспекту слідчих дій приділено чільне місце, ми сконцентруємо свою увагу на окремих особливостях допиту осіб у злочинах, пов'язаних з використанням комп'ютерних технологій. На перший погляд, проведення допиту, даної категорії злочинів, не становить особливих труднощів. Однак варто погодитися з позицією науковців про те, що ця легкість лише удавана, оскільки допитувані далеко не завжди дають правдиві, повні й об'єктивні покази, тому досягти бажаного результату вдається після тривалого процесу спілкування з допитуваним, використовуючи при цьому певний комплекс тактичних прийомів. Слідчий повинен визначити коло обставин предмета допиту, а саме:

- обставини, пов'язані з самою подією злочину (час, місце, спосіб, наслідки тощо);
- обставини, які встановлюють чи спростовують винність конкретних осіб та мотиви їх дій, що впливають на ступінь та характер відповідальності обвинуваченого;
- обставини, які відносяться до характеру та розміру шкоди, нанесеної злочином тощо [1, с. 599].

Формування підготовчого етапу до планування допиту слідчим повинен містити більш конструктивні аспекти, які мають цікавити слідство, а саме:

- з'ясувати специфіку організації і планування справи, особливо питань, що стосуються технічних аспектів підготовки та реалізації злочинних замислів;
- визначити обставини, які потребують уточнення інформації:

  а) відомості про потерпілу сторону;

б) технічні та конструктивні особливості комп'ютерної системи, що піддавалася впливу;

в) засоби комп'ютерної техніки, що використовувалися злочинцем при скоєнні злочину;

- підготувати доказові або інші матеріали для пред'явлення в разі фіксації ходу слідчої дії.

Згідно з нормами Кримінально-процесуального кодексу України розрізняють такі види допиту:

- допит свідка;
- допит потерпілого;
- допит підозрюваного;
- допит обвинуваченого;
- допит експерта.

Більш детально на окремих з них зупинимося залежно від процесуального становища учасників.

2.4.1. Допит свідків

Особливий інтерес становить тактика допиту свідків у категорії злочинів, що розглядаються. Зазначених суб'єктів можна допитувати про факти, які стосуються справи, а також про особу підозрюваного або обвинуваченого та потерпілого – ч. 1 ст. 167 КПК України. Свідками при розслідуванні неправомірного доступу до комп'ютерної інформації можуть бути суб'єкти, що спостерігали за злочином, бачили особу (осіб), які його скоювали, а також з інших джерел володіють обставинами вчиненої протиправної дії. Предметом допиту свідків, як відзначив М.І. Порубов, є: «…отримання інформації, якій притаманні не лише події злочину, але і дані про обставини, що йому передували і сприяли або знаходилися у причинному зв'язку з фактом розслідування, а також даних, що можуть бути використані в процесі розслідування для виявлення нових доказів, перевірки і оцінки вже відомих» [172, с.108]. При такому допиті необхідно деталізувати раніше

встановлені обставини, або з'ясувати факти, що стали відомі при проведенні інших слідчих дій. Вітчизняні вчені-криміналісти П.Д. Біленчук, М.В. Гуцалюк, В.Д. Гавловський, Б.В. Романюк, В.С. Цимбалюк сюди відносять:

- предмет посягання (комп'ютерна програма, технічні засоби, база даних) наражався на неправомірний вплив засобу посягання (шкідливої комп'ютерної програми чи технічного засобу) чи ні, його призначення та зміст;
- як здійснюється законний доступ до інформаційних ресурсів автоматизованої системи (далі по тексту АС);
- як міг бути здійснений незаконний доступ до АС;
- чи має АС технологічний зв'язок з іншими мережами, якщо так, то яким чином (система кодів, паролів тощо);
- як організовано інженерно-технічний (апаратний) захист АС;
- яким чином ведеться облік користувачів комп'ютерної системи;
- як здійснюється режим доступу персоналу та інших осіб до приміщення організації [34, с. 209].

Викладена точка зору авторів є слушною і вона на достатньому рівні відтворює зміст питань, які повинен з'ясувати слідчий при проведенні допиту осіб, які виступають як свідки з обставин справи, що розслідується. Разом з тим, окреслене коло слідчим можна доповнити ще й такими суттєвими запитаннями як:

- за яких обставин свідок спостерігав злочин;
- чи знає свідок, яку мету переслідував злочинець, здійснюючи неправомірний доступ до комп'ютерної інформації;
- хто із співробітників міг сприяти вчиненню злочину;
- чи мали місце подібні явища, як на них реагували керівники тощо.

Як уже зазначалося вище, тактика проведення допиту свідків у категорії злочинів, що розглядається, має свої особливості. З цією метою перед початком проведення допиту слідчому необхідно:

- ознайомитися зі спеціальною літературою, що стосується предмета допиту;
- приділити увагу пізнанням у сфері електронного документообігу, режиму конфіденційної інформації, засобів і методів її захисту та безпечної обробки;
- отримати кваліфіковані консультації відповідних спеціалістів даного напряму;
- детально ознайомитися з результатами проведених слідчих дій (документами, предметами, протоколами тощо).

А також, виходячи з переліку встановлених завдань, слідчий має:

- вивчити дані про особу, яку він допитуватиме;
- отримати необхідну інформацію з місця проживання, навчання, роботи;
- зібрати якомога більше криміналістично-значущої для процесу розслідування інформації про конкретного суб'єкта та ін.

Важливі дані можна отримати із особових справ за місцем роботи. Необхідно враховувати, що свідками цієї категорії справ часто є особи з вищою або спеціальною освітою, достатньо високим інтелектом, досконало володіють спеціальною термінологією, яка іноді не зовсім зрозуміла практичним працівникам правоохоронних органів. У зв'язку з цим слідчому необхідно деталізувати покази особи, яка допитується постановкою уточнюючих запитань, що розкривають зміст тих чи інших термінів та визначень, які вживає даний суб'єкт. При описанні конфігурацій систем чи схем руху інформації можуть виявитись дуже корисними рукописні схеми, які складає та додає до протоколу особа, що піддається допиту [81, с. 314]. Оскільки осіб, ідеальних джерел відображення, які виступають свідками у комп'ютерних злочинах може бути не один, а кілька, то слідчому необхідно визначити черговість проведення допиту суб'єктів залежно від обсягу даних, якими вони володіють та їх значущості для результатів слідства. За умови, що особа злочинця не встановлена і не відома, а також відсутні прямі очевидці

обставин вчинення злочину, в якості інших суб'єктів-свідків допиту можуть бути такі особи:

- заявники (потерпілого або представника потерпілої сторони);
- особи, які виявили ознаки злочину (оператори, програмісти, користувачі ЕОМ (комп'ютерів), мережеві адміністратори, інженери-системники, співробітники служби контролю та охорони тощо);
- особи, котрі безпосередньо відповідають за конкретну ділянку роботи (керівники відділу, особа, за якою закріплено програмне забезпечення, внутрішня служба охорони відділу);
- особа, яка безпосередньо не відповідає за ділянку, з якої було вчинено злочин, але з огляду на службові обов'язки наділена владно-розпорядницькими функціями (президент, директор, керуючий);
- особи, що працюють на конкретній виробничій ділянці або операції, які забезпечують проведення технологічного циклу;
- особи, на яких покладено забезпечення пусконалагоджувальних робіт, супровід програмного устаткування, ремонт та обслуговування комп'ютерів, спеціалістів засобів і систем електрозв'язку операційних машин.

Під час проведення слідчої дії, окрім ведення протоколу допиту, бажано б використовувати інші техніко-криміналістичні засоби фіксації процесуального заходу. Це можуть бути: аудіо- та відеозаписуюче обладнання, у тому числі і цифрове аналогове обладнання, а також персональний комп'ютер (стаціонарний чи переносний типу «Note book»). Таке техніко-криміналістичне забезпечення дозволяє слідчому детально фіксувати весь хід процесуального заходу. Як зазначає В.Г. Гончаренко: «Застосування звукозапису при допиті допоможе уникнути або пом'якшити деякі організаційно-тактичні недоліки цієї слідчої дії» [61]. Допит свідків та інших процесуальних суб'єктів у злочинах з ЕОМ (комп'ютерів) та їх автоматизованих мережених систем має ті самі умовні стадії, що і при «традиційних» діях:

а) з’ясовуються необхідні дані про особу, яка допитується (заповнюються анкетні дані частини протоколу слідчої дії);

б) довільна форма викладення змісту інформації, якою володіє допитувана особа, що стосується події злочину;

в) стадія запитань-відповідей;

г) фіксація ходу та результатів допиту.

Але при цьому є і свої індивідуальні особливості. Скажімо, під час вільної розповіді свідка при зазначеній слідчій дії, можливе вживання допитуваною особою термінології, яка не зовсім зрозуміла слідчому (прикладом тому є спілкування з програмістом, інженером-системником або ж «хакером-профі» тощо). За умови допиту у «традиційних» злочинах, слідчий намагається не перебивати вказаного суб’єкта з етичних та психологічних намірів, а також послідовного, логічного ведення русла справи. Винятком може бути випадок, коли свідок відволікається від змісту предмета допиту. За таких обставин справи, слідчий повинен призупинити у викладенні змісту інформації вказану особу для уточнення не зрозумілих йому окремих даних. Або ж позначити собі на окремому аркуші паперу не сприйняту спеціальну термінологію, з метою її уточнення на стадії запитання-відповіді, без зазначення виясненого у протоколі допиту у якості свідка.

У деяких випадках для отримання найгрунтовнішого результату процесуальної дії, можна запросити фахівця у сфері комп’ютерних технологій чи експерта. Їх присутність при допиті додасть впевненості слідчому у формулюванні запитань свідкові (потерпілому, підозрюваному, обвинуваченому). Спеціалісти даного напряму зможуть давати кваліфікаційні пояснення з незрозумілої слідчому термінології, а також, з дозволу слідчого, задавати питання суб’єктам, що допитуються за обставинами справи в рамках своєї компетентності. За загальними процесуальними вимогами поставлені запитання не повинні містити підказки елементів відповіді. У ході допиту може відбутися ситуація розгубленості або ж певних провалів у пам’яті свідків через їх емоційно-збуджений стан. З метою активізації забутого при першому

допиті слідчий має актуалізувати (наштовхнути) про певні обставини справи, особливо в ситуації задавненого факту злочину. Для більш змістовного сприйняття скоєної протиправної дії, слідчому доцільно призначити повторний допит особи, коли людина заспокоїться та емоції поступляться місцем об'єктивній оцінці того, що відбулося. На цьому етапі сумбурність попереднього допиту зміниться на логічну послідовність викладу обставин події, окреслення суттєвих деталей, окремих подробиць, які можуть мати важливе значення для розкриття та розслідування комп'ютерних злочинів.

На стадії запитань-відповідей допиту свідків слідчому необхідно приділити увагу саме тим питанням, які виведуть хід процесуальної дії на конкретний рівень розуміння суті скоєного злочину, що в кінцевому результаті може вказати на особу злочинця та ймовірні мотиви вчиненого. Таким чином, слідчому потрібно з'ясувати такі питання:

- за яких обставин зазначена особа бачила (спостерігала) факт неправомірного доступу до автоматизованої системи, комп'ютерної мережі чи мережі електрозв'язку;
- день, час, місце, обставини та умови вчинення комп'ютерного злочину;
- чи знайома свідкові особа, яка, на її думку могла вчинити комп'ютерний злочин;
- чи повідомила особа-свідок про факт події, що відбулася;
- чи цікавився хто-небудь до вчинення злочину комп'ютерним програмно-технічним забезпеченням, конкретною комп'ютерною інформацією потерпілої особи;
- чи не з'являлись у приміщенні, де розміщена комп'ютерна техніка, сторонні особи, а також чи не зафіксовані випадки роботи співробітників з комп'ютерною інформацією, яка не належить до їх компетенції;
- чи не було будь-яких збоїв у роботі комп'ютерної системи (відключення електропостачання, непланова перевірка

комп’ютерного устаткування, ремонтні роботи тощо), якщо були, то які саме і хто їх проводив тощо.

2.4.2. Допит потерпілого

Вказана слідча дія проводиться з додержанням вимог, зазначених у частинах 1, 2, 3 ст. 167 КПК України. Перед початком допиту слідчий попереджає потерпілого про кримінальну відповідальність за дачу завідомо неправдивих показань за ст. 384 КК України. Після цього з’ясовує стосунки між потерпілим і підозрюваним або обвинуваченим та пропонує потерпілому розповісти про все відоме йому в справі. Забороняється ставити запитання, у формулюванні яких міститься відповідь, частина відповіді або підказування до неї (навідні запитання) – ч. 2 ст. 171 КПК України. Особливістю допиту потерпілого у зазначеній категорії справ є те, що слідчому доводиться мати справу з потерпілим, який або ж спеціалізується на комп’ютерних технологіях, або ж є власником чи користувачем відповідної електронної інформації. У будь-якому випадку розуміється на ЕОМ (комп’ютерах) та їх автоматизованих системах. Перед слідчим постає завдання не лише допитати дану особу, а й вияснити питання:

а) чи дійсно відбувся факт злочину, що виступає підтвердженням тому;

б) чи можливо відбувся автоматичний збій у комп’ютерній системі і суб’єкт добросовісно помилився, сприйнявши це за скоєний злочин;

в) чи не відбулася імітація злочину з використанням комп’ютерних технологій.

Під час допиту потерпілих слід вирішити такі питання:

- що саме стало предметом посягання (комп’ютерні та периферійні засоби, електронна інформаційна база даних, комп’ютерні програми, окремі файли тощо);
- яким чином відбувся неправомірний доступ до комп’ютерної мережі;
- шлях законного доступу до електронних інформаційних ресурсів автоматизованих систем;

- хто персонально має доступ до конкретного комп'ютерного оснащення, що піддався злочинним діям;
- чи забезпечене комп'ютерне оснащення засобами захисту та контролю, якщо так, то якими;
- як здійснюється захист комп'ютерної інформації, засоби та методи захисту;
- як організовано інженерно-технічний (апаратний) захист автоматизованих систем;
- як здійснюється режим доступу персоналу та інших осіб до приміщення організації.
- чи має автоматизована система технологічний зв'язок з іншими мережами, якщо так, то яким чином (система кодів, паролів тощо);
- у чому виявляються несанкціоновані дії злочинців (внесенні шкідливих, небезпечних програм (вірусів), викраденні або ж перекрученні комп'ютерної інформації, блокуванні роботи комп'ютерів, підміні даних, зміні коду тощо);
- дані про комп'ютерне забезпечення, яке підпало під злочин, його технічні характеристики, функціональне призначення, системи мереж електрозв'язку (локальні, віддалені);
- як часто перевіряються і оновлюються програми ліцензованого антивірусного характеру, які результати останніх перевірок;
- як часто оновлюється, поповнюється, опрацьовується програмне забезпечення і яким чином;
- хто персонально займається придбанням комп'ютерної техніки, де саме, яким чином здійснюється її ремонт та профілактика;
- який на даному об'єкті порядок роботи з електронною інформацією, як вона надходить, обробляється і передається мережами електрозв'язку;

- хто, окрім потерпілого, є абонентом комп'ютерної мережі, до якої підключені комп'ютери даного підприємства, організації, установи, компанії яким чином здійснюється доступ до мережі, хто із користувачів має право працювати в мережі, які у них повноваження;
- чи були випадки неправомірного доступу до комп'ютерної інформації раніше, якщо так, то як часто;
- чи могли наслідки, що настали, бути результатом необережної, некваліфікованої дії особи, яка є користувачем (найманим працівником) і відповідає за збереження та рух комп'ютерної інформації
- чи можливе пошкодження або знищення комп'ютерної інформації бути результатом несправності, виходу з ладу ЕОМ (комп'ютерів), автоматизованих системи, комп'ютерних мереж чи мереж електрозв'язку.

2.4.3. Допит підозрюваного

Важливе місце відводиться в науковій криміналістичній літературі тактиці допиту підозрюваного у вчиненні злочину. Реалізація вказаного слідчого заходу має бути розпочата з роз'яснення особі його прав, що передбачені ст. 43-1 КПК України, а також повідомлено, у вчиненні якого злочину він підозрюється, про що робиться відмітка у протоколі допиту – ч. 3 ст. 107 КПК України. Побутують у даному аспекті рекомендації до формування слідчим питань, які повинен він з'ясувати при допиті підозрюваного в конкретному випадку. Розглянемо окремі з них. Піддаючи аналізу допиту слідчим зазначеної вище особи, точка зору одних науковців-процесуалістів і криміналістів зводиться до таких даних:

- рівня професійної підготовленості підозрюваного (за своїми здібностями, він може, виступати як автор шкідливої комп'ютерної програми);
- наявності досвіду роботи у створенні комп'ютерних програм певного класу, на конкретній алгоритмічній мові програмування;

- рівня знань алгоритмів роботи комп'ютерних програм, які підпадали під неправомірний вплив (зміну) тощо [34, с.208].

У свою чергу наступні дослідники акцентують увагу на:

- навичках та досвіду роботи з комп'ютерною технікою і комп'ютерним програмним забезпеченням;
- використанні на комп'ютері за місцем роботи правомірного доступу до комп'ютерної техніки та конкретного виду програмного забезпечення;
- правомірного доступу до мережі INTERNET та роботи в INTERNETI;
- закріплення за ним за місцем роботи ідентифікаційних кодів і паролів для користування комп'ютерною мережею та ін. [8, с. 68].

Інші зазначають, що при допиті підозрюваної особи в кожному конкретному випадку, як мінімум необхідно отримати відповіді на такі питання:

- місце його мешкання, роботи чи навчання, професія;
- взаємостосунки з співробітниками, сімейний стан;
- спосіб приватного життя;
- сфера інтересів, звички, схильності;
- коло знайомих;
- навички з програмування, ремонту та експлуатації засобів обчислювальної техніки;
- до якої комп'ютерної інформації має доступ. Які операції з інформацією він має право проводити;
- якими засобами обчислювальної техніки, машинними носіями, пристроями він володіє і які використовував для вчинення правопорушення;
- звідки підозрюваний міг знати пароль (код) доступу до інформації. Чи має підозрюваний обмеження на доступ у приміщення, де розташована комп'ютерна техніка;

- яким способом він здійснив неправомірний доступ до комп'ютерної інформації;
- чи відомі йому особи, що цікавились паролями та кодами комп'ютерних програм потерпілої сторони та ін. [34, с. 211].

Підсумовуючи викладене, доходимо висновку, що викладений авторами підхід до формування питань слідчим на початковому етапі розслідування та проведення допиту підозрюваної особи, в цілому відповідають поставленим вимогам зазначеного процесуального заходу, хоч є окремі суттєві зауваження. Необхідно більш конкретизовано підходити до формування та вияснення обставин, що передували та лягли в основу можливого вчинення особою комп'ютерного злочину.

Початковий етап допиту особи має встановити наступні обставин справи, що цікавлять слідство. По-перше:

- яким родом діяльності в житті займається підозрювана особа, чи пов'язаний злочин з його професією;
- як давно виникло бажання у підозрюваної особи вчинити злочин такого характеру;
- чи з власної ініціативи підозрюваний скоював злочин, чи під впливом, тиском інших осіб;
- особа сама скоювала злочин чи у складі групи у тому числі організованої;
- комп'ютерний злочин особа вчинила в перше чи це уже мало системний характер;
- за якими критеріями здійснювався відбір об'єкта злочину;
- що послужило мотивами скоєного злочину;
- яку мету переслідувала протиправна особа реалізовуючи злочин, пов'язаний з використанням ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

По-друге:

- наскільки добре володіє знаннями комп’ютерних технологій, якими саме;
- яке програмно-операційне забезпечення використовувалося для досягнення поставленої протиправної мети;
- способи і методи, що використовувалися для проникнення у чуже комп’ютерно-програмне забезпечення;
- конкретне місце, з якого ймовірно за все було вчинено злочин;
- які конкретні операції з несанкціоновано-заволоділо комп’ютерною інформацією виконувалися підозрюваною у злочині особою;
- кому адресувалася викрадена комп’ютерна інформація;
- хто замовляв вчинити протиправні шкідливі чи небезпечні дії з комп’ютерною інформацією власника або ж добросовісного користувача;
- чи має у власному розпорядженні, користуванні комп’ютерне обладнання, а також чи користується послугами комп’ютерних технологій у своїх знайомих, друзів, комп’ютерних клубах тощо;
- чи має власну систему захисту, контролю та паролів доступу до операційного обладнання (якщо так, то її детальний виклад);
- хто, окрім підозрюваної особи, володіє даними про персональний захист конкретного комп’ютера та його електронних даних;
- чи користується підозрюваний суб’єкт всесвітньою мережею INTERNET, як часто, в який саме час і якою сферою найбільше цікавиться і чому та ін.

Головне, слідчому при допиті підозрюваної особи необхідно уникнути конфліктної ситуації, тим самим переконати зазначеного суб’єкта у сприянні слідству. Застосування правильної тактики слідчим відносно підозрюваного, може позитивно вплинути на результативність процесуальної дії. Особа, розуміючи своє становище, не позбавлена можливості щирого зізнання у скоєному і викритті всіх причетних до злочину (організаторів, пособників,

підмовників, виконавців), якщо такі є. Однак протиправність може бути вчинена одноособово, і суб'єкт визнає вину, частково чи повністю, тоді він повинен логічно довести свій злочинний задум та його механізм реалізації, або ж навпаки, спростувати висунуті проти нього криміналістично-значущі дані розслідування справи.

2.5. Висунення криміналістичних версій при розслідуванні зазначеної категорії злочинів

Розкриття злочину – це процес встановлення об'єктивної істини у справі, який здійснюють на основі загальних положень теорії пізнання. Його суть полягає у зверненні слідчого до фактів і подій минулого, де було скоєно злочин. Відповідно до норм кримінально-процесуального законодавства України, завдання попереднього слідства полягає у викритті осіб, винних у вчиненні злочинів, шляхом збирання й перевірки доказів, що здійснюються з метою визначення предмета судового розгляду. З огляду на це, зазначене слідство – це виявлення, розгляд, перевірка й оцінка фактичних даних, що мають значення доказів у кримінальній справі та відіграють роль засобу встановлення обставин останньої. Вони повинні відповідати вимогам допустимості, а саме:

1) виходячи з джерел, перелічених у ч.2 ст.65 КПК України;
2) мати відношення до предмета доказування;
3) відповідати вимогам процесуальної форми, тобто сукупності визначених процесуальним законом умов необхідних, з одного боку, – для виконання органами слідства тих дій, які сприяють здійсненню їх функцій у сфері розслідування, а з другого, – для здійснення громадянами-учасниками кримінального судочинства дій, спрямованих на реалізацію їх прав і виконання покладених на них обов'язків;
4) відповідати вимогам принципів та гарантій кримінального судочинства.

Основу організації розслідування будь-якої категорії справ становить його планування, що здійснюється на основі криміналістичних версій. Як відзначено в криміналістичній літературі, розшукова версія відіграє роль чинника, що детермінує поведінку суб'єкта розшуку [24, с. 219]. Таким чином, методом організації розслідування виступає планування дій слідчого, а логічною основою безпосереднього планування слугують слідчі версії – одна з різновидів криміналістичної версії. Уперше у вітчизняній криміналістиці визначення версії запропоновано у 1940 р. відомим вченим Б.М. Шавером. Під слідчою версією він розумів припущення слідчого, яке ґрунтується на матеріалах справи, про характер злочину, мотиви, внаслідок яких його скоєно, про спосіб, яким могли вчинити злочин [101, с. 28]. Подальша розробка цього вчення належить радянським криміналістам: С.О. Голунському, М.В. Криленку, С.Л. Рубінштейну. У п'ятидесяті — сімедесяті минулого століття дане вчення продовжили та розвинули: Р.С. Бєлкін, О.М. Васильєв, А.М. Колесниченко, І.М. Лузгін, А.М. Ларін, В.І. Попов, М.В. Салтевський, В.Ю. Шепітько та ін. Але й до нині залишаються між науковцями неординарні твердження в розумінні застосування понять гіпотези та версії, особливо, що стосується розшукової версії. Окремі аспекти різних трактувань охарактеризуємо коротко.

Гіпотеза (від грец. hypothesis – підстава, передбачення) – це передбачуване судження про закономірності (причинного) зв'язку явищ [29].

Версія (від франц. version, від лат. verso – тлумачу, зважую) – форма мислення, різновид окремої (часткової) гіпотези [116, с. 26].

В юридичному розумінні ці слова вживаються як синонім будь-якого припущення, передбачення, здогадки, які виникають у процесі більш або менш складної розумової діяльності. Версія детермінована з проблемною ситуацією, з питаннями, які не дістали вирішення у процесі розслідування. Однак потрібно зазначити, що в криміналістиці не існує єдиного визначення стосовно поняття криміналістичної версії. На думку автора, більш виваженим і змістовним у цьому плані є наступні трактування.

М.В. Салтевський вважає, що криміналістична версія – це засноване на зібраній інформації з розслідуваної справи припущення (імовірне судження) слідчого, дізнавача, прокурора, суду про подію злочину і злочинця в цілому або окремі факти і осіб, причинні та інші зв'язки між обставинами, що підлягають дізнанню [185, с. 29]. У свою чергу М.П. Шаламов під криміналістичною версією розуміє обґрунтоване передбачення про факти, явища або групу фактів, явищ, котрі мають чи можуть мати значення по справі. Версія вказує на наявність і пояснює походження цих фактів, явищ та їх зміст і зв'язок між собою та служить цілям встановлення істини по справі [209, с. 287–290]. М.П. Яблоков у криміналістичній версії вбачає логічно-побудований і заснований на фактичних даних попередньо обґрунтований умовивід слідчого (інших суб'єктів пізнавальної діяльності по кримінальній справі), про зміст діяння, що досліджується, його окремих обставинах і деталях та їх зв'язку між собою, які вимагають відповідної перевірки і направлені для встановлення істини по справі [129, с. 93]. В.О. Коновалова аргументує, що це обґрунтоване припущення про наявність і обставини розслідуваної події, дії конкретних осіб і наявність у цих діях складу певного злочину [132, с. 213].

Отже, з викладеного можна дійти висновку про те, що версія, з одного боку, є окремим методом криміналістичної науки, а з другого, – ймовірною інформаційно-логічною моделлю проблемної ситуації, результатом розумової діяльності слідчого. З гносеологічної точки зору, версія є методом і засобом пізнання істини, що випливає з її логічної природи. Вона являє собою форму переходу від незнання до знання про подію, що розслідується, відповідно, має охоплювати процес відображення явищ матеріального світу об'єктивної природи предмета дослідження. Однією з форм пізнання невідомого є гіпотеза. За своєю природою, версії – різновид часткових гіпотез.

На відміну від наукових гіпотез версії не переслідують мети створення наукової теорії, а їх перевірка здійснюється в термін, встановлений для розслідування [133, с. 112]. Формування криміналістичних версій відбувається

на підставі фактичних даних про обставини справи. Вони можуть бути отримані будь-якими способами в рамках закону, включаючи навіть і не процесуальну форму. Як позитивне хотілося б зазначити, що важливу роль при побудові версій відіграють положення науки і практики, а також достатність знань, професійного досвіду особи, яка буде реалізовувати цей захід.

Висування версій є «підсумком, логічним результатом всієї свідомої діяльності слідчого в процесі розслідування злочину» [9, с. 5]. Він застосовує для цього весь багаж знань, арсенал логічних прийомів і засобів: індукцію, дедукцію, аналогію, аналіз, синтез, порівняння, абстрагування тощо. Базуючись на фактичних даних, криміналістичні версії повинні дати пояснення отриманій інформації і обґрунтувати в ній кореляційні зв'язки. Отримані в процесі дослідження версій знання повинні мати вірогідний характер. Подальший його перехід до набуття достовірних знань, відпрацьовується в процесі перевірки висунутих версій, результатом яких є виявлення фактичних даних, що підтвердять або ж спростують версії. Організаційний аспект версій полягає в тому, що він «визначає напрямок розслідування, є його організаційним початком, ядром планування діяльності слідчого» [25, с. 366]. Використання систем типових версій вносить у розслідування елемент точності, повноти розслідування, допомагає слідчому проаналізувати відомі йому аналогічні ситуації і відібрати ті, що підходять під конкретний випадок з літературних джерел. Ознайомлення зі схемою таких версій дозволяє одночасно охопити та перспективно намітити всі можливі основні напрямки розслідування [104, с. 10]. Тактична роль криміналістичної версії неперевершена, адже вона визначає весь процес розслідування, слугує вагомою підставою для складання плану подальших слідчих дій та оперативно-розшукових заходів. Особливої ваги вона набуває у злочинах, пов'язаних з використанням комп'ютерних технологій, де надзвичайно важко визначити межу між скоєною протиправною дією та інсценованою. Інсценування – це обстановка події визначеного місця, яка створена штучним шляхом, яка може поєднуватися з відповідною удаваною поведінкою осіб та

надання ними неправдивих свідчень про обстановку, яку вони самі створили, з метою викликати у слідчого та інших осіб хибну уяву того, що відбулося з метою приховання істини [162]. Тому на початковому етапі розслідування, після проведення огляду місця події, навряд чи можна буде висунути основну (остаточну) версію про обставини справи, що підлягає дослідженню, найшвидше це буде робоча версія і не одна, а кілька. Виходячи з загальноприйнятої класифікації, версії, за обсягом встановлення обставин події, поділяються на:

- загальні, призначені для пояснення сутності події в цілому, її характеру, причинного зв'язку між факторами;
- окремі – ймовірне судження про місце, час, засоби вчинення злочину, походження окремих слідів злочину тощо.

Особливу роль при огляді місця події може відіграти висування загальної версії при інсценуванні комп'ютерного злочину з метою приховання викраденого, скоєння шляхом присвоєння, розтрати чи зловживання службовим становищем [112, с. 229–230]. У такій ситуації особи, які інсценують злочин, впевнені у тому, що не залишили жодних слідів, що могли б вказати на їх причетність до скоєного. Але це не завжди так. Як засвідчує вітчизняна та світова практика, злочинці на місці скоєння злочину з різних причин залишають різнотипні сліди. На думку автора, їх походження може бути викликане такими факторами:

- недостатністю знань і практичних навичок у користуванні комп'ютерними системами;
- ігнорування системами захисту та контролю комп'ютерно- технічного забезпечення;
- поспішністю виконання свого протиправного замислу через брак часу;
- доручення реалізації злочинного задуму іншим некомпетентним особам;

- самовпевненістю у тім, що працівники правоохоронних органів не виявлять слідів скоєного або ж їх можна буде схилити до однієї з вигаданих, хибних версій.

Окремо хотілося б відзначити ознаки інсценування комп'ютерних злочинів на місці події. Досить виважено до цього питання підійшов В.Є. Козлов, який згрупував їх таким чином:

- виявлення на місці скоєння злочину слідів, яких не повинно бути за умови, коли б подія була не мнимою, а реальною;
- сліди, не виявлені з огляду на їх відсутність, але які повинні були з'явитися на випадок реальності інсценованої події;
- сліди, що відносяться до числа характерних для інсценованої події слідів, але їх стан не відповідає тому, в якому вони повинні знаходитися в конкретно визначеній ситуації [112, с. 230].

Однак, слід доповнити цю точку зору автора такими умовами:

- коли ми маємо справу не з ймовірним, а точним місцем скоєння злочину;
- якщо нам достовірно відомо, що місце, звідки було вчинено злочин одне, а не кілька;
- коли ми володіємо обставинами справи про місце вчинення злочину і місце настання наслідків протиправних дій, а вони, у свою чергу, можуть співпадати або ж навпаки.

При цьому необхідно врахувати той факт, що трапляються випадки, коли потерпіла особа (на яку падає підозра про штучно створений умовний злочин), не вчиняла й не імітувала комп'ютерний злочин, просто добросовісно помилялася у тому, що скоєне протиправне діяння відбулося. За такої умови працівникам слідчо-оперативної групи, фахівцям та експертам цієї сфери доведеться не лише дослідити об'єкт (предмет) посягання, а й переконати заявника в тому, що несанкціоновані дії не відбулися (внутрішньо і ззовні), а також висунути кваліфіковані версії-гіпотези того, що послужило причиною

порушення роботи автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Версії можуть мати таке трактування:

- відбувся автоматичний збій в програмно-операційній комп'ютерній автоматизованій системі, що спричинив руйнування чи знищення програми, комп'ютерної інформації, а користувач сприйняв це за вчинений злочин;
- недотримання регламентних робіт, а також порушення правил експлуатації технічного комп'ютерного обладнання, що потягло за собою негативні наслідки;
- ігнорування або ж несвоєчасне застосування систем безпеки комп'ютерних даних спричинило внесення в програмно-операційне забезпечення різного характеру шкідливих чи небезпечних програм, які зруйнували чи модифікували комп'ютерну інформацію;
- неналежне виконання операторами програмного забезпечення, спеціалістами у сфері обслуговування комп'ютерного устаткування і іншими працівниками конкретної установи, технологічних умов поводження з ЕОМ (комп'ютерами), АС, комп'ютерними мережами чи мережами електрозв'язку, які призвели до блокування, порушення маршрутизації, часткового чи повного знищення електронної інформації тощо.

Особливий інтерес розгляду питання у злочинах зазначеної категорії становлять криміналістичні версії, що визначаються за ступенем ймовірності:

- типові – пояснюють події в цілому на підставі даних узагальненого досвіду судової, експертної, оперативно-розшукової практики;
- конкретні – робочі версії, над якими працює у той чи інший момент слідчий.

Якщо другий вид версій не викликає особливих розбіжностей у вчених у понятті, трактуванні та їх застосуванні, то перший потребує окремих суттєвих уточнень. Скажімо, бачення Р.С. Бєлкіна базується на тому, що під типовою версією розуміється: «Характерне для даної ситуації з погляду відповідної

сфери наукового знання або узагальненої практики (оперативно-розшукової, судової, слідчої, експертної)». На його думку, типові версії мають дуже обмежене пізнавальне значення, оскільки вони, базуються на мінімальних фактичних даних, можуть дати тільки загальне пояснення події, що недостатньо для успішного завершення розслідування. Тому типова версія конкретизується у процесі доказування по мірі накопичення дізнавачем (слідчим) необхідної інформації. Але разом з тим, «…можна стверджувати, що вона є організаційним початком розслідування та «ядром» планування дій слідчого» [1, с. 472 – 475]. Г.А. Матусовський типову слідчу версію визначає як припущення, побудоване на основі аналізу однотипних ситуацій, спільності певних необхідних явищ та зв'язків.

Особливого значення такі версії набувають у випадках, коли доводиться оперувати в ситуаціях з недостатньо повною інформацією, характерною для початку розслідування [145, с. 40]. М.О. Селіванов та Л.Г. Видонов трактують, що типова версія – це засноване на спостереженнях умовне міркування, яке виражає ймовірний зв'язок між певними видами елементів криміналістичної характеристики [191, с. 5–6]. Доповнюючи та розвиваючи далі свою концепцію, М.О. Селіванов, порівнює типові версії з результатом узагальненого досвіду слідчої роботи, як деякі абстракції [188, с.108], умовні міркування типу: «Якщо при розслідуванні виявляються якісь ознаки злочину певного виду, то ймовірно, злочин скоєний особою з такими-то даними, за таким-то мотивом» [190, с. 52].

У той час позиції Я.В. Пєщака зводиться до «…сутності достовірних знань, які є результатом отриманого надбання і досвіду слідчої роботи» [169, с. 47 – 48]. І.О. Возгрін вважає: «слідчі версії, що найчастіше висуваються при розслідуванні тих чи інших видів злочинів, називаються типовими версіями» [49, с. 152]. А М.В. Салтевський конкретизує і уточнює: «Версія, що пояснює групу однорідних фактів, обставин, наприклад злочинів, називається типовою» [69, с. 31]. Протилежної думки дотримується О.М. Ларін. Відкидаючи пізнавальну роль типової версії, як різновиду слідчих версій,

наголошує: «вони являють не припустиме, а позитивне знання, що відбиває не конкретну ситуацію, а усі, узагальнені попередньою практикою, ситуації даного виду» [136, с. 7 – 9]. На думку автора, для того, щоб стати позитивним надбанням, знанням, досвідом тощо, типові версії повинні мати бездоганні і вичерпні дані про всі обставини справи. Але, як правило, цього практично досягнути неможливо через об'єктивні, так і суб'єктивні причини. Тому, що типові версії можуть нести у собі не точні, а передбачливі, умовно-наближені знання. В основному типова версія розглядається через призму вихідних даних, що і орієнтують слідчого, оперативного працівника, експерта тощо на вияснення загальних аспектів обставин справи. З гносеологічної сторони типову версію допустимо розглядати за аналогією з категорією загального, оскільки загальне існує в окремому і проявляється через нього [185, с. 31].

Типові версії виконують методичну функцію, а процес розслідування спрямовується на їх конкретизацію, який є залежним від отриманої слідчим інформації [188, с. 108 – 109]. Таким чином, підхід вчених з різних точок зору до аналізу висування типових криміналістичних версій, у черговий раз дає нам зрозуміти, що для кожного з видів протиправних дій він індивідуальний і складність його прямо пропорційна залежності конкретно вираженого злочину. А тому підставою для їх побудови виступає науково-обґрунтований досвід фахівців у розслідуванні зазначеної категорії справ, розумінні суті скоєного, виведенні криміналістичної характеристики.

Саме розробка типових версій являє собою аналіз взаємозв'язку між елементами криміналістичної характеристики в залежності від тієї чи іншої вихідної ситуації. Відповідно, для побудови таких версій необхідно мати хоча б часткові вихідні дані, підкріплені початковими, можливо, подальшими слідчими діями і оперативно-розшуковими заходами, які дадуть поштовх і правильний хід організації розслідування справи. Виходячи з матеріалів вітчизняної та зарубіжної практики у злочинах даної категорії в основу типових версій можна покласти саму мету вчинення такого злочину.

У першому розділі даної монографічної праці було зазначено, що основною метою комп'ютерних злочинів є:

- отримання матеріальної вигоди задля наживи;
- порушення роботи ЕОМ (комп'ютерів), АС, комп'ютерних мереж і мереж електрозв'язку шляхом несанкціонованих дій, пов'язаних з блокуванням роботи технічного засобу; пошкодженням та знищенням окремих електронних машинних документів; внесенням у програмно-технічне забезпечення шкідливих та небезпечних програм; порушенням маршрутизації інформації, яка надходить комп'ютерними мережами чи мережами електрозв'язку та ін.;
- несанкціоновані дії злочинців, пов'язані розповсюдження конфіденційної і таємної інформації та порушення авторських прав. (див. ст. 54 – 60).

Відповідно до встановленої мети монографічної праці, спробуємо сформувати та проаналізувати типові криміналістичні версії, цієї категорії злочинів.

1. Комп'ютерний злочин скоєний з метою отримання матеріальної вигоди, задля наживи

Піддаючи аналізу цей напрям злочинної діяльності, слід насамперед ретельно вивчити матеріали вихідної інформації про злочин, зокрема: обставини справи (місця, часу, обстановки, умов, механізму вчинення тощо). Відповідно, характерні сліди залишені на місці скоєння злочину та можливі сліди приховування несанкціонованих дій осіб. Виявити і встановити шляхи впливу на комп'ютерну інформацію, остання, як правило, залишається без будь-яких змін та модифікацій. З неї відбираються конкретні дані таким чином, щоб не порушити робочого ритму програмно-операційної системи і не видати своєї несанкціонованої присутності у чужих файлах. Можливий інший варіант, коли злочинця зафіксувала система допуску, доступу та контролю під час підбору чи зламування кодів і паролів. А також, коли особа, вчиняючи свої протиправні дії заплуталася чи проігнорувала системи безпеки комп'ютерно-

технічного забезпечення, і залишила по собі явні, специфічні сліди відображення. Не винятком може бути і шпигування за рухом електронної машинної інформації, її вивченням, виявленням слабких місць в комп'ютерній мережі чи мережі електрозв'язку з метою вибору сприятливого часу для її викрадення і використання в корисних цілях. До переліку ймовірних суб'єктів-жертв можемо віднести будь-які установи державної чи приватної форми власності, які у своїй виробничій діяльності використовують маршрутизацію комп'ютерної інформації, що пов'язана з сферою їх діяльності.

1.1. Комп'ютерні злочини у сфері банківської та кредитно-фінансової діяльності

Це найбільш розповсюджена і приваблива сфера злочинної діяльності. На її долю припадає 80–90 % усіх протиправних дій з використанням комп'ютерних технологій. До переліку категорії потерпілих суб'єктів можемо віднести:

- банки та банківські установи різних форм власності;
- державні, госпрозрахункові, комерційні установи, підприємства, організації, фірми тощо, які проводять фінансові операції, фінансову звітність, аудит та ін.

Відповідно до спрямованості комп'ютерних злочинів це може бути:

а) розкрадання та переведення на інші рахунки безготівкових коштів;

б) підроблення фінансових рахунків та інших платіжних документів;

в) легалізація злочинних прибутків;

г) незаконне отримання пільгових та інших видів кредитів тощо.

Зазначені протиправні дії можуть здійснюватися особами-злочинцями як ззовні, так і внутрішньо, працюючим персоналом, тобто, як сторонніми суб'єктами, так і самими працівниками, що перебувають у трудових відносинах з потерпілою стороною. Суттєву допомогу у розслідуванні злочинів у цій сфері може надати віктимологічний суб'єкт, за умови, що він зацікавлений у встановленні об'єктивної істини, а саме: виявленні і притягненні до відповідальності винних осіб. Провідні структури у своєму

арсеналі використовують не лише найсучасніші комп'ютерно-технічні засоби відомих виробників світу, а й належну систему безпеки від несанкціонованого втручання до їх конфіденційної сфери. Таким чином, через власні мережі безпеки захисту виробничого процесу можуть надати вагому допомогу слідству у вирішенні питання, щодо розслідування справи. На підставі викладеного висунемо кілька криміналістичних версій.

Версія 1.1.1. Комп'ютерний злочин скоєно з метою наживи шахрайським шляхом, співробітником даної установи, який є бухгалтером, менеджером, оператором, програмістом програмно-операційного забезпечення або ж іншим найманим працівником, що має доступ до ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку і досконало володіє навичками роботи з ними.

Таку версію можна висунути, коли є достатні підстави вважати, що в банківських, кредитно-фінансових інших установах встановлено факт ведення так званої «подвійної» фінансової документації, бухгалтерії, що може виражатися у незаконному перерахунку коштів підставним юридичним чи фізичним особам, за не існуючо-виконаний об'єм роботи особам, які не мають і не мали відношення і не перебували у жодних правовідносинах з віктимологічною особою. Злочини такого роду вчиняють суб'єкти з числа працюючого чи співпрацюючого з потерпілою особою персоналу, які володіють достатніми знаннями у сфері комп'ютерних технологій і мають доступ та допуск до конфіденційних комп'ютерних даних законного власника чи уповноваженої особи. Фактичними підставами для такого виду посягання у суб'єктами злочину, може бути:

- занадто велика довіра з боку керівництва організації до даної особи, як високопорядної людини, бездоганного працівника, безкорисного і самовідданого ідеї благополуччя і процвітання установи;
- повна або часткова відсутність контролю за діями цього працівника з боку керівного складу посадових осіб, що дає можливість суб'єкту зловживати своїм службовим становищем;

- не задовільна заробітна платня, яка не відповідає кількості виконаного об'єму роботи, що тягне за собою відповідне невдоволення;
- ведення «подвійної бухгалтерії», що дає можливість здійснювати подвійні перерахунки коштів на завчасно підготовлені фінансові рахунки, власні або ж підставних осіб, з подальшою їх конвертацією тощо.

Несанкціоновані дії, як правило, супроводжуються внесенням змін у електронну машинну інформацію, бази даних на короткий проміжок часу для здійснення фінансового шахрайства, з подальшим поверненням даних до початкового стану. Здебільшого вони виконуються злочинцем у робочий час, щоб не привертати до себе уваги в позаурочний час або ж вихідні дні. Фінансова недостача, в основному, виявляється під час бухгалтерських звітів, перевірок іншими уповноваженими структурами чи аудиту. Аналогічні протиправні дії можуть виконувати й інші суб'єкти підприємства (наладчики комп'ютерів, спеціалісти по обслуговуванню та проведенню регламентних робіт, охоронці тощо). При виконанні несанкціонованих дій, вони дотримуються головного правила – не залишати по собі слідів скоєного або ж звести їх до мінімуму і скласти собі алібі про всяк випадок.

Таким чином, при проведенні слідчих дій, особливо на початковому етапі, працівникам правоохоронних органів, при своєчасному і достовірному отриманні інформації про обставини справи, що розслідується, вдається звузити коло суб'єктів, які наймовірніше мають доступ до конкретного комп'ютерного забезпечення, що дає можливість обгрунтованому висуненню криміналістичної версії.

Версія 1.1.2. Комп'ютерний злочин скоєно з метою наживи сторонньою особою, яка досконало володіє навичками комп'ютерних технологій і є поінформованою про виробничий процес, а також конфіденційну комп'ютерну інформацію потерпілої сторони.

Такого змісту версія висувається практичними працівниками правоохоронних органів, коли є достатні підстави вважати, що злочин було скоєно сторонньою особою по відношенню до суб'єкта-жертви, з віддаленого (зовнішнього) комп'ютера. Потерпілою стороною у даному випадку можуть бути такі ж самі суб'єкти підприємницької діяльності, що зазначені і у попередньому варіанті криміналістичної версії (див. версію 1.1.1). Характерними ознаками даної протиправної дії суб'єктів є:

- добра комп'ютерна оснащеність і вміння досконало володіти навичками комп'ютерних технологій;
- професійний підбір або ж вміння зламувати системи доступу до баз даних комп'ютерного забезпечення, а також обходження систем безпеки (охорони) при проникненні в чужі програмні забезпечення;
- своєрідність вчинення злочину і жорстокість поводження з чужими базами даних, окремими файлами;
- неодноразовість здійснення такого виду протиправних дій за допомогою ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку і надзвичайна жадібність у заволодінні коштами;
- вміння професійно знищувати або ж заплутувати сліди скоєного ним комп'ютерного злочину.

Здійснюється такий злочин стороннім суб'єктом з використанням глобальної мережі INTERNET. Це можуть бути «хакери» та їх різновиди, що орієнтуються в комп'ютерних мережах чи мережах електрозв'язку на достатньому, професійному рівні володіють знанням ЗЕОТ (засобами електронно-обчислювальних машин) або ж інший фахівець, що спеціалізується на комп'ютерних засобах. За таких обставин справи, слід переглянути у відділі кадрів установи, що виступає потерпілою стороною, всіх осіб, які працювали раніше у цій організації. Звернути увагу на осіб з спеціальною програмно-технічною освітою.

Можлива така ситуація, що суб'єкт перебував у трудових правовідносинах раніше з потерпілою стороною, був достатньо

поінформований з специфікою діяльності підприємства, володів даними конфіденційної чи таємної комп'ютерної інформації, знав системи допуску, доступу та контролю, але з тих чи інших причин звільнився чи був звільненим з роботи і, як прояв своєї невдоволеності, почав займатися протиправною діяльністю або ж передав інформацію іншій зацікавленій особі. На цьому етапі досудового слідства необхідно опитати керівний склад підприємства та працюючого персоналу на предмет такої категорії осіб, що звільнилися. Перевірити електронні журнали реєстрації роботи персоналу в мережі INTERNET та ін. Шляхом оперативно-розшукових заходів, з отриманням відповідних санкцій, встановити негласне спостереження за виробничим процесом віктимологічної особи та взяти на відповідний термін під контроль вхідну та вихідну електронну інформацію зазначеного об'єкта, включаючи телефонну мережу зв'язку.

Як наглядний матеріал можемо навести приклад з комп'ютерним шахрайством, що відбулося у м. Москві на при кінці 90-х років. Група з 14 осіб протягом півроку вчинила 269 шахрайств з використанням кредитних карток платіжних систем VISA, MASTER CARD, AMERICAN EXPESS на загальну суму більш, як 80 тис. доларів США. У 1996 р. при спробі зняття 1,5 млрд. крб. через банкомати банків у Пермі, Москві та Санкт-Петербурзі, злочинні дії осіб були зупинені, а суб'єкти притягнуті до кримінальної відповідальності [190, с. 2].

Версія 1.1.3. Комп'ютерний злочин вчинено з метою наживи організованою злочинною групою осіб за попереднім зговором з використанням ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку.

Реальна, логічна, науково-обгрунтована криміналістична версія, яка є найбільш розповсюдженою з-поміж інших версій. Злочинний елемент для досягнення своїх протиправних задумів формує групу з притаманними їй складовими. Вони організовуються на принципах ієрархічної побудови і мають досить налагоджену систему поінформованості про суб'єкта підприємницької

діяльності, що становлять для них «злочинну цінність». До кола осіб такої групи входять:

- особи, які володіють комп'ютерними інформаційними даними, при тому досконаліть їх знань у ЗЕОТ не є обов'язковою. Достатньо хоча б одного суб'єкта – професіонала, який би реалізовував злочинний задум групи;
- суб'єкти, що можуть організувати безпроблемний доступ до електронних інформаційних технологій, окремих баз даних об'єкта, який буде піддаватися несанкціонованим діям;
- особи, котрі володіють достовірними даними про предмет безпосереднього злочинного посягання.

Такими можуть бути злочинці як з числа працюючого у потерпілої сторони персоналу, так і сторонні суб'єкти. Тобто:

- сторонні особи, які виконують суто технічну роботу і в жодних стосунках з організацією-жертвою не перебувають, і не перебували;
- особи, які володіють окремою інформацією про саму установу, специфіку її виробничої діяльності, але у виробничих і партнерських стосунках не перебувають і не перебували;
- особи, що донедавна працювали або ж співпрацювали з суб'єктом-жертвою, але з окремих міркувань перейшли на бік протиправної діяльності;
- особи, котрі перебувають у виробничих відносинах з зазначеною установою. Як правило це керівники та віднесені до переліку керівного складу суб'єкти, які належно обізнані в специфіці фінансової діяльності свого ж підприємства. А також інші штатні працівники установи, що володіють зацікавленими даними і мають доступ, хоча б опосередковано, до засобів комп'ютерних технологій (програмісти, оператори, обслуговуючий персонал комп'ютерного забезпечення, працівники служби охорони тощо).

Відпрацьовуючи таку криміналістичну версію практичні працівники правоохоронних органів повинні звернути увагу на характерні особливості несанкціонованого проникнення у базу даних комп'ютера потерпілої сторони. Злочинці, за такої умови, вчиняють протиправні дії з віддаленого комп'ютерного забезпечення, використовуючи при цьому INTERNET і вплив на ЕОМ, АС та її систему через модемний зв'язок. Ймовірно, на місці настання шкідливих чи небезпечних наслідків будуть залишені й інші сліди зовнішнього втручання в комп'ютерні мережі, які теж повинні бути враховані і зафіксовані в процесуальних документах. Як зазначав у своїй праці Г. Гросс: «… у всіх протоколах огляду потрібно відзначати не тільки те, що знайдено, але й найбільш важливі «негативні» обставини, для того, щоб було зрозуміло, що ніщо не пропущено» [78, с. 21].

Якщо ж відсутній спосіб проникнення в системи захисту, а також зламування систем допуску, доступу та контролю до об'єкта дослідження, тоді висновок один – у злочинну організовану групу входить штатна особа з того ж самого підприємства, яке видає себе, разом з іншими, потерпілою стороною. Для правильності висунення криміналістичної версії слід врахувати і той факт, що місце з якого вчинений злочин може бути не одне, а кілька, причому надзвичайно віддаленими одне від одного, що тим самим ускладнює методику розслідування злочину, пов'язаного з використанням комп'ютерних технологій. Одним з таких прикладів є широковідома справа В. Лєвіна, колишнього жителя Санкт-Петербурга, Росія, який за попереднім зговором з іншими особами вчинив злочин світу, викравши 10 – 12 млн. доларів США з міжнародного банку «Сіті банк & Америка» [168, с.5 – 6].

2. Порушення роботи автоматизованих систем шляхом знищення електронної інформації, модифікації комп'ютерних програм, блокування роботи технічного оснащення операційних ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку.

Про такі злочини можемо говорити, коли є достатні підстави вважати, що відбулося протиправне порушення роботи автоматизованих комп'ютерних

систем чи роботи мереж електрозв'язку і воно виявлене власником, добросовісним користувачем, а також іншим суб'єктом. Тобто, зафіксовано зміни, які відбулися або відбуваються у окремо взятій комп'ютерній програмі, файлі, мережі та ін. поза волею її власника. До таких змін відносимо:

- повне чи часткове знищення електронної інформації або ж доведення її до стану непридатності;
- внесення до бази даних, в окремі файли ЕОМ (комп'ютерів), АС, комп'ютерні мережі тощо шкідливих, у тому числі небезпечних, програм-вірусів активного характеру;
- тимчасове призупинення, виведення з ладу, а також повне блокування роботи технічного обладнання, комп'ютерного програмного забезпечення, окремих інформаційних комп'ютерних даних.

Протиправні дії вчиняють особи, які належно володіють знаннями у сфері комп'ютерних технологій, використовуючи для цього інше комп'ютерне устаткування забезпечене доступом до глобальної, міжнародної мережі INTERNET та шкідливу чи небезпечну електронну інформаційну програму, за допомогою якої скоюється злочин зазначеної категорії. Основними мотивами злочинців цього напряму є: користь, помста, зухвалість, ревнощі та ін. Виходячи з викладеного, висунемо такі типові слідчі версії.

Версія 2.1. Комп'ютерний злочин скоєно особою з метою внесення у базу електронних даних, окремого програмного забезпечення, файлу тощо, інформації, що містить шкідливі чи небезпечні дії, які в кінцевому результаті спричиняють непередбачувані наслідки добросовісному власникові.

Висуваючи цю версію, необхідно виходити з того, що в базі даних, окремому файлі програмного забезпечення виявлено шкідливу комп'ютерну програму (вірус), яка спричинила чи спричиняє свій негативний вплив на роботу ЕОМ (комп'ютери), автоматизовані системи та саму комп'ютерну інформацію і піддає її руйнуванню, модифікуванню, знищенню електронних даних. Внесення такого роду різнопланових паразитичних програм у добросовісну програму, можуть здійснювати особи, що є штатними

працівниками установи, а також сторонні особи, що перебувають поза виробничою діяльністю юридичної особи.

На етапі відпрацювання слідчими цієї версії необхідно отримати кваліфіковані консультації відповідних спеціалістів про характер вірусної атаки, її специфіку та наслідки. Це дасть можливість встановити професійні дані, якими володіє протиправна особа, що вчинила такого роду злочин. При дослідженні скоєного слід визначити:

- яким чином і хто персонально виявив шкідливу програму в ЕОМ (комп'ютері) та її мережі;
- безпосередньо в якому програмному документі і в який час;
- кількість програмних забезпечень, що піддалися зараженню даним вірусом;
- якою мережею (локальною, віддаленою) з'єднані між собою комп'ютери;
- якими антивірусним оснащеннями забезпечені комп'ютерні мережі даної установи; як часто вони перевіряються; хто персонально за них несе відповідальність;

З'ясування зазначеного кола обставин дасть можливість слідчому встановити – чи причетний штатний персонал до протиправної дії, чи несанкціоноване втручання було вчинено ззовні без будь-якої сторонньої допомоги. За умови вчинення злочину штатними співробітниками установи, слідчому необхідно опитати та допитати працюючий персонал, провести оперативно-розшукові заходи та невідкладні слідчі дії з метою затримання підозрюваних осіб. При зовнішньому несанкціонованому втручанні осіб-злочинців у чуже програмне забезпечення необхідно дослідити шляхи проникнення в ЕОМ (комп'ютери) та їх програмне забезпечення та виявити, зафіксувати і вилучити залишені комп'ютерні сліди. Детальне вивчення фахівцями специфічних матеріальних слідів відображення дасть можливість встановити направленість протиправної дії, а можливо й психологічну налаштованість особи-злочинця. Адже не винятком може бути злочинець-

початківець, що оволодіває знаннями комп'ютерних технологій; хакер-жартівник; суб'єкт з числа психічно хворих, неврівноважених осіб тощо, який володіє навичками комп'ютерних технологій, але страждає одним із видів комп'ютерного захворювання, зокрема: комп'ютерною фобією та ін.

Версія 2.2. Комп'ютерний злочин скоєно суб'єктом протиправної діяльності з метою впливу на роботу ЕОМ (комп'ютерів), автоматизованих систем, що спричинило блокування, зупинення чи порушення роботи комп'ютерних мереж і мереж електрозв'язку.

Таку версію та подібну їй висувають суб'єкти, уповноважені законом здійснювати розслідування злочинів, за умови наявних ознак протиправних дій, до яких вдаються комп'ютерні злочинці, переслідуючи ту чи іншу мету. Це може бути:

- тимчасове призупинення роботи автоматизованої системи та її складових, яке пов'язане з несанкціонованим втручанням у дану сферу діяльності;
- блокування комп'ютерної мережі чи мережі електрозв'язку, що порушує роботу всього системно-технічного забезпечення;
- часткове або ж повне виведення з ладу автоматизованого, комп'ютерно-технічно та мережевого електрозв'язку, що спричиняє непередбачувані наслідки для законних власників та добросовісних споживачів, які є користувачами цих телекомунікаційних систем.

Мотивом і метою перелічених вище злочинних дій здебільшого є: хуліганські наміри, помста, заздрість, ревнощі, кар'єризм, конкуренція та ін. Злочини такого характеру вчиняють як штатні працівники установи, так і сторонні особи. Тому висуваючи запропоновану версію, практичні працівники повинні зважено підійти до визначення того, яким саме чином було здійснено даний злочин. Розглянемо два варіанти.

1) Протиправна дія вчинена суб'єктом з числа штатного працюючого персоналу, що виступає потерпілою стороною.

Наявними ознаками злочину повинні бути сліди не зовнішнього, а внутрішнього впливу на автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку. Тобто, відсутній механізм стороннього проникнення до зазначеного телекомунікаційного забезпечення. Суб'єкт злочину – особа (особи), що належним чином володіють знаннями ЕОМ (комп'ютерів) і пов'язаних з їх діяльністю систем.

За такої слідчої ситуації, яка склалася, слід допитати в якості свідків: оператора, комп'ютерного програміста, інженера-системника технічного та системного забезпечення тощо. Проглянути у відділі кадрів особові справи працюючого персоналу для встановлення осіб, які:

- володіють і попередньо займалися забезпеченням чи обслуговуванням комп'ютерного устаткування як у цій, так і в інших структурах;
- осіб, котрі щойно були прийняті на роботу в дану установу і мають відношення до ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку;
- працівників, які недавно звільнилися чи були звільнені з даної установи, але перебувають у дружніх чи ділових стосунках з окремими суб'єктами організації, в якій вчинено комп'ютерний злочин.

2) Злочин вчинено суб'єктом (суб'єктами) зовні за допомогою інших ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку.

Така протиправна дія скоюється особою (особами) з використанням глобальної мережі INTERNET або ж іншої телекомунікаційної мережі з використанням модемного зв'язку. Відповідно суб'єкт протиправної дії має залишити по собі характерні сліди злочину – підбір або ж зламування кодів та паролів до програмного забезпечення, які повинна зафіксувати система безпеки, шляхи проникнення та результат злочинного замислу. За умови відсутності явних слідів зламування систем захисту, можна дійти такого висновку:

- особа-злочинець самостійно володіє інформацією про системи доступу, допуску та контролю конкретного технічного оснащення, що підпало під несанкціоновані дії;
- особі-злочинцеві надана інформація про предмет злочину іншим суб'єктом з числа:

  а) працюючого персоналу;

  б) тих, що працювали;

  в) тих, які від інших осіб володіють інформацією про предмет злочину та системи обходження заходів безпеки доступу до комп'ютерного оснащення.

За такої ситуації практичні працівники повинні залучити до участі в розслідуванні фахівців та експертів у сфері комп'ютерних технологій з метою детального вивчення інших можливих слідів скоєного та відстежування місця звідки найімовірніше було вчинено даний злочин.

3. Незаконне заволодіння, розповсюдження та використання електронної інформації комп'ютерними злочинцями, яка знаходиться в ЕОМ (комп'ютерах) добросовісних її власників і містить таємні чи конфіденційні дані.

Про таку категорію злочинів йде мова, коли слідство володіє достатніми даними, що комп'ютерна інформація, яка перебувала у власності держави, і мала статус таємної інформації, чи у володінні, користуванні окремих фізичних або юридичних осіб, і мала конфіденційний характер, - не санкціоновано потрапила до інших осіб. Оскільки такі комп'ютерні інформаційні дані мають обмежений доступ користувачів, вони наділені правом захисту відповідно до чинного законодавства, зокрема: ст. 428 Закону України «Про державну таємницю» від 21.09.1999 р. ст.30 Закону України «Про інформацію» від 03.04.2003 р. та ін. нормативно-правових актів. Детальне викладення змісту такої категорії злочинів зазначене у підрозділі 1.3.5. «Слідові картина злочинів» цієї монографічної праці.

Чільне місце при дослідженні зазначеної категорії злочинів посідає порушення конфіденційної інформації, яка знаходиться в ЕОМ (комп'ютерах) та її системах, що наділена авторськими правами.

Предметом посягання є сама комп'ютерна конфіденційна електронна інформація, яка знаходиться у володінні чи користуванні суб'єктів всіх форм власності і охороняється законом. А також інформація, що захищена авторським та суміжним правами, яка виникає у зв'язку зі створенням і використанням творінь науки, культури, мистецтва тощо. На підставі того, що комп'ютерні технології наразі практично витіснили традиційні друкарські машинки, деякою мірою і графічні навички авторського письма, частково замінили з паперового викладу матеріалу на електронний, тим самим дали підґрунтя окремій категорії осіб займатися злочинним комп'ютерним промислом неналежної їм тієї чи іншої інформації. До переліку злочинних посягань можуть відноситися будь-які інформаційні дані, що знаходяться на електронних комп'ютерних носіях, про державну чи комерційну таємницю; наукові розробки-дослідження; військову, виробничу та наукову новизну, що становлять відповідну зацікавленість для інших недобросовісних суб'єктів. Це комп'ютерна електронна інформація, яка є:

- у власному володінні, користуванні та розпорядженні добросовісних суб'єктів різних форм діяльності, а також суб'єктів наукової і творчої інтелігенції;
- на правах власності у фізичних та юридичних осіб, що займаються відкриттям у певній сфері діяльності, розробкою окремих проектів, програмних продуктів тощо;
- студійних розробок, які створюють та продукують власне відео, музичну, кіно продукцію;
- видавництв, майстерень тощо, що займаються випуском продукції літератури, живопису, графіки та ін.

Така конфіденційна електронна інформація часто-густо викрадається з самими магнітними носіями або ж без них, з метою швидкої реалізації за

здешевлену ціну, до моменту випуску даної продукції її добросовісним власником. Прикладом тому може бути порушена кримінальна справа у м. Красноярську в 1994 р., де з НДІ «Біофізика » злочинцями був викрадений магнітний диск з розробками у сфері медицини, які вважалися ноу-хау у дослідженні імунології людини, вартість яких оцінювалася у 720 тис. доларів США [152, с. 1]. Виходячи з викладеного, можемо висунути такі типові слідчі версії:

Версія 3.1. Злочин скоєно особою шляхом впливу на комп'ютерну інформацію з метою заволодіння, знищення чи маніпуляції електронними даними, що спричинило непередбачувані наслідки для її власника.

Висуваючи цю версію слідчому, оперативному працівникові та іншим учасникам кримінального процесу слід достовірно мати інформацію про те, що дійсно такий злочин стався, а не відбулося добросовісної помилки (самообману) з боку потерпілої сторони. При цьому мають бути наявні ознаки скоєного, зокрема:

- фіксація комп'ютерно-технічними засобами несанкціонованих дій з електронними даними, що знаходяться у самій комп'ютерній системі чи окремому файлі;
- повна чи часткова заміна комп'ютерних інформаційних даних;
- доведення певної електронної інформації до стану непридатності;
- знищення окремих інформаційних даних у комп'ютерній системі.

Злочини такого виду може скоювати як одна особа, так і сформована злочинна група. Усе залежить від складності протиправної дії та конкретного наміру, з якою метою його вчинили. За даної версії злочин має прямий умисел. Рідше трапляються характерні злочини за умови допитливості суб'єкта, що в кінцевому результаті призвели до настання негативних наслідків. При висуненні та відпрацюванні цієї версії і визначенні кола осіб, що можуть мати відношення до даної справи, необхідно як і в попередніх версіях, вияснити можливу причетність до злочину штатного працюючого персоналу потерпілої сторони. А також встановити:

- наявність непорозумінь та конфліктних ситуацій віктимологічної сторони з суб'єктами, що працюють, працювали або ж перебували в партнерських стосунках з зазначеною юридичною чи фізичною особою;
- з'ясувати, чи ніхто не виражав їм у письмовій, електронній чи усній формі своє невдоволення, погрози тощо;
- встановити, чи були раніше аналогічні або ж інші випадки несанкціонованого втручання у сферу діяльності потерпілої сторони.

Виходячи зі змісту виявленого і встановленого, слідчий може дійти висновку про морально-психологічний клімат і взаємовідносини, які панують в установі, чи усталені погляди соціуму у суспільстві, що внесе відповідну ясність до визначення кола ймовірних суб'єктів скоєного злочину.

Версія 3.2. Комп'ютерний злочин скоєно з метою порушення авторських прав суб'єктом, що є фахівцем в сфері ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку і володіє даними про предмет злочину

Така версії висувається виходячи із змісту слідчої ситуації, що склалася. Складність її відпрацювання полягає у тім, що до переліку осіб, які мають доступ до комп'ютерних технологій можемо віднести практично весь працюючий персонал, який задіяний у виробничих стосунках конкретного підприємства. Протиправним діям цього виду злочину притаманна така мета:

- нажива – викрадення та реалізація чужої конфіденційної електронної інформації, яка приносить швидкі і добротні прибутки. Збут комп'ютерної інформації шляхом тиражування програм на гнучких дискетах та лазерних дисках. Розмноження музичних компакт-дисків, відеофільмів, друкованої продукції тощо;
- помста – одна з форм вираження злості, незадоволення, ганебного ставлення до інших осіб з тих чи інших життєвих поглядів. Може виражатися через викрадення будь-якої електронної інформації, що

належить іншому суб'єкту на правах власності та захищена авторським правом;

- кар'єризм – досягання поставленої мети будь-якими чесними та нечесними шляхами. Викрадення, привласнення та використання у своїх цілях чужої інтелектуальної праці.

Такого роду злочини можуть учинятися як одноособово, так і групою осіб все залежить від питомої ваги предмету посягання. За даної слідчої ситуації практичним працівникам необхідно насамперед встановити, кому саме належить авторське право на викрадений продукт; хто мав до нього вільний доступ; кількісний і персональний склад осіб, що були задіяні у процесі виготовлення такої продукції; конкуруючих та зацікавлених у цьому витворі су'єктів; механізм передачі цієї конфіденційної електронної інформації іншій стороні.

Версія 3.3. Комп'ютерний злочин скоєно з метою порушення авторських прав суб'єктом (суб'єктами), які безпосередньо не мають доступу до зацікавлених електронних даних, а отримують таку інформацію опосередковано від інших суб'єктів.

На противагу попередній версії, ця має встановити механізм отримання протиправною особою зацікавлених даних предмета посягання. Мова йде про сторонню особу-злочинця, яка, можливо, суто технічно виконувала чиєсь замовлення. Не винятком може бути виконання протиправних дій організованою групою осіб за участю суб'єкта, який володіє зацікавленими даними або ж має доступ до комп'ютерного забезпечення, в якому міститься комп'ютерна інформація про предмет злочину. Метою протиправності є користь, нажива, рідше помста чи кар'єризм. При висуненні та відпрацюванні цієї версії практичним працівникам належить звернути увагу на те, яким саме чином відбулося порушення авторських прав. Розглянемо два варіанти несанкціонованих дій:

1) Викрадення конфіденційної електронної інформації відбулося безпосередньо шляхом проникнення у помешкання до потерпілої особи чи на

її робоче місце. Копіювання зацікавлених даних було проведено на завчасно підготовлені та принесені з собою магнітні носії. До таких дій злочинець може вдатися видаючи себе за фахівця-експерта чи дослідника зазначеного напрямку діяльності. На умовах довіри, обіцянок або ж неуважності особа потрапляє у стан ошуканості.

2) Злочин вчинено ззовні шляхом проникнення у базу даних комп'ютерних мереж чи мереж електрозв'язку з використанням INTERNET та іншого телекомунікаційного забезпечення. При цьому не завжди можна відновити слідову картину злочину, а також встановити місце, звідки було вчинено несанкціоноване проникнення до чужої комп'ютерної інформації. Однією з прогалин власників авторського права є відсутність або ж неналежне захищення своєї електронної (машинної) інформації системами комп'ютерної безпеки. Ігнорування прогресивними розробками аутентифікації та ідентифікації доступу до баз даних програмного забезпечення. Використання криптографії через електронні ключі при передачі та обміні комп'ютерною інформацією з іншими абонентами та ін.

Відпрацювання та перевірка версії про ймовірних осіб, що скоїли такий злочин, відбувається за аналогічною схемою, яка викладена при описанні версії 1.1.2.

2.6. Організація і планування розслідування комп'ютерних злочинів

Розслідування злочинів з використанням ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку, як і інша категорія злочинів, вимагають від слідчого надзвичайно багато розумових знань, практичних навичок, вирішення великої кількості організаційних питань для встановлення істини за конкретно визначеною кримінальною справою. Планування розшукової роботи, насамперед, означає узгодженість між елементами розшукової діяльності слідчого і оперативно-розшуковими підрозділами та спільно проведеними процесуальними заходами

в рамках кримінально-процесуального закону. Вона може виражатися в наступному:

- у єдності цілей розшукових заходів, які здійснюються в процесі розшуку, додатковому характері тих чи інших відносно одне одного, комплексності їх планування і проведення;
- у тісній взаємодії і діловій безперервній співпраці між суб'єктами розшукової діяльності у цілому –слідчим і оперативними співробітниками [142].

Від дій слідчого при вирішенні організаційних питань залежить:

- своєчасність і правильність підготовки та проведення початкових та подальших слідчих дій і оперативно-розшукових заходів;
- взаємодія, при потребі, з практичними структурами (МВС, СБУ, ДПА, НДІСЕ) та з іншими державними і комерційними організаціями, а також окремими суб'єктами, які можуть надати кваліфіковану допомогу;
- раціональність і ефективність розстановки сил та правильності, своєчасності застосування науково-технічних засобів для виявлення, фіксації і вилучення слідів скоєного.

Планування розслідування являє собою творчий розумовий процес, який включає в себе визначення змісту і порядку роботи щодо встановлення всіх обставин скоєного злочину і викриття винних відповідно до вимог закону з найменшими затратами часу, сил і засобів [134, с. 274–275]. Існують різні точки зору стосовно організації планування розслідування справ, пов'язаних з використанням комп'ютерних технологій. Окремі вчені-криміналісти вважають, що планування може мати усний характер, оскільки у своїй основі становить не статичний, а динамічний розвиток, який залежить від конкретних обставин справи. Інша частина фахівців схильна до обов'язкового складання плану і саме у письмовій формі перед, або ж після проведення огляду місця події, не залежно від того, чи він змінюватиметься, чи ні у процесі слідства.

Складання плану організації розслідування у категорії злочинів, що досліджується, повинен мати гнучкий характер. Тобто, якщо слідчий володіє достатньою кількістю вихідної інформації про ознаки злочину, він може на початковій стадії при порушенні кримінальної справи скласти хоча б попередній, простий письмовий план розслідування та подальшої організації відповідних заходів. У цій ситуації доцільно буде згадати Ганса Гросса, який на зорі зародження науки криміналістики рекомендував, що задатком успішного проведення розслідування справ є у «більшості випадків складання плану, по можливості не складного» [78, с. 20]. За інших обставин, коли слідчий володіє лише окремим загальним уявленням про злочин у сфері використання ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку, план проведення відповідних організаційних заходів може мати і усний характер. Письмового викладення слідчим він набуде після проведення початкових слідчих дій та оперативно-розшукових заходів, за умови, коли зібрано мінімальний набір інформації про обставини злочину і можна вже говорити про висування типових слідчих версій. При цьому, письмова форма може мати різне викладення (таблиці, схеми, картки, графіки тощо), залежно від зручності користування тим чи іншим учасниками кримінального процесу. Сама організація розслідування складається з:

- визначення завдань розслідування з урахуванням вчиненого злочину;
- побудови (висунення) слідчих версій;
- аналізу версії та визначення обставин (питань), які необхідно встановити;
- визначення слідчих дій, оперативних засобів та інших перевірочних та профілактичних заходів, необхідних для встановлення запланованих обставин;
- вибору конкретних виконавців і термінів виконання [35, с. 268].

Не виникає суперечностей між авторами і стосовно мети планування розслідування, а до таких відносяться:

- забезпечення повноти, об'єктивності та всебічності розслідування;

- визначення направлення і змісту діяльності слідчого на всіх етапах розслідування;
- раціональне використання часу, сил і засобів;
- ефективність застосування криміналістичних прийомів і засобів роботи з інформацією, яка виступає джерелом доказів [130, с. 196].

Між вченими-криміналістами Р.С. Бєлкіним, Л.Я. Драпкіним, І.М. Лузгіним, М.І. Порубовим, В.А. Образцовим, А.Г. Філіпповим існують окремі розбіжності дискусійного характеру у визначенні основоположних принципів планування розслідування злочинів, але ми не ставимо за ціль полемізувати в цьому питанні. Як на автора, більш виважене трактування цього питання викладено вітчизняними криміналістами: П.Д. Біленчуком, В.С. Кузьмічовим, Г.І. Прокопенком, М.В. Салтевським, В.Ю. Шепітьком та ін. Вони наголошують, що основними принципами планування є: індивідуальність, динамічність, реальність та конкретність [116, с. 31]; [185, с. 106]; [132, с. 210]; [35, с. 268]. Перелічені принципи без винятку мають застосовуватися при організації планування розслідування всіх категорій злочинів, включаючи і комп'ютерні. З-поміж всіх інших, особливий інтерес злочинів, що досліджуються, становлять принципи індивідуальності та реальності. При організації розслідування, віднесених до цієї категорії злочинів, слідчий повинен індивідуально підходити до реалізації комплексу спланованих дій з урахуванням відповідних можливостей. Для цього необхідно:

- на достатньому рівні (хоча б користувача) бути обізнаним у сфері комп'ютерних технологій;
- вміти грамотно підійти до формування слідчо-оперативної групи з можливим залученням відповідних спеціалістів з різних структур та підрозділів;
- забезпечити підготовку та правильно використати необхідні техніко-криміналістичні засоби;

- завчасно продумати і визначити, за потреби, установу, де буде проводитися програмно-технічна експертизи тощо.

Принцип реальності включає в себе організацію та проведення відповідних заходів шляхом не уявних надуманих дій слідчого, а конкретної оцінки ситуації, що склалася. Слід враховувати реальні можливості слідства використовуючи при цьому всі передбачені законом засоби досягнення істини, будувати реальні версії і шляхи їх перевірки [174, с. 4]. Звичайно, застосування цього принципу не завжди супроводжується достовірною і повною оцінкою того, що відбулося. На практиці, слідчий доволі часто стикається з рядом проблемних аспектів у визначенні об'єму скоєного злочину, способу вчиненої дії, фактичних наслідках, виявленні слідів протиправності та встановленні кола осіб, що вчинили комп'ютерний злочин та ін.

У цьому сенсі дає про себе знати, як один із чинників, недостатність знань і практичних навичок у осіб, на яких покладається розслідування такої категорії кримінальних справ. Окремі працівники відповідних структур мало у чому вбачають різницю планування розслідування справ між „традиційними" та „нетрадиційними" видами злочинів, що є суттєвою помилкою. Потрібно враховувати специфіку вчинених комп'ютерних злочинів, а від неї вже реально відштовхуватися до тактичних особливостей організації та проведення тих чи інших процесуальних заходів. Зважимо, що планування розслідування не зводиться тільки до складання плану розслідування – це частина великої проблеми розкриття злочинів. Планування є обов'язковою складовою загального процесу організації розслідування [81, с. 285].

Розглядаючи організацію планування розслідування справ, пов'язаних з використанням комп'ютерних технологій, ми не ставимо за мету нав'язати свою точку зору в розробці алгоритмізації всього комплексу тактичних заходів, яких повинні дотримуватися практичні працівники у цьому аспекті справ, адже запропонований виклад має суб'єктивний характер бачення автора. У той самий час вважаємо за необхідне внести суттєві пропозиції у розробку окремих питань планування, що стосуються вивчення та дослідження

комп’ютерної злочинності, особливо на початковому етапі розслідування справи, від якого залежить подальший хід та результат довершеної конкретної кримінальної справи у злочинах зазначеної категорії.

У цьому сенсі доцільним є планування діяльності слідчого при розслідуванні комп’ютерних злочинів таким чином, щоб початковий етап мав кілька підетапів, це дасть можливість звернути увагу уповноважених законом осіб на особливостях та тонкощах цієї категорії злочинів на відміну від інших вчинених злочинів.

Перший підетап – розпочинається з отримання вихідної інформації про злочин і закінчується підготовчими діями перед виїздом на огляд місця події. Він окремими елементами збігається з підготовчим етапом розслідування справи, але має свої індивідуальні особливості. Перш за все:

- викладені підетапи застосовуються при окремих слідчих діях – це огляд місця події, обшук, виїмка;
- його дії спрямовані на сприяння та орієнтування слідчого у визначенні організаційних заходів, пов’язаних з підготовкою та проведенням невідкладних слідчих дій.

Як приклад, можемо проаналізувати розвиток подій за такою схемою:

1) факт вчинення комп’ютерного злочину став відомим правоохоронним органам у відповідності до (ч.1ст.94) Кримінально-процесуального кодексу України. Тобто зазначений злочин відбувся з усіма відповідними складовими. За цієї обставини розвиток підетапу переходить на рейки підготовчих дій та проведення слідчих та оперативно-розшукових заходів;
2) факт протиправних дій злочинця зафіксовано під час скоєння злочину і є реальна можливість прослідкувати за даним суб’єктом, а також вжити всіх заходів по його затриманню «на гарячому». Такий розвиток подій має ідеальний вигляд для прийняття слідчим одного з тактичних рішень, а саме:

- встановити спостереження за діями особи, що вчиняє протиправність, з метою виявлення всіх можливих каналів, якими проходитиме електронна інформація, тим самим зафіксувати кінцевий пункт надходження викрадених даних та ймовірних причетних до цього суб'єктів;
- у мінімальний відрізок часу вжити всіх заходів по затриманню злочинця на місці події з речовими доказами.

Якщо ж прийнятий слідчим другий варіант тактичного рішення, тоді потрібно терміново провести спланований відповідний захід, паралельно контролюючи через ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку протиправні дії, що вчиняє злочинець, з метою не випустити його з поля зору, а разом з тим не дозволити нанести надзвичайно складних матеріальних, технічних та інших збитків. По закінченню невідкладної слідчої дії, за даним фактом порушується кримінальна справа, разом з тим в наявності є підозрюваний суб'єкт (суб'єкти), а також джерело доказового значення.

Коли ж слідчий прийняв перший варіант тактичного рішення, він на власний розсуд визначає:

- окремі обставини проведення слідчої дії;
- формує слідчо-оперативну групу та готує необхідні техніко-криміналістичні засоби;
- намічає оперативно-розшукові заходи, а саме:

а) вивчення місцевості, де буде проводитися слідча дія;

б) встановлює негласний перегляд комп'ютерної інформації, яка надходитиме каналами електрозв'язку, включаючи телефонні розмови;

в) проводить опитування осіб, ідеальних джерел доказового значення, котрі можуть надати допомогу слідству;

г) збирає інші дані у вигляді довідок, схем, графіків тощо.

Однак зволікати з реалізацією намічених слідчих і оперативно-розшукових заходів стосовно комп'ютерних злочинів теж не слід. Адже сліди скоєного мають специфічну ознаку, пов'язану з віртуальністю електронної інформації у комп'ютерних мережах чи мережах електрозв'язку, за яких швидкість зникнення хоча б частини доказової інформації може негативно вплинути на кінцевий результат розслідування даної кримінальної справи.

Другий підетап – бере початок з прибуття на місце події і закінчується початком слідчої дії. Саме на цьому підетапі формуються підвалини подальшого ходу конкретної слідчої дії. Сформована слідчо-оперативна група від теоретичних настанов потрапляє у реальну (практичну) обстановку, де буде проводитися конкретний процесуальний захід. Доволі часто трапляються не передбачувані обставини справи, які на початковому підетапі не були відомі або до кінця врахованими та продуманими. Наприклад, частина комп'ютерного обладнання, згідно з графіком профілактичних заходів, була виведена тимчасово з робочого стану, окремі програми піддалися інсталяції. Або ж на час прибуття для проведення слідчої дії виявлено факт знеструмлення даного об'єкту за незалежними від них причинами й інший термін, на який буде перенесено процесуальний захід, може мати втрату електронної інформації тощо. За обставин без проблемності наміченої слідчої дії слідчому необхідно переконатися, що:

- слідчо-оперативна група сформована правильно;
- всі учасники процесу, включаючи понятих, проінструктовані й готові виконувати покладені на них обов'язки;
- техніко-криміналістичні засоби для виявлення, фіксації, вилучення предмета дослідження, а також допоміжний інвентар є у достатній кількості у належному стані і відповідають призначенню;
- керівний та робочий персонал повідомлений про проведення даної слідчої дії і на час її проведення відлучений від закріплених персональних місць та ін.

За цих умов слідчо-оперативна група може переходити до практичного, поетапного виконання спланованого процесуального заходу.

Третій підетап – розпочинається після проведення окремо взятої слідчої дії, коли наступає оптимізація слідчим даних про обставини справи. На цьому підетапі:

- підсумовується хід проведеного процесуального заходу;
- аналізується виявлена електронна комп'ютерна інформація, що має значення для розслідування справи;
- переглядається попередньо складений план розшуку, при потребі оновлюється чи уточнюється;
- висуваються типові слідчі версії;
- розробляється план подальших слідчих дій.

Таким чином, слідчий, реально оцінюючи ситуацію із злочинами, пов'язаними з використанням комп'ютерних технологій, на підставі отриманого результату переводить слідство у творчий процес. Порівнюються і оцінюються типові версії, а на їх основі з урахуванням виявлених електронних даних розробляються конкретні слідчі версії. Слідство в цей час вирішує головне завдання – визначає правильне спрямування розслідування, вибирає із кількості версій найбільш реальні, а з них одну, істинну [123, с. 18–19].

РОЗДІЛ 3. ПОДАЛЬШИЙ ЕТАП РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ЩО СКОЮЮТЬСЯ З ВИКОРИСТАННЯМ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

3.1. Завдання та зміст подальшого етапу розслідування комп'ютерних злочинів

Подальший етап розслідування комп'ютерних злочинів, як і іншої категорії злочинів, залежить від змісту отриманих даних на початковому етапі розгляду справи. Однак подальші дії слідчого спрямовані на збір інформації, що має доказове значення та перевірку і оцінку отриманих даних. На цьому етапі вирішується головне завдання пред'явлення суб'єкту, що скоїв злочин обвинувачення у справі та проведення допиту обвинуваченого. Виходячи зі змісту слідчих ситуацій, що склалися на початковому та подальшому етапах, можна говорити про наявність попереднього зговору, кількісний склад учасників злочину, їх ієрархічну будову та розподіл ролей між всіма суб'єктами вчиненої протиправної дії. У ході подальшого етапу розслідування проводяться ті слідчі дії, які будуть викривати причетних до злочину осіб, або ж навпаки, доказувати невинуватість суб'єкта, який підозрюється у вчиненому. Це можуть бути допити, очні ставки, пред'явлення для впізнання, обшуки та виїмки, призначення і проведення експертиз, відтворення обстановки та обставин події тощо. Слідчим доведеться працювати з іншими суб'єктами, що не фігурували у справі, яка розглядається, насамперед – це нові свідки, потерпілі, підозрювані, обвинувачені тощо. З'являться у справі й інші речові докази, які підсилять факт доказового значення. Якісного змісту набуде подальша організація планування розслідування справи, висунення та відпрацювання слідчих та розшукових версій, проведення окремих слідчих дій та ін. З урахуванням зазначеного вище розслідування комп'ютерних злочинів переходить у площину практичної реалізації намічених процесуальних заходів.

3.2. Допит свідків

На початковому етапі розслідування комп'ютерних злочинів було зроблено детальну викладку по підготовці та проведенню допиту свідків. Подальший етап також включає у себе допит цієї категорії осіб. Однак слід зазначити, що це може бути як повторний допит раніше уже допитаних осіб-свідків, так і допит досі незафігурованих суб'єктів, що володіють інформацією про обставини справи, яку розслідують. Основними тактичними завданнями допитів свідків є: виявлення елементів складу злочину у діях осіб, що вчиняли протиправні дії, встановлення обставин, місця і часу злочину, їх способів і мотивів, а також сприятливих умов, ознак зовнішності причетних до злочину осіб, які мають відношення до скоєння злочину [129, с. 629]. Особливого значення слідчому необхідно приділити при допиті спеціалістів, у якості свідків, які задіяні у виробничому процесі. Зокрема у операторів ЕОМ (комп'ютерів), слід з'ясувати наступні питання: правила ведення журналів операторів, порядок прийому-здачі змін, режим роботи операторів; правила експлуатації, зберігання, знищення комп'ютерних роздруківок, категорію осіб, що мають до них доступ; порядок доступу в приміщення, де знаходиться комп'ютерна техніка та ін.

У процесі допиту програмістів встановити: перелік програмного забезпечення, що використовується та його класифікація (ліцензійне, власне); паролі захисту програм, окремих пристроїв комп'ютера, періодичність їх змін; технічні характеристики комп'ютерної мережі, хто є адміністратором мережі, порядок придбання програмного забезпечення; наявність у робочих програмах спеціальних протоколів, які реєструють вхід до комп'ютера користувачів, який їх зміст тощо.

У співробітника, який відповідає за інформаційну безпеку або адміністратора комп'ютерної мережі (при її наявності) з'ясувати: наявність спеціальних технічних засобів захисту електронної інформації; порядок доступу користувачів до комп'ютерної мережі; порядок ідентифікації користувачів комп'ютерів; розклад робочого дня користувачів комп'ютерної

мережі; порядок доступу співробітників до комп'ютерної техніки в неробочий час; порядок присвоєння та зміни паролів користувачів.

У співробітників, які займаються технічним обслуговуванням обчислювальної техніки, слід вияснити: перелік та технічні характеристики засобів комп'ютерної техніки, встановленої в організації, а також перелік захисних технічних засобів; періодичність технічного обслуговування, проведення профілактичних та ремонтних робіт; дані про випадки виходу комп'ютерно-технічного обладнання з ладу; випадки незаконного підключення до телефонних ліній зв'язку, встановлення додаткового електрообладнання та ін.

У начальника обчислювального центру або керівника підприємства (організації) слід дізнатися: чи діють в установі спеціальні служби по експлуатації мереж та служби безпеки, їх склад та обов'язки; організаційну структуру обчислювального центру; чи сертифіковані технічні пристрої обчислювальної техніки; чи діють правила експлуатації ЕОМ (комп'ютерів), автоматизованої системи, комп'ютерної мережі, який порядок ознайомлення з ними та контролю за їх виконанням; які співробітники підприємства були звільнені протягом даного періоду часу та з яких мотивів; чи мали місце випадки незаконного проникнення до приміщень, де встановлена комп'ютерна техніка, несанкціонованого доступу до комп'ютерної інформації. Зазвичай при повторних допитах сумбурність первинних показань змінюється логічною послідовністю викладу обставин події, його дрібних подробиць і деталей, що часом мають важливе значення для розслідування злочинів з використанням комп'ютерних технологій.

За умови виникнення розбіжностей, неточностей, протиріч у викладених допитуваними особами даних, слідчий може провести між зазначеними учасниками кримінального процесу очну ставку на предмет встановлення істини у справі, яка розслідується.

Проаналізувавши спектр з'ясованих питань допиту осіб як свідків, можна вийти на коло суб'єктів (суб'єкта), які ймовірніше підпадає під статус підозрюваного (обвинуваченого) у вчиненні злочину даної категорії.

3.3. Допит обвинуваченого

Цей процесуальний захід є однією з найскладніших слідчих дій. Слід зазначити, що обвинувачені починають давати правдиві показання в тих випадках, коли переконаються, що слідством встановлене коло фактичних даних. Процесуально допит обвинуваченого закріплений та визначений у межах ст. 143 КПК України. Ця слідча дія може розглядатися в контексті продовження допиту підозрюваного або ж мати самостійний характер. Особливого змісту вона набуває при допиті обвинуваченого у сфері злочинів з використанням комп'ютерних технологій. Під час допиту обвинуваченого необхідно з'ясувати, які зміни в роботу комп'ютерних систем були внесені, які віруси використовувались, чи існує з точки зору обвинуваченого можливість швидко усунути чи зменшити шкоду, спричинену несанкціонованим проникненням у ЕОМ (комп'ютери), автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку. Які дані і кому передавалась [1, с. 960]. Коло питань, що необхідно з'ясувати при допиті у обвинуваченого, визначається конкретною ситуацією, яка склалася по кримінальній справі. Досягти бажаного результату можна лише використавши елемент психологічної налаштованості у допиті обвинуваченого. Особливістю цієї процесуальної дії є одержання слідчим відомостей про певні факти, що мали місце в минулому, і психологічне ставлення особи, що допитується до цих фактів. Тому дуже важливо при допиті врахувати особливості психологічних процесів, психологічного стану і психологічних властивостей допитуваного [79, с. 9]. Саме тому основу тактики допиту обвинуваченого складають психологічні закономірності, які виявляються в процесі вивчення і виявлення психологічних особливостей допитуваного, механізму формування його показань, установлення з ним психологічного контакту, а також у виборі методів

психологічного впливу з метою одержання правдивих показань і встановлення істини по справі. Ґрунтовне трактування аспекту дослідження комп'ютерних злочинів подав В.О. Голубєв. Він зазначив, що при допиті обвинуваченого має уточнюватися такий комплекс питань:

- алгоритм функціонування шкідливої комп'ютерної програми;
- на яку інформацію та яким чином впливає шкідлива комп'ютерна програма чи технічний засіб;
- шлях отримання даних про засоби захисту інформації, що використовується та способи її подолання;
- яким чином були локалізовані фізичні, технічні та програмні засоби захисту інформації;
- чи здійснювалось незаконне копіювання комп'ютерної інформації;
- чи відомі особи, які займаються подібною діяльністю. В яких відносинах з ними знаходиться обвинувачений;
- чи знав обвинувачений, хто є законним власником інформації, до якої здійснювався неправомірний доступ;
- механізм використання отриманої інформації;
- хто організував злочин, як були розподілені ролі, хто ці ролі виконував [68, с. 157].

Точка зору науковця є досить слушною і виваженою. Однак, слід внести деякі уточнення стосовно допиту обвинуваченого, безпосередньо у елемент механізму організації скоєння злочину. Слідчий має врахувати індивідуальні особливості зазначеної особи, особливо встановити її можливий зв'язок з організованою злочинністю (транснаціональною) та криміналітетом, можливо міжнародним. При допиті слід мати на увазі, що час хакерів-одиночок, котрі вчиняли «чисті» комп'ютерні злочини з нечітко вираженими злочинними намірами (більшість з метою професійного самоутвердження) відходять у минуле, на зміну їм приходять організовані злочинні групи, які використовують комп'ютерні технології для скоєння «традиційних», у тому числі тяжких і особливо тяжких злочинів у різних галузях господарства і

управління, на виробництві, в кредитно-фінансовій системі, у сфері обслуговування населення та цивільних прав, безпеки держави тощо [8, с. 68 – 69]. Необхідно тактично-вдумливо підходити до реалізації процесу допиту обвинуваченої особи. Основним критерієм організованої групи є чітке ієрархічне розподілення ролей між її членами. Отже, щоб не втратити можливості виявлення та дослідження злочинного ланцюга, слідчому потрібно, по можливості, у безконфліктній формі вияснити специфіку діяльності протиправної структури.

До числа специфічних особливостей механізму скоєння злочинів транснаціональними злочинними об'єднаннями належить те, що вони використовують всі можливі канали зв'язку для вчинення різноманітних злочинів [37, с. 103]. Тому, виходячи з конкретної слідчої ситуації, що склалася у злочинах, які розглядаються за участю організованих груп, слідчому необхідно вияснити такі питання:

- кількісний склад злочинної групи та сфери їх втручання;
- хто ініціатор і яка ієрархічна структура злочинної групи;
- адресне місце розташування групи: явки, паролі;
- комп'ютерно-технічне та інше забезпечення групи;
- обставини місця, часу обстановки за якими злочинна група реалізує свої протиправні наміри;
- критерії відбору об'єктів, що піддаються таким злочинам;
- зв'язок з потерпілою стороною;
- тактика підготовчих дій до вчинення злочину (підкуп осіб, прослуховування інформації, негласне (таємне) спостереження та інше);
- шляхи обходження системи безпеки та контролю, а також отримання паролів, кодів, криптографічних ключів тощо;
- яким чином використовується викрадений продукт злочину;
- механізм приховування злочину з інформаційними технологіями тощо.

Аналіз кримінальних справ показує, що при розслідуванні незаконного втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку залежно від того, наскільки обвинувачений визнає свою вину, можуть складатися наступні слідчі ситуації:

1. Обвинувачений визнає власну вину і дає розгорнуті правдиві свідчення.
2. Обвинувачений частково визнає власну вину, але заперечує свою участь в основних епізодах злочинної діяльності.
3. Обвинувачений визнає власну вину, але не встановлені всі епізоди злочинної діяльності.
4. Обвинувачені (при вчиненні злочину організованою групою чи за попередньою змовою або організованою групою) заперечують власну причетність до злочину, дають суперечливі свідчення.
5. Обвинувачений визнає власну вину, але не називає співучасників злочину [69].

Для успішного проведення допиту названих учасників кримінального процесу необхідно ретельно вивчити матеріали порушеної кримінальної справи, особливості особи підозрюваного чи обвинуваченого, перевірити наявні докази, що вказують на вину конкретної особи тощо. До притягнення особи як обвинуваченої, слідство повинно володіти двома категоріями доказів. У першій з них передбачається доказування обставин, які свідчать, що злочин, який розслідується мав місце, у другій – що ця протиправна дія скоєна даним суб'єктом, який притягується до кримінальної відповідальності.

3.4. Проведення обшуків та виїмок

Обшук та виїмка, як й інші слідчі дії є вагомими процесуальними заходами у злочинах вчинених з використанням комп'ютерних технологій. Пошук об'єктів протиправної діяльності та осіб, причетних до вчинення злочинів – це досить трудомісткий процес, що вимагає спеціальних теоретичних пізнань, значної кількості часу, фахової підготовленості, вміння на практиці застосовувати складні програмні апаратно-технічні засоби тощо.

Вдало висловив свою думку стосовно даного питання В.Г. Гончаренко: «Неспростовною істиною є твердження, що лише за наявності добре обґрунтованої і глибокої теорії може бути належна практика, ефективна діяльність людини у певній галузі» [62, с. 3]. Переносячи акцент на розслідування комп'ютерних злочинів, слід зазначити, що дані слідчі дії за своєю структурою мало чим відрізняються від аналогічних дій з «традиційною» категорією злочинів, але водночас мають ряд особливостей, на яких би і слід зупинитися.

Потрібно зазначити, що згідно ст. 177 КПК України обшук — це самостійна слідча дія, яка проводиться в тих випадках, коли є достатні підстави вважати, що знаряддя злочину, речі й цінності, здобуті злочинним шляхом, а також інші предмети й документи, які мають значення для встановлення істини в справі чи забезпечення цивільного позову, знаходяться в певному приміщенні або місці чи у будь-якої особи, а також коли він має достатні дані про те, що в певному приміщенні або місці переховується особа, яка вчинила злочин. У процесі обшуку здійснюється пошук і примусове вилучення об'єктів, що мають значення для правильного вирішення задач кримінального судочинства.

Виїмка ч. 1 ст. 178 КПК України – це теж самостійна слідча дія, яка проводиться у випадках, коли є точні дані, що предмети чи документи, які мають значення для справи знаходяться у певної особи чи в певному місці. Ці процесуальні дії, як і інші, доцільно розділити на три етапи: підготовчий (до виїзду на місцевість), робочий (дослідний) та заключний (фіксація ходу результатів обшуку та виїмки).

Одним з тактичних завдань підготовчого етапу є отримання вихідної інформації та додатковий збір даних про об'єкт, можливо суб'єкта (суб'єктів) злочину, формування відповідної слідчо-оперативної групи для успішної реалізації наміченого заходу. А також забезпечення охорони об'єкту; вивчення обстановки; проведення інструктажу слідчо-оперативної групи; запрошення понятих та ознайомлення їх з правами та обов'язками, при потребі,

запрошення інших учасників слідчих дій; підготовка необхідних техніко-криміналістичних засобів для виявлення, фіксації та вилучення предметів обшуку; забезпечення транспортних засобів перевезення вилученого та доставка його до експертної установи тощо.

Немає потреби в черговий раз повторюватися на формуванні загальних аспектів підготовчого етапу слідчої дії, вони достатньо викладені в даній монографії в характеристиці огляду місця події (Див. с. 102). Зупинимося на тому, що є визначальним для цієї категорії слідчих дій:

- перш за все, це психологічна налаштованість слідчого на проведення обшуку чи виїмки;
- підготовка кадрів для проведення зазначених слідчих дій має бути продуманою, вчасною, достатньо мобільно організованою;
- визначення оптимальних умов (місця, часу, обстановки, обставин, сприятливих умов) успішної реалізації слідчих дій;
- уміння не реагувати на ознаки певної невизначеності, не достатньої впевненості, можливої доцільності, передчуття відсутності результативності тощо.

Аналізуючи наукові праці дослідників у цьому питанні слід сказати, що окремі з них сприймають слідчий обшук та виїмку у досить вузькому розумінні. Основне коло питань вони формулюють лише у зазначенні рекомендацій, яких має дотримуватися слідчий та інші суб’єкти кримінального процесу при відшуканні та виявленні об’єктів злочинного діяння. Але, слід зазначити, що слідчі дії мають включати в себе більший об’єм дослідження. Визначальними елементами характеристики цих процесуальних заходів є:

- ймовірне місце проведення обшуку чи виїмки;
- дані про комп’ютерно-технічне забезпечення та периферійне устаткування, яке підлягає обшуку;
- програми та програмне забезпечення, що є об’єктом обшуку;
- особистий обшук.

Місцем проведення обшуку чи виїмки предметів у злочинах, пов'язаних з використанням комп'ютерних технологій, можуть бути: житлові (будинки, квартири, дачі, кімнати) або ж службові (офіси, офісні кімнати, кабінети, класи, зали, клуби), іноді не житлові приміщення (кімнати в цокольних будовах, підвали, напівпідвали, гаражі, сараї тощо). Залежно від конкретного місця, території, кількості приміщень, засобів охорони, об'єму комп'ютерного оснащення, різновидів і технічних характеристик тощо, слідчий разом з оперативним співробітником розробляє план проведення процесуальних заходів. Якщо ж йдеться про особистий обшук особи, його помешкання чи місце переховування предмету дослідження, то окрім названого, слідчий має встановити:

- чи володіє особа, що буде піддаватися обшуку спеціальною освітою або ж професійними навичками у сфері ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;
- коло знайомих особи; чи є серед них фахівці у сфері комп'ютерних технологій, де працюють, мешкають (суб'єктивні характеристики);
- яке комп'ютерно-технічне обладнання є у власності чи користуванні особи, в якої проводитиметься обшук, його технічні характеристики;
- чи приєднане комп'ютерне обладнання до локальної чи віддаленої мережі, якщо так, то до якої, а також чи має вихід до INTERNET – технологій тощо;
- місце розташування комп'ютерної системи у приміщенні, оснащення можливими кодами та паролями допуску до режиму роботи та ін.

На стадії підготовки до проведення слідчої дії, коли предметом обшуку є дані про комп'ютерну техніку та периферійне забезпечення, слідчому та оперативно-розшуковому підрозділу слід мати попередню розвідувальну інформацію про:

- місцезнаходження (місце-розташування) комп'ютерного технічного забезпечення, з якого здійснювався злочин;

- кому і на яких правах належить комп'ютерно-технічне забезпечення, чи приєднане до локальної, віддаленої мережі, а також чи має вихід до мережі INTERNET;
- персонально за ким закріплений комп'ютер;
- система доступу, допуску та контролю до засобів комп'ютерної техніки (ЗКТ);
- марка, модель комп'ютера та окремого комп'ютерного забезпечення;
- периферійні пристрої, засоби зв'язку і комунікації;
- інші відомості про систему, що є об'єктом дослідження;
- стороння інформація, яка можливо сприятиме успішному розслідуванню справи [50, с.162-166].

Досить суттєвим і актуальним у тактиці обшуку та виїмки залишається питання вибору часу проведення слідчих дій даної категорії. У цьому питанні точки зору вчених-криміналістів мають не споріднений характер. Одні схильні до думки, що обшук та виїмку найкраще проводити у робочий час, коли автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку перебувають у робочому режимі. Разом з тим, працюючі на них особи максимально завантажені виробничими справами, і раптова поява слідчо-оперативної групи, з санкціонованою вмотивованою постановою на виконання процесуальної дії, застане всіх зненацька. Інші ж дотримуються протилежного, зокрема: особистий обшук та виїмка мають бути проведені у ранковий час (з 6.00 до 8.00), коли особа, що підпадає під зазначену слідчу дію знаходиться у не підготовленому стані, а відповідно, не має можливості приховати сліди своєї протиправної дії з використанням комп'ютерних технологій. Якщо ж це стосується обшуку та виїмки в юридичних установах, організаціях, структурах, підприємствах, фірмах тощо, то дана слідча дія має бути проведена до початку робочого часу зазначеного вище переліку установ, коли технічні комп'ютерні системи є не задіяними в процесі, а також відсутній його обслуговуючий персонал [213, с. 209]. Окремі науковці дотримуються ще й такої думки, як знеструмлення приміщення перед початком проведення зазначених слідчих

дій. Вони трактують, що це досить ефективний тактичний прийом, особливо у тих випадках, коли «підлягає обшуку будівля, що стоїть окремо і в ній знаходиться багато комп'ютерної техніки зі значною кількістю електронної інформації, яка цікавить слідство, а через велику площу приміщень, в яких має відбутися обшук, немає можливості його розпочати одночасно. До того ж ці приміщення можуть знаходитися на різних поверхах і охоронятися» [107, с. 13 – 14]. На погляд автора, запропонована точка зору є не зовсім слушною.

По-перше, деякі установи, що використовують велику кількість комп'ютерного обладнання у своїй виробничій діяльності цілодобово, не залежно від того, чи є персонал на робочому місці чи ні, можуть за допомогою системи програмування отримувати зовнішню електронну інформацію, яка можливо буде корисною для слідства. Таким чином, під час знеструмлення приміщення, вона просто не надійде. По-друге, слід врахувати, що сучасні ЕОМ (комп'ютери), автоматизовані системи, комп'ютерні мережі і мережі електрозв'язку забезпечені автономним живленням на випадок нестандартних ситуацій типу: знеструмлення, пожежі, стихійного лиха тощо, а отже, у момент припинення централізованого електропостачання, спрацює система включення внутрішніх акумуляторів устаткування. По-третє, даний захід може послужити «хакерам», своєрідним сигналом до дії, і як результат – у лічені секунди злочинець (злочинці) знищать сліди своєї протиправної діяльності. По-четверте, як наслідок миттєвого знеструмлення окремо взятого об'єкта можливе відключення системи збереження конфіденційної електронної інформації, що спричинить само по собі пошкодження даних електронної інформації або ж її знищення. Таким чином, запропонований тактичний прийом не приведе до питомого результату. Слушним є твердження М. Осипенка: «Не припускайте, щоб хто-небудь проводив будь-які дії з комп'ютером. Ризик, пов'язаний з безпосереднім втручанням у систему, значно більший, ніж малий шанс дистанційного впливу на систему ззовні» [163, с. 10].

Спірним залишається питання форм проведення обшуку та виїмки. Як відомо, у кримінальному процесі та криміналістиці визначені дві типові форми слідчих дій: попереджувальна і раптова. Слідчий, виходячи з обставин справи на власний розсуд вирішує питання про вибір однієї з них, залежно від категорії складності вчинених суб'єктом зазначених протиправних дій. Застосування попереджувальної форми проведення обшуку можливе за умови, коли відомо, що реалізація злочину з використанням комп'ютерних технологій відбулася ззовні. Це одна з тих ситуацій, за якої місце вчинення злочину не співпадає з місцем настання негативних наслідків. У інших випадках засобами, що забезпечують непередбачуваність змісту й характеру дій слідчого протидіючій стороні, є форма раптовості проведення обшуку. Як відзначив А.П. Самонов, фактор миттєвості (раптовості) не є порушенням закону. Було б легковажним попереджувати підозрюваних про проведення у них обшуку, а потім шукати докази, які б мали значення для визначення їх вини [187, с. 118]. Проте в юридичній літературі зустрічаються думки про протиправність використання раптовості у слідчій діяльності. Так, І.Ф. Пантєлєєв вважає, що твердження про наявність конфліктів у слідчій діяльності: «…не узгоджується з самою сутністю й принципами кримінального процесу. Ця ідея породжує проникнення у кримінальний процес невідповідних йому методів, спрямованих на те, щоб дезінформувати; збити з пантелику; заставити зненацька; визвати стан розгубленості допитуваного; розпалити конфлікт між співучасниками злочину» [166, с. 54].

З точки зору автора, тактика слідчої діяльності як комплекс найбільш доцільних криміналістичних прийомів, характеризується не лише елементами, що визначають загальний порядок та індивідуальний підхід при проведенні слідчих дій, а й особливості її здійснення за складних, несприятливих ситуацій, коли зацікавлені особи перешкоджають процесу розслідування. За подібних обставин вона виступає засобом подолання протидії, оскільки без активних дій, що забезпечують поступовість тактичних прийомів, реалізація задач практично неможлива. Слушною у цьому питанні є думка А.Ф. Коні,

який зазначив: «Чим раптовішим є уявлення, яке викликає велике душевне хвилювання, тим більше воно заволодіває увагою, і тим швидше внутрішні переживання затуляють зовнішні обставини... Неочікувана небезпека, що виникла, викликає самовільне перебільшення розмірів та форм, за яких вона відбулася насправді» [109, с. 167]. У той час Н.М. Ахтирська дотримується іншої позиції. Вона констатує, що раптовість при провадженні слідчих дій може бути досягнута за рахунок різноманітних факторів – часу, місця, характеру й виду заходів, що проводить слідчий. Опитування засуджених засвідчило, що у 71 % випадків неочікуваними для них були місце й час проведення слідчої дії; у 46,5 % випадків раптовість досягалася самим фактором проведення слідчої дії, колом притягнутих осіб і характером використаних доказів [14, с. 1 – 17] Слід зазначити, що фактор часу досягається раптовістю та забезпечується проведенням дій у той момент, коли відповідні особи не передбачали і не очікували цього. Однак, при попереджувальному характері слідчих дій необхідно врахувати, що вони мають розпочатися до того, як підозрюваний, обвинувачений чи інша протидіюча розслідуванню особа отримає інформацію про можливість їх проведення. Якщо ж зацікавлений суб'єкт вже інформований, тоді обшук чи виїмку слід провести у інший час, а на цей період доцільно встановити за об’єктом зовнішнє спостереження. Найбільш сприятлива ситуація у використанні цього прийому зазвичай складається на початковому етапі розслідування, коли раптовість, як правило, пов’язана зі швидкістю та невідкладністю слідчих дій, а також одночасним їх здійсненням (обшук) щодо кількох осіб. Застосування таких тактичних прийомів раптовості може використовуватися при порушенні кримінальної справи або без такої, за матеріалами, зібраними органом дізнання в процесі здійснення оперативно-розшукових заходів. У таких випадках складається ситуація, за якої слідчий або оперативний працівник заздалегідь можуть вивчити отриману інформацію та визначити час, порядок і послідовність її використання з метою досягнення бажаного результату. Їх дії набувають цілеспрямованого, планового характеру

у той час, коли зацікавлені у протидії слідству особи їх не очікують. Це дозволяє провести затримання всіх підозрюваних одночасно та виключити можливість узгодження між ними своїх дій. А разом з тим провести одночасно обшуки у кількох ймовірних місцях, що мають відношення до справи даної категорії. Реалізація фактора раптовості характеризується своєрідною закономірністю. Суть якої полягає у тому, що ефективність раптовості обмежена часом, необхідним для перебудови особою своїх дій та намірів, вибором засобів та способів протидії раптовості. Після цього раптовість перестає діяти.

Особливої уваги вимагає робочий етап проведення обшуку чи виїмки. Він включає в себе: заходи щодо відсторонення осіб від працюючих технічних засобів, за умови проведення обшуку у робочий час; персонального встановлення осіб, що працюють з комп'ютерними системами та їх обслуговують, при виявленні сторонніх суб'єктів, встановлення мети їх перебування у цьому місті; складання планів та схем приміщення і розташування в ньому технічних засобів; проведення фотографічної і відеофіксації наявних комп'ютерних забезпечень; детального описання зображення на моніторах кожного з працюючих комп'ютерів (фіксації конкретної програми на момент проведення обшуку); з'ясування причин не використання (не включення комп'ютерів) та ін.

Своєрідністю обшуку чи виїмки доказів у злочинах зазначеної категорії є те, що вказана слідча дія може мати не лише короткочасний, а й довготривалий характер. Тому особам, які працюють у установі, де проводитиметься слідча дія, у тактовній формі повинні пояснити, з якою метою проводиться даний процесуальний захід, щоб уникнути всіляких непорозумінь, разом з тим закликати до сприяння і співпраці з правоохоронними органами. Одночасно можна буде проводити спостереження за поведінкою осіб після оголошення мети обшуку, це можливо послужить своєрідним орієнтиром у подальшому ході слідчої дії. Як наголошує В.І. Комісаров: «Особливо пильно необхідно спостерігати, щоб ніхто з працюючих з комп'ютерними технологіями не міг

внести будь-якого плану змін у роботу операційної системи. Спостереження має сприяти послідовній координації вивчення об'єктів, а також своєчасному прийняттю слідчим заходів проти намагань знищити чи приховати речові докази або створити умови, які будуть ускладнювати проведення слідчої дії» [106, с. 116]. У зв'язку з цим слідчий може вибрати один з таких тактичних прийомів запобігання:

а) попросити всіх залишити свої робочі місця і на період проведення даного заходу перейти до іншого приміщення у межах установи;

б) з метою виявлення можливого злочинця, причетного до протиправної дії або ж особи, що володіє хоча б деякою інформацією про злочин, залишити всіх працюючих з комп'ютерними системами у приміщенні, в якому буде проводитися обшук, але при цьому заборонити:

- всім працівникам у приміщенні, в якому проводитиметься обшук, торкатися засобів комп'ютерної техніки;
- вимикати технічні засоби від електромережі та переставляти чи переносити з одного робочого місця на інше або за межі приміщення окремі вузли комп'ютерного оснащення;
- намагатися пошкодити засоби комп'ютерної техніки з метою знищення інформації і цінних даних;
- без дозволу слідчого телефонувати або відповідати на телефонні дзвінки, бо це може послужити відповідним сигналом для знищення інформації [6, с.232].

Не менш важливим напрямом під час проведення обшуку є ретельна перевірка записів, які ведуться в установі: документації у автоматизованій системі, комп'ютерній мережі; вихідна та оперативна електронна інформація про діяльність підприємства; особисті дані про співробітників; список структур, з якими установа співпрацювала чи співпрацює тощо. Більш вужче коло питань підлягатиме дослідженню, коли відомий підозрюваний і якого вже ідентифіковано. Тоді можна швидше зафіксувати виявлені та вилучені речові

докази, які мають відношення до справи та розглянути інший об’єм питань, що виник у ході проведення даного заходу.

Таку інформацію можна отримати від самого підозрюваного суб’єкта злочину або ж від інших осіб, з числа тих, які володіють будь-якими даними, що цікавить слідство. Це надасть певні відомості про способи вчинення злочинцем протиправної дії та їх ймовірні мотиви і мету. В окремих випадках бажано, щоб підозрюваний був присутній при огляді його комп’ютера, оскільки саме він може надати найважливішу інформацію про особливості функціонування комп’ютерної системи:

- паролі, коди доступу;
- перелік інстальованих комп’ютерних програм (програм, які є у комп’ютері);
- місцезнаходження окремої інформації на машинному носії (окремих директорій, у тому числі прихованих) [30, с. 66 – 67].

Така особа може добровільно допомогти слідству розібратися у тонкощах функціонування комп’ютерної техніки, зокрема відтворенні шляхів проникнення в систему та вчинення там протиправних заходів, пов’язаних з використанням комп’ютерних технологій. Але у жодному разі не слід цілком покладатися на щирість підозрюваної особи, а тому неприпустимо дозволити їй самій працювати за комп’ютером – це може послужити доброю нагодою для знищення слідів скоєного. Інша ситуація, коли обшук чи виїмка проводитиметься слідчо-оперативною групою у конкретної особи (осіб) з використанням фактору раптовості. За такої ситуації слідчий повинен враховувати психологію особи, в якої проводитиметься зазначений захід. Доречним буде знати старшому слідчо-оперативної групи, професійні навички та звички такого суб’єкта, його склад характеру, фізичний стан, захоплення-уподобання тощо. Адже можлива ситуація, коли злочинець завчасно подбав про свою безпеку та приховав сліди вчиненого. Тому в окремих випадках при проведенні зазначених слідчих дій необхідно шукати схованки, де можуть

зберігатися змінні комп'ютерні носії інформації. Це можуть бути різні ніші у стінах, підлозі, вентиляційних отворах; окремі речі й предмети з подвійним дном (підвіконня, столи, стільці тощо). На особливу увагу заслуговує пошук схованок з магнітними носіями. Така дія ускладнюється неможливістю використання металошукача або рентгенівської пошукової установки, оскільки їх застосування може призвести до знищення електронної інформації. Тому слід виважено підходити до відшукання зазначених джерел доказового значення. Такі носії електронної даних вилучаються і приєднуються до матеріалів кримінальної справи з дотриманням установленого процесуального порядку. Разом з тим не слід забувати і про сам комп'ютер та його технічне забезпечення, що можуть служити прекрасним місцем для приховання предметів розшуку. Але лише у виняткових ситуаціях, за допомогою спеціаліста дозволяється відкривати корпуси апаратних засобів комп'ютерної техніки, щоб виявити спеціально відключені внутрішні носії інформації, наприклад, додатковий жорсткий диск. У всіх інших випадках системний блок як основний системний центр має бути вилучений цілісно для дослідження його місткості за спеціальних лабораторних умов. Неграмотний демонтаж жорсткого диску на місці проведення обшуку чи виїмки, а також упакування і транспортування призведе до знищення електронної інформації, яка на ньому містилася. Хоча в цьому аспекті є й інші думки фахівців, які присвятили свої наукові праці вивченню злочинів з використанням комп'ютерних технологій. В.В. Агафонов та А.Г. Філіппов зазначають: «Якщо в розпорядженні оперативно-слідчої групи немає переносного персонального комп'ютера з пишучим CD-ROM, досить вилучити жорсткий диск (або диски, коли їх декілька) з виявленого комп'ютера. Вилучення має відбутися з дотриманням усіх процесуальних правил. При вилученні жорсткого диска бажано вести відеозапис» [130, с. 92]. Скажімо, М.Г. Шурухнов, І.П. Левченко, І.М. Лучин, вважають, що коли у складі групи немає спеціаліста з комп'ютерної техніки здатного кваліфіковано здійснити демонтаж жорсткого диска, тоді доцільно провести вилучення системного блока комп'ютера. У деяких випадках

можливе вилучення принтера, однак, на відміну від друкарської машинки, ідентифікація надрукованої на ньому інформації за залишеними слідами досить складна, навіть якщо це голковий принтер. Для лазерного або струменевого принтера подібний аналіз практично неможливий [213, с. 28]. Таким чином, трактуючи свою точку зору, автори переносять акцент з дослідження апаратних засобів в експертних установах і відповідних умовах на «польове» криміналістичне дослідження на місці проведення зазначеної слідчої дії. Однак, слід пам'ятати, що однією з найважливіших умов проведення обшуку, виїмки тощо є суворе дотримання встановлених правил поводження з комп'ютерною технікою і носіями інформації, кваліфіковане проведення пошуку доказів, потрібної інформації. Окрім зазначеного технічного оснащення на місці проведення процесуального заходу слідчо-оперативній групі необхідно переглянути й інші носії електронної інформації**.** А тому не слід обмежуватись пошуком криміналістично-значущих даних лише у комп'ютері, необхідно уважно оглянути наявну документацію як електронну, так і паперову. Більшу частину електронних даних, що зберігаються й обробляються комп'ютером, завжди можна скопіювати на переносні носії інформації – гнучкі магнітні дискети чи флеш-карти. Якщо спеціаліст немає можливості продивитися дискети чи CD-ROM (лазерні) диски та інші магнітні носії на місці, їх необхідно вилучити для подальшого дослідження з дотриманням процесуальних норм. Стосовно комп'ютера, що знаходився у працюючому режимі, то на магнітний носій слід скопіювати програми і файли даних, які зберігаються на його носієві або в оперативній пам'яті. А також переписати електронну інформацію на жорсткий диск персонального комп'ютера оперативно-слідчої групи, або ж скопіювати її на CD-диск за допомогою CD-ROMa. Реалізація обшуків та виїмок проводиться в присутності понятих, що розписуються на роздруківках інформаційних даних, виготовлених у ході слідчої дії та протоколі процесуального заходу. У свою чергу, слід запрошувати понятих з осіб, що володіють хоча б мінімальними знаннями у сфері комп'ютерних технологій. Нерозуміння змісту виконуваних

правоохоронцями дій людина, що запрошена як понятий, а пізніше допитана у суді, може не переконати суд у визнанні тих чи інших обставин доказами [111, с. 56 – 59].

На заключній стадії слідчої дії складається протокол та описи до нього, виготовляються плани і схеми приміщень, що підлягали обшуку, проводяться додаткові фотографування й відеозапис. У процесуальному документі у послідовній формі у міру того як здійснювався обшук чи виїмка, слід зафіксувати:

- в якому місці виявлений і вилучений протиправний предмет чи об’єкт дослідження;
- його найменування, кількість, спосіб виготовлення та призначення;
- за наявності вказати марку; модель; заводський номер та серію; рік випуску і виробника;
- якщо ж це комп’ютерна інформація, то де виявлена; на якому носії була розміщена; якого характеру та змісту; її функціональне призначення; можливо відомо кому адресувалася [111, с. 78 – 82].

При вилученні комп’ютерів необхідно шляхом індивідуального опитування працюючого персоналу установи-жертви вияснити мережеві імена користувачів та їх паролі; вилучити всі комп’ютери та магнітні носії; при огляді документів звернути особливу увагу на робочі записи співробітників, де можуть зазначатися паролі і коди доступу; скласти список всіх позаштатних і тимчасово працюючих спеціалістів фірми з метою виявлення програмістів та інших спеціалістів з обчислювальної техніки, які працюють на дану фірму. Якщо можливо встановити їх паспортні дані, адреси і місця постійної роботи [53, с. 51]. Також вилучений процесор упаковується та опечатується в спеціальних оболонках, які забезпечують надійність його транспортування. Портативні комп’ютери, дискети, інші носії інформації, що можуть використовуватися разом з комп’ютерами (дискети, лазерні диски) також упаковуються в окремі пакети чи коробки та опечатуються. У протоколі

зазначаються порядок й номери печаток. Вилучене обладнання необхідно застерегти від ударів, вологості, прямого потрапляння сонячних променів, різкого температурного перепаду тощо.

Ще однією суттєвою особливістю обшуку та виїмки є те, що не завжди слідчо-оперативній групі, яка виїжджає на вказані процесуальні заходи вдається досягти бажаного результату. Це викликане такими факторами як суб'єктивного, так і об'єктивного характеру:

- недостатньою підготовкою до проведення обшуку та виїмки;
- слабкою обізнаністю учасників слідчо-оперативної групи у сфері комп'ютерних технологій;
- запрошення для участі у слідчій дії в якості спеціалістів та консультантів осіб, які неналежно відносяться до зазначеного заходу, тобто не вболівають за результативність проведеної дії;
- використанням правоохоронцями лише традиційно-використовуваних технічних засобів для виявлення, фіксації та вилучення джерел доказового значення, тим самим ігнорування комп'ютерними засобами;
- поспішність і неуважність при проведенні зазначених процесуальних дій;
- недотримання учасниками слідчої дії регламентованих процесуальних заходів безпеки, культури та етики при провадженні обшуку чи виїмки;
- неналежне поводження з виявленими та вилученими об'єктами криміналістичної ідентифікації, що мають доказове значення по справі, яка розслідується, тощо.

При цьому не слід сплутувати прогалини та помилки, яких допускаються слідчі під час проведення окремих слідчих дій із своєрідними тактичними прийомами, до яких може вдаватися слідчий, реалізовуючи процесуальний захід. Одним з таких прийомів є відстрочка виконання обшуку чи виїмки. На

перший погляд, вона може бути сприйнята іншими учасниками, які володіють інформацією про слідчу дію, а також і самим суб'єктом, що скоїв злочин як «бездіяльність» чи «безпорадність» слідчо-оперативної групи і, безпосередньо, її керівника. Таким чином, причетні до вчинення протиправних дій особи самозаспокоюються, що обшук відбувся і результат їх злочинної діяльності не виявлений. Тому «білокомірцеві» злочинці можуть продовжувати свої протиправні дії і надалі або ж вжити заходів щодо переховування раніше схованого предмета злочину. Слідчий зі свого боку, вдаючись до зазначеного тактичного прийому, може вирішити таке:

- дати зрозуміти особі, у якої проводився обшук, що процесуальна дія завершена безрезультатно, інформація про ймовірне місце скоєння злочину не підтвердилася і подальші заходи такого характеру не мають сенсу;
- встановити негласне спостереження за суб'єктом та за об'єктом, що цікавить слідство, у відповідності до дотримання вимог чинного законодавства;
- зачекати та вибрати момент, коли особа повторно повернеться до своїх протиправних дій, пов'язаних з вчиненням чи приховуванням злочину з використанням комп'ютерних технологій тощо.

Логічним завершенням відстрочки виконання слідчої дії є повторний (раптовий) обшук. Такий характер несподіваності для осіб, що знаходилися в полі зору правоохоронних органів, дасть ефект шокової терапії. Підозрюваний суб'єкт, що деякою мірою знизив рівень заходів безпеки своєї злочинної діяльності, тим самим наразив себе на непідготовленість до повторної процесуальної дії. Прикладом тому можуть слугувати статистичні дані опитування засуджених за такі злочини, де у 88,2 % випадків повторний обшук був результативнішим, що пояснюється появою предметів, які раніше перебували в іншому місці. Проведені через деякий час обшуки виявилися більш ефективними, оскільки злочинці певною мірою заспокоюються після первинного обшуку, а особи, яким були віддані на тимчасове зберігання певні

докази, намагаються, по можливості, скоріше повернути їх безпосереднім власникам [14, с. 12 – 14].

Таким чином, застосовані слідчим ці та інші тактичні прийоми заслуговують на увагу і є досить дієвим механізмом у діяльності правоохоронних органів при проведенні зазначеної категорії слідчих дій у злочинах, пов'язаних з використанням комп'ютерних технологій.

3.5. Призначення і проведення необхідних видів судових експертиз

Узагальнена світова практика розслідування комп'ютерних злочинів, засвідчує, що у більшості протиправних дій з використанням електронних (комп'ютерних) технологій, останній використовувався як засіб для скоєння і приховування вчиненого. Саме тому виявлені та вилучені на місці події об'єкти криміналістичної ідентифікації мають бути дослідженими у спеціально призначених науково-дослідних центрах та філіях судових експертиз. Згідно зі ст.75 КПК України, слідчий призначає експертизу у тому разі, коли для вирішення певних питань при провадженні у справі необхідні наукові, технічні та інші спеціальні знання. Актуальним питанням спільності і відмінності науки криміналістики і криміналістичної експертизи достатньо уваги приділено у працях В.Г. Гончаренка [64].

У свою чергу, судова експертиза являє собою комплекс дій, спрямованих у встановленому порядку досліджень спеціалістами конкретних об'єктів, а також винесення ними кваліфікованих висновків по справі, що розслідується. Перелік експертиз, що можуть проводитися у справах про злочини цієї категорії, досить широкий. Це ті самі традиційні експертизи (трасологічна, дактилоскопічна, техніко-криміналістична експертиза документів тощо), судово-економічна (бухгалтерська, фінансово-економічна, аудиторська та ін.). Принципове значення для розслідування комп'ютерних злочинів мають спеціалізовані експертизи – комп'ютерно-технічна та програмно-технічна [115, с. 62 – 63]. Це дві схожі за формою і змістом експертизи. О.Р. Росинська зазначає, що у рамках цього роду експертиз їх можна поділити на два види:

- технічна експертиза комп’ютерів і їх комплектуючих. Вона проводиться з метою вивчення конструктивних особливостей комп’ютера його периферійних пристроїв, у тому числі магнітних носіїв, а також різного характеру неполадок, що виникають у цих технічних пристроях чи носіях;
- експертиза даних і програмного забезпечення, що здійснюються з метою вивчення інформації, яка зберігається у комп’ютері і на його магнітних носіях [181, с. 173].

Викладена вище точка зору дослідників безперечно заслуговує на увагу, однак потребує певного уточнення. Разом з позитивним, тобто виокремлення їх у окремий вид експертиз, виникають певні труднощі у роботі слідчих при виборі тієї чи іншої експертизи і визначенні категорії запитань, адже межа між ними має умовний характер. У зв’язку з цим, доречною буде позиція, запропонована вітчизняними науковцями-криміналістами, зокрема: І.В. Горою, В.А. Колесником, А.В. Іщенком. Ці автори обидві експертизи відносять до класу інженерно-технічних експертиз і визначають її як судову комп’ютерно-технічну експертизу, що поділяється на апаратно-комп’ютерну, програмно-комп’ютерну, інформаційно-комп’ютерну та комп’ютерно-мережеву експертизу. Тим самим це дає чітке розмежування того, що й куди відноситься. У свою чергу, судова апаратно-комп’ютерна експертиза визначає вид, властивості апаратного засобу, умови застосування, наявність фізичних дефектів, встановлює причинний зв’язок між можливостями апаратних засобів та результатами їх використання.

Судова програмно-комп’ютерна експертиза визначає загальні характеристики операційної системи, її функціональні властивості, визначає фактичний стан програмного об’єкта, склад відповідних файлів, їх параметри тощо. Судова інформаційно-комп’ютерна експертиза встановлює властивості вид інформації у комп’ютерній системі, наявність відхилень від типових об’єктів (шкідливі включення, порушення цілісності тощо), встановлює первісний стан інформації на фізичних носіях та ін. Судова комп’ютерно-

мережева експертиза визначає властивості й характеристики апаратного засобу і програмного забезпечення, встановлює місце, конфігурацію мережі та її компоненти, відповідність виявлених характеристик типовим для конкретного класу засобів мережної технології тощо [88, с. 215 – 216].

Перед судовою комп'ютерно-технічною експертизою, як і перед іншими експертизами, є чітко визначені задачі роду, виду, підвиду та задачі експертного дослідження. Основу даного виду експертизи становить вирішення діагностичних та ідентифікаційних питань, що постають перед експертом. Зокрема, діагностичні – у виявленні механізму події, місця, часу, послідовності дій, явищ, причинний зв'язок між ними, кількісних та якісних характеристик об'єктів їх властивостей, а ідентифікаційні у тотожності об'єктів за їх відображеннями. Отже, діагностичні завдання за видовою характеристикою поділяються таким чином.

- ***Діагностика апаратно-комп'ютерних засобів:***
  - визначення виду (типу, марки), властивостей апаратних засобів, а також їх технічних та функціональних характеристик;
  - стан апаратних засобів, наявність поломок, дефектів;
  - характеристика носіїв даних апаратних засобів;
  - відтворення умов, обстановки, фактичних даних використання апаратних засобів на місці події.
- ***Діагностика програмно-комп'ютерних засобів:***
  - встановлення складу і кількісних характеристик програмно-комп'ютерний засобів;
  - характеристика фактичного стану програмного забезпечення, окремих програм та наявність можливих у них відхилень;
  - встановлення причинного зв'язку між діями користувача комп'ютерної системи відносно програмного забезпечення і наслідками, що наступили.

- ***Інформаційно-комп'ютерна діагностика:***
  - характеристика та зміст інформації, що знаходиться на електронних комп'ютерних носіях;
  - виявлення ознак втручання та внесення змін у інформаційні дані;
  - встановлення механізму і обставин події виходячи з інформації, що знаходиться на комп'ютерних носіях та його копіях.
- ***Комп'ютерно-мережева діагностика:***
  - загальна характеристика комп'ютерної мережі та її складових;
  - використання типового комп'ютерно-мережевого оснащення та виявлення у них ознак відхилень від встановлених стандартів;
  - причини внесення змін у комп'ютерно-мережеве забезпечення та імовірні наслідки їх застосування;
  - встановлення зв'язку між зміною у комп'ютерно-мережевому оснащенні і суб'єктами, які співпрацюють з даним комп'ютерним забезпеченням.

Стосовно ідентифікаційних завдань комп'ютерно-технічної експертизи, то її призначення полягає у встановленні факту індивідуально-конкретної тотожності або групової належності об'єктів, що підлягають детальному експертному дослідженню. У цьому аспекті можна виділити кілька видів ідентифікації.

- ***Встановлення індивідуально-конкретної тотожності:***
  - ідентифікація комп'ютерної системи у цілому;
  - встановлення цілого за частинами;
  - ідентифікація окремо взятого програмного забезпечення, програми, файлу тощо.
- ***Встановлення групової приналежності:***
  - ідентифікація апаратних засобів (наприклад, за формою, місцем і часом виготовлення, серійним номером тощо);
  - тотожність оригіналу інсталяційній версії та її копії у співвідношенні до комп'ютерного носія;

- встановлення групової приналежності програмного забезпечення за загальними ознаками (наприклад, класу, виду, найменування, версії).

- ***Визначення загального джерела походження (як різновид встановлення групової приналежності):***
  - тотожність носія інформації та дисковода, відповідно здійсненого запису;
  - тотожність інсталяційної версії програмного забезпечення і встановлених копій даного програмного забезпечення у кількох комп'ютерних системах;
  - визначення загального джерела походження інформації на носіях, даних комп'ютерних системах тощо [181, с. 264 – 269].

При вирішенні експертизи апаратно-комп'ютерних засобів слідчим перед експертом можуть бути поставлені такі питання:

а) Діагностичні:

1. До якої моделі відноситься представлений на експертизу комп'ютер та його оснащення його технічні характеристики?
2. В якому стані знаходиться комп'ютерна техніка? Чи придатна для подальшої експлуатації, якщо ні, яка причина?
3. Чи відповідає технічним параметрам зборки виробника чи ні?
4. Яке відхилення від технічних норм міститься у комп'ютерній системі?

б) Ідентифікаційні:

1. Чи мають комп'ютерні компоненти єдине джерело походження?
2. Чи можна провести ідентифікацію вилученого комп'ютерного устаткування та його комплектуючих щодо аналогічних комп'ютерних систем?
3. Яка конфігурація і складові комп'ютерної системи та чи можливо за допомогою цих засобів здійснити протиправні дії конкретного змісту?

Питання, що можуть бути поставлені при експертизі програмно-комп'ютерних засобів.

а) Діагностичні:

1. Що собою являє програма, яка міститься у комп’ютерній системі, її функціональні характеристики?
2. Призначення програмного продукту і термін його використання?
3. Шляхи встановлення, введення програмно-комп’ютерних засобів та наслідки їх використання?

б) Ідентифікаційні:

1. Чи міг програмно-комп'ютерний засіб бути встановленим конкретним спеціалістом, знавцем кібернетичних технологій?
2. Яким саме чином відбулося встановлення і в який час?
3. Чи адаптований програмно-комп’ютерний засіб до конкретного типу комп’ютерних систем чи ні?

При вирішенні зазначеної експертизи інформаційно-комп’ютерного забезпечення вирішуються питання такого змісту.

а) Діагностичні:

1. Технічний стан інформації, яка є на комп’ютерних носіях?
2. Зміст інформації, що міститься на магнітних носіях?
3. Чи можливе відновлення видалених, знищених і заархівованих файлів?

б) Ідентифікаційні:

1. Чи могла окремо взята програма бути виконаною конкретним суб’єктом?
2. Яким чином була встановлена присутність інформаційних слідів?
3. Чи можна провести ідентифікацію інформаційно-комп’ютерного забезпечення або конкретних інформаційних даних відносно комп’ютерно-апаратних засобів?

При експертизі з комп’ютерно-мережевими засобами перед експертом слідчий ставить такі питання.

а) Діагностичні:

1. Що собою являє поданий на експертизу конкретний комп’ютерно-мережевий засіб, його функціональне призначення, характеристики?

2. Яким чином він міг потрапити до мережевого забезпечення, час встановлення і термін придатності?
3. Шкідливість і небезпечність даного комп'ютерно-мережевого засобу?

б) Ідентифікаційні:

1. В якому стані комп'ютерно-мережевий засіб знаходиться і чи підлягає ідентифікації?
2. Спосіб його виготовлення та основні складові?
3. Чи є даний пристрій адаптованим з іншої сфери, чи спеціально виготовлений?
4. Чи відповідають технічні параметри встановленим нормам для такого виду забезпечень чи ні?

Перелік названих та інших запитань може бути поставлений слідчим перед експертною установою в залежності від предмета дослідження. Однак, слідчому необхідно при підготовці до експертизи дотримуватися таких вимог:

- до винесення постанови про призначення відповідної експертизи проконсультуватися з фахівцями щодо доцільності її проведення, формулювання вірності поставлених питань, характеру і особливостей підготовки матеріалів, що будуть подані експертам;
- по можливості ознайомити експертів з усіма матеріалами справи, що відносяться до предмета експертизи (протоколами огляду місця події, документів і предметів, а також допитів відповідних осіб; матеріалами ревізій, інвентаризацій, аудиту, висновками інших спеціалістів, що мають відношення до процесу розслідування тощо).

ЗАГАЛЬНІ ВИСНОВКИ ДОСЛІДЖЕННЯ

Результати монографічного дослідження дозволяють сформулювати основні висновки, рекомендації, пропозиції і можуть слугувати певним внеском у загальну теорію науки криміналістики, а також у практичну діяльність щодо виявлення, розслідування злочинів, пов'язаних з використанням комп'ютерних технологій:

1. Злочини, що вчиняються з використанням комп'ютерних технологій являють собою одне із складних соціальних явищ у суспільстві. Кваліфіковане розслідування правоохоронними органами такої категорії злочинів – одне з ключових питань для будь-якої держави, у тому числі й України. Міжнародний характер протидії цьому феномену сучасності – запорука подальшої стабільності і розвитку всіх сфер людського буття.

2. Підставою для порушення кримінальної справи про скоєний злочин, у тому числі й комп'ютерний, є достатні дані, що вказують на наявність ознак складу злочину. Виходячи зі змісту кримінально-правової характеристики, комп'ютер та його програмне забезпечення може бути як предметом злочину, так і засобом, за допомогою якого реалізовується задум злочинця. Внесені законодавцем зміни до Кримінального та Кримінально-процесуального кодексів України від 23.12.2004 р. розширили можливість регулювати злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку і уникнули прогалин, які були допущені у першій редакції Розділу XVI Кримінального кодексу України.

3. Криміналістична характеристика комп'ютерних злочинів є узагальненою інформаційною моделлю, що являє собою систематизований опис типових криміналістично значущих ознак, які мають суттєве значення для виявлення та розслідування зазначеної вище категорії злочинів. З урахуванням недостатності знань практичних працівників правоохоронних органів, на яких покладається завдання розслідувати «нетрадиційні» злочини,

доцільним буде формування наступних структурних елементів її криміналістичної характеристики. А саме:

- предмет без посереднього злочинного посягання;
- деякі обставини скоєння злочину (місце, час, обстановка, умови).
- способи вчинення та можливого приховування злочинів;
- слідова картина злочинів;
- особа злочинця та особа потерпілого;
- мета і мотиви вчинення злочину.

а) Предмет без посереднього злочинного посягання. Ним виступає саме посягання на речі матеріального світу і предмети; комп'ютерна інформація та комп'ютерні продукти у тому числі й інтелектуального характеру, індивідуальної державної чи приватної власності, які становлять собою конкретно визначену матеріальну цінність.

Даний елемент криміналістичної характеристики злочинів носить конструктивну ознаку, оскільки мова йде про злочини, що скоюють особи з використанням саме комп'ютерних технологій. Найбільш поширеними вони є: у сфері економіки, зокрема банківській, кредитно-фінансовій; військовій галузі, у тому числі стратегічних військових сферах; міжнародних трансграничних, глобалізаційних сферах; державотворчому процесі та ін.

б) Деякі обставини скоєння злочину (місце, час, обстановка, умови). Особливістю комп'ютерних злочинів є те, що місце, звідки було скоєно протиправну дію (місце, де виконувалися дії об'єктивної сторони складу злочину) та місце настання шкідливих наслідків (місце, де наступив результат злочину) можуть не співпадати. Таким місцем може бути будь-яке приміщення різної форми власності, в якому знаходиться комп'ютерно-технічне оснащення, забезпечене виходом до глобальної мережі типу INTERNET. Час вчинення протиправних дій з використанням комп'ютерних технологій завжди конкретно визначений.

в) Способи скоєння злочинів даної категорії запропоновані Ю.М. Батуріним і викладені у п'яти групах, більше відображують способи

протиправних дій, аніж способи вчинення комп'ютерних злочинів. Їх зміст повинен бути сформований наступним чином:

- способи безпосереднього доступу до комп'ютерної інформації або операційної системи;
- способи видаленого (опосередкованого) доступу;
- способи виготовлення, розповсюдження на технічних носіях шкідливих програм для ЕОМ.

г) Слідова картина комп'ютерних злочинів. Її можна розглядати як сукупність абстрагованої інформації про типові матеріальні й ідеальні сліди-ознаки та умови скоєння суб'єктом протиправних дій з використанням комп'ютерних технологій:

- «Слідова картина» незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем комп'ютерних мереж чи мереж електрозв'язку
- «Слідова картина» створення з метою використання, розповсюдження або збуту шкідливих програм чи технічних засобів, а також їх розповсюдження або збут.
- «Слідова картина» несанкціонованого збуту або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації.
- «Слідова картина» несанкціонованих дій з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчиненої особою, яка має право доступу до неї.
- «Слідова картина» порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється.

- «Слідова картина» перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

д) Особа злочинця та особа потерпілого. За статистичними даними вітчизняної та зарубіжної практик, вік осіб, що вчиняють комп'ютерні злочини, сягає від 15 до 45 років. Матеріали експертних досліджень визначають, що на момент вчинення протиправних дій вік 33 % злочинців не перевищував 20 років; 13 % – були старші 40 років; 54 % мали вік від 20 до 40 років.

е) Мотиви і мета вчиненого злочину. Вони залежать від багатьох факторів, зокрема, на що саме була спрямована протиправна дія. Виходячи з аналізу світової та вітчизняної практик, їх можна побудувати у такій послідовності:

- корисливі – на долю яких припадає 66 % комп'ютерних злочинів;
- політичні – 17 % (шпигування, підрив фінансово-економічної діяльності та кредитної політики);
- цікавість, допитливість – 7 %;
- хуліганські наміри – 5 %;
- помста – 5 %.

4. Початковий етап розслідування комп'ютерних злочинів, вимагає належного відношення до підготовки та порушення кримінальних справ, пов'язаних з використанням ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку. Особлива роль на цьому та інших етапах розслідування відводиться формуванню висококваліфікованої слідчої та оперативно-розшукової групи. Недоцільно, щоб спеціалістами у зазначеній категорії злочинів, для проведення процесуальних заходів були запрошені особи зі сторони, оскільки вони не вболівають за результативність справи. Осередком сформованої групи спеціалістів, мають бути штатні працівники правоохоронних органів, які належним чином володіють знаннями

у сфері комп’ютерних технологій. Понятими слід запрошувати осіб, які б хоч мінімально володіють навичками зазначених вище високих технологій, але не з числа суб'єктів потерпілої сторони, щоб не наразити слідство на самого злочинця або іншу зацікавлену у справі особу.

5. З метою надання практичної допомоги слідчому у вирішенні організаційних питань забезпечення початкового етапу розслідування комп’ютерних злочинів, пропонується ряд рекомендацій, що стосуються підготовки та проведення процесуальних заходів. З урахуванням того, що у тактиці слідчих дій розслідування такої категорії злочинів є свої особливості на відміну від «традиційних» видів злочинів, слідчому необхідно зосередити увагу на наступному:

а) підготовчий етап має складатися з двох стадій: до виїзду на слідчий огляд та дії на місці події до початку робочого етапу. Особлива роль на цьому етапі повинна відводитися оперативно-розшуковій діяльності правоохоронних органів та формуванню складу робочої групи, яка виїжджатиме на слідчу дію;

б) робочий (дослідний) етап повинен включати загальний огляд (статичну) та детальну (динамічну) дії. Чільне місце на цьому етапі відводиться роботі спеціалістів з електронними документами, які можуть нести доказову інформацію про скоєний злочин;

в) на заключному етапі проведення слідчої дії має відбуватися не лише грамотне оформлення належних процесуальних документів, а й правильність вилучення виявлених речей та предметів доказового значення, а також поводження з електронними носіями інформації.

6. Беручи до уваги той факт, що злочини у цій сфері є складними як для розслідування так і зібрання матеріалів, що мають доказове значення по справі – пропонується у якості теоретичної допомоги слідству розглянути такі типові слідчі ситуації, що можуть скластися на початковому етапі розслідування такої категорії злочинів:

- виявлено факт несанкціонованого втручання в інформацію, що циркулює у банківській чи кредитно-фінансовій сфері, але відсутні дані про спосіб вчинення злочину та причетних до нього осіб;
- виявлено факт внесення будь-якого плану змін у комп'ютерну інформацію, при цьому спосіб доступу до баз даних відсутній або ж має опосередкований характер, суб'єкт злочину невідомий;
- виявлено факт внесення змін у комп'ютерну інформацію, зафіксовано спосіб доступу до баз даних, окремих програм, відома імовірна особа злочинця;
- виявлено факт внесення в програмне забезпечення чи окремі файли шкідливих, небезпечних вірусних програм, спосіб зараження та особа злочинця невідомі;
- виявлено факт знищення інформації у комп'ютерній мережі, дані про спосіб вчинення та причетних до злочину осіб невідомі;
- виявлено факт викрадення (заволодіння) комп'ютерною інформацією, при цьому дані про спосіб доступу до інформацію та про суб'єкта злочину невідомі;
- виявлено факт модифікації баз даних чи маніпуляції інформацією в окремих програмних файлах, дані про спосіб та про ймовірного суб'єкта відомі.

7. Для ефективного проведення процесуальних слідчих заходів слідчо-оперативна група повинна мати необхідне техніко-криміналістичне забезпечення. У зв'язку з цим, доцільно, паралельно з традиційними криміналістичними валізами, налагодити випуск спеціалізованого науково-технічного спорядження для виявлення, фіксації та відбору комп'ютерних інформаційних слідів на місці скоєння злочину. Аналіз практики засвідчує, що з-поміж технічних засобів, що використовується при проведенні окремих слідчих дій у злочинах з комп'ютерних технологій, найбільш використовуваними є: фотографування, близько – 40 % та відеозапис – 28 %. Спеціалізоване під комп'ютерну техніку і програмне забезпечення оснащення

використовується у 9% випадків, а пошукове обладнання для виявлення інформації і вплив на неї, у 2 % випадків.

8. Враховуючи**,** що основу організації розслідування злочинів, у тому числі й зазначеної категорії, становить планування, а воно здійснюється, виходячи з криміналістичних версій, пропонується кілька типових версій, які можуть застосовуватися працівниками правоохоронних органів при розслідуванні кримінальних справ у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем**,** комп'ютерних мереж і мереж електрозв'язку, зокрема:

- Комп'ютерний злочин скоєно з метою отримання матеріальної винагороди задля наживи;
- Комп'ютерні злочини у сфері банківської та кредитно-фінансової діяльності
- *Версія 1. Комп'ютерний злочин скоєно з метою наживи шахрайським шляхом, співробітником даної, який є бухгалтером, менеджером, оператором, програмістом програмно-операційного забезпечення або ж іншим найманим працівником, що має доступ до ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку і досконало володіє навичками роботи з ними.*
- *Версія2. Комп'ютерний злочин скоєно з метою наживи сторонньою особою, яка досконало володіє навичками комп'ютерних технологій і є поінформованою про виробничий процес , а також конфіденційну комп'ютерну інформацію потерпілої сторони.*
- *Версія 3. Комп'ютерний злочин вчинено з метою наживи організованою злочинною групою осіб за попереднім зговором з використанням ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку.*
- Порушення роботи автоматизованих систем шляхом знищення електронної інформації, модифікації комп'ютерних програм, блокування роботи технічного оснащення операційних ЕОМ

(комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку.

- *Версія 1. Комп'ютерний злочин скоєно особою з метою внесення у базу електронних даних, окремого програмного забезпечення, файлу та ін., інформації, що містить шкідливі чи небезпечні дії, які в кінцевому результаті спричиняють непередбачувані наслідки добросовісному власникові.*
- *Версія 2. Комп'ютерний злочин скоєно суб'єктом протиправної діяльності з метою впливу на роботу ЕОМ (комп'ютерів), автоматизованих систем, що спричинило блокування, зупинення чи порушення роботи комп'ютерних мереж і мереж електрозв'язку.*
- Незаконне заволодіння, розповсюдження та використання електронної інформації комп'ютерними злочинцями, яка знаходиться в ЕОМ (комп'ютерах) добросовісних її власників і містить таємні чи конфіденційні дані.
- *Версія 1. Злочин скоєно особою шляхом впливу на комп'ютерну інформацію з метою заволодіння, знищення чи маніпуляції електронними даними, що спричинило непередбачувані наслідки для її власника.*
- *Версія 2. Комп'ютерний злочин скоєно з метою порушення авторських прав суб'єктом, що є фахівцем в сфері ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку і володіє даними про предмет злочину.*
- *Версія 3. Комп'ютерний злочин скоєно з метою порушення авторських прав суб'єктом (суб'єктами), які безпосередньо не мають доступу до зацікавлених електронних даних, а отримують таку інформацію опосередковано від інших суб'єктів.*

9. У рамках дотримання процесуальних норм, окрім основного ведення протоколу допиту, доцільно використовувати інші науково-технічні засоби фіксації інформації (аудіо-, відеозаписуючі пристрої). Разом з тим на стадії вільної розповіді допустимо слідчому призупиняти допитуваного суб'єкта за умови використання ним спеціальної комп'ютерно-технічної термінології, тощо з метою уникнення непорозумінь і неточностей при оформленні процесуального документа, а також неправильного сприйняття слідчим окремого факту події, що розслідується. Особливо це може стосуватися допиту операторів, програмістів-комп'ютерників, системників, персоналу який обслуговує комп'ютерне забезпечення та ін.

10. Тактика проведення обшуку та виїмки об'єктів доказового значення на подальшому етапі розслідування зазначеної категорії злочинів має відповідати таким критеріям:

- психологічній налаштованості слідчого на проведення процесуальної дії;
- умінню не реагувати на ознаки певної невизначеності, недостатньої впевненості, передчуття відсутності результативності проведення слідчого заходу;
- визначенню оптимальних умов (місця, часу, обстановки, обставин, сприятливих умов) успішної реалізації слідчих дій;
- вибору та застосуванню попереджувальної форми чи фактору раптовості під час обшуку, виїмки на місці скоєння злочину;
- особливостям використання традиційних технічних засобів (магнітних шукачів тощо) при виявленні відповідних схованок під час проведення окремих слідчих дій.

11. Логічне завершення розслідуваного злочину у сфері з використанням електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку, залежить від своєчасного і грамотного проведення необхідних експертиз. Окрім традиційних криміналістичних: дактилоскопічних, трасологічних, фоноскопічних,

фінансово-економічних, техніко-криміналістичних експертиз документів тощо, важливе значення має судова комп'ютерно-технічна експертиза, різновид класу інженерно-технічних експертиз. Основу цього виду експертиз становить вирішення діагностичних та ідентифікаційних питань, що ставлять перед експертом. Вони сприяють розв'язанню таких розшукових завдань: встановленню факту знаходження пошукової інформації на технічних носіях, які представлені на експертизу; отримання розшукової інформації про професійні якості злочинця.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика /Учеб. для вузов. – М.: Издательская группа НОРМА – ИНФРА. – М., 1999. – 971 с.
2. Азаров Д.С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації: Автореф. канд. юрид. наук. – К., 2002. – 18 с.
3. Азаров Д. Особливості механізму вчинення злочинів у сфері комп'ютерної інформації //Юридична Україна. – 2004. – № 7 (19). – С. 64 – 68.
4. Азаров Д. Порушення роботи автоматизованих систем – злочин в сфері комп'ютерної інформації //Право України. – 2001. – № 12. – С.72 – 74.
5. Антонов С. Компьютерные преступления в банковской сфере //Юридическая практика. – 1997. – № 8. – С. 7 – 9.
6. Айков Девид, Сейгер Карл, Фонсторх Уильям Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями /Перевод с анг. В.И.Воропаева, Г.Г. Трехалина – М.: Мир, 1999. – 351 с.
7. Алексеев А, Евсеев Г., Мураховский В., Симонович С. Новейший самоучитель работы на компьютере. – М.: Изд-во «Десс», 1999. – 654 с.
8. Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. – М.: Изд-во «Юрлитинформ», 2001. – 150 с.
9. Арцишевский Г.В. Выдвижение и проверка следственных версий. – М.: Юрид.лит., 1978. – 104 с.
10. Архів Чернігівського обласного суду: Кримінальна справа № 11-335/200, ухвала від 20.04.2000 р.
11. Архів Дарницького районного суду м. Києва: Кримінальна справа № 1-503, вирок від 16.01.2001 р.
12. Афанасьев В.Г. Системность и общество. – М., 1980. – 368 с.

13. Ахтирська Н. Про удосконалення кримінального законодавства України в сфері боротьби з кіберзлочинністю //htth://www.crime-research.org.
14. Ахтырская Н. Особенности тактики обыска при расследовании компьютер. преступлений //http: // www/ crime-research. org. – С. 1– 17.
15. Бахин В.П. Криминалистическая методика. Лекция. – К., 1999. – 27 с.
16. Бахин В.П. Следственная ситуация и тактическое решение //Специализированный курс криминалистики (для слушателей вузов МВД СССР, обучающихся на базе сред. спец. юрид. образ.): Учеб. / Под ред. проф. М.В.Салтевского. – Киев: НИ и РИО КВШ МВД СССР, 1987. – С. 195 – 204.
17. Баранов О. Цифрове законодавство //Дзеркало тижня. – 2002. – № 20.
18. Баранов О. Уголовная ответственность за компьютерные преступления //Безопасность информации. – 1996. – № 2. – С.4 – 9.
19. Баранов О. Кримінологічні проблеми комп'ютерної злочинності //Інформаційні технології та захист інформації: Зб. наук. праць. – Запоріжжя: Юридичний інститут МВС України, 1998. – Вип. 2. – С.64 – 69.
20. Батурин Ю.М. Проблемы компьютерного права. – М.: Юрид. лит., 1991. – 271 с.
21. Баулін О.В., Карпов Н.С., Поповченко О.І., Савицький Д.О. Спрощене досудове провадження в Україні: історія, сучасність, перспективи: Навч. посіб. – К.: Семенко Сергій, 2004. – 151 с.
22. Батурин Ю.М., Жодзинский А.М. Компьютерная преступность и компьютерная безопасность. – М., 1991. – 158 с.
23. Бачило И.Л., Семилетов С.И. Основные направления организационно-правового регулирования использования глобальных сетей, включая Интернет /Информационное право: информационная культура и информационная безопасность. Материалы Всероссийской научно-практической конференции Санкт-Петербургского гуманитарного университета профсоюзов, 17 – 19 октября 2002 г. – С.90 – 100.

24. Белкин Р.С. Курс криминалистики: В 3-х т. Частные криминалистические теории. – М.: Юристъ, 1997. – Т. 2. – 464 с.
25. Белкин Р.С. Курс криминалистики. В 3-х т. Криминалистические средства, приемы и рекомендации. – М.: Юристь, 1997. – Т. 3. – 480 с.
26. Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. От теории к практике. – М.: Юридическая литература, 1988. – 302 с.
27. Белкин Р.С. Противодействие расследованию и пути преодоления криминалистическими и оперативно-розыскными средствами и методами //Криминалистическое обеспечение деятельности уголовной милиции и органов предварительного расследования /Под ред. Т.В. Аверьяновой, Р.С. Белкина. – М., 1997. – С. 130.
28. Беляков К.И. Управление и право в период информатизации: Монографія. – Киев: КВЩ, 2001. – 308 с.
29. Большая энциклопедия: CD-ROM. – М.: Кирилл и Мефодий, 1997.
30. Біленчук П.Д., Біленчук Д.П., Міщенко В.Б., Мотлях О.І. Національна безпека України: сучасні інформаційні технології і можливі джерела безпеки //Вісник Академії праці і соціальних відносин ФП України. – 1998. – № 1. – С. 61 – 72.
31. Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соціально-правові та кримінолого-криміналістичні аспекти: Навч. посіб. – К.: Українська академія внутрішніх справ, 1994. – 72 с.
32. Біленчук П., Котляревський О. Портрет комп'ютерного злочинця: Навч. посіб. – К.: B&B, 1997. – 48 с.
33. Біленчук П.Д., Дубовий О.П., Салтевський М.В., Тимошенко П.Ю. Криміналістика. Підруч. – К.: Атіка, 1998. – С. 416.
34. Біленчук П.Д., Романюк Б.В., Цимбалюк В.С. Комп'ютерна злочинність. Навч. посіб. – К.: Атіка, 2002. – 240 с.
35. Біленчук П.Д., Лисиченко В.К., Клименко Н.І. Криміналістика: Підруч. /За ред. П.Д. Біленчука. – 2-е вид., випр. і доп. – К.: Атіка, 2001. – 544 с.
36. Біленчук П.Д., Головач В.В., Салтевський М.В. Криміналістика. Підруч.

для вищих навч. закл. /За ред. П.Д.Біленчука. – К.: Українська правнича фундація, Вид-во «Право», 1997. – 253 с.

37. Биленчук П.Д., Еркенов С.Е., Кофанов А.В. Транснациональная преступность: состояние и трансформация. Учеб. пособ. для высш. учеб. завед. – Киев: Атика, 1999. – 270 с.
38. Бірюков В.В. Використання комп'ютерних технологій для фіксації криміналістично значимої інформації у процесі розслідування. Дис. канд. юрид. наук. – 12.00.09. – Луганськ, 2000. – 175 с.
39. Бурчак Ф.Г. Квалификация преступлений. Изд. 2-е, доп. – Киев.: Изд-во полит. лит-ры Украины, 1985. – 119 с.
40. Васильев А.Н. Тактика отдельных следственных действий. – М.: Юридическая литература, 1981. – 112 с.
41. Васильев А.Н., Яблоков Н.П. Предмет, система и теоретические основы криминалистики. – М.: МГУ, 1984. – 144 с.
42. Вертузаєв М., Попов А. Запобігання комп'ютерним злочинам та їх розслідування // Право України . – 1998. - № 1. – С. 101 – 103.
43. Вертузаєв М.С., Голубєв В.О., Котляревський О.І., Юрченко О.М. Безпека комп'ютерних систем: злочинність у сфері комп'ютерної інформації та її попередження Під заг. ред. О.П.Снігірьова. – Запорізький юридичний інститут МВС України, Національна академія внутрішніх справ України. – Запоріжжя : ПВКФ "Павел", 1998. – 315 с.
44. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия /Под ред. акад. Б.П. Смагоринского. – М.: Право и Закон, 1996. – 182 с.
45. Вехов В.Б. Криминалистическая характеристика компьютерных преступлений и совершенствование практики их расследования и предупреждение /Под ред. Б.П. Смагоринского. – Волгоград: ВЮИ МВД России, 1998. – 206 с.
46. Винокуров С.И. Криминалистическая характеристика преступлений, ее содержание и роль в построении методики расследования //Методика

расследования преступлений: Общие положения. – М., 1976. – С. 101.

47. Возгрин И.А. Научные основы криминалистической методики расследования преступлений. – СПб.: СПб ЮИ МВД России, 1993. – Ч. 4. – 80 с.

48. Возгрин И.А. Криминалистические характеристики преступлений и следственные ситуации в системе частных методик расследования //Следственная ситуация. – М., 1985. – С. 69.

49. Возгрин И.А. Криминалистическая методика расследования преступлений. – Мн.: Высш. школа, 1983. – 215 с.

50. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО Изд-во «Юрлитинформ», 2002. – 496 с.

51. Гавловський В.Д., Цимбалюк В.С. Кіберзлочинність як чинник державної інформаційної політики України //Боротьба з організованою злочинністю і корупцією (теорія і практика). Координаційний комітет по боротьбі з корупцією і організованою злочинністю при Президентові України. Міжвід. наук.-дослід. центр. – 2002. – № 5. – С. 106 – 116.

52. Гавловський В.Д., Романюк В.С. Проблеми організації боротьби з правопорушеннями, що вчиняються з використанням сучасних інформаційних технологій //Публікації Центру дослідження проблем комп'ютерної злочинності. – www/crime-recearch.org/library/Gav-Rom-Cim.htm

53. Гаврилин Ю.В. Рассследование неправомерного доступа к компьютерной информации. Учеб. пособ. – М.: – Книжный мир, 2001.– 88 с.

54. Гавло В.К. Следственная ситуация //Следственная ситуация. Сб. науч. тр. – М.: Всесоюзн. ин-т изуч. причин. и разраб. мер предупреждения преступности, 1995. – С. 38 – 41.

55. Гавло В.К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений. – Томск: Томский ун-т,

1985. – 119 с.

56. Герасимов И.Ф. Криминалистическая характеристика преступлений в методике расследования //Методика расследования преступлений. – М., 1976. – С. 96.

57. Герасимов И.Ф. К вопросу о следственных ситуациях //Следственная ситуация: Сб. науч. тр. – М.: МВШ МВД СССР, 1984. – С.6 – 11.

58. Гончаренко В.И. Научно-технические средства в следственной практике: Моногр. – Киев: Изд-во при Киевском государственном ун-те издательского объединения «Вища школа», 1984. – 147 с.

59. Гончаренко В.И., Кушнир Г.А., Подпалый В.Л. Понятие криминалистической характеристики преступлений //Криминалистика и судебная экспертиза. – Киев: Вища шк., 1986. – Вып. 33. – С. 6 –7.

60. Гончаренко В.И. Использование данных естественных и технических наук в уголовном судопроизводстве (методологические вопросы). – Киев: Вища школа, 1980. – 157 с.

61. Гончаренко В. И. Использование звукозаписи, фотографии и киносъемок в уголовном судопроизводстве. – Киев: Вища школа, 1980. – 41с.

62. Гончаренко В.Г. Теорія криміналістики і адвокатська практика //Адвокат. – 2003. – № 2 (35). – С. 3 – 6.

63. Гончаренко В.Г. Право і криміналістика //Вісник Академії адвокатури України. – 2004. – Вип. 1. – С. 40 – 43.

64. Гончаренко В.И. Единство и отличие криминалистики и криминалистической экспертизы //Теорія та практика судової експертизи і криміналістики. – Харків: Право. – 2002. – Вип. 2. – С. 55 – 59.

65. Голубєв В. Кібертероризм – загроза національній безпеці та інтересам України //Юридичний журнал. – 2004. – № 1 (19). – С. 132 – 134.

66. Голубєв В. Комп'ютерна злочинність //Юридичний вісник України. – 2002. – № 6 (9). – С. 1 – 4.

67. Голубєв В.О., Гавловський В.Д., Цимбалюк В.С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій /За заг. ред. докт. юрид. наук, проф. Р.А.Калюжного. – Запоріжжя: Просвіта, 2001. – 252 с.
68. Голубєв В.О. Розслідування комп'ютерних злочинів /Моногр. – Запоріжжя: Гуман. ун-т «ЗІДМУ», 2003. – 296 с.
69. Голубєв В.О. Розслідування комп'ютерних злочинів. Монографія. – Запоріжжя: Гуман. ун-т «ЗІДМУ», 2003. – 157 с.
70. Горелик И.И. Мотив и цель преступления //Уголовное право. Часть общая. Т. 1. – Минск: Высшая школа, 1978. – С. 84.
71. Голик Ю.В. Случайный преступник.–Томск: Изд-во Томского ун-та, 1984. –166 с.
72. Глотов О.М. Некоторые проблемы предварительного следствия в связи научно-технической революцией //50 лет советской прокуратуры и проблемы усовершенствования предварительного следствия. – Л.: Изд-во Ленингр. ун-та, 1972. – С. 5 – 13.
73. Глушков В.О., Бєляков К.І., Орлов С.О. Інформаційні відносини: кримінально-правовий аспект. Про Проект Концепції стратегії реалізації державної політики щодо боротьби з кіберзлочинністю в Україні. /http://mndc. naiau. kiev. ua /KONC/ ceber. httm.
74. Гуцалюк М. Протидія комп'ютерній злочинності //Право України. – 2003. – № 6. – С.114 – 117.
75. Гуцалюк М. Протидія міжнародній комп'ютерній злочинності //Вісник прокуратури. – 2003. – № 9 (27). – С.60 – 64.
76. Гуцалюк М. Хроніка вірусної атаки на Укртелеком //htth://www.ukrtel.net
77. Гуцалюк М. Координація боротьби з комп'ютерною злочинністю //Право України. – 2002. – № 5. – С. 121 – 126.
78. Гросс Г. Руководство для судебных следователей как система /Пер. с нем. 4-го изд. Л. Дудкина и Б. Зиллера. – СПб., 1903. – 234 с.
79. Грязін В.І. Тактика допиту обвинуваченого при розслідуванні злочинів

– проти держави. Моногр. – К.: Інститут економіки та права «Крок», 2001. 136 с.

80. Даль В.И. Толковый словарь живого великорусского языка. – М., 1979.
81. Дулов А.В., Грамович Г.И., Лапин А.В. Криминалистика: Учеб. пособ. /Под ред. А.В.Дулова. – Минск: ИП ”Экоперспектива”, 1998. – 415 с.
82. Духов В.Е. Экономическая разведка и безопасность бизнеса. – Киев: ИМСО МО Украины, НВФ “Студцентр” , 1997.
83. ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. Видання офіційне. – К.: Держстандарт України, 1994.
84. Ермолович В.Ф. Криминалистическая характеристика преступлений. – Минск: Изд-во «Амалфея», 2001. – 303с.
85. Жарова А.К. Правовые проблемы обращения информации в Интернете. Опыт Республики Узбекистан: Автореф. дисс. канд. юрид. наук. – М., 2002. – С. 23.
86. Жирний Г.Ю. Про формування окремих криміналістичних методик розслідування злочинів у сфері використання автоматизованих електронно-обчислювальних систем / Правові основи захисту комп’ютерної інформації від протиправних посягань: Матеріали міжвузівської науково-практичної конференції (22 грудня 2000 р.). – Донецьк: Донецький інститут внутрішніх справ, 2001. – 324 с.
87. Журавльов В.П., Муженко П.М. Психолого-тактичні аспекти розслідування злочинів, вчинених організованими угрупуваннями //Боротьба з організованою злочинністю і корупцією (теорія і практика). Координаційний комітет по боротьбі з корупцією і організованою злочинністю при Президентові України. Міжвідомчий науково-дослідний центр, 2002. – № 5. – С. 28 – 37.
88. Іщенко А.В., Колесник В.А., Гора І.В. Криміналістика: Посіб. для підгот. до іспитів /А.В. Іщенко, В.А. Колесник, І.В. Гора. – 2-е вид., допов. та перер. – К.: Вид-во ПАЛИВОДА А.В., 2004. – 232 с.
89. Іщенко А.В., Красюк І.П., Матвієнко В.В. Проблеми криміналістичного

забезпечення розслідування злочинів: Монографія. – К.: Національна академія внутрішніх справ України, 2002. – 212с.

90. Ищенко А.В. Бахин В.П. Понятие и сущность криминалистической рекомендации //Криминалистика и судебная экспертиза. – Киев, 1993. – № 46. – С.15 – 23.

91. Іщенко А.В. Методологічні проблеми криміналістичних наукових досліджень: Монографія. /За ред. І.П. Красюка. – К.: Національна академія внутрішніх справ України, 2003. – 359 с.

92. Ищенко П.П. Специалист-криминалист в следственных действиях (уголовно-процессуальные и криминалистические аспекты). – М.: Юрид. лит., 1990. – 158 с.

93. Іщенко А.В., Ієрусалимов І.О., Удовенко Ж.В. Теорія і практика криміналістичного забезпечення процесу доказування в розслідуванні злочинів: Навч. посібник. – К.: Центр учбової літератури, 2007. – 160 с.

94. Карпов Н.С. Теоретичні основи та практика використання передового досвіду органів внутрішніх справ у протидії злочинній діяльності /Під наук. ред. В.П. Бахіна. Монографія. – К.: Національна академія внутрішніх справ України, 2003. – 124 с.

95. Карпов Н., Вертузаев М. К вопросу о борьбе с компьютерными преступлениями в Украине //Международный научно-практический правовой журнал "Закон и жизнь". – 2004. – № 7 (152). – С.29 – 32.

96. Калюжный Р.А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект): Автореф. дисс. д-ра юрид. наук, – Институт государства и права им. В.М.Корецкого. – Киев, 1992. – 23 с.

97. Карчевский Н.В. Компьютерная информация как предмет уголовно-правовой охраны /Правові основи захисту комп'ютерної інформації від протиправних посягань: Матер. міжвуз. наук.-практ. конф. (22 грудня 2000 р.). – Донецьк: Донецький інститут внутрішніх справ, 2001. – С. 54 – 67.

98. Карнеева Л.М. Доказывание в уголовном процессе. – М.: ГКУ МВД России, 1994. – 46 с.
99. Касаткин А.В. Тактика собирания и использования компьютерной информации при расследовании преступлений. Дисс. канд. юрид. наук. – М., 1997. – 24 с.
100. Карагодин В.Н. Выдвижение версий об обстоятельствах скрываемого преступления /Версии и планирование расследования. Межвуз. сб. науч. трудов. – Свердловск: Свердловский юридический институт, 1985. – С. 20 – 27.
101. Кесарева Т.П. Криминальная паутина. Мошенничество в системе электронной торговли через Интернет // Интерпол в России. – 2000. – № 3. – С. 26 – 27.
102. Колесник В.А. Розслідування комп'ютерних злочинів. Наук.-метод. посіб. – К.: Вид-во НА СБУ, 2003. – 124 с.
103. Колесник В.А., Гора І.В. Криміналістика: Посіб. для підгот. до іспитів. – К.: Вид-во ПАЛИВОДА А.В., 2003. – 146 с.
104. Колесник В.А. Тактика использования оперативно-розыскных материалов в уголовном судопроизводстве (Актуальні проблеми сучасної криміналістики) //Матеріали науково-практичної конференції: У 2-х ч. – Сімферополь – Алушта, 19 – 21 вересня 2002 р. – Сімферополь: Доля, 2002. – Ч. 2. – 248 с.
105. Колесниченко А.Н. Научные и правовые основы расследования отдельных видов преступлений: Автореф. дисс. д-ра юрид. наук. – Харьков, 1967. – С. 16.
106. Колесниченко А.Н., Матусовский Г.А. О системе версий и методике их построения. Криминалистика и судебная экспертиза. – К.: Высш. шк., 1970. – Вып. 7. – С. 7 – 13.
107. Комиссаров В.И. Теоретические проблемы следственной тактики. – Саратов: Изд-во Сарат. гос. ун-та, 1987. – 129 с.
108. Комиссаров В.И. Научные, правовые и нравственные основы

следственной тактики /Под ред. проф. А.Н.Васильева. – Саратов: Изд-во Сарат. ун-та. – 1980. – 123 с.

109. Комисаров В., Гаврилов М., Иванов А. Обыск с извлечением компьютерной информации //Законность. – 1999. – № 3. – С. 12 – 15.

110. Колмаков В.П. Следственный осмотр. – М.: Юрид. лит., 1969. – 196 с.

111. Кони А.Ф. Избр. произв. – М., 1959. – Т. 1. – С. 167.

112. Колдин В.Я. Задачи, объекты и этапы судебной идентификации //Правоведение. – 1967. – № 3. – С. 131.

113. Котляревський О.І., Киценко Д.М. Комп'ютерна інформація як Речовий доказ у кримінальній справі /Інформаційні технології та Захист інформації: Зб. наук. праць. – Запоріжжя, 1998. – Вип.2. – 128 с

114. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. – М.: Горячая линия – телеком, 2002. – 336с.

115. Компьютерная преступность в США //Проблемы преступности в капиталистических странах. – 1990. – № 9. – С.3 – 5.

116. Компьютерная преступность в Швейцарии: формы проявления и характеристика преступников //Проблемы преступности в капиталистических странах. – 1987. – № 9. – С. 5 – 10.

117. Клименко Н.І., Біленчук П.Д. Судова експертиза в розслідуванні комп'ютерних злочинів як форма використання спеціальних знань // Теорія та практика судової експертизи і криміналістики. – Харків: Право. – 2002. – Вип.2. — С. 62 – 64.

118. Кузьмічов В.С., Прокопенко Г.І. Криміналістика. Навч. посіб. /За заг. ред. В.Г. Гончаренка, Є.М. Моісеєва. – К.: Юрінком Інтер, 2001. – 368 с.

119. Кудрявцев В.Н. Общая теория квалификации преступлений. – 2-е изд., перераб. и дополн. – М.: Юристъ, 2001. – 304 с.

120. Курс уголовного права. Общая часть. Т. 1: Учение о преступлении: Учеб. для вузов / Под ред. Н.Ф.Кузнецовой, И.М.Тяжковой. – М.: Зерцало, 1999. – 592 с.

121. Курс Советского уголовного права: В 5 т. – Л.: Изд-во Ленинград. ун-та., 1968. – Т. 1. – 645 с.
122. Куранова Э. Д. Об основных положениях методики расследования отдельных видов преступлений //Вопросы криминалистики. – 1962. – № 6-7. – С. 165 – 167.
123. Кукарникова Т.Э. Проблема криминалистического исследования электронных документов //Вести Тул. ГУ. Серия: «Современные проблемы законодательства России, юридических наук и правоохранительной деятельности». – Тула: Изд-во Тул. гос. ун-та, 2000. – Вып. 3. – С.11 – 16.
124. Куркін В.О., Мотлях О.І. Типові криміналістичні ситуації у розслідуванні організованої злочинної діяльності //Вісник Академії праці і соціальних відносин ФП України. – 2004. – № 2 (26). – С. 20 – 24.
125. Кулагин Н.И. Планирование расследования сложных многоэпизодных дел: Учеб. пособ. – Волгоград, 1976. – 62 с.
126. Крылов В.В. Информационные компьютерные преступления. – М.: ИНФРА- М-НОРМА, 1997. – 285 с.
127. Крылов И.Ф., Бастрыкин А.И. Розыск, дознание, следствие: Учеб.пособ. – Ленинград: Изд-во Ленинград. ун-та, – 1984. – 216 с.
128. Крылов И.Ф. Несколько замечаний по поводу протокола осмотра места происшествия. – Вильнюс, 1967. – С. 121 – 126.
129. Криминалистика: Учеб. для вузов /И.Ф.Герасимов, Л.Я. Драпкин, Е.П. Ищенко; под. ред. И.Ф. Герасимова, Л.Я. Драпкина. – 2-е изд., перераб. и доп. – М.: Высш. шк., 2000. – 672 с.: ил.
130. Криміналістика. Навч.-довід. посіб./ М.В.Салтевський.– К., 1999. –159 с.
131. Криминалистика: Учеб. /Отв. ред. Н.П.Яблоков. – 2-е изд., перераб. и доп. – М.: Юристъ, 1999. – 718 с.
132. Криминалистика: Учеб. /Под ред. А.Г. Филиппова (отв. ред.),

А.Ф.Волынского. – М.: Спартак, 1998. – 543 с.

133. Криминалистика /Под ред. В.А. Образцова. – М.: Юрист, 1995. –592 с.

134. Криміналістика: Підруч. для студ. юрид. спец вищ. закл. освіти /За ред. В.Ю.Шепітька. – 2-е вид., перер. і допов. – К.: Концерн Видавничий Дім «Ін Юре», 2004. – 728 с.

135. Криміналістика. Криміналістична тактика і методика розслідування злочинів. Підруч. для студ. юрид. вузів і факульт. / За ред. В.Ю. Шепітька. – Харків: ООО «Одиссей», 2001. – 528 с.

136. Криминалистика: Учеб. Техника, тактика, организация и методика расследования преступлений /Под ред. Б.П.Смагоринского. – Волгоград: ВСШ МВД России, 1994. – Т. 2. – 560 с.

137. Лавров В.П. Некоторые научные аспекты изучения способов сокрытия преступлений //Способы сокрытия следов преступлений и криминалистические методы их установления. – М.: Академия МВД СССР, 1984. – С. 39.

138. Ларин А.М. От следственной версии к истине. – М.: Юрид. лит., 1976. – 199 с.

139. Левиашвили М.Ш. Объект уголовно-правовой охраны и его значение для классификации преступлений //Уголовно-правовые исследования: Сб., посвящ. 80-летию со дня рожд. Т.В.Церетели. – Тбилиси: Мецниереба, 1987. – С.94 – 103.

140. Лисиченко В.К. Криминалистическое исследование вещественных доказательств методами, основанными на применении радиоактивных изотопов: Автореф. дисс. канд. юрид. наук. – Киев, 1960. – 14 с.

141. Лисиченко Б.В. К вопросу о способе сокрытия преступления. //Вопросы криминалистики и судебной экспертизы. – Саратов, 1976. – 48 с.

142. Лисенко В. Слідчі ситуації та відповідні комплекси процесуальних й інших дій //Прокуратура. Людина. Держава. – 2004. – № 9. – С. 79 – 86.

143. Лузгин И.М., Лавров В.П. Способ сокрытия преступления и его

криминалистическое значение. – М.: МФЮЗО при Академии МВД СССР, 1980. – 30с.

144. Лузгин И.М. Расследование как процесс познания. – М., 1965. – 75 с.

145. Матишевський П.С. Кримінальне право України. Заг. част. Підруч. – К.: Юрінком Інтер, 2000. – 272 с.

146. Маклаков Г.Ю., Рижков Е.В. Особливості оперативно-рошукової діяльності при розслідуванні злочинів у сфері високих технологій //http: //www crime-research. org. – 12 с.

147. Матусовский Г.А. Методика расследования хищений: Учеб. пособ. – К., Изд-во: УМК ВО, 1988. – 88 с.

148. Маркусь В.О. Криміналістика. Навчальний посібник – К.: Кондор, 2007. – 558 с.

149. Марущак А.І. Правомірні засоби доступу громадян до інформації: науково-практичний посібник. – Біла Церква: Вид-во «Буква, 2006. – 432 с.

150. Мінченко А.В. Правова інформатика. Інформатика в історичному аспекті: Навч. посіб. – К.: Арістей, 2003. – 296 с.

151. Михеєнко М.М., Нор В.Т., Шибіко В.П. Кримінальний процес України. 2-ге вид., перероб. і допов. – К.: Либідь, 1999. – 534 с.

152. Михайленко О.Р. Складання процесуальних актів у кримінальних справах. – Юрінком. – К., 1996. – 256 с.

153. Мотлях О.І. Захист інформації у комп'ютерних системах: актуальність та новизна підходів //Вісник Академії праці і соціальних відносин Федерації профспілок України. – 2001. – № 1(10). – С. 57 – 62.

154. Мотлях О.І. Інформаційна безпека: пріоритетні напрями, шляхи розвитку та вдосконалення //Вісник Академії праці і соціальних відносин Федерації профспілок України. – 2000. – № 1 (5). – С. 40 – 45.

155. Мотлях О.І. Тактичні основи проведення обшуку у злочинах, пов'язаних з інформаційними технологіями //Вісник Академії праці і соціальних відносин ФП України. – 2002. – № 2. – С.157 – 160.

156. Мотлях О.І., Куркін В.О. Криміналістика: криміналістична техніка. Навч. посіб. – К.: АПСВ, 2006. – 128 с.
157. Мосесов А., Блинов Ф. Понедельник. День тяжелый //Неделя. – 1994. – № 41.
158. Моїсеєв О.М. Залучення спеціаліста до розслідування комп'ютерних злочинів /Правові основи захисту комп'ютерної інформації від протиправних посягань: Матеріали міжвузівської науково-практичної конференції (22 грудня 2000 р.). – Донецьк: Донецький інститут внутрішніх справ, 2001. – С. 81 – 85.
159. Мусаева У.А. Розыскная деятельность следователя в делах о преступлениях в сфере компьютерной информации. Автореф. канд. юрид. наук. – М., 2000, – 18 с.
160. Музика А.А., Азаров Д.С. Законодавство України про кримінальну відповідальність за «комп'ютерні» злочини: науково-практичний коментар і шляхи вдосконалення. / А.А. Музика, Д.С. Азаров. – К.: Вид. ПАЛИВОДА А.В., 2005. – 120 с.
161. Науково-практичний коментар Кримінального кодексу України від 5 квітня 2001р. / За ред. М.І.Мельника, М.І.Хавронюка. – К., 2001. – 1104 с.
162. Науково-практичний коментар до Кримінального кодексу України. /За заг. ред. М.О.Потебенька, В.Г.Гончаренка. – К.: Форум, 2001. У 2-х ч. Особл. част. – 942 с.
163. Науково-практичний коментар до Кримінального кодексу України: За станом законодавства і Постанов Пленуму Верховного суду України на 1 грудня 2001 р. /За ред. С.С. Яценка. – К., 2002. – 936 с.
164. Науково-практичний коментар Кримінального кодексу України. – 4-те вид., переробл. та доповн. / За ред. М.І.Мельника, М.І.Хавронюка. – К.: Юридична думка, 2007. – 1184 с.
165. Невмержицький Є.В. Корупція в Україні: причини, наслідки, механізм протидії: Монографія. – К.: КНТ, 2008. – 368 с.

166. Кримінальний кодекс України: Науково-практичний коментар /Ю.В. Баулін, В.І., Борисов, С.Б. Гаврик та ін.; За заг. Ред. В.В. Сташиса, В.Я. Тація. – Вид. третє, переробл. та доповн. – Х.: ТОВ «Одісей», 2007. – 1184 с.

167. Кримінально-процесуальний кодекс України. Науково-практичний коментар. За заг. Ред. В.Т. Маляренка, В.Г. Гончаенка – Вид. четверте, перероблене та доповнене – К.: «Юрисконсульт», КНТ. – 2007. – 896 с.

168. Наказ Міністерства внутрішніх справ України «Про створення у структурі ДСБЕЗ підрозділів по боротьбі з правопорушенням у сфері інтелектуальної власності та високих технологій», № 429 від 31.05.01 р.; Наказ Міністерства внутрішніх справ України «Про затвердження Типового положення про підрозділи ДСБЕЗ по боротьбі з правопорушеннями у сфері інтелектуальної власності та високих технологій», № 737 від 19.08.01 р.

169. Овчинский В.С. Интерпол в вопросах и ответах. – М.: ИНФРА – М., 2001. – С. 135 – 136.

170. О результатах работы органов предварительного следствия в 2000 году: Аналитическая справка СК при МВД России //Инф. бюллет. СК МВД России. 2001. – №2. – С.11 – 32.

171. Овечкин В.А. Общие положения методики расследования преступлений, скрытых инсценировками: Автореф. дис. …канд. юрид. наук: Харьк. юрид. ин-т. – Харьков, 1975.

172. Осипенко М. Компьютеры и преступность //Информационный бюллетень НЦБ Интерпола в Российской Федерации. – 2004. – № 10. – С. 16.

173. Панов Н.И. Способ совершения преступления и уголовная ответственность. – Харьков: Вища школа, 1982. – 161 с.

174. Панфилова Е.И., Попов А.С. Компьютерные преступления. – СПб.: Санкт-Петербургский институт Генеральной прокуратуры РФ, 1998. – 48 с.

175. Пантелеев И.Ф. Ошибочные рекомендации в теории уголовного процесса и криминалистики //Социальная законность. – 1997. – № 7. – С. 54.
176. Пещак Я.В. Следственные версии. – М.: Юрид лит., 1976. – С. 47 – 48.
177. Полевой Н.С., Крылов В.В. Компьютерные технологии в юридической деятельности. – М.: Изд-во «БЭК», 1994. – 304 с.
178. Потапов С.М. Введение в криминалистику. – М.: Госюриздат, 1946. – 146 с.
179. Поливанюк В. Використання спеціальних знань при розслідуванні кримінальних справ щодо злочинів, вчинених у сфері використання комп'ютерних технологій // http:// www /Crime-reserarch.org.
180. Порубов Н.И. Научные основы допроса на предварительном следствии. 3-е изд., перераб. – Мн.: Выш. школа, 1978. – 176 с.
181. Пособие для следователя: Расследование преступлений повышенной общественной опасности /Под. ред. Н.А. Селиванова, А.И. Дворкина. – М.: Лига разум, 1998. – С. 385 – 386.
182. Попова В.В., Родин А.Ф., Самоделкин С.М. Планирование расследования преступлений отдельных видов / Под ред. С.М.Самоделкина. – Волгоград, 1995. – 64 с.
183. Приполов І.І. Правовідносини у процесі розшукової діяльності органів внутрішніх справ //Вісник Академії праці і соціальних відносин ФП України. – 2004. – № 2 (26). – С.24 – 37.
184. Проблемы безопасности ЭВМ // Иностран. Печать о тех. оснащении полиции кап. государств. – 1990. – № 11. – С.90 – 101.
185. Проект Концепції стратегії реалізації державної політики щодо боротьби з кіберзлочинністю в Україні / http:// mndc. naian. kiev. ua
186. Радутний О.Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю. Автореф. дис… канд. юрид. наук: Нац. юрид. академія. – Харків, 2002. – 21 с.

187. Романюк Б.В., Камлик М.І., Гавловський В.Д. Виявлення та розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій: Посіб. /За заг. ред. проф. Я.Ю.Кондратьєва. – К.: Національна академія внутрішніх справ України, 2000. – 64 с.
188. Розенфельд Н.А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. Дисс. канд. юрид. наук. – К., 2003. – 200 с.
189. Розенфельд Н. Відповідальність за незаконне втручання в роботу ЕОМ (комп'ютерів) //Вісник прокуратури. – 2002. – № 4(16). – С.23 – 27.
190. Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. – М.: Право и закон, 2001. – 416 с.
191. Руководство для следователей / Под общ. ред. В.В.Мозякова. – М.: Изд-во «Экзамен», 2005. – 912 с.
192. Салтевский М.В. Криминалистика: В современном изложении юристов: Учеб. и практич. пособ. – Харьков: Рубикон, 1996. – 432 с.
193. Салтевський М.В. Криміналістика. Навч.-довід. посіб. – К., 1999. 159 с.
194. Салтевський М.В. Криміналістика. Методика і тактика. – Харків: Консум, 2001. – Ч. 2. – 527 с.
195. Салтевский М.В. Осмотр компьютерних средств на месте происшествия //Методические рекомендации. – Харьков: Академия правовых наук Украины, НИИ изучения проблем прест., 1999. – 7 с.
196. Самонов А.П. Психология преступных групп. – Пермь, 1991. – С. 117 – 123.
197. Селиванов Н.А. Советская криминалистика: система понятий. – М.: Юрид. лит., 1982. – 152 с.
198. Селиванов Н.А. Проблемы борьбы с компьютерной преступностью //Законность. – 1993. – № 8. – С. 36 – 40.
199. Селиванов Н.А. Типовые версии, следственные ситуации и их значение для расследованния //Соц. законность. – 1985. – №7. – С. 52 – 56.

200. Селиванов Н.А., Видонов Л.Г. Типовые версии по делам об убийствах: Справ. пособ. – Горький, 1981. – 56 с.

201. Сергеев Л.А. Сущность и значение криминалистической характеристики преступлений. Руководство для следователей. – М., 1971.

202. Сегай М.Я. Криминалистическая идентификация и особенности ее применения в отдельных видах советской криминалистической экспертизы: Дисс. канд. юрид. наук. – Киев, 1959. – 346 с.

203. Семилетов С.И. Электронный документ как продукт технологического процесса документирования информации и объект правового регулирования. /Информационное право: информационная культура и информационная безопасность. Матер. Всерос. науч.-практ. конфер. – Санкт-Петербург. гуман. ун-та профс. 17 – 19 октября 2002 г. – С.79 – 90.

204. Советский энциклопедический словарь. – М.: Советская энциклопедия, 1982. – 1600 с.

205. Снігірьов О.П., Сергач О.І. Деякі правові проблеми злочинності в сфері комп'ютерної інформації //Інформаційні технології та захист інформації. Зб. наук. праць. – Міністерство внутрішніх справ України. Запорізький юридичний інститут. – 1998. – Вип. 1. – С. 59 – 64.

206. Снетков В.А. Все резервы – в действие //Советская милиция. – 1988. – № 1. – С. 11.

207. Старченко Ю.О. Окремі аспекти протидії "хакерській" діяльності в Україні //Інформаційний бюлетень. – 2000. – № 2. – С. 40 – 41.

208. Старушкевич А. Організація огляду місця події. Аналіз криміналістично- значимої інформації при розслідуванні злочинів у сфері комп'ютерної інформації //Вісник прокуратури. – 2003. – № 12. – С. 77 – 86.

209. Стахівський С.М., Грошевий Ю.М. Докази і доказування у кримінальному процесі. Науково-практичний посібник. – К.: КНТ,

Видавець Фурса С.Я., 2006. – 272 с.

210. Таций В.Я. Объект и предмет преступления в советском уголовном праве. – Харьков: Вища школа, 1998. – 196 с.

211. Таций В.Я. Объект и предмет преступления в советском уголовном праве. – Харьков: Вища школа, 1998. – 196 с.

212. Тищенко Є.Ф., Селюк А.В. Розслідування комп'ютерних злочинів. Наук.-метод. посіб. – К.: Вид-во НА СБУ, 2003. – 124 с.

213. Тлиш А.Д. Проблемы методики расследования преступлений в сфере экономической деятельности, совершаемых с использованием компьютерных технологий и пластиковых карт. Автореф. дисс. канд. юрид. наук. – 12.00.09. – Краснодар, 2002. – 24 с.

214. Турчин Д.А. Теоретические основы учения о следах в криминалистике. – Владивосток: Изд-во Дальневосточного ун-та, 1983. – 185 с.

215. Уголовное право. Общая часть /Отв. ред. И.Я.Козаченко, З.А.Незнамова. – М.: Издательская группа ИНФРА-НОРМА, 1997. – 516 с.

216. Филиппов А.Г., Целищев А.Я. Понятие и криминалистическое значение следственной ситуации //Сов. государство и право. – 1982. – №8. – С. 71 – 75.

217. Фокина А.А. Роль криминалистической характеристики преступлений в укреплении связи науки криминалистики и практики расследования //Криминалистика и судебная экспертиза. – Киев, 1990. – Вып. 41.

218. Шаламов М.П. Теория улик. – М.: Госюриздат, 1960. – 182 с.

219. Шаламов М.П., Винберг А.И., Белкин Р.С. Криминалистика. – М.: Изд-во «Юридическая литература», 1966. – 606 с.

220. Шевченко В.Ф., Суслов С.О. Розкриття та розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку //Бюлетень МВС по обміну досвідом роботи. – 2003. – № 135. – С.60 –76.

221. Шилан Н.И., Кривонос Ю.М., Бирюков Г.М. Компьютерные

преступления и проблемы защиты информации: Учеб. пособ. – Луганск: РИО ЛИВД, 1999. – 64 с.

222. Шурухнов Н.Г., Пушкин А.В., Соцков Е.А., Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации: Науч.-практ. пособ. – М.: Щит. – М., 1999. – 254 с.

223. Шурухнов Н.Г., Левченко И.П., Лучин И.Н. Специфика проведения обыска при изьятии компьютерной информации //Актуальные проблемы и социальные усовершенствования деятельности органов внутренних дел в новых экономических условиях. – М., 1997. – 259 с.

224. Яблоков Н.П. Общие положения методики расследования и научно-технический прогресс //Методика расследования преступлений. – М., 1976. – С. 38.

225. Яблоков Н П. Криминалистика. – М.: Норма, 2000. – 384 с.

226. Янішевський Д.О. Встановлення відповідальності за “комп’ютерні злочини” //Боротьба з організованою злочинністю і корупцією (теорія і практика). Координаційний комітет по боротьбі з корупцією і організованою злочинністю при Президентові України. Міжвідомчий науково-дослідний центр. – 2002. – № 5. – С.117 – 123.

227. Якимов И.Н. Криминалистика: Уголовная тактика. – М., 1929. – 240с.

Наукове монографічне видання

Мотлях Олександр Іванович

Кандидат юридичних наук, професор, завідувач кафедри кримінального права і процесу Інституту повітряного, космічного і екологічного права та масових комунікацій Національного авіаційного університету

Методика розслідування комп'ютерних злочинів

Монографія