МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний економічний університет
Юридичний факультет
Кафедра кримінального права та процесу

КАРИЙ Володимир Вікторович

Правові та організаційні засади розслідування злочинів в сфері мобільних телекомунікацій України.

спеціальність: 081 – Право
магістерська програма – Право

Магістерська робота

Виконав студент групи ПРм-21
В.В. Карий
_____

Науковий керівник
к.ю.н., доцент Олійничук Р.П.
_____

Магістерську роботу допущено до захисту:
“___” _____20___ р.
Завідувач кафедри
_____Н.З. Рогатинська

ТЕРНОПЛЬ - 2018

ЗМІСТ

ВСТУП

Актуальність теми. Конституція України проголосила, що людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю, а права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави (ст. 3). Значної шкоди цій цінності завдає злочинність, яка втручається у всі сфери життєдіяльності людини.

В XXI столітті під час бурхливого розвитку науково-технічного прогресу, у зв'язку з кількісною і якісною зміною засобів і послуг мобільного зв'язку, надзвичайно актуальною стала проблема неправомірного доступу до систем мобільних телекомунікацій та користування їх ресурсами.

Несанкціонований доступ до систем зв'язку та інші незаконні дії відносно елементів зазначених систем завдають значних матеріальних збитків. Відповідно до оцінок фахівців, від 10 до 30 % трафіку операторів зв'язку відноситься на нелегальні дзвінки.

Можливість контролювати мережі зв'язку має особливе значення для терористичних угруповань, що обумовлює їх співпрацю з кримінальним співтовариством у галузі інформаційних технологій. За даними аналітиків, прибутки від вказаної злочинної діяльності дорівнюють прибутку з наркоторгівлі.

Кримінальний кодекс України не містить норм, що безпосередньо передбачають відповідальність за подібні порушення, а тому окремої статистики про злочини у сфері мобільного зв'язку не ведеться. Проте, узагальнені відомості Державної судової адміністрації України за фактами

порушених кримінальних проваджень у сфері інформаційних технологій і телекомунікацій свідчать про їх невпинне зростання. За даними МВС України кількість злочинів у сфері інформаційних технологій і телекомунікацій за останні десять років збільшилася практично у 10 разів.

У законодавстві та юридичній літературі не сформувалося єдиного підходу до методики виявлення, документування та розслідування даного виду злочинів. Значний внесок у вивчення зазначеної проблеми зробили провідні українські та зарубіжні вчені-юристи, а саме: О. Я. Баєв, Р. С. Белкін, В. Д. Гавловський,Ю. В. Гаврилін, В. О. Голубєв, Б. Д. Завідов, І. В. Лазарева, В. А. Мещеряков, О. М. Піменов, Н. А. Розенфельд, Г. В. Семенов, О. І. Усов, та інші.

Ці автори зробили вагомий внесок у загальну теорію і практику розслідування злочинів, створили наукове підґрунтя для подальших творчих пошуків. Їх роботи мають значну наукову і практичну цінність. Саме вони і склали теоретичну основу даногодослідження. Водночас, низка аспектів досліджуваної проблеми, залишається дискусійною і вирішується суперечливо.

Недосконаліть кримінального законодавства, висока латентність, відсутність виробленої судової і слідчої практики створюють суттєві труднощі у діяльності правоохоронних органів з розкриття і розслідування несанкціонованого доступу до мереж мобільного зв’язку. Підвищенню результативності такої роботи може сприяти: по-перше, отримання криміналістичних знань про злочини, пов’язані з несанкціонованим доступом до телекомунікаційних мереж, по-друге, розробка науково-обґрунтованих рекомендацій щодо виявлення, розкриття і розслідування таких злочинів, що визначає актуальність і зумовлює вибір теми даного дослідження та визначає його основні напрями.

Мета і завдання дослідження. Метою дослідження є комплексне вивчення кримінально-процесуальних і криміналістичних проблем розкриття

та розслідування злочинів, пов’язаних з незаконним втручанням у роботу мереж мобільного зв’язку.

Для досягнення зазначеної мети у процесі дослідження ставилися завдання:

- визначити проблеми, пов’язані з кримінально-правовою кваліфікацією злочинів у сфері мобільних телекомунікацій;

- встановити особливості мереж мобільного зв’язку як середовища вчинення злочинів, виявити закономірності і чинники, що визначають специфіку злочинного діяння;

- встановити характерні ознаки цих злочинівта здійснити їх криміналістичну класифікацію;

- сформувати криміналістичну характеристику злочинів, що пов’язані із втручанням у сферу мобільних телекомунікацій;

Об’єкт дослідження – кримінально-процесуальні та оперативно-розшукові відносини, що формуються у процесі діяльності з виявлення та розслідування злочинів у сфері мобільних телекомунікацій.

Предмет дослідження – правові та організаційні засади розслідування злочинів у сфері мобільних телекомунікацій України.

Методологічна основа дослідження представлена такими методами: формально-логічний, вжитий для проведення аналізу норм чинного законодавства України, що регулює суспільні відносини у сфері мобільних комунікацій; історико-правовий метод, що застосовувався при вивченні історичного аспекту формування норм, що передбачають відповідальність за злочини у сфері мобільних телекомунікацій; теоретико-прогностичний метод дозволив розробити пропозиції щодо вдосконалення чинного законодавства у сфері розслідування злочинів у сфері мобільних телекомунікацій України.

Нормативно-правову основуроботи становлять Конституція України, чинне кримінальне та кримінальне процесуальне законодавство України, законодавство зарубіжних країнінші міжнародні нормативно-правові акти, укази Президента України, постанови Верховної ради України, відомчі

нормативні акти Міністерства внутрішніх справ та Міністерства інфраструктури України.

Наукова новизна одержаних результатів полягає у тому, що сформульовано ряд положень та висновків, що мають теоретичне і безпосередньо практичне значення, а саме: узагальнено криміналістичну характеристику злочинів у сфері мобільних телекомунікацій; систематизовано знання про способи вчинення злочинів, виявлено закономірності, що їх обумовили та передумови існування у мережах мобільного зв'язку.

Практичне значення одержаних результатів полягає у тому, що вони можуть бути основою подальших наукових досліджень та сприяти вдосконаленню законодавства України у частині запобігання та протидії, а також розслідування злочинів у сфері мобільних телекомунікацій.

Структура й обсяг дипломної роботи. Робота викладена на 92 сторінках комп'ютерного тексту і складається із вступу, трьох розділів, що поєднують вісім підрозділів, висновків, списку використаних джерел, який включає 96 найменувань.

РОЗДІЛ 1.
ЕВОЛЮЦІЯ МОБІЛЬНИХ ТЕЛЕКОМУНІКАЦІЙ У КРИМІНАЛЬНО-ПРАВОВОМУ КОНТЕКСТІ

1.1. Телекомунікаційні системи: поняття та етапи розвитку

Телекомунікації як передача інформації голосом на відстані були відомі за часів правління перського царя Кіра (VI століття до н.е.). Для цього на службі перебувало понад 30000 осіб, які називались «царські вуха». Знаходячись на вершинах пагорбів та вартових вежах у межах чутності один одного, вони передавали меседжі, призначені царю, та його накази. Грецький історик Діодор Сицилійський (I ст. до н.е.) свідчить, що за день новини таким телефоном передавались на відстань тридцятиденного переходу. Юлій Цезар відзначав, що й галли мали подібну систему зв'язку та навіть швидкість передачі меседжу – 100 кілометрів на годину [41].

Термін «телекомунікації» походить від двох слів: грецького tele, що означає діючий або здійснюваний на далекій відстані, та латинського communico, що означає форма зв'язку чи спілкування. Отже, можна казати, що: телекомунікації — це засоби віддаленого інформаційного зв'язку[4].

Створення першої телекомунікаційної системи можна віднести до 1832 року, коли російський винахідник П. Л. Шиллінг створив перший електромагнітний телеграф (відстань між двома апаратами в першій продемонстрованій установці становила 100 м). Для створення телеграфного коду, що давав змогу здійснювати одноразову передачу кожної букви за найменшої кількості робочих знаків, П. Л. Шиллінг використав принцип китайських гексаграм (Книга Перемін), які складаються з шести ліній двох

типів — неперервних і переривчастих.

У 1837 році американець Семюел Морзе розробив перший практично придатний електромагнітний телеграф (сигнал був надісланий за допомогою дроту завдовжки 1700 футів). Через рік Морзе створив також свою знамениту азбуку (сучасний варіант азбуки Морзе – International Morse, яким нині користуються моряки, був затверджений 1939 року і дещо відрізняється від оригіналу).У 1876 році Олександр Грехем Белл (1847–1922), професор фізіології органів мови Бостонського університету, запатентував у США свій винахід — телефон [35, с. 42].

Ще однією віхою в історії телекомунікацій називають 7 травня 1895 року. Російський фізик і електротехнік О.С. Попов на засіданні російського фізико-хімічного товариства в Петербурзі продемонстрував дію створеного ним радіоприймача, використовуючи як джерело електромагнітного випромінювання вібратор Герца. З 1897 року вчений почав працювати над створенням бездротового телеграфування і передав на відстань близько 200 метрів свою першу радіограму, що складалася з одного слова «Герц». У літку 1897 року дальність радіозв'язку сягала 5 км. І лише у 1901 році відстань радіопередачі вдалося продовжити до 150 км.

У той час, коли в Росії О.С. Попов закінчив створення бездротового телеграфування, у Італії, подібними питаннями займався Гульельмо Марконі (1874-1937), який запатентував свій винахід 2 травня 1889 року у Великобританії [41].

Винайдення й удосконалення системи радіозв'язку сприяли створенню у подальшому радіотелеграфу, радіомовлення і навіть радіотелефону. У лабораторіях Белла (м. Сент-Луїс) у 1946 році були розроблені основні принципи мобільної (сотової) телефонії. З появою перших комп'ютерів, мереж зв'язку розвиток телекомунікацій відбувався двома шляхами: вдосконалення засобів зв'язку та обчислювальної техніки. У останні два десятиріччя XX століття намітилось об'єднання цих шляхів. Будь-яка

сучасна телекомунікаційна система поєднує у собі як засоби зв'язку, так і обчислювальну техніку [41].

Можна виділити такі п'ять етапів розвитку телекомунікацій (а відповідно і п'ять типів телекомунікаційних систем), а саме:

– 1832 р. — створення і розвиток телефону і телеграфу (кабельні телекомунікаційні системи);

– 1895 р. — поява радіо і телебачення (радіохвильові телекомунікаційні системи);

– 1957 р. — використання супутників для передачі інформації (супутникові телекомунікаційні системи);

– 1968 р. — поява комп'ютерних мереж (комп'ютерні телекомунікаційні системи);

– 80-ті роки XX століття — злиття засобів зв'язку і обчислювальної техніки — інтегровані телекомунікаційні системи.

Нарешті, у 1969 році телекомунікаційні компанії розпочали займатися створенням єдиної мережі мобільного зв'язку. Передбачалося, що її абоненти зможуть використовувати один телефон і номер, навіть перетинаючи кордони держав. Першим таке рішення запропонував випускник Стокгольмської технічної школи Естен Мякітоло, якого вважають батьком сучасної мобільної телефонії [47, с. 7].

З початку 1970-х років у результаті технологічного стрибка у різних сферах життєдіяльності водночас у ряді країн починають розвиватися системи бездротових засобів електрозв'язку: системи персонального радіовиклику – пейджингові системи, відомчі і транкингові системи рухомого радіозв'язку; бездротова телефонія і т. ін. Перший же комерційний стільниковий телефон з'явився на ринку лише у 1983 році. Він важив 500 грамів і продавався за три з половиною тисячі доларів.

Не дивлячись на значні потреби у послугах радіозв'язку і на явні його переваги перед традиційними дротяними засобами зв'язку, впровадження бездротових комунікацій зіштовхнулось з обмеженістю частотного ресурсу.

Проблема була вирішена у результаті появи концепції розподілу обслуговуваної території на невеликі ділянки, які стали називатися стільниками. Кожен стільник має обслуговуватися передавачем з обмеженим радіусом дії і фіксованою частотою, що дало змогу без взаємних перешкод використовувати ту ж саму частоту повторно у іншому стільнику. Реалізація даного принципу організації зв'язку на апаратному рівні обумовлена появою перших широкодоступних систем мобільного (стільникового) зв'язку на початку 1980-х років.

Практичне застосування мобільного зв'язку почалося у 1978 році, коли в Чикаго розпочали випробовування першої дослідної системи мобільного зв'язку на 2 тис. абонентів. У той самий час в Європі наприкінці 70-х років почалися роботи зі створення єдиного стандарту для п'яти північноєвропейських країн: Швеції, Фінляндії, Норвегії, Данії й Ісландії [48, с. 58].

Проте, мобільний зв'язок одержав широкий розвиток лише після того, як відбулося об'єднання систем мобільного зв'язку з технологіями, які забезпечують персоніфікацію доступу й індивідуалізацію інформації, що надається. Всі ці стандарти є аналоговими і відносяться до першого покоління систем мобільного зв'язку. Новий етап в розвитку мобільного зв'язку – це створення систем на основі цифрових методів обробки сигналу.

У 1982 році Європейська Конференція Адміністрацій Пошти і Електрозв'язку (CEPT) створила групу для розробки єдиного європейського стандарту цифрового мобільного зв'язку. Результатом роботи цієї групи став стандарт GSM.У 1991 році в Європі з'явився стандарт DCS-1800 (Digital Cellular System 1800 Мгц), створений на базі стандарту GSM [52, с. 7].

На початку 70-х років були створені і почали поширюватися у провідних країнах світу аналогові стільникові мережі. В процесі їх використання ставали очевидними певні недоліки, зокрема: незначна кількість послуг, невисока якість звуку у зоні з поганим прийомом, низька місткість мережі. Це зумовило пошук нових рішень і призвело до

формування системи мобільного зв'язку другого покоління (2G)– цифрові стільникові системи.

Водночас з розвитком мобільних мереж розвивалися також супутникові системи зв'язку, і на початку 90-х років виникла ідея створення засобів мобільного зв'язку третього покоління (3G), що об'єднували б технології безпровідного доступу, наземного мобільного і супутникового зв'язку. Міжнародним союзом електрозв'язку (ITU) було розроблено програму IMT-2000 з метою стандартизації і сприяння впровадженню національних, регіональних і міжнародних систем мобільного зв'язку третього покоління (3G). У межах Європейського Союзу система 3G одержала назву «Universal Mobile Telecommunication System» (UMTS).

Таким чином, концепція IMT-2000 передбачає різноманітні можливості створення 3G-мереж, багато з яких є несумісними і не відповідають вимогам сьогодення. Тому ряд компаній, серед яких Alcatel, Ericsson, Motorola, Nokia, NTT DoCoMo, Siemens, приступили до розробки концепції побудови систем четвертого покоління (4G), а також виступили ініціаторами організації Всесвітнього форуму з розвитку безпровідних технологій — WWRF (Wireless World Research Forum).

Мобільний зв'язок четвертого покоління передбачає швидкості передачі даних до 100 Мбіт/с (для термінального обладнання з підтримкою телеконференцій) і до 10—20 Мбіт/с для звичайних мобільних терміналів. Як радіотехнологія швидше за все використовуватиметься IMT-MC [62].

Перша стільникова система в Україні стандарту NMT-450 була впроваджена в комерційну експлуатацію в 1992 році оператором «Український мобільний зв'язок» (UMC). У квітні 1996 року була введена в дію перша цифрова стільникова система України, що відповідала стандарту D-AMPS, оператором «Цифрові стільникові мережі України» (DCC).У грудні 1996 року була введена також у комерційну експлуатацію мережа устандарті GSM-1800 оператора Golden Telecom(GT).

На даний день основними конкурентами на ринку мобільного зв’язку України є оператори «Київстар», «Vodafone»та «Lifecell»[8].

Варто наголосити, що коли були введені у дію перші аналогові мобільні мережі, забезпечення безпеки в них було на дуже низькому рівні. В історії мобільного зв’язку був випадок, коли в період стрімкого зростання кількості абонентів мобільних операторів в Нью-Йорку близько 30% розмовного часу виявилося не сплаченим. Фінансові втрати телефонних компаній тоді досягли критичної точки.

Для того, щоб краще зрозуміти проблеми, пов’язані з використанням бездротових засобів зв’язку, варто зрозуміти, що вони собою являють, яким чином працюють. Сучасні бездротові засоби персонального зв’язку включають мобільні телефони мобільного зв’язку, бездротові стаціонарні радіотелефони, смартфони та планшетні компютери. Вони є складною мініатюрною прийомо-передавальною радіостанцією. Кожному стільниковому телефонному апарату надається свій електронний серійний номер (ESN), який кодується у мікрочіпі телефону при його виготовленні і повідомляється виробниками апаратури фахівцям, які здійснюють його обслуговування.

Мобільний стільниковий телефон має необмежену дальність дії, яку забезпечує стільникова структура зон зв’язку. Вся територія, що обслуговується стільниковою системою зв’язку, розподілена на окремі прилеглі одна до одної зони зв’язку або «стільники». Телефонний обмін в кожній з таких зон керується базовою станцією, здатною приймати і передавати сигнали на великій кількості радіочастот. Крім того, ця станція підключена до звичайної дротової телефонної мережі і оснащена апаратурою перетворення високочастотного сигналу мобільного телефону в низькочастотний сигнал дротового телефону і навпаки, чим забезпечується сполучення обох систем [94].

Періодично (з інтервалом 30-60 хвилин) базова станція випромінює службовий сигнал. Прийнявши його, мобільний телефон автоматично додає

до нього свої MIN- і ESN-номери і передає кодову комбінацію, що вийшла, на базову станцію. У результаті цього здійснюється ідентифікація конкретного мобільного телефону, номеру рахунку його власника і прив'язка апарата до певної зони, в якій він знаходиться у цей момент часу. Коли користувач дзвонить зі свого телефону, базова станція виділяє йому одну з вільних частот тієї зони, в якій він знаходиться, вносить відповідні зміни в його рахунок і передає його виклик за призначенням. Якщо мобільний користувач під час розмови переміщається з однієї зони зв'язку в іншу, базова станція зони автоматично переводить сигнал на вільну частоту нової зони.

Стаціонарний бездротовий радіотелефон об'єднує в собі звичайний дротовий телефон, представлений самим апаратом, підключеним до телефонної мережі і приймально-передавальний радіопристрій у вигляді телефонної трубки, що забезпечує двосторонній обмін сигналами з базовим апаратом. Залежно від типу радіотелефону, відстань зв'язку між трубкою і апаратом (з урахуванням наявності перешкод і відображаючих поверхонь) складає в середньому до 50 метрів.

На сьогоднішній день мобільний зв'язок на Україні є найбільш динамічний і швидкодіючий сектор ринку телекомунікацій. Проте, так вже влаштований світ, будь-який технічний винахід, що розширює наші можливості і створює додатковий комфорт, неминуче містить в собі і негативні сторони, які можуть являти потенційну небезпеку для користувача. Не є винятком у цьому плані і сучасні засоби мобільного зв'язку.

У сучасних умовах соціально-економічного і науково-технічного розвитку України не викликає сумніву факт використання послуг мобільного зв'язку як основного товару, що має значну цінність. Тенденції у цій галузі суспільних відносин нагально демонструють можливості засобів мобільного зв'язку, які постійно збільшуються, їх загальна доступність, постійно зростаючі надприбутки компаній, що надають різного роду послуги мобільного зв'язку, привертають підвищену увагу кримінальних структур і

елементів.

1.2. Предмет злочинного посягання у сфері мобільних телекомунікацій України

Розвиток електронних технологій і телекомунікаційних мереж у сучасному інформаційному суспільстві створив передумови для появи принципово нового виду злочинів – отримання незаконного прибутку за допомогою використання ресурсів телекомунікаційних мереж, простіше кажучи, шахрайство чи «телекомунікаційне шахрайство», під яким Г. В. Семенов розуміє неправомірну діяльність, пов'язану з несанкціонованим користуванням послугами зв'язку [12, с. 100].

За прогнозами вітчизняних і зарубіжних фахівців в XXI ст. кількість злочинів у галузі інформаційно-телекомунікаційних технологій буде неухильно збільшуватися, оскільки, по-перше – ці діяння приносять колосальні прибутки; по-друге – організовані злочинні групи стали надавати доволі важливе значення отриманню конфіденційної інформації про діяльність державних і приватних комерційних структур для реалізації своїх злочинних намірів і забезпечення власної безпеки [13, с. 7].

Такі протиправні дії, як використання інформаційних ресурсів з корисливою метою спричиняють значні збитки державі та операторам зв'язку. Тому не випадково питанню захисту галузі зв'язку Президентом України, Урядом України приділяється особливе значення. Адже злочинність у галузі зв'язку має каскадний ефект, тягне за собою недоотримання прибутків, перевантаження мереж, незадоволення абонентів, порушення безпеки та ін.Так, за даними «Міжнародної Спілки Телекомунікацій» (ITU), збитки від мобільних злочинів у світовій стільниковій індустрії становлять щорічно порядком $25 млрд., або від 3 до 7% від загальної суми прибутків.

Підраховано, що фінансові збитки від цих злочинів, збільшуються на 12% щорічно. Багато компаній, як правило, не афішують свої втрати. Тому боротьба з шахрайством, крадіжками трафіку та контроль пропуску трафіку за прихованими схемами потребує додаткових матеріальних витрат та адміністративних заходів [14, с. 4]. З вищенаведеного можна зробити висновок про високий ступінь латентності таких діянь, недосконаліть законодавства, насамперед кримінального, відсутність належних механізмів, сил та засобів, які можна було б використовувати для запобігання «телекомунікаційним злочинам», а також для їх виявлення, розслідування і розкриття [15].

Юридичні дефініції поняття «телекомунікаційне шахрайство», «телекомунікаційний злочин» на сьогоднішній день українське законодавство ще не розробило, а деякі його норми, що передбачають відповідальність за діяння, пов'язані з використанням телекомунікаційного обладнання, далекі від досконалості і не повністю охоплюють ті дії, які можна вважати кримінально небезпечними для суспільних відносин.

Одним з різновидів «телекомунікаційного шахрайства» є несанкціонована маршрутизація вхідного міжнародного трафіку в телефонну мережу загального користування. Перша така кримінальна справа в Україні була порушена прокуратурою м. Києва відносно посадових осіб ТОВ «Голден Телеком» за ч. 2 ст. 364 КК України. Справа отримала широкий суспільний резонанс. Вперше на Україні був початий процес з крадіжки телефонного трафіку [7].

Прокурорська перевірка відносно ТОВ «Голден Телеком» була розпочата у вересні 2001 року, за наслідками якої була порушена кримінальна справа. Представники ТОВ «Голден Телеком», що є оператором місцевого, міжміського і міжнародного зв'язку, направляли у телефонну міську мережу міжнародні телефонні дзвінки з підміною вхідних номерів. Отже, оператор зв'язку одержував міжнародні дзвінки, після чого замінював номер на номер міського телефонного зв'язку. На підставі порушення пункту

6.10 положення «Про діяльність операторів міжнародного і міського зв'язку в телефонній мережі загального користування України» ТОВ «Голден Телеком» не виплачувало державному оператору зв'язку – компанії «Укртелеком» – значні суми грошей. Збитки склали сотні мільйонів гривень [19].

Залежно від рівня підготовки і можливостей, злочинців у сфері мобільних комунікацій поділяють на групи за «спеціальностями»:

а) фродистери - злісні неплатники, яких поділяють на дві групи: кримінальні елементи й несумлінні клієнти (перші, маючи контракт із компанією, використовують підроблені документи, а другі користуються справжніми, але платити не бажають і потрапляють в категорію безнадійних боржників); чіткої межі між ними немає. Щорічно близько 1,5 млн. власників мобільних телефонів усіма правдами й неправдами намагаються ухилитися від сплати рахунків за користування. Середній розмір збитку від шахрайства цього типу (за даними закордонних операторів) оцінюється приблизно в $600 млн.

б) фрікери - телефонні пірати, зусилля яких спочатку зосереджувалися на створенні обладнання, що обманюють АТС з метою одержання безкоштовних дзвінків (проте технології розвиваються, і у полі зору фрікерів виявився мобільний зв'язок, де можна займатися тим же, з меншим ризиком); будучи професійно підготовленими фахівцями, фрікери являють серйозну загрозу для майбутніх мереж мобільного зв'язку. Адже вже сам факт організації безкоштовного роумінгу, а також переконфігурування послуг і форм оплати й тим більше перепрограмування мережного обладнання є небезпечним для абонентів та операторів зв'язку;

в) хакери, які з мережі Інтернет успішно перейшли до мобільної; їхня головна мета - атаки на мережні інфраструктури для проникнення в бази даних операторських компаній. Якщо раніше для хакерів це було переважно розвагою, то останнім часом, одержуючи більші рахунки за послуги мобільного зв'язку, вони шукають обхідні шляхи, продаючи свої послуги.

г) вірусописателі, або вірусологи (virus-maker) є ще небезпечнішими ніж «інтернетівські». Віруси, створені ними, здатні потенційно зруйнувати бази даних операторів, знищити гроші у мобільних банкоматах і завдати мережі іншої шкоди;

д) кракери. Це різновид хакерів, що спеціалізується у сфері програмного забезпечення та займається зломом захисту програмного забезпечення телекомунікацій, крім того, вони розробляють програми, проникають у мережу та створюють шляхи доступу до конфіденційної інформації, що має велику ліквідність в грошовому виразі;

є) кардери – це ті, хто підробляє пластикові карти і саме сьогодні ці злочини вважаються одними із найсерйозніших у сфері високих технологій. Їх діяльність межує з хакерською, особливо якщо потрібно зламати карткову базу даних оператора зв'язку. Найбільш уразливе місце в схемі - prepaid-карти, а точніше, схований у ній цифровий код. Способів його зчитування багато, зокрема, це професійне видалення захисного шару на карті з наступним його відновленням або заміною на новий код, зчитування з іншої карти (так званий метод shave & paste - «збрити й наклеїти»).

ж) інсайдери - це співробітники операторських компаній, котрі передають злочинцям інформацію про шляхи проникнення у телекомунікаційну мережу оператора. Іноді вони й самі займаються цим. Витік інформації, або так зване внутрішнє шахрайство, завжди було великою загрозою для безпеки телекомунікаційних мереж. Частка втрат операторів від внутрішнього шахрайства перевищує 20% загального прибутку. Інсайдеру, як нікому іншому, відомі всі «тонкощі» роботи мережі й процедури додавання нових абонентів.

з) просто злодії**,** оскільки кримінальний доступ до стільникового зв'язку за допомогою викрадених або загублених мобільних телефонів одержує все більше поширення. У вчиненні різного роду злочинів викрадені телефони, виявляється, відіграють не останню роль. Злочинці використовують їх так само, як викрадені автомобілі. Проте викрадений

мобільний телефон діє лише невеликий відрізок часу (поки володар не повідомить про викрадення), протягом якого злодії встигають анонімно вчинити злочин або зробити безліч дорогих дзвінків. Рекорд був зафіксований, коли за один день злочинцями за допомогою викраденого телефону був нанесений збиток на суму близько 15 тис. фунтів стерлінгів [20, с. 54].

«Фрікинг» зародився в США в 1960-і роки. Молоді американці випадково з'ясували, що з будь-якого таксофона можна дзвонити абсолютно безкоштовно: досить лише свиснути в трубку свистком «Капітан Джонс» – популярною в ті роки дитячою іграшкою. Частота свистка – 2600 Гц – співпадала з частотою сигналу, яким таксофон оповіщав телефонну станцію про сплату за розмови. З цього часу число 2600 стало загальноприйнятим символом міжнародного фрікерського руху [21, с. 24].

Наприклад, термін «роумінг» визначений в Законі України «Про внесення змін в Закон України «Про збір на обов'язкове державне пенсійне страхування», відповідно до нього роумінг – це послуга мобільного рухомого зв'язку, який забезпечує можливість абонентів здійснювати двосторонній зв'язок без надання будь - якої попередньої заяви або з наданням під час переміщення абонента здійснюється передача його обслуговування іншій базовій станції як у межах України, так і поза її межами [3]. Проте, ситуацію, коли телекомунікаційні терміни визначаються лише з метою оподаткування, навряд чи можна вважати нормальною.

На жаль, на вищезгаданих фактах перелік проблем нормативно-правового регулювання діяльності з надання послуг мобільного зв'язку не закінчується. Пригадаємо дискусії, які розгортались навколо тарифікації повної і неповної хвилини розмови, за що Антимонопольний комітет України і наклав стягнення на найбільшого оператора мобільного зв'язку «Київстар». Проблемне питання відносно зняття обов'язкової сплати за з'єднання у монополістів стільникового (мобільного) зв'язку ВАТ «Укртелеком», ЗАТ «Київстар», ТОВ «Голден Телеком», ЗАТ «Українські радіосистеми», ТОВ

«Астеліт», ЗАТ «Український мобільний зв'язок», ТОВ «Інтернаціональні телекомунікації» і ЗАТ «Телесистеми України»також мало місце [8].

З 2004 року ринок електрозв'язку України діє за новими правилами, встановленими Законом України «Про телекомунікації», прийнятим Верховною Радою України 18 листопада 2003 року. Закон встановлює правову основу діяльності у галузі телекомунікацій і визначає повноваження держави щодо управління та регулювання зазначеної діяльності, а також права, обов'язки та засади відповідальності фізичних і юридичних осіб, які беруть участь у цій діяльності або користуються телекомунікаційними послугами.

Порядок користування послугами телефонного зв'язку на сьогоднішній день регулюється «Правилами надання та отримання телекомунікаційних послуг», які затверджено постановою Кабінету Міністрів України від 11 квітня 2012 року № 295 [5]. Правила містять перелік послуг, який може бути розширений оператором зв'язку залежно від його технічних можливостей, встановлюють права і обов'язки операторів та абонентів, а також положення про порядок оплати за послуги і про відповідальність сторін.

Незначний поки ще досвід боротьби із таким видом злочинів дозволяє виокремити їх особливості, зокрема, до особливостей протиправних діянь на вітчизняних телекомунікаційних мережах:

– 70% збитків від правопорушень насамперед пов'язано зі зловживаннями працівників, підрядчиків та дилерів телекомунікаційних компаній;

– дії правопорушників сприймаються як законні, санкціоновані;

– порушники використовують сучасні технології, апаратне та програмне забезпечення;

– дії правопорушників, як правило, динамічні у часі і розподілені у просторі.

Останнім часом проблема інформаційної безпеки детально досліджується відповідними установами та організаціями багатьох країн

світу. Згідно з Концепцією національної безпеки України, інформаційна безпека визначена однією з невід'ємних складових національної безпеки держави [46].

На нашу думку, окремого розгляду також заслуговує питання про віднесення «перепрошивання» мобільних телефонів до злочинів, які вчинюються у мережах мобільних телекомунікацій. До недавнього часу перепрограмуванням телефонів звичайні споживачі практично не займалися – не було відповідного досвіду, програмного забезпечення, широкого кола споживачів, що вивчають «нутрощі» апаратів. Зміна заводського програмного забезпечення була справою інженерів у сервісних центрах, представників компаній або підпільних майстрів, які адаптували неофіційно ввезені апарати під вітчизняні реалії, зокрема, додавали в них російський (український) мовний пакет.

Де-юре, подібна діяльність, пов'язана зі зміною програмного забезпечення виробника в телефонах без відповідного дозволу, є незаконною і більш того може переслідуватися згідно українського законодавства. Де-факто, дане питання не хвилювало не тільки українські органи влади, а й самих виробників, завдання, що стояли перед представництвами, описувалися, в першу чергу, як продаж телефонів, в другу – їх супровід. Із зростанням ринку мобільних телефонів воно стало привертати увагу органів влади, починаючи з митниці і закінчуючи МВС. Не секрет, що підпільний ринок викрадених мобільних телефонів в Україні достатньо значний, а правоохоронні органи не мають можливості боротися з лавиною подібних крадіжок [45, с. 245].

Таким чином, предметом розглядуваних нами злочинів є елементи мережі мобільного зв'язку, послуги мобільного зв'язку, а також інформація, що циркулює у мережі мобільного зв'язку, яка є власністю оператора та абонента (фізичної або юридичної особи) і знаходиться під охороною закону.

1.3. Види злочинів, пов’язаних з втручанням у сферу мобільного зв’язку, та кримінально-правова відповідальність

Для класифікації важливими є найбільш суттєві ознаки, на основі яких в один клас входили б максимально схожі злочини [50]. Ці положення повною мірою відносяться до криміналістичної класифікації злочинів, які досліджуються у роботі.

Класифікація злочинів, що вчиняються у сфері мобільних телекомунікацій, виводить на передній план суто криміналістичні підстави і в першу чергу спосіб вчинення злочину. Інші його елементи (система мобільного зв’язку, кримінальні цілі і тому інше.), як правило, відображаються у способі вчинення або в особливостях його застосування.

Як підкреслює Р.С. Бєлкін, на практиці конкретний злочин визначається за декількома класифікаціями, і це відображається у змісті конкретних методик. Деякі класифікації можуть не мати значення для даної методики, проте у всіх випадках – без жодних винятків, зберігає своє значення класифікація за способом вчинення злочину. Беручи до уваги визначення криміналістичного поняття спосіб вчинення злочину, а також особливості середовища вчинення злочинів – сфера мобільних телекомунікацій, при розробці криміналістичної класифікації даних злочинів, за основу має бути узятий аналіз системи мобільного зв’язку як складного багаторівневого об’єкту і виявлення набору типових елементарних операцій на кожному з його рівнів.

Змістовна сторона кримінальних дій у сфері мобільних телекомунікацій має диференціюватися залежно від характеру локальних типових завдань (цілей), які злочинцю варто досягти на певному етапі реалізації даного різновиду злочинів [30, с. 130].

Змістовна сторона кримінальних дій у мережах мобільного зв'язку має диференціюватися залежно від характеру локальних типових завдань (цілей), які злочинцю варто досягти на певному етапі реалізації даного різновиду злочинів для досягнення кінцевої мети.

Беручи до уваги вищезазначене, типовими для здійснення даної злочинної діяльності будуть такі дії:

1) дії для отримання різного ступеня доступу до системи мобільного зв'язку (її функціональних і процедурних елементів). Для цього варто мати абонентську рухому станцію, апаратне і програмне забезпечення, а також ідентифікаційні дані, які дозволяють працювати у цій системі, тобто бути підключеним до системи;

2) користування послугами мобільного зв'язку (абонентська активність) і надання такої можливості іншим особам.

Так, різні дії злочинця, щодо отримання доступу до системи мобільного зв'язку, залежать від даної системи, мов би здійснюються у відношенні до неї і в середині неї. Тим самим, загальні принципи технічної побудови системи мобільного зв'язку у цілому індукують свої властивості і визначають типові завдання високого рівня, зокрема, обов'язковість доступу до системи і користування її ресурсами. Надалі типові завдання нижчого рівня визначаються вже різними елементами системи мобільного зв'язку [68].

Узагальнюючи характеристику мережі мобільного зв'язку, ми дійшли висновку, що її основними елементами, в найзагальнішому розумінні, є:
1) апаратно-технічні засоби підтримки системи мобільного зв'язку (система базових станцій, центри комутації, ефірний інтерфейс, мобільні телефони);
2) інформаційні засоби підтримки системи мобільного зв'язку (програмне забезпечення, дані і бази даних, що дозволяють системі здійснювати свої функціональні можливості);
3) допоміжні засоби підтримки системи мобільного зв'язку (центри технічного обслуговування, роботи з клієнтами та ін.).

Оскільки дії з доступу є обов'язковими для злочинів у сфері мобільних телекомунікацій, ми вважаємо, що більш вдалою була б класифікація, в основу якої будуть покладені елементи системи мобільного зв'язку, доступ до яких здійснюється.

На підставі аналізу літератури можна виділити таку класифікацію дій при вчиненні злочинів у сфері мобільних телекомунікацій:

1) дії, пов'язані з доступом до системи мобільного зв'язку:

а) доступ до апаратно-технічних засобів підтримки системи мобільного зв'язку: незаконне заволодіння мобільним телефоном (ст. 185, 186, 187 КК України і інші способи заволодіння чужим майном, передбачені Особливою частиною КК України); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361^1 КК України);

б) доступ за допомогою підключення мобільного телефону через допоміжні засоби підтримки системи мобільного зв'язку (центри роботи з клієнтами, дилерами тощо): умисне надання невірних даних шляхом пред'явлення підроблених документів, що засвідчують особу, при укладенні договору на надання послуг мобільного зв'язку (ст. 358 КК України); створення фіктивної організації з метою неправомірного користування ресурсами (послугами) мобільного зв'язку і отримання майнової вигоди (ст. 205 КК України); здійснення без державної реєстрації, як суб'єкта підприємницької діяльності, що містить ознаки підприємницької та яка підлягає ліцензуванню, або здійснення без одержання ліцензії видів господарської діяльності, що підлягає ліцензуванню відповідно до законодавства, чи здійснення таких видів господарської діяльності з порушенням умов ліцензування, якщо це було пов'язано з отриманням доходу у великих розмірах (ст. 202 КК України виключено в 2011 році, проте практика притягнення до відповідальності існувала);

в) доступ до інформаційних засобів підтримки системи мобільного зв'язку – програмного забезпечення, даних і баз даних, що дозволяють

системі мобільного зв'язку здійснювати свої функціональні можливості: несанкціоноване отримання ідентифікаційних даних користувачів за допомогою засобів комп'ютерної техніки, перепрограмування ідентифікаційних даних легальних користувачів, проникнення в комп'ютерну систему захисту для видалення механізмів захисту або переконфігурації системи базових станцій з метою використання (або подальшої реалізації) наявних в системі функціональних можливостей, або з метою користування ресурсами мобільного зв'язку (ст. 362 КК України).

2) дії, пов'язані з користуванням ресурсами мобільного зв'язку (кримінальна абонентська активність):

а) користування ресурсами мобільного зв'язку без її належної оплати і (або) реєстрації (ст. 190, ст. 192 КК України) полягає у тому, що її ефективність залежить не тільки від правильності підбору тих або інших чинників, що пояснюють системний характер цієї методики, але і від визначеності і однозначності предмету застосування.

У криміналістичній науці вже окреслились підходи до визначення сутності злочинів у сфері мобільних телекомунікацій, проте відповідної дефініції до сьогоднішнього часу ще не вироблено. Більш того, перелічені більшістю авторів специфічні характеристики злочинів у сфері мобільних телекомунікацій не дозволяють чітко визначити межі даного явища [59, с. 52].

Під злочинами у сфері мобільних телекомунікації розуміється система (комплекс) кримінально караних послідовних дій спрямованих на несанкціонований доступ до системи мобільного зв'язку, користування її ресурсами і (чи) надання такої можливості іншим особам.

Отже, з урахуванням вищевикладеного, предмет криміналістичної методики розслідування досліджуваного виду злочинів, можна визначити як закономірності вчинення злочинів у сфері мобільних телекомунікацій і засновані на пізнанні цих закономірностей прийоми і рекомендації, щодо ефективного розкриття і розслідування.

Серйозним кроком у формуванні нормативної бази, що регулює відносини, пов’язані з розвитком і функціонуванням мобільного зв’язку в Україні, стало відповідне правове закріплення відповідальності за вчинення суспільно небезпечних дій кримінального характеру. Адже у результаті швидкого розвитку галузі мобільного зв’язку в нашій країні та високих тарифах на сплату послуг цієї галузі, користування засобами мобільного зв’язку стало привабливим об’єктом для злочинної діяльності, зокрема, прослуховування переговорів, визначення місцеположення абонента і його пересувань (характерні для вбивств, вчинених на замовлення), блокування з’єднань, умисно створюваними перешкодами і тому інше [4].

Найбільш яскравим прикладом використання мобільного зв’язку у злочинних цілях з’явилися дії щодо доступу і користування його ресурсами без їх належної оплати. За даними Асоціації боротьби із шахрайством у галузі зв’язку (CFCA) щорічні збитки операторів і абонентів від шахрайських дій оцінюються більш ніж у 12 млрд. доларів. У середньому, втрати оператора зв’язку від шахрайства становлять від 3 до 5% загальної суми прибутків.

Зазначена проблема була предметом безпосереднього обговорення на засіданнях Юридичної комісії в Палаті представників та Сенаті США. Як наголошувалося в одній з доповідей, якщо не вжити термінових заходів, то витрати на компенсацію шкоди від злочинів у цій галузі зростатимуть щорічно на 40 % [95].

Кримінальне законодавство багатьох зарубіжних країн містить спеціальні норми і нормативно правові акти, які передбачають кримінальну відповідальність за неправомірний доступ до сфер мобільного зв’язку і користування їх ресурсами (Великобританія: Закон «Про телекомунікації» Telecommunication Act) 1984 р., Закон «Про шахрайство в телекомунікаціях» (Telecommunication (Fraud) Act) 1997 р.; Закон Угорщини «Про захист інформації про особу і використання інформації, що має суспільний інтерес», 1992 р.;Нідерланди: статті 138а, 55 Кримінального кодексу Нідерландів;

Італія: стаття 615-ter Кримінального кодексу Італії; Іспанія: стаття 248.2 Кримінального кодексу Іспанії і тому інше.) [32, с. 5–9; 52, 36; 37].

Захист інформації (запобігання вільному доступу до інформації, усунення технічних каналів її витоку тощо) в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах та мережах електрозв'язку забезпечується комплексом організаційних, програмних і технічних заходів. Подолання захисту може проявлятися у зламі паролів, кодів доступу тощо. Спосіб подолання зазначених заходів безпеки не матиме значення для кваліфікації, звичайно, якщо само воно не буде містити ознак іншого складу злочину (наприклад, знищення програмних або технічних засобів) [51, с. 451].

Якщо особа має право доступу до інформації, яка оброблюється в ЕОМ, автоматизованих системах, комп'ютерних мережах чи мережах електрозв'язку, то її дії кваліфікуються за ст. 362 КК «Несанкціоновані дії з інформацією, яка оброблюється у ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї» або ст. 363 КК «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».

Суб'єктивна сторона злочину характеризується умисною формою вини. Злочинні дії при подоланні програмного та технічного захисту для отримання несанкціонованого доступу можуть бути вчинені лише з прямим умислом. Особа, яка здатна втрутитись у роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку має відповідні знання, вміння та навички. Безперечно особа усвідомлює соціальну небезпечність несанкціонованого втручання, його протиправність; передбачає наслідки у вигляді витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації; бажає або свідомо припускає настання цих наслідків,

ставиться до їх настання байдуже. Мотив переважно корисливий, або можливі – помста, хуліганство, підрив репутації, приховування іншого злочину тощо [42, с. 156; 69].

Отже, термін «злочини, які пов'язані з втручанням у роботу мереж мобільного зв'язку» можна розглядати як злочинну діяльність, у яку включаються не тільки кримінальні дії з користування ресурсами (послугами) системи мобільного зв'язку, а і кримінальні дії щодо доступу до даної системи, передбачені самостійними складами КК України [72, с. 15–21].

Вважаємо за необхідне розглянути детальніше таку діяльність:

І. Злочинні дії, з отримання доступу до системи мобільного зв'язку:

а) привласнення абонентських рухомих станцій мобільного зв'язку. Як відомо, мобільний телефон – не тільки засіб зв'язку у сучасному місті, а й дуже дорогий електронний пристрій – за вартістю багато моделей дорівнюють хорошому кольоровому телевізору, сучасному DVD-програвачу або стереосистемі. Крім того телефони, у порівнянні з перерахованими вище пристроями, мають для будь-якого злочинця беззаперечні переваги – вони компактні за розмірами і вагою, не мають серйозного захисту і ними можна заволодіти безліччю різних способів. Не дивно, що сьогодні офіційні зведення рясніють повідомленнями про крадіжки, пограбування і навіть розбійні напади, предметом посягання яких є мобільні телефони. Явище стало настільки поширеним, що ця категорія злочинів за кількістю виходить на перше місце і перевищує кількість інших вчинених крадіжок, зокрема квартирних. Тільки за офіційними даними, щорічно у м. Києві фіксується близько 5000 зареєстрованих випадків незаконного заволодіння мобільними телефонами. Проте практика свідчить, що тільки кожен другий звертається до правоохоронних органів у разі втрати мобільного телефону. Отже, латентних злочинів на порядок більше, причому це число постійно зростає.

Існує безліч варіантів заволодіння засобами зв'язку, загалом їх можна виокремити на такі основні категорії:

1) крадіжки (ст. 185 КК України). Варто зауважити, що за останній час відбулося колосальне збільшення кількості абонентів мобільних мереж (мобільні телефони має 80% жителів України). Це призвело до того, що проблеми, пов'язані з крадіжками мобільних телефонів, набули масовий характер. Мобільний телефон можуть викрасти з сумки, розрізав її, витягнути з кишені (особливо задньої), або зрізати з ременя, якщо телефон закріплений там, за допомогою пластикової прищіпки, яка, легко ламається. Більше проблем виникає з новими моделями телефонів, вагою менше 80 – 90 г. і майже не відчуваються у кишені. Найчастіше стільникові телефони крадуть у транспорті при великому скупченні пасажирів.

Чимало мобільних телефонів викрадають з роздягалень різних публічнихмісць. Не менш поширеними є крадіжки телефонів із офісів. Можна навіть вести мову про категорію так званих «щипачів», які ходять з кабінету в кабінет у різних установах і видивляються, де й що погано лежить – від калькуляторів до мобільних телефонів.

2) грабіж (ст. 186 КК України). Інакше його ще називають «метод ривка», який складає близько 50%. В цих ситуаціях власник телефону не тільки потерпає через втрату цінної речі, а й нерідко зазнає фізичного насилля [57, с. 597].

Як показує практика, грабіжники вибирають найчастіше дітєй, молодих жінок та чоловіків після сорока років. Коли батьки споряджають дитину мобільним телефоном за тисячу-півтори гривень і відправляють до школи, то не задумуються, що перетворюють її на потенційну жертву насилля. Підійти до підлітка і відібрати телефон не становитиме великих труднощів для злочинця.

Молоді жінки та дівчата найчастіше піддаються грабіжницьким нападам темної пори доби. З рештою, їх можуть просто зустріти у темному під'їзді й насильно відібрати телефон під загрозою фізичної розправи чи зґвалтування.

3) шахрайство (ст. 190 КК України). Злочинці із задоволенням експлуатують всі добрі емоції, які потерпілий може відчувати до людей, які звертаються до нього за допомогою.

Третя категорія жертв – чоловіки за сорок. Саме вони найчастіше повертаються додому темної пори добряче напідпитку. Збити з ніг і понишпорити у кишенях – не так уже й складно.

За останні кілька років зловмисники цілковито оновили методи обману власників телефонів, але основну ставку, як і раніше, роблять на просту людську жадібність. Основним каналом крадіжок мобільних грошей стали sms-сервіси, за допомогою яких шахраї одержують невикористані коди скретч-карток для поповнення рахунку і змушують жертву переводити кошти на свої рахунки. Цим промишляють і одинаки, що заробляють $200 – 500 на місяць, і цілі групи, які одержують $10 – 50 тис.

Але найпопулярніший спосіб обману – розсилка повідомлень про псевдопризи. Схема шахрайства виглядає дуже просто: потенційній жертві надходить повідомлення про перемогу в акції, яку влаштовує оператор, та можливість одержати приз. Виклик здійснюється з мобільного тієї самої мережі, причому іноді використовуються номери з діапазонів, зарезервованих для службових телефонів компанії-оператора. Вони зазвичай не викликають у абонентів підозру, тому багато хто вірить, що на зв’язок справді вийшли представники оператора. Зміст sms може бути різним залежно від винахідливості шахрая. Найпростіше повідомлення виглядає так: «Ваш номер виграв приз від національного оператора мобільного зв’язку. Зателефонуйте за телефоном...». Або: «МТС вітає вас! Номер вашого телефону став одним із 10 переможців. Отримайте свій подарунок. Телефонуйте... Світ розваг на wap.mts.com.ua».

Останнім часом, щоб додати більшої переконливості обману, зловмисники розсилають sms про перемогу абонента у спільних акціях операторів з іншими компаніями. Приміром, власник мобільного телефону дізнається, що виграв автомобіль у спільній акції АвтоЗАЗ-ДЕУ, Київстару й

МТС. Крім того, нібито від імені оператора може надійти пропозиція під час акції перевести певну суму грошей й отримати бонус (наприклад, при поповненні рахунку на 60 грн обіцяють потроїти суму на балансі абонента). Закінчуються такі повідомлення зазвичай однаково – проханням для одержання призу або бонусу зателефонувати операторові та продиктувати номер картки для поповнення рахунку (зазвичай на 100 – 200 грн), яку, певна річ, треба попередньо купити [39, с. 60].

З впровадженням операторами мобільного зв'язку послуги з переказу коштів з одного номера на інший з'явилася нова шахрайська схема. Власник мобільного телефону отримує повідомлення про надходження на його рахунок 15 грн, переведених за допомогою послуги «мобільний переказ». Через хвилину йому телефонує шахрай і просить повернути помилково переказані гроші. Безперечно людина не знає точного стану свого мобільного рахунку і повертає нібито помилково отримані гроші тому, хто телефонував.

Іноді шахраї повідомляють новину про злам сервера Київстару й пропонують ввести набір цифр, щоб подвоїти суму на своєму рахунку. Але під кодом зашифрована послуга з переказу коштів, і абонент, скориставшись нею, переказує гроші зі свого рахунку на рахунок шахрая.

Не рідко до мобільного шахрайства причетні працівники операторів мобільного зв'язку, дилери і контент-провайдери. На сайті оператора клієнту через інтернет пропонували замовити у контент-провайдера послугу встановлення місцезнаходження того, хто телефонує і для цього пропонували набрати спеціальний код для її активації. Але код виявився номером, закріпленим за провайдером у Північній Америці. Тільки-но абонент набирав цей код, йому нараховували дорогий міжнародний трафік [76].

До шахрайства можливо віднести: надання невірних даних при укладанні контракту на користування послугами мобільного зв'язку (ст. 358 КК України); незаконне втручання у роботу мереж електрозв'язку, що призвело до знищення, перекручення, блокування інформації або до порушення встановленого порядку маршрутизації (ст. 361 КК України);

створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів (сканерів, абонентських рухомих станцій мобільного зв'язку з можливостями сканування, модифікація абонентських рухомих станцій і їх програмного забезпечення і тому інше.), а також їх розповсюдження або збут (ст. 361^1) [82; 70].

Для виявлення мобільного шахрая і доведення справи до суду правоохоронним органам зазвичай бракує доказової бази. Sms не може бути доказом, це лише передумова для пошуку зловмисника. Виявити місце, звідки шахраї розсилають повідомлення, можна лише приблизно.

«Наприклад, можливо визначити, що зловмисники перебувають у радіусі 500 метрів, де розташовані кілька дев'ятиповерхових будинків – вони можуть бути у кожній з квартир. Шукати важко, а невеликі втрати абонентів зазвичай не варті цього, такого висновку доходять опитані респонденти. Як правило, ловлять осіб, найнятих лідерами угруповань для розсилання sms [40].

Злочинні дії, які полягають у отриманні обманним шляхом ресурсів (послуг) мобільного зв'язку без мети їх належної сплати (кримінальне користування ресурсами (послугами) мобільного зв'язку), а саме:

а) заподіяння майнової шкоди шляхом обману або зловживання довірою (ст. 192 КК України);

б) привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем (ст. 191 КК України);

в) шахрайство (ст. 190 КК України);

Отже, злочини, які пов'язані з втручанням у роботу мереж мобільного зв'язку, з позиції кримінального права являють собою ряд самостійних складів, які відносяться до різних глав Кримінального кодексу України. Як наслідок, виникає низка питань пов'язаних з їхньою кваліфікацією [83, с. 14; 84, с. 130–133; 71].

Дії кваліфікуються як неправомірний доступ до комп'ютерної інформації за ст. 361 КК України в тому випадку, якщо ця інформація

охороняється законом. Ідентифікаційні номери користувачів послуг мобільного зв'язку потенційно є конфіденційною інформацією, а точніше її різновидом – комерційною таємницею. Відповідно до ст. 505 Цивільного кодексу України комерційною є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі при сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, зважаючи на це має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Дійсно, і з точки зору чинного законодавства, і з позиції технічних особливостей побудови сфер мобільного зв'язку ефір є відкритим до сканування. Тим самим, виникає питання: чи є доступ до ідентифікаційних номерів користувачів, що знаходяться в ефірі, вільним?

Надання інформаційним ресурсам режиму комерційної таємниці (інформації з обмеженим доступом) здійснюється власником (у цій ситуації – компанія мобільного зв'язку) виданням внутрішніх актів, а також забезпеченням її реальної охорони (використання алгоритмів шифрування, ключів захисту і тому інше.), що не можна віднести до деяких операторів аналогових стандартів мобільного зв'язку, тому, що ці стандарти не забезпечують шифрування ідентифікаційних даних користувачів на рівні радіотракту.

За своїм змістом, до складу відносин, що виникають у сфері діяльності з надання послуг мобільного зв'язку, входять, в більшості випадків майнові права зобов'язального характеру – право вимоги компанії-оператора до абонента про сплату відповідних коштів за договором на надання послуг мобільного зв'язку, право вимоги контрагентів компанії-оператора оплати, за використані її абонентами канали зв'язку, право вимоги абонента щодо надання відповідно до договору послуг зв'язку і інше.

Використання ідентифікаційних номерів легальних абонентів для користування ресурсами мобільного зв'язку без мети належної сплати є не чим іншим, як придбанням права користування вказаними ресурсами, зокрема і рахунком (балансом) легального абонента. На нашу думку, кримінальна відповідальність за отримання обманним шляхом ресурсів мобільного зв'язку без мети їх належної оплати має наступати за ст. 190 КК України у тому випадку, коли злочинцем здійснюється використання мереж інших операторів, зважаючи на це оператор (який, у даному випадку, також буде потерпілим), до якого злочинець підключився, оплачує проведені злочинцем з'єднання іншим операторам, у мережах яких ці з'єднання проводилися.

Кримінальна відповідальність за ст. 192 КК України наступає у разі використання злочинцем тільки мереж оператора, до якого він підключений. Сюди ж варто віднести і злочинні дії, що включають надання можливості користування ресурсами мобільного зв'язку без належної оплати іншими особам. Ми вважаємо, що притягнення до кримінальної відповідальності за ст.192 КК України має наступати у тому випадку, коли сума шкоди досягає меж, що характеризують значний розмір для потерпілого, відповідно, суспільну небезпеку діяння, яка вимагає саме застосування заходів кримінальної відповідальності. Тим самим, існує нагальна потреба законодавчого встановлення і закріплення у ст. 192 КК України нижньої межі майнової шкоди, заподіюваної даного роду діяннями.

Висновки до Розділу 1

На підставі аналізу наукових джерел виділяється п’ять етапів розвитку телекомунікацій: а) з 1832 р. – створення і розвиток телефону і телеграфу – кабельні телекомунікаційні системи; б) з 1895 р. – поява радіо і телебачення – радіохвильові телекомунікаційні системи; в) з 1957 р. – використання супутників для передачі інформації – супутникові телекомунікаційні системи; г) з 1968 р. – поява комп’ютерних мереж – комп’ютерні телекомунікаційні системи; д) 80-ті роки XX століття – злиття засобів зв’язку і обчислювальної техніки – інтегровані телекомунікаційні системи, в т.ч. смартфони.

Злочини у сфері мобільних технологій можна класифікувати на: а) шахрайство, що завдає збитків операторам стільникового зв’язку, дилерам і абонентам; б) перехоплення конфіденційної інформації, або так зване мобільне шпигунство; в) порушення режиму мережного обслуговування абонентів з хуліганських спонукань або з інших причин, не пов’язаних з перехопленням інформації.

До особливостей протиправних діянь на вітчизняних телекомунікаційних слід віднести: а) зловживання працівників, підрядчиків та дилерів телекомунікаційних компаній; б) дії правопорушників сприймаються як законні, санкціоновані; в) порушники використовують сучасні технології, апаратне та програмне забезпечення; г) дії правопорушників, як правило, динамічні у часі і розподілені у просторі.

Під злочинами, які пов’язані з втручанням у роботу мереж мобільного зв’язку слід розуміти злочинну діяльність, яка включає не тільки кримінальні дії з користування ресурсами (послугами) системи мобільного зв’язку, а і кримінальні дії з доступу до даної системи, передбачені самостійними складами КК України.

РОЗДІЛ 2.

КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА ЗЛОЧИНІВ У СФЕРІ МОБІЛЬНИХ ТЕЛЕКОМУНІКАЦІЙ

2.1. Криміналістичний портрет особи злочинця та мотивація його дій щодо втручання у роботу мереж мобільного зв'язку

Оптимізація діяльності щодо виявлення і розслідування злочинів багато в чому залежить від знання співробітниками правоохоронних органів інформативних властивостей осіб, які їх вчиняють. Характеристику осіб, які вчинили злочини у сфері мобільних телекомунікацій, доцільно почати з їх типології, тобто з опису тих істотних ознак, які причино пов'язані із злочинною поведінкою і дозволяють фіксувати відповідні тенденції.

Досліджуючи типологію осіб, які вчинили злочини у сфері мобільних телекомунікацій, доцільно виділити групу так званих «фрікерів» (своєрідний аналог «хакерів» щодо злочинів у сфері комп'ютерної інформації), яких в найзагальнішому вигляді можна визначити як фахівців, що мають спеціальні знання у галузі побудови і функціонування програмних і апаратних засобів підтримки систем електрозв'язку, використовують свої інтелектуальні здібності, наявні технічні знання для розробки способів протиправного доступу до мереж електрозв'язку і користування їх послугами, а також для здійснення інших протиправних дій у мережах електрозв'язку [55, с. 401].

Серед основних ознак, що вказують на вчинення злочинів у сфері мобільних телекомунікацій саме цією групою осіб, можна виділити наступні:

- наявність продуманої підготовки до вчинення злочину;

- спрямованість дій на апаратно-програмні засоби захисту інформації засобів мобільного зв'язку;

- використання технічних і програмних засобів кустарного і виробничого походження з метою зчитування і запису ідентифікаційної інформації для подальшого отримання доступу до системи мобільного зв'язку.

Зазначені особи можуть діяти як в своїх інтересах, так і на користь інших осіб.

Крім «фрікерів» серед осіб, які вчиняють злочини у сфері мобільних телекомунікацій, можна виділити такі групи:

- особи, які не мають знань у галузі побудови і функціонування програмних і апаратних засобів підтримки систем електрозв'язку, а лише деякі професійні навички роботи з ними на рівні користувача. Як правило, їх дії полягають у неправомірному доступі до мережі мобільного зв'язку в роумінгу, придбанні вже готових програмно-апаратних комплексів, призначених для неправомірного доступу до мереж електрозв'язку;

- особи, які не мають спеціальних технічних знань та невисокого рівня знань для користувача. Частіше за все дії цих осіб спрямовані на розкрадання мобільних телефонів, умисне надання невірних даних при укладанні контракту на користування послугами мобільного зв'язку (використання підроблених документів, створення фіктивної організації і таке інше).

Очевидно, що рамки поняття «особа передбачуваного злочинця» достатньо широкі, зважаючи на це доцільно використовувати вироблені у криміналістиці підстави розподілу. На підставі вивчення узагальнень МВС України, можнадійти висновку, що злочини у сфері мобільних телекомунікацій переважно вчиняють чоловіки – 91%, частка участі жінок незначна – 9%. Крім того практично у всіх відомих випадках дії щодо неправомірного доступу до сфер мобільного зв'язку здійснювалися особами чоловічої статі [92, с. 40].

Правопорушники мають різний соціальний статус і рівень освіти. Основну масу склали особи, які не працюють – 36% і студенти – 34%. Іншу частину склали особи, які працюють в комерційних організаціях – 18% і

приватні підприємці – 12%. У числі суб'єктів злочину закономірно переважають особи з вищою (38%) і неповною вищою освітою (34%). Меншу частину складають особи, які мають середню спеціальну (9%) і середню освіту (19%).

З числа осіб, які вчинили злочини у сфері мобільних телекомунікацій, лише 9% були працівниками (колишніми працівниками) операторів мобільного зв'язку.

За віковими групами правопорушники диференціюються на групи: 18-24 років – 38%, від 25 до 29 років – 38%, 30-39 років – 16%, 40-49 років – 8%.

З числа осіб, які вчинили злочини у сфері мобільних телекомунікацій, громадяни України і країн СНД склали 89%, іноземці – 11%. Групу останніх складали в більшості своїй громадяни Палестини, Лівану, Сірії, Пакистану. Переважна більшість злочинців проживали у місті, де здійснювалися кримінальні дії щодо доступу до мереж мобільного зв'язку, а також користування їх послугами (за винятком кримінальних дій в роумінгу). Серед осіб, які вчинили злочини у сфері мобільних телекомунікацій, раніше притягувалися до кримінальної відповідальності тільки 8%. Переважна кількість злочинців на момент вчинення злочину до кримінальної відповідальності не притягувалася.

За кількісними характеристиками кримінальні дії у мережах мобільного зв'язку можна розділити на вчиненні групою - 45% і поодинці - 55%. Вчинення злочину однією особою, як правило, пов'язане тільки з неправомірним користуванням послугами або простими способами доступу до сфер мобільного зв'язку (придбання клонованого мобільного телефону, ручне або автоматичне введення нових ідентифікаційних номерів і тому інше.). Диференціація груп залежно від кількості учасників наступна: група у складі двох осіб – 23%, у складі трьох – п'яти осіб – 14%, у складі п'яти і більше осіб – 8%.

Характеристика особи передбачуваного злочинця була б односторонньою без відповідного опису мотиваційної і цільової

спрямованості його поведінки при вчиненні злочинів у сфері мобільних телекомунікацій. Варто наголосити, що мотив і мета займають особливе місце у характеристиці особи, як елемента криміналістичної характеристики злочинів у мережах мобільних телекомунікацій.

Загалом, мету можна визначити як категорію, яка визначає насамперед результат, на досягнення якого спрямована свідома діяльність людини. У поняття мети включається не тільки певне об'єктивне знання, а й зміст, негативний у відношенні до тієї реальності, яка не задовольняє людину і тому підлягає модифікації, перетворенню, або пристосуванню до неї. Тим самим, вона стає передумовою майбутньої діяльності, мотивом і тому одним з основних детермінуючих чинників діяльності людини [49, с. 541].

Усвідомлення мети і наслідків її досягнення у формі тих або інших змін в зовнішньому світі примушує злочинця обирати засоби і спосіб досягнення мети, використання яких скорочує небажані для злочинця наслідки [38].

Кримінальні дії щодо доступу до системи мобільного зв'язку і користування її ресурсами за своєю багаторівневою структурою є складними. Зважаючи на це, виникає потреба дослідження не тільки загальних питань цільової і мотиваційної детермінації, а й виокремлення конкретної кінцевої і проміжної мети, фіксації так званого «древа» цілей, оскільки природа діяльності визначається ієрархічною взаємодією мети, засобу і результату діяльності [26].

В існуючих на даний час дослідженнях злочинів, які вчиняються у мережах мобільних телекомунікацій, є лише уривчасті дослідження мети і мотивів даного різновиду злочинів. Так, П. Іванов, використовуючи матеріали європейської конференції користувачів SAS Institute-SEUGF 18, виділяє такі типи мотивації як: надання друзям можливості безкоштовно користуватися послугами зв'язку; приховування свого місцезнаходження від силових або податкових органів; спроба власних сил, яка полягає в обході засобів захисту, побудованих оператором; користь [96].

У доповіді помічника директора ФБР Дж. Наварета, виділяються такі мотиви використання клонованих телефонів:

- по-перше, клонований мобільний телефон-вдала покупка для злочинця (у багатьох столичних місцях за цей телефон можна отримати кілька сотень доларів, що нижче за вартість телефонів, які продаються і підключаються легально);

- по-друге, клонований мобільний телефон, як правило, продається на готівковій основі, без кредитних (касових) чеків (отже, злочинці можуть легко отримувати клонований телефон без «паперових» слідів);

- по-третє, дзвінки з клонованого мобільного телефону, практично неможливо відстежити (тому ці телефони активно використовуються членами організованої злочинності, особливо в районах з незаконним обігом наркотиків). Це виразно простежується в тому, що організації, які торгують наркотиками, багато уваги приділяють конспірації. Вони купують 10-20 мобільних телефонів на кілька тижнів або навіть днів і потім швидко роз'єднують і замінюють їх, щоб уникнути переслідування [81].

Ці дослідження безумовно вимагають доповнень і систематизації. Як вже неодноразово зазначалося, для здійснення задуму із користування ресурсами системи мобільного зв'язку, в першу чергу, варто здійснити відповідні підготовчі дії – доступ до даної системи як абонента, а в інших випадках, здійснення абонентської активності – користуватися послугами мобільного зв'язку і надавати таку можливість іншим особам.

Таким чином, обов'язковими елементами цієї категорії злочинів будуть:

1) проміжна мета – неправомірне отримання доступу до системи мобільного зв'язку, яке може спрямовуватися зацікавленою особою на: розкрадання (або інший кримінальний спосіб заволодіння) чужих мобільних телефонів; придбання клонованого мобільного телефону; укладання контракту на користування послугами мобільного зв'язку за фіктивними документами; отримання ідентифікаційних даних легальних користувачів

(виробництво і експлуатація сканерів, мобільних телефонів з можливостями сканування, модифікація мобільних телефонів і їх програмного забезпечення та інші, не пов'язані з використанням спеціальних технічних засобів дії) системи мобільного зв'язку і перепрограмування їх в мобільний телефон, чисту SIM карту або створення емулятора SIM-карти; проникнення в комп'ютерну систему для видалення механізмів захисту або переконфігурації системи базових станцій, модифікації білінгової або облікової інформації та інше;

2) кінцева мета:

– неправомірне користування ресурсами системи мобільного зв'язку без їх належної оплати і (або) реєстрації для: користування ресурсами системи мобільного зв'язку без їх належної оплати (економія витрат).

– перешкоджання встановленню місця знаходження злочинця і прослуховування його переговорів з метою виключення можливості встановлення злочинних діянь або окремих їх обставин, а також подій некримінального характеру.

Тим самим, наступним елементом криміналістичної характеристики, який детермінує способи вчинення злочинів у мережах мобільних телекомунікацій, є мотивація даного різновиду злочинів.

Аналогічно, як і при вивченні цільової спрямованості вчинення злочинів у мережах мобільних телекомунікацій, варто виходити з певної ієрархії мотивів даного різновиду злочинів. Проте, першорядну роль в аналізі способів вчинення злочинів відіграватимуть мотиви, які визначають загальну цільову спрямованість. За наявними даними, а також моделюючи можливі ситуації, можна сформулювати наступний класифікаційний ряд мотивів:

1) економічні мотиви (у структурі злочинів, які вчиняються у мережах мобільних телекомунікацій, ця мотивація є переважаючою). Крім того, корисливий мотив поділяють на: економію витрат і отримання доходів.

2) мотивація «ухилення від викриття» характерна для організованої злочинності (особливо при використанні двійників мобільних телефонів).

Останнім часом подібних висновків дійшли і співробітники оперативних підрозділів, які відзначають, що в організованих злочинних угрупуваннях стало популярним використання клонованих мобільних телефонів при вчинені злочинів, пов'язаних з викраданням людей, вимаганням, погрозою насильством або фізичним знищенням, здійсненням шахрайських дій через підставні фірми, організацією терористичних актів, угонів автотранспорту та ін. Тобто в тих випадках, коли злочинці мають надійний постійний телефонний зв'язок, як між собою, так і з об'єктом злочинного посягання, а місцезнаходження їх визначити дуже складно [16, с.145].

Крім того, намітилася тенденція до розповсюдження кримінальних дій у мережах мобільного зв'язку на міжнародному рівні зважаючи на розвиток послуг роумінгу. МВС України має інформацію про осіб, задіяних у цій протиправній діяльності на території нашої держави. Злочинне середовище у сфері телекомунікацій характеризується оперативниками як високоінтелектуальне, організоване, таке, що має глибокі взаємозв'язки, структуру та інформованість про діяльність правоохоронних органів. Діяльність груп розповсюджується не тільки на Україну і прилеглі держави, також і на країни далекого зарубіжжя (Південно-східна Азія, Латинська Америка, Близький Схід) [54,с. 381];

3) дослідницький інтерес (зазначений тип мотивації найчастіше визначає дії осіб з високим рівнем технічної освіти, для підтвердження своїх професійних можливостей, перевірки і демонстрації власної кваліфікації або задоволення власної допитливості);

4) хуліганські мотиви (вид мотивації властивий попередній категорії осіб, проте з яскраво вираженими антисоціальними установками).

5) підрив фінансової основи компанії оператора мобільного зв'язку і її авторитету. Мотив має два аспекти: а) призводить до спроби дискредитації заходів безпеки, які застосовує оператор мобільного зв'язку; б) призводить до спроби отримати переваги під час конкуренції.

З врахуванням того, що деякі оператори мобільного зв'язку несуть втрати від такої злочинної діяльності у розмірі 0,5-20% від прибутку, а також те, що використання у повністю завантаженій мережі великої кількості клонованих апаратів (більше 10% від розрахункової місткості мережі) призводить до значного погіршення роботи мережі через перевантаження [9, с. 179], цілеспрямовані дії організованих злочинних угрупувань можуть призвести до ослаблення конкурентоспроможності, уповільнення розвитку і інших наслідків, які є бажаними для конкурентів.

Взагалі, за рідкісним винятком, у мотивації даного різновиду злочинів достатньо складно виокремити «чистий» мотив. У більшості випадків зазначені мотиви, як і мета даних кримінальних проявів, інтегруються. Це відбувається не тільки через особливості суб'єктів вчинення злочинів, а і завдяки технічним цінностям побудови системи мобільного зв'язку. Так, заподіюючи матеріальну шкоду оператору при використанні клонованого телефону, злочинець отримує не тільки можливість уникнути викриття, а і користується ресурсами системи зв'язку без їх належної оплати, і навпаки.

2.2. Технології вчинення злочинів у сфері мобільних телекомунікацій

Базовим елементом криміналістичної характеристики злочинів і основою криміналістичних рекомендацій щодо їх розкриття та розслідування завжди виступали дані про функціональну сторону злочинної діяльності. Саме під діями (їх сукупністю) в криміналістичній літературі розуміється спосіб вчинення злочину.

У наукових дослідженнях кримінального циклу існують різні визначення способу і змісту. З існуючих у криміналістичній науці визначень способу вчинення злочину найбільш чіткою та вдалою є концепція, згідно з

якою криміналістичне поняття способу вчинення злочину формулюється як взаємоспрямована система дій щодо підготовки, вчинення і приховування злочину, які взаємозв'язані з зовнішнім середовищем і властивостями особи, а також можуть бути скомпоновані з використанням відповідних знарядь і засобів, місцем і часом [9, с. 16].

Резюмуючи зазначене вище, під способом вчинення злочинів у мережах мобільних телекомунікацій розуміється система дій, спрямованих на підготовку, скоєння і приховування даної категорії злочинів, що виражаються в несанкціонованому доступі до системи мобільного зв'язку, користуванні її ресурсами і (або) наданні такої можливості іншим особам, об'єднаних загальною цільовою спрямованістю – несанкціоноване користування ресурсами системи мобільного зв'язку без їх належної сплати і (або) реєстрації, детермінованих суб'єктивними і об'єктивними чинниками.

Для повноцінного розуміння способу вчинення даного різновиду злочинів доцільно звернутися до розгляду його структури.

В криміналістичній літературі існує наступна класифікація способів вчинення злочину:

1) повноструктурні або найбільш кваліфіковані способи (підготовка, вчинення, приховання злочинів);

2) менш кваліфіковані або усічені способи (вчинення і приховання злочинів; підготовка і вчинення злочинів);

3) некваліфіковані або спрощені (складаються тільки з дій щодо вчинення злочинів) [11, с. 124].

Не дивлячись на те, що спосіб вчинення злочину – динамічна система щодо того або іншого виду злочинної діяльності, в злочинах, які вчиняються у мережах мобільних телекомунікацій, вони складаються з підготовчих дій (дії злочинця, направлені на отримання доступу до системи мобільного зв'язку) і дій щодо скоєння [дії, щодо користування ресурсами (послугами) мобільного зв'язку (абонентська активність) і надання такої можливості іншим особам].

За наведеною вище класифікацією, способи вчинення злочинів у мережах мобільних телекомунікацій можуть здаватися менш кваліфікованими або усіченими (підготовка і скоєння злочинів). Проте, це не зовсім вірно. У «чистому вигляді» вони зустрічаються вкрай рідко, тому що, як правило, одні і ті ж типові дії щодо підготовки та вчинення даного різновиду злочинної діяльності несуть функціональне навантаження з їх приховання.

Аналіз наявної інформації свідчить про збільшення кількості злочинів, пов'язаних із несанкціонованим втручанням у роботу мереж електрозв'язку шляхом використання емуляторів (підробних) чіп-карт. Такі дії злочинців призводять до заподіяння значних економічних збитків державі. Найпоширенішим шляхом розповсюдження інформації щодо незаконного виготовлення та збуту емуляторів є мережа Інтернет. На деяких сайтах розміщується інформація про можливість продажу, функціональні схеми та програмне забезпечення для виготовлення емуляторів, детальна інструкція з їх подальшого використання, яка також містить поради з дотримання умов конспірації при використанні емуляторів телефонних карток, що свідчить про обізнаність їх виробників про відповідальність за вказану діяльність.

Так, упродовж кількох місяців, з України здійснювалися міжнародні телефонні розмови, оплачувати які було нікому, бо номерів, з яких надходив сигнал замовлення, на київських АТС не існувало. «Фантоми» наговорили на десятки тисяч американських доларів. Зв'язківці зазнали збитків, які у майбутньому могли бути значно більшими, якби за розслідування цієї справи не взялися органи безпеки. Спрощена схема роботи нелегальних телефоністів полягала у «клонуванні» службових номерів українських мобільних операторів, переведених через Інтернет в телекомунікаційну мережу. Іншими словами, ділки заробляли гроші, торгуючи трафіком переговорів, викраденим у зв'язківців.

З'ясувавши механізм скоєння злочину, вдалося встановити зловмисників та затримати їх на гарячому у Криму. Саме там, в одному з

науково-дослідних інститутів в орендованому під офіс невеликому приміщенні, розташовувалася підпільна телефонна станція. Для людей зовні вона виглядала як набір комп'ютерів та електронних блоків і у розібраному стані вміщалася у вантажному фургоні ГАЗелі. Загальна ж вартість вилученого обладнання, за попередньою оцінкою експертів Українського державного центру «Укрчастотнагляд», становить майже 400 тис. дол.

У відповідних підрозділах СБУ вивчили технічні «ноу-хау» від злочинців. З результатами досліджень були ознайомлені фахівці національних операторів зв'язку. Ними вжито заходи щодо запобігання подібних втручань до телефонної мережі держави у майбутньому [22].

Hacking fraud – дії, які полягають у проникненні в комп'ютерну систему захисту для знешкодження механізмів захисту або переконфігурації системи базових станцій з метою використання (або подальшої реалізації) наявних в системі функціональних можливостей або користування ресурсами мобільного зв'язку.

У найзагальнішому вигляді процедура білінгу виглядає так: при активації з'єднання службові дані надходять через систему базових станцій в комутатор, і, якщо номер, який викликається, доступний, відкривається канал, що з'єднує абонентів.

Комутатор вирізняє кілька видів з'єднань, інформацію щодо яких передають на буферний комп'ютер від комутатора відразу після закінчення з'єднання (у системах, що передбачають так званий on-line billingбуферний комп'ютер відсутній і дані про з'єднання передаються від комутатора безпосередньо на сервер оцінки). Буферний комп'ютер передає кожні кілька хвилин на сервер оцінку інформації про певну кількість з'єднань.

Сервер оцінки, одержавши дані від буферного комп'ютера, запитує у сервера базу даних: номер абонента, його тарифний план і номер його рахунку. Після цього сервер оцінює розмову за такими параметрами: тип розмови і час з'єднання. Після цього сервер оцінки надсилає на сервер бази даних номер абонента і вартість його з'єднання. Сервер бази даних здійснює

відповідно до інформації, одержаної від сервера оцінки, списування коштів з рахунку абонента, змінюючи його баланс.

Оскільки білінгові процедури реалізовані на базі засобів і мереж комп'ютерної техніки оператора, то наступний спосіб неправомірного копіювання може здійснюватися за допомогою локального або видаленого доступу до даної мережі через Інтернет.

Злочини, вчинені персоналом оператора, є досить серйозною загрозою, тому що персонал використовує відомі йому слабкості системи. Це і змінення абонентських даних, і передача конфіденційної інформації, і корекція білінгових записів, і створення пільгових умов для певної групи абонентів. Причиною таких дій, які достатньо важко виявити і припинити, може бути збагачення або тиск з боку представників «тіньової економіки». Не можна виключати і можливості безпосереднього введення у штат технологічних і інших ключових підрозділів операторів «резидентів» або членів кримінальних структур [23, с. 165].

У більшості досліджень, присвячених злочинам, які вчиняються у сфері мобільних телекомунікацій, виділяється як самостійний спосіб доступу до мережі мобільного зв'язку. Під ним найчастіше розуміється вчинення дій щодо доступу до мобільного зв'язку, які полягають у застосуванні знань про процедури його функціонування, використання недоліків в роботі білінгової або облікової системи з метою користування ресурсами системи мобільного зв'язку без відповідної сплати і реєстрації [33, с.24].

Як основні різновиди procedural fraud можна виділити roaming fraud і card fraud. У разі roaming fraud, злочинець враховує, що процедура білінгу (головним чином міжнародного) може проводитися після закінчення тривалого часу, після того, як були здійснені з'єднання. У даному випадку використовується часовий проміжок, що виникає між моментом активації функції роумінгу і тим часом, коли оператори вже обмінялися білінговою інформацією. Через затримки у білінгових операціях злочинець може певний час користуватися ресурсами мобільного зв'язку без належної сплати, не

дивлячись на те, що сума грошових коштів на його рахунку вже вичерпана [34, с. 178].

Дії, які відносяться до card fraud, ґрунтуються на використанні слабо захищених програмних засобів тих операторів, які здійснюють білінгові операції і аутентифікацію. Якщо інформація про передплачені карти стає надбанням кількох осіб, які водночас намагаються активізувати такі карти, то у випадку, коли є проміжок часу між кредитуванням телефонного рахунку і виведенням карти з обігу, фальшиві копії карт можуть бути використані цими особами.

У переважній більшості випадків варіанти card fraud вчиняються за сприянням співробітників компанії-оператора, адже вони найбільш обізнані про деталі функціонування мережі, про процедури додавання нових абонентів і розширення списків доступних послуг, а також про способи налаштування тестової телефонної лінії, в якій виклики не враховуватимуться білінговою системою [64].

Якщо для класифікації способів доступу до системи мобільного зв'язку, найбільш прийнятною підставою виступають її базові елементи, то для класифікації користування ресурсами системи – підставою до класифікації виступатимуть також елементи системи, але вже іншого роду: різновиди ресурсів (послуг), процедури і порядок їх надання і використання, зона покриття та інші, які дозволяють злочинцю діяти тим або іншим чином, і які відповідно дозволяють сформувати уявлення про тип його поведінки. За характером поведінки абонента, незаконна абонентська активність розрізняється таким чином:

а) постійна (стабільна) кримінальна поведінка – спосіб вчинення дій спрямований на користування ресурсами мобільного зв'язку, коли характер, тривалість і інші параметри не змінюються протягом тривалого часу (злочинцем здійснюється велика кількість тільки коротких, або тільки довгих за тривалістю, рідких або частих дзвінків тільки на певні номери, в певні населені пункти, країни, регіони тощо.).

Так, незаконне використання пільгового тарифу оператора мобільного зв'язку включає дві дії абонента-злочинця, а саме: отримання права користування пільговим тарифом певної служби і отримання абонентом – злочинцем (або групою таких абонентів) кількох номерів телефонів для того, щоб дзвонити спрямовано за номером цієї служби. Залежно від оплати служби з пільговим тарифом видозмінюється механізм кримінальних дій і його характерні ознаки. Якщо така служба отримує частину прибутків від мережі, то на її номер надходять тривалі дзвінки, що повторюються. Якщо прибуток такої служби залежить від кількості отриманих дзвінків, то їй надходить велика кількість коротких дзвінків.

Прикладом може служити класичний випадок, що відбувся з одним з українських операторів. Зловмисники зареєстрували фіктивну фірму, орендували платний номер у Франції і купили в українського оператора 50 телефонів, підключених відповідно кредитного тарифного плану. Ці телефони перевезли до Франції і встановили на автодозвін до орендованого платного номеру. Так вони згенерували величезну кількість дуже дорогого трафіку, що отримував цей номер. У кінці місяця оператор мобільного зв'язку France Telecom сплатив орендарям номеру кілька сотень тисяч доларів. Єдиним потерпілим від шахраїв виявився український мобільний оператор, якому французька компанія виставила великі роумінгові рахунки – його збиток склав близько півмільйона доларів [65].

Часовий чинник відіграє велику роль у поведінці злочинця. Чим менше у нього часу на незаконну абонентську активність, тим менше будуть проміжки між з'єднаннями. Наприклад, для такого виду незаконної абонентської активності як надання можливості користування ресурсами мобільного зв'язку іншим особам характерні часті з'єднання за певний період часу з різними номерами за межами країни.

б) періодична (нестабільна) кримінальна поведінка – спосіб здійснення дій спрямованих на користування ресурсами мобільного зв'язку, коли характер, тривалість і інші параметри періодично або постійно змінюються.

Як правило, постійне безпосереднє користування ресурсами мобільного зв'язку характерне для осіб, які прагнуть перешкодити встановленню їх місця знаходження і прослуховуванню їх переговорів.

У всіх інших випадках, злочинець, отримавши доступ до системи мобільного зв'язку, як правило, перевіряє можливість користування її ресурсами шляхом проведення особистих переговорів, а надалі для отримання прибутку надає можливість користування ресурсами системи іншим особам. Надання можливості користування ресурсами мобільного зв'язку іншим особам поділяється на:

- безпосереднє, коли мобільний телефон (SIM-карта) передається в тимчасове або постійне користування іншим особам;

- опосередковане – за допомогою використання функціональних можливостей системи мобільного зв'язку.

Як приклад, можна навести використання злочинцем функції масової переадресації виклику з метою отримання прибутку. Цей спосіб описаний в літературі таким чином: «Злочинець стає клієнтом компанії мобільного зв'язку, купує телефон, а потім дає рекламу в засобах масової інформації про надання послуг дешевого зв'язку з будь-якою країною світу. Клієнт, що вступив з ним у контакт, називає номер, з яким він хоче зв'язатися. Потім злочинець «вішає» свою трубку, встановлює переадресацію на цей номер і зв'язок здійснюється у зворотному напрямі через комутатор. Крім того номер злочинця не зайнятий і може використовуватися знову». Таким чином можна водночас обслуговувати безліч міжнародних дзвінків, одержати за них гроші і зникнути [74, с. 16].

Одним із розповсюджених способів злочинної діяльності є клонування. Вибір клонування як способу підключення до мережі мобільного зв'язку, а також цифрового стандарту членами організованого злочинного угрупування є не випадковим. Це істотно ускладнює діяльність правоохоронних органів спрямованих на розкриття і розслідування злочинної діяльності даного угрупування.

На підставі наведеної класифікації варто підкреслити, що, загалом способи вчинення злочинів у мережах мобільних телекомунікацій супроводжуються вельми кваліфікованими і досить складними способами приховування, що, відповідно, ускладнює процес їх виявлення, розкриття і розслідування. Здійснене дослідження продемонструвало, що у більшості випадків злочинцями використовуютьсярізні кількісні і якісні комбінації декількох основних способів.

2.3. Особливості встановлення і доказування злочинів у сфері мобільного зв'язку

Поєднання елементів зовнішнього середовища, учасників посягання дозволяє вірно оцінити ситуацію, що склалася, і обгрунтувати слідчі версії на підставі аналізу взаємозв'язків обстановки вчинення злочину та іншими елементами криміналістичної характеристики. Оцінка відомостей, що характеризують обстановку, дозволяє отримати дані про: обставини і умови, що передували, сприяли і перешкоджали злочину; проведення підготовчої роботи злочинцем; обставини, що вплинули на вибір способів, знарядь і засобів; жертв посягання; осіб, які скористалися ситуацією, що створилася, для вчинення злочину [10].

Так, під обстановкою у криміналістиці найчастіше розуміють матеріальні, виробничі і соціально-психологічні чинники середовища, в якому відбувається злочинне діяння. Відносно зазначеного, існують різні бачення щодо складу елементів обстановки скоєння злочину. Наприклад, В. О. Образцов відносить до них територіальну, кліматичну, демографічну та інші специфіки регіону, у якому вчинений злочин, і обставини, що характеризують безпосереднє місце, час, умови та інші особливості [18, с. 19].

Слушною з цього приводу є думка, що в структурі обстановки вчинення злочину відбиваються:

1) матеріальне середовище (час, місце, об'єкт, макро- і мікропогодні умови);

2) організаційно-управлінське середовище (промислово-функціональні об'єкти, а також правоохоронні елементи);

3) соціально-психологічне середовище (мікроклімат у колективі за місцем роботи, ціннісна орієнтація, психологічна обстановка за місцем проживання) [31, с. 44].

Отже, характеризуючи обстановку вчинення злочинів у мережах мобільних телекомунікацій як елемент криміналістичної характеристики, не можна не звернути увагу на те, що особливістю дій, які входять в дану категорію злочинів, є їх опосередкування засобами комп'ютерної техніки даної системи, оскільки фактично, сукупність мобільних телефонів, базових станцій і комутаторів є комп'ютерною мережею, що виконує специфічні завдання.

У разі вчинення злочинів у мережах мобільних телекомунікацій, місцем знаходження ресурсів буде система мобільного зв'язку як сукупність технічних, процедурних і функціональних елементів. Тим самим, особливістю способів вчинення будь-яких злочинів у мережах мобільних телекомунікацій, як, втім, й інших злочинів, вчинення яких опосередковано засобами комп'ютерної техніки, є те, що вони будуть обумовлені специфікою побудови і функціонування технічної системи.

Речовими об'єктами, що мають відношення до середовища здійснення несанкціонованого доступу, є апаратно-технічні, програмні об'єкти системи мобільного зв'язку (абонентські рухомі станції, базові станції, центри комутації, а також білінговий і розрахунковий центри і їх програмне забезпечення та інше.); документи (договори на надання послуг мобільного зв'язку-паспорт, довіреність тощо.).

Просторово-конструктивні чинники (параметри протяжності ділянок, що відображають, на місцевості, конструктивну своєрідність споруд та їх окремих приміщень, у яких вчинений злочин) у сфері мобільного зв'язку мають певну специфіку. Це відноситься, перш за все, до несанкціонованого доступу, що реалізовується видаленими способами. В цьому випадку існують кілька місць, рознесених в просторі, де здійснюється несанкціонований доступ до мережі мобільного зв'язку: а) місце безпосереднього застосування знарядь злочину; б) місце настання шкідливих наслідків [56, с. 207].

Місцем безпосереднього застосування знарядь злочину при віддаленому доступі можуть бути:

1) постійне або часте місцезнаходження злочинця (місце проживання, місце роботи, місце задоволення особистих інтересів - клуби, торгівельні центри і тому подібне, де є персональний комп'ютер, модем телефонна лінія, встановлені спеціальні технічні засоби для виготовлення і застосування знарядь злочину);

2) нефіксована прив'язка до географічного положення (при пересуванні на вулиці, автодорозі та інше.).

Місцем настання шкідливих наслідків при здійсненні несанкціонованого доступу є місцезнаходження компанії – оператора мобільного зв'язку, де встановлені апаратно-технічні і програмні засоби обробки інформації у мережі мобільного зв'язку, що фіксують сліди технічного доступу [43, с. 158].

Згідно з позицією Г. В. Семенова злочини у сфері мобільних телекомунікацій можуть вчинятись тільки в зоні покриття оператора зв'язку, під якою розуміється територія, у межах якої забезпечується можливість підключення до системи мобільного зв'язку і користування її ресурсами [46, с. 80].

Розглядаючи місце здійснення несанкціонованого доступу при безпосередніх (прямих) способах, які найчастіше виражаються в шахрайському підключенні до мереж мобільного зв'язку і махінаціях з боку

працівників оператора зв'язку, варто наголосити, що місцем злочину у цих випадках є офіс і службові приміщення компанії-оператора мобільного зв'язку. Ця ситуація відрізняється тим, що місце скоєння злочину і місце настання шкідливих наслідків співпадають, а тому на практиці, їх набагато простіше визначити. Дослідження показали, що місцем підготовки та приготування знарядь злочину при прямих і видалених способах зазвичай є місце проживання або роботи злочинця і співучасників, «підпільна лабораторія», нелегальні ринки, мережа «Інтернет» [66, с.209].

Тимчасові показники обстановки несанкціонованого доступу виражаються в часі підключення до мережі мобільного зв'язку, тривалості неправомірного доступу, часі здійснення тих або інших кримінальних дій на різних етапах, і їх співвідношенні між собою. Вибір часу скоєння злочину багато в чому визначається відносною його сприятливістю для реалізації задуму злочинця і специфікою способу несанкціонованого доступу. На часовий чинник середовища злочинів у сфері мобільного зв'язку може впливати:

- робочий час компанії оператора мобільного зв'язку (у цей період доступне програмне забезпечення системи мобільного зв'язку, можливе укладення договору на надання послуг зв'язку шахрайським способом та інші дії);

- періоди позаштатних ситуацій (збої, помилки в роботі мережі мобільного зв'язку, якими може скористатися злочинець);

- терміни можливого доступу до послуг мобільного зв'язку (наприклад, при знаходженні в роумінгу рахунки від роумінгових партнерів компанії - оператора мобільного зв'язку поступають із затримкою до десяти днів, що дає можливість недобросовісному абонентові інтенсивно користуватися зв'язком не дивлячись на заборгованість; використання вкраденої або загубленої мобільної станції можливе до подачі письмової заяви від легального абонента про блокування телефону; період дії пільгового тарифу,

який в злочинних цілях може використовувати зловмисник, має тимчасові рамки і тому подібне).

Таким чином, речові, просторово-конструктивні і тимчасові чинники значно впливають на обстановку вчинення злочинів у сфері мобільного зв'язку, пов'язаних з несанкціонованим доступом. Проте середовище даних злочинних діянь не можна зводити до сукупності безпосередньо фізичних (простір, час) умов, в яких діяв злочинець. Воно охоплює ширше коло явищ, до яких можна віднести: 1) нормативно-правове регулювання діяльності оператора мобільного зв'язку; 2) організацію роботи системи мобільного зв'язку; 3) технологічний процес надання послуг мобільного зв'язку, правила роботи з абонентами; 4) систему захисту мережі мобільного зв'язку від несанкціонованого доступу; 5) склад, службове положення працівників, їх професійні і особисті якості, ділові і особисті зв'язки між ними; 6) наявність (відсутність) різного роду недоліків в діяльності оператора мобільного зв'язку, контролі, обліку, охороні системи мобільного зв'язку і т. ін.); 7) зв'язок між суб'єктом і предметом посягання, що забезпечує можливість доступу до нього.

Розглядаючи складові обстановки злочинів у сфері мобільного зв'язку, варто відзначити, що найважливішими серед них є технологічний процес надання послуг зв'язку і система його захисту від несанкціонованого доступу. Це пов'язано з тим, що специфічні умови діяльності оператора мобільних телекомунікацій багато в чому визначають механізм і спосіб вчинення злочинів, пов'язаних з несанкціонованим доступом.

Таким чином, констатуємо, що під час аналізу способів вчинення злочинів у мережах мобільних телекомунікацій за технічними ознаками їх можна класифікувати таким чином:

1) щодо проникнення у систему мобільного зв'язку:

- відсутність належної аутентифікації або модулів захисту ідентифікаційних даних легальних користувачів на рівні ефірного радіоінтерфейсу і мобільного телефону;

- відсутність частої зміни ідентифікаційних даних легальних користувачів. Відповідно до вище викладеного, можна дійти висновку, що абсолютно захищених від неправомірних дій з технічної точки зору стандартів не буває. Крім того, загальною причиною є не стільки недосконаліть алгоритмів захисту та їх апаратного забезпечення, а й можливість оператора у робочому режимі змінювати ідентифікатори легальних абонентів. Найефективніше, звісно, боротися з крадіжками телефонів силами їхніх виробників. Розроблені останніми роками телефони від провідних виробників уразливіші до не досить кваліфікованої зміни програмного забезпечення і після перепрошивки кустарними засобами можуть працювати з помилками. Для смартфонів із гнучкішими операційними системами, які допускають самостійну установку програмного забезпечення,розроблено додатки, що самостійно блокують апарат у разі несанкціонованої зміни SIM-карти й навіть надсилають повідомлення про це на заздалегідь визначений номер.

Крім того, паралельно потрібно буде зобов'язати операторів відмовляти в реєстрації в мережах не лише телефонам із «чорних списків», а й трубкам, чиї коди не значаться в базі даних легально завезених телефонів. Запуск ефективного механізму тотального контролю українського IMEI-простору потребуватиме також реєстрації кодів усіх наявних трубок і, можливо, прив'язки їх до номерів телефонів. Це дасть можливість виявити власників телефонів з однаковим IMEI і «приводити їх у відповідність». Цей факт має слугувати введенню практики реєстрації паспортних даних власників пакетів наперед оплаченого сервісу. Проте дані нововведення обмежуватимуть конституційні права особи, що є недопустимим, а тому є неможливими без внесення змін до Конституції України [1].

На думку МВС, необхідно також внести зміни в положення про комісійну торгівлю: заборонити суб'єктам підприємницької діяльності приймати на комісію телефони без надання комітентом підтверджуючих документів на право власності, а також документа, який засвідчує особу.

Крім того, пропонується підсилити відповідальність підприємців, котрі не складають акти комісійного продажу та не фіксують анкетні дані комітентів.

Виробникам слід ускладнити процедуру зміни програмного забезпечення, зробивши її доступною лише для спеціально авторизованих сервіс-центрів. Або змінити програмне забезпечення й апаратну частину нових моделей так, аби IMEI розташовувався в незмінній ділянці пам'яті чи взагалі в окремому її модулі. Проте виробники – не мобільні оператори, і вказівками МВС зобов'язати їх до цього неможливо.

Так, за оцінками фахівців, якщо прийняти повний захист від несанкціонованого доступу за 100, то можна вважати, що базові аналогові системи захищені лише на 5%. При використанні аутентифікації ступінь захищеності підвищується до 80% [28];

– відсутність у оператора інформації про платоспроможність клієнта. Реалізація мобільних телефонів в кредит і відсутність у оператора повної інформації про клієнта обумовлюють доступ до мережі мобільного зв'язку способом – контрактного шахрайства. Ці дії поширені у регіонах, де компанії реалізують телефонні апарати в кредит без перевірки даних, що засвідчують особу [63]. Сьогодні оператори продають мобільні телефони у кредит, крім того укладаючи договір на надання послуг зв'язку лише на підставі паспортних даних, що, безумовно, сприяє вчиненню підписного шахрайства. Окрім того, у більшості операторів існують кредитні тарифні плани, що є додатковим чинником до збільшення числа випадків підписного шахрайства;

2) користування ресурсами мобільного зв'язку:

– відсутність статистичних даних щодо поведінки кожного з легальних абонентів і варіантів зміни вказаної поведінки залежно від того або іншого виду кримінального доступу до мережі мобільного зв'язку;

– відсутність можливості щоденної перевірки трафіку легальних абонентів (головним чином роумерів) на наявність незаконної абонентської активності;

– відсутність ведення статистичного портрету (профілю) користувача в рамках мережі підключення і роумінгу;

– відсутність програм детектування, що дозволяють відстежувати кримінальну абонентську активність [86].

Отже, вищенаведені чинники обумовлюють кримінальні дії з користування ресурсами мобільного зв'язку та вказують на відсутність програмно-апаратних комплексів з виявлення злочинів, які вчиняються у мережах мобільних телекомунікацій.

За результатами такого аналізу ми дійшли наступного висновку: система мобільного зв'язку, як сукупність складових її елементів, що детермінують кримінальні дії щодо доступу до неї і користування її ресурсами, відіграє вирішальну роль у формуванні способів вчинення злочинів у мережах мобільних телекомунікацій.

Слід також підкреслити, що система мобільного зв'язку як основоположний елемент обстановки даних злочинів існує в певних просторових межах. Тим самим, варто перейти до питання про місце вчинення злочинів у мережах мобільних телекомунікацій.

При дослідженні криміналістичних категорій «обстановка вчинення злочину» і «місце вчинення злочину» розглядаються разом. Подібна закономірність не викликає сумнівів, оскільки обстановка вчинення злочину як фрагмент об'єктивної реальності має властивість бути протяжною і знаходиться у постійному русі і розвитку, тобто існує у певних просторово-часових рамках. Зважаючи на це, абсолютно справедливо, що категорії «місце» і «обстановка» нерозривні одна від одної. Кожне місце вирізняється своєю обстановкою, кожна обстановка характеризує певне місце» [93, с. 145].

Тобто, визначення поняття «обстановка вчинення злочину» безпосередньо пов'язане з його просторово-часовою локалізацією і головним чином з визначенням і розмежуванням понять «місце події» і «місце злочину». Ми вважаємо, що підхід до визначення обстановки вчинення злочину і його просторової локалізації залежить від характеру певних

криміналістичних завдань і мети при вивченні зазначених категорій злочинів. До того ж, вивчення місця вчинення злочину криміналістичною тактикою полягає у вирішенні завдань оптимізації і підвищення ефективності криміналістичного дослідження обстановки місця злочину, зокрема розв'язання тактичних завдань при провадженні певних слідчих дій і використанні отриманих даних під час розслідування. На підставі того, що місце вчинення злочину локалізувалося в просторово обмеженій ділянці, у межах якої був вчинений злочин або виявлені його матеріальні наслідки, що, безсумнівно, дало результат при визначенні тактики огляду, обшуку і таке інше, відповідно до цього, слід вважати, що у цьому разі мова йде про місце події [90, с. 198].

З врахуванням викладеного, під місцем вчинення злочину розуміють простір, у межах якого під впливом різних об'єктивних і суб'єктивних чинників склалася специфічна система явищ, процесів і станів, яка обумовлює особливості скоюваних на цій ділянці простору злочинів [87, с.142].Об'єктивними чинниками є:

– стандарт мобільного зв'язку, в якому працює оператор і його особливості, тому, що принципи організації мережі у різних стандартах відрізняються, що обумовлює спосіб несанкціонованого доступу;

– покоління мобільного зв'язку, що впливає на можливість надання абонентам послуг різного класу і на вибір механізму несанкціонованого доступу;

– нормативно-правове регулювання розвитку телекомунікаційного ринку, надання послуг мобільного зв'язку, що визначає принципи організації мережі мобільного зв'язку і порядок надання послуг;

– наявність і технічний стан засобів обліку, захисту інформації і охорони мережі мобільного зв'язку від несанкціонованого доступу.

До суб'єктивних чинників можна віднести:

– відсутність або недосконалість системи захисту мережі мобільного зв'язку від несанкціонованого доступу;

– недоліки технологічного процесу у наданні послуг мобільного зв’язку;

– недосконаліть правил роботи з абонентами;

– помилки у роботі співробітників компанії - оператора зв’язку;

– помилки в програмному забезпеченні системи зв’язку;

– порушення правил роботи з захищеною законом комп’ютерною інформацією оператора зв’язку;

– психологічні умови роботи співробітників компанії – оператора мобільного зв’язку.

Щодо цього різновиду злочинів варто підкреслити, що суттєве значення для визначення місця вчинення злочинів у мережах мобільних телекомунікацій має територія, на яку функції даної системи розповсюджуються. Тобто, місце вчинення злочину не має чітко визначених меж просторового характеру, а пов’язане з функціональною територією системи мобільного зв’язку і її технічними особливостями [88], точніше із зоною обслуговування даної системи.

Підводячи підсумок вищесказаному, слід зазначити, що криміналістично важливими елементами злочинної події несанкціонованого доступу до мереж стільникового радіотелефонного зв’язку, є предмет злочинного посягання (елементи мережі стільникового зв’язку; послуги зв’язку; інформація, що знаходиться у мережі стільникового зв’язку); способи підготовки, вчинення і приховання, слідова картина злочину; дані про особу злочинця; обставини, що сприяючи вчиненню злочину. Закономірно взаємозв’язані один з одним, ці елементи утворюють криміналістичну характеристику злочину, тобто інформаційну модель, що є основою методики розслідування злочинів, пов’язаних з несанкціонованим доступом до мереж зв’язку і призначену для організації роботи спрямованої на виявлення, розкриття і розслідування даних суспільно-небезпечних діянь.

Висновки до Розділу 2

Під способом вчинення злочинів у мережах мобільних телекомунікацій слід розуміти систему дій з підготовки, вчинення і приховування несанкціонованого доступу до системи мобільного зв'язку, користування його ресурсами і (або) наданні такої можливості іншим особам, об'єднаних загальною цільовою спрямованістю – несанкціоноване користування ресурсами системи мобільного зв'язку без їх належної оплати і (або) реєстрації, визначених суб'єктивними і об'єктивними чинниками.

Способи вчинення злочинів у мережах мобільних телекомунікацій, як певна сукупність дій злочинця, спрямованих на здійснення вольового акту – досягнення поставленої мети, визначаються їх мотивацією. Вони характеризуються вельми кваліфікованими і досить складними діями і прийомами приховування, що суттєво ускладнює процес виявлення, розкриття і розслідування даної групи злочинів. Для досягнення визначеної мети у більшості випадків злочинцями широко використовуються різноманітні кількісні і якісні комбінації декількох основних способів.

Характеризуючи обстановку вчинення злочинів у мережах мобільних телекомунікацій як елемент криміналістичної характеристики, слід звернути увагу на те, що особливістю дій, які входять в дану категорію, є їх опосередкування засобами комп'ютерної техніки даної системи, оскільки сукупність мобільних телефонів, базових станцій і комутаторів є комп'ютерною мережею, що виконує специфічні завдання.

Особливістю способів вчинення будь-яких злочинів у мережах мобільних телекомунікацій, як, втім, й інших злочинів, вчинення яких опосередковано засобами комп'ютерної техніки, є те, що вони обумовлюються специфікою побудови і функціонування технічної системи.

Вирішальну роль у формуванні способів вчинення злочинів у мережах мобільних телекомунікацій відіграє система мобільного зв'язку, як

сукупність складових її елементів, які детермінують кримінальні дії щодо доступу до неї і користування її ресурсами.

РОЗДІЛ 3. ОРГАНІЗАЦІЯ ТА ПРОВЕДЕННЯ СЛІДЧИХ ДІЙ У СПРАВАХ ЗЛОЧИННОГО ПОСЯГАННЯ У СФЕРІ МОБІЛЬНИХ ТЕЛЕКОМУНІКАЦІЙ

3.1. Перевірка інформації та початок досудового розслідування щодо втручання у роботу мереж мобільного зв'язку

Початок досудового розслідування є початковою і однією з найважливіших стадій кримінального процесу. Кримінальне процесуальне значення даної стадії полягає у тому, що тільки після внесення відомостей до ЄРДР у встановленому законом порядку допускається провадження слідчих дій та застосування до осіб заходів процесуального примусу.

Відповідно до ст. 214 КПК України слідчий, прокурор, інша службова особа, уповноважена на прийняття та реєстрацію заяв і повідомлень про кримінальні правопорушення, зобов'язані прийняти та зареєструвати таку заяву чи повідомлення. Відмова у прийнятті та реєстрації заяви чи повідомлення про кримінальне правопорушення не допускається.До Єдиного реєстру досудових розслідувань вносяться відомості про:

1) дату надходження заяви, повідомлення про кримінальне правопорушення або виявлення з іншого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення;

2) прізвище, ім'я, по батькові (найменування) потерпілого або заявника;

3) інше джерело, з якого виявлені обставини, що можуть свідчити про вчинення кримінального правопорушення;

4) короткий виклад обставин, що можуть свідчити про вчинення кримінального правопорушення, наведених потерпілим, заявником чи виявлених з іншого джерела;

5) попередня правова кваліфікація кримінального правопорушення з зазначенням статті (частини статті) закону України про кримінальну відповідальність;

6) прізвище, ім'я, по батькові та посада службової особи, яка внесла відомості до реєстру, а також слідчого, прокурора, який вніс відомості до реєстру та/або розпочав досудове розслідування;

7) інші обставини, передбачені положенням про Єдиний реєстр досудових розслідувань.

У Єдиному реєстрі досудових розслідувань автоматично фіксується дата внесення інформації та присвоюється номер кримінального провадження.

Слідчий невідкладно у письмовій формі повідомляє прокурора про початок досудового розслідування, підставу початку досудового розслідування та інші відомості, передбачені частиною п'ятою цієї статті.

Якщо відомості про кримінальне правопорушення до Єдиного реєстру досудових розслідувань внесені прокурором, він зобов'язаний невідкладно, але не пізніше наступного дня, з дотриманням правил підслідності передати наявні у нього матеріали до органу досудового розслідування та доручити проведення досудового розслідування.

Про вчинення кримінальних дій у мережі мобільного зв'язку можуть свідчити:

– відсутність та швидке зменшення грошових коштів на рахунку легального абонента чи невиконання зобов'язань зі сплати роумінгових з'єднань;

– при одній з позначених вище обставин, невідомі легальному користувачу номери в трафіку використання його мобільного телефону (найчастіше міжміські і міжнародні з'єднання);

– за інших рівних умов, часте блокування роботи мобільного телефону і інші збої в роботі (особливо якщо це відбувається в зоні обслуговування оператора, а також з урахуванням місцеположення абонента);

– зміна в режимі використання мережі зв'язку, зафіксована персоналом компанії, системою захисту компанії (наприклад, фіксація з'єднань одного і того ж мобільного телефону з різних «сот», які не межують з мінімальною розбіжністю в часі);

– відсутність грошових коштів при активації передплатної карти;

– відомості про кримінальні дії з доступу до системи мобільного зв'язку та інше.

Безумовно, запропонований перелік є умовним і має орієнтуючий характер. Не зважаючи на це, очевидно, що достатніми для початку досудового розслідування за статтями 190 і 192 КК України будуть дані, які вказують на об'єкт і елементи об'єктивної сторони (головним чином, злочинний результат). Крім того не вимагається встановлення достатніх даних, які вказують на дії злочинця й інші елементи об'єктивної сторони.

Настадії відкриття провадження у цій категорії злочинів варто вирішити дві групи завдань – загальні і спеціальні.

До загальних відносяться завдання, які випливають з положень кримінального-процесуального закону і виникають незалежно від характеру і об'єму початкової інформації, необхідної для законного і обґрунтованого вмотивованого рішення у справі, наприклад: чи є повідомлення про злочин приводом для початку досудового розслідування; чи містяться в зверненні відомості про ознаки злочину та інше.

Спеціальні завдання доповнюють загальні, проте через свою специфіку вони є різними для кожної справи. Вони залежать від наявної інформації, ступеня її визначеності на конкретному етапі, джерел її отримання та цілого ряду інших об'єктивних і суб'єктивних чинників (обставин).

Внаслідок зазначених обставин, у момент прийняття уповноваженими особами повідомлення про вчинення злочинів у мережах мобільних

телекомунікацій складаються такі типові початкові ситуації, які за критерієм інформаційної визначеності можна розділити на такі групи:

І. Ситуації, в яких повідомлення про злочин і матеріали, що додаються до повідомлення, містять достатні дані для вирішення питання внесення відомостей до ЄРДР:

а) заявники (оператор мобільного зв'язку) власними силами виявили факт кримінального доступу до мережі мобільного зв'язку і користування її ресурсами, інші ознаки злочинів, які вчинюються у мережах мобільних телекомунікацій, виявили дані підозрюваної особи і заявили про це в правоохоронні органи.

Компанії мобільного зв'язку здійснюють періодичний моніторинг абонентської активності і стану абонентських рахунків користувачів. В даному випадку використовуються спеціальні апаратно-програмні комплекси, які дозволяють розпізнати нетипову для того або іншого абонента поведінку (так звана аномальна абонентська активність) і виявити вчинення кримінальних дій на ранніх етапах. Як правило, служба безпеки компанії проводить власну перевірку випадків аномальної активності у мережі мобільного зв'язку, після проведення якої, навіть у разі виявлення ознак злочину, компанія-оператор задля збереження професійного іміджу і недопущення розголошування конфіденційної інформації, не звертється до правоохоронних органів, погашаючи збитки легальному абоненту.

У ситуаціях, коли про вчинення кримінальних дій оператор повідомляє в правоохоронні органи, крім заяви посадовців компанії, передаються і матеріали перевірки. Як свідчить аналіз кримінальних справ, рішення оператора мобільного зв'язку про звернення до правоохоронних органів із заявою про відкриття кримінального провадження безпосередньо залежить від того, чи встановлено службою безпеки оператора особу, підозрювану у вчиненні кримінальних дій. Тим самим зазначена слідча ситуація є найбільш поширеною [89, с. 148].

Типовими завданнями, що виділяються у всіх ситуаціях, є дії з перевірки в повідомленні:

– ознак вчинення злочинів даної категорії або приготування до їх вчинення;

– наявності причинного зв'язку між кримінальними діями і наслідками, що наступили;

– характеру і попереднього розміру шкоди, заподіяної у результаті злочинних дій, і інших суттєвих для розслідування обставин, що фігурують у повідомленні;

– участі або неучасті особи (осіб), зазначених в заяві, у вчиненні даного злочину;

– місцезнаходження слідів і засобів вчинення злочинів;

– інших значущих для відкриття провадження обставин.

При затриманні злочинця на місці вчинення злочину слід вилучити: мобільний телефон, документи, які засвідчують його особу, електронні і паперові записники, що є у затриманого, та інші.

Крім того потрібно виключити можливість втрати доказової інформації, забезпечити умови, при яких злочинець не зможе позбавитися речових доказів (передусім це мобільний телефон), або знищити їх (при падінні, попаданні вологи та інших випадках мобільний телефон може вийти з ладу і можливість отримання доказової інформації буде зведена до нуля).

б) заявники (оператор мобільного зв'язку) власними силами виявили факт кримінального доступу до мережі мобільного зв'язку і користування її ресурсами та(чи) інші ознаки злочинів, які вчинюються у мережах мобільних телекомунікацій, проте не змогли самі встановити вину особи (осіб), зважаючи на це звернулися у правоохоронні органи із заявою. Дана ситуація схожа з попередньою.

3.2. Проведення окремих слідчих дій при розслідуванні злочинів у сфері мобільних телекомунікацій

Беручи до уваги специфіку вчинення злочинів у мережах мобільних телекомунікацій, встановлення обставин, які входять до предмету доказування, ускладнено необхідністю кваліфікації кількох складах злочинів, не пов'язаних між собою кримінально-правовими ознаками. Зазначені обставини встановлюються під час розслідування шляхом проведення процесуальних (головним чином слідчих) дій, загальна тактика яких, при розслідуванні даної категорії злочинів, мало чим відрізняється від традиційних положень, зокрема, у галузі розслідування злочинів у сфері комп'ютерної інформації, які досить повно і детально викладені в криміналістичній літературі [91, с. 43].

Огляд є однією з найбільш поширених слідчих дій в структурі методик розслідування різних категорій злочинів, у процесі якого розв'язується цілий ряд планових завдань розслідування. Досить часто, весь хід розслідування злочину залежить від своєчасності і результативності проведення огляду. Відповідно до ст. 237 КПК України з метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення слідчий, прокурор проводить огляд місцевості, приміщення, предметів та документів [80, с. 214].

З цього різновиду злочинів місцем події буде не ділянка місцевості (у його традиційному розумінні), а елементи апаратно-програмного комплексу системи мобільного зв'язку «всередині» яких був вчинений злочин або виявлені його матеріальні наслідки. Проводячи огляд у цій категорії злочинів слідчий не може обмежитися лише безпосереднім сприйняттям об'єктів і явищ. Кожен об'єкт пізнання вимагає спеціальної технології дослідження, особливої методики вивчення і обробки [78, с. 135].

Обумовлюється це тим, що протиправна діяльність може вчинятися практично в будь-якій точці зони покриття оператора мобільного зв'язку, проте злочинний результат обов'язково буде відображений в апаратно-технічних і інформаційно-програмних засобах даної мережі. Зважаючи на це виникає нагальна потреба використовувати спеціальні програмні і технічні засоби для сприйняття інформації мобільного зв'язку, яка знаходиться у середині мережі.

Отже, використання програмно-технічних засобів веде до активного інтерактивного обміну інформацією з елементами апаратно-технічної підтримки мережі мобільного зв'язку, що вимагає знань складних технічних подробиць побудови і функціонування як сфер мобільного зв'язку в цілому, так і окремих її елементів [53, с. 193].

Специфічні об'єкти, завдання, коло присутніх осіб та осіб, які беруть участь в огляді, методи його проведення приводять до появи низки особливостей слідчої дії з цієї категорії злочинів. Результати проведених досліджень показали, що справах, пов'язаних з розкриттям і розслідуванням кримінальних дій у мережах мобільного зв'язку типовими об'єктами огляду є:

1) приміщення, автотранспорт і інші місця, де здійснювалося зберігання, клонування мобільних телефонів, виробництво інших радіоелектронних пристроїв, підробка документів.

У процесі огляду згадуваних об'єктів можуть бути виявлені:

- викрадені у легального користувача, клоновані мобільні телефони;

- телефони, допрацьовані на технічному і програмному рівні для здійснення сканування ідентифікаційних даних (номерів) легальних користувачів (ESN, MIN і ін.);

- скануючи технічні пристрої, засоби комп'ютерної техніки злочинця;

- пристрої мікроелектроніки (плати, схеми і т. ін.), паперові носії (рукописні записи, роздруківки);

2) предмети, пов’язані з вчиненням злочинів у мережах мобільних телекомунікацій:

- мобільний телефон злочинця;

- інші радіоелектронні пристрої;

- засоби комп’ютерної техніки злочинця і оператора мобільного зв’язку, паперові носії і таке інше [77].

При проведенні огляду предметів, пов’язаних з кримінальними діями у мережах мобільного зв’язку можуть бути виявлені:

- сліди пальців рук, мікрочасток і інших предметів на клавіатурі, всередині мобільного телефону (інших радіоелектронних пристроях), на поверхні комп’ютера і його пристроях, змінних носіях інформації, паперових носіях і т. ін.;

- сліди вчинення злочину у вигляді інформації в телефоні [75].

У протоколах оглядів, як правило, відображалися марка телефону, серійний номер, запрограмовані абонентські телефонні та ідентифікаційні номери, занесені злочинцем в «електронний записник» телефону, а також дії слідчого і спеціаліста, спрямовані на отримання даної інформації; сліди на магнітних, оптичних і інших носіях комп’ютерної техніки (програмне забезпечення, за допомогою якого здійснюється сканування, декодування, запис і зберігання необхідних даних, підробка документів та інші супутні злочини, продукти застосування цих спеціальних програм тощо) [6].

Підготовка до огляду місця події у справах вказаної категорії включаєрозв’язання ряду організаційних питань як загальних для будь-якого слідчого огляду, так і специфічних, прийнятних тільки для даної категорії злочинів. До загальних відноситься запрошення понятих, інструктаж учасників огляду, до специфічних – обов’язкова участь в огляді спеціалістів у галузі інформаційних технологій, а також вирішення питання про фізичні і інтелектуальні можливості понятих належним чином засвідчити факт проведення, хід і результати слідчого огляду та інше. [73, с. 46].

Іншим важливим питанням залучення понятих є наявність у останніх певних знань і навичок у галузі обчислювальної техніки і інформаційних технологій, тому, що вони мають чітко усвідомлювати мету того, що відбувається, і сенс окремих дій, у випадках, коли об'єктами слідчої дії є засоби апаратно-технічної підтримки системи мобільного зв'язку.

В даному випадку, доцільно при виборі понятих орієнтуватися на студентів останніх курсів вищих навчальних закладів радіотехнічних спеціальностей, а також співробітників науково-дослідних інститутів.

Специфіка функціонування мобільних телефонів, а також інших апаратно-технічних засобів підтримки мережі мобільного зв'язку та інших аналогічних об'єктів слідчого огляду полягає в тому, що їм протипоказані високі і низькі температури, механічні дії, вологість, а також дія електричних і магнітних полів. Також, при вилученні мобільного телефону не можна відключати його. При подальшому включенні можуть бути потрібні коди блокування, необхідні для роботи телефону і, відповідно, повноцінного дослідження його інформаційного змісту.

Важливе значення мають коди блокування SIM-карти. При кожному включенні апарату потрібне введення PIN-коду для активації SIM-карти. У разі неправильного набору PIN-коду більше трьох разів, для розблокування SIM- карти потрібен вже інший код – PUK. Якщо відповідне число разів код PUK також вводиться невірно, то SIM-карта блокується остаточно і її розблокування стає практично неможливим. Зважаючи на це, втрачається можливість дослідження важливої для слідства інформації у пам'яті SIM-карти.

У даному випадку, слідчому варто враховувати, що PIN-код може мінятися користувачем, PUK-код постійний. Первинний PIN-код, а також PUK-код містяться в базі даних компанії оператора мобільного зв'язку, стосовно чого доцільно на підготовчій стадії огляду одержати ці коди блокування для мобільного телефону, який є об'єктом огляду.

В процесі огляду мобільного телефону слідчий може зустрітися з іншими різновидами блокування. Зокрема, окремими паролями можуть захищатися: послуга заборони викликів (всіх вихідних викликів, міжнародних викликів, всіх вхідних викликів тощо), голосова пошта і таке інше.

У будь-якому випадку, якщо слідчий у порядку огляду стикається з блокуванням певної інформації в мобільному телефоні, а її власник і оператор відмовляються надати відповідні паролі, або у слідчого відсутні підстави вважати їх достовірними, виникає потреба призначення експертизи, оскільки для зчитування інформації з такого телефону важливі спеціальні знання у галузі програмування. Огляд мобільного телефону в даному варіанті буде тільки «зовнішній», з метою ідентифікувати його для подальшого вилучення інформації.

Загальний порядок огляду мобільного телефону умовно можна розділити на два етапи:

1) зовнішній огляд (під час огляду місця події) з фіксацією зовнішньої будови і стану (статична стадія огляду). Зовнішній огляд труднощів, як правило, на практиці не викликає.

2) огляд і фіксація інформаційного змісту (динамічна стадія огляду). Дослідження інформаційного змісту здійснюється за допомогою меню користувача мобільного телефону.

Інформаційний вміст мобільного телефону має в собі великий об’єм інформації. Тим самим, її дослідження і фіксація може зайняти тривалий час. Більш того, ряд складових інформаційного змісту телефону (дані абонента) відносяться до конфіденційної інформація власника абонентської станції (текстові SMS і голосові повідомлення), з якого вони відправлені, дата і час отримання повідомлення; телефонні номери з відповідними іменами їх власників, зміст органайзера і т. ін.) і може бути оглянуто та вилучено у порядку обшуку і виїмки [67, с. 110].

Не менш важливими є процедура обшуку та виїмки. При розслідуванні даної категорії злочинів обшук і виїмка є одними з найбільш затребуваних слідчих дій, направлених на встановлення обставин, що входять в предмет доказування [61, с.209]. В процесі підготовки до обшуку (на підготовчій стадії) особливе значення має збирання шляхом проведення оперативно-розшукових заходів і слідчих дій наступної орієнтуючої і доказової інформації:

1) відомості про місце проведення обшуку (зокрема точна адреса і призначення будови (житлове, виробниче, торгове, офісне приміщення), його планування, призначення кожної з кімнат, наявність підсобних приміщень, підвалів, горищ, кількість вікон, дверей, інші відомості);

2) відомості про те, чи знаходиться місце проведення обшуку або виїмки в зоні дій оператора мобільного зв'язку, у мережі якого передбачається наявність кримінальних дій;

3) відомості про наявність індустріальних і інших об'єктів, які є джерелами радіоперешкод в місці обшуку;

4) відомості, що характеризують апаратно-технічні засоби: мобільні телефони, монітори мобільного зв'язку, інші радіоелектронні засоби, засоби обчислювальної техніки, пристрої безперебійного живлення, роз'єми, з'єднання і інші об'єкти мікроелектроніки в обшукуваному приміщенні, призначення, зовнішній вигляд, розмірні характеристики, індивідуальні ознаки і таке інше.

5) відомості про наявність в апаратно-технічних засобах програмних або програмно-апаратних засобів захисту від несанкціонованого доступу;

6) відомості про використовувані телекомунікаційні засоби: з наявністю модему для зв'язку комп'ютерів через телефонну мережу, чи об'єднані декілька комп'ютерів в локальну мережу в середині організації, чи є сервер, чи є підключення до регіональної або глобальної мережі [27, с.81];

7) дані про особу, у якої проводиться обшук, осіб, які проживають разом з ним, професійні знання і навички з володіння вказаними вище

об’єктами, рід діяльності (зокрема, чи є він або його родичі співробітниками оператора, дилера мобільного зв’язку, установи, яка своєю діяльністю пов’язана з наданням послуг зв’язку, їх посада), риси характеру і таке інше [24, с.115].

Таким чином, успішний результат проведення обшуку в значній мірі визначається ретельністю і якістю його підготовки.

Особистий обшук затриманого. Так, при проведенні особистого обшуку затриманого за підозрою у вчиненні кримінальних дій у мережах мобільного зв’язку, потрібно звертати увагу на такі об’єкти: SIM-карти, мобільні телефони, інші засоби бездротового зв’язку, карти оплати послуг мобільного зв’язку, елементи мікроелектроніки, документи, що засвідчують особу, і електронні записники, документи, які дозволяють використання тих або інших радіоелектронних засобів, інші носії програмного і апаратно-технічного походження, а також інших документів, які мають відношення до предмету доказування у цій категорії справ.

А особливості обшуку за місцем проживання і роботи підозрюваних у справах даної категорії злочинів пов’язані, насамперед, з розширенням кола самих об’єктів. Часто мова йде про об’єкти, яким властива можливість швидкого і повного знищення [25, с.74].

При проведенні за місцем проживання і роботи підозрюваного об’єктами пошуку, як правило, є ті ж об’єкти, що й при особистому обшуку, а також:

1) засоби комп’ютерної техніки, модем, програматори, зокрема складові робочого місця підозрюваної особи, різного роду носії інформації, представленої у вигляді придатному для її автоматизованої обробки;

2) монітори мобільного зв’язку, скануючи технічні пристрої, інші радіоелектронні засоби;

3) допоміжні системи, які забезпечують нормальне функціонування апаратно-технічних засобів (пристрої безперебійного живлення і таке інше);

4) матеріали і обладнання, використовуване для клонування мобільних телефонів;

5) грошові кошти і майно, здобуте злочинним шляхом;

6) записи, що відносяться до роботи на засобах комп'ютерної техніки, графік робочого часу і графік часу присутності на робочому місці підозрюваної особи, а також інструкції про посадові обов'язки підозрюваної особи [29, с. 34].

При проведенні обшуку у приміщеннях організацій (операторів мобільного зв'язку, дилерів тощо) до об'єктів пошуку відносять: первинні облікові документи, використані для оформлення господарських операцій (договори, накладні, платіжні доручення, рахунки фактури і т. ін.); установчі документи, ліцензії, сертифікати, документи бухгалтерської звітності; технічна документація на використовуване обладнання; об'єкти, характерні для пошуку при проведенні інших видів обшуків [44, с. 204].

За наявності достатніх підстав вважати, що відомості, які мають значення для кримінальної справи, можуть міститися у повідомленнях телекомунікаційних сервісів, мова має йти не тільки про проведення обшуку мобільного телефону, а й про арешт поштово-телеграфних відправлень, їх огляд і виїмку у оператора мобільного зв'язку.

Метою цієї слідчої дії є: отримання додаткової доказової та іншої інформації, яка має значення для справи, запобігання обміну інформацією певних осіб між собою, а також забезпечення таємниці слідства. Технічні особливості телекомунікаційних сервісів систем мобільного зв'язку обумовлюють ряд специфічних тактичних рекомендацій окремого характеру при розслідуванні даної категорії злочинів, а саме:

а) проведення виїмки зазначених повідомлень, адресованих абоненту, у оператора мобільного зв'язку мало ефективно, тому, що у базі даних оператора зберігатимуться повідомлення, які не дійшли до абонента (відповідно зростає ефективність обшуку мобільного телефону (SIM-карти),

зважаючи, що повідомлення можуть бути збережені особою, яка відправляє (одержує) повідомлення);

б) якщо зазначені повідомлення посилаються на електронну пошту, то ефективність виїмки зростає, оскільки відправлення розміщується не тільки в комп'ютері особи, яка отримала повідомлення, а й на сервері провайдера або безкоштовному поштовому Інтернет-сервері, який одержує дане повідомлення. Подібний висновок можна зробити і для повідомлень голосовою поштою, оскільки вони зберігаються системою оператора мобільного зв'язку до тих пір, поки користувач їх не видалить [17, с. 83].

в) велике значення для успішного проведення обшуку і виїмки мають дані щодо активації абонентом тих чи інших телекомунікаційних сервісів (це завдання може бути вирішене у порядку оперативно-розшукових заходів, або шляхом направлення офіційного запиту слідчого оператору мобільного зв'язку);

г) при прийняттісудомрішення про накладення арешту на повідомлення телекомунікаційних сервісів оператора мобільного зв'язку і їх виїмку в ухвалі має бути зазначені підстави проведення цієї процесуальної дії, відомості про абонентській номер і особу, за якою він закріплений, дата арешту, порядок інформування слідчого про повідомлення); залежно від слідчої ситуації може бути зазначено в ухвалі на існування нагальної потреби блокувати деякі команди управління телекомунікаційним сервісом (переадресація, видалення) і забезпечити зберігання телекомунікаційних повідомлень у режимі конфіденційності і цілісності. Ухвала направляється відповідному оператору мобільного зв'язку, а також організаціям, які надають послуги доступу в інформаційні мережі, через які доставляється повідомлення з (на) абонентську рухому станцію [85, с. 14];

д) специфіка об'єктів виїмки і обшуку робить необхідним забезпечити участь у обшуку спеціаліста головним чином інженера з засобів зв'язку або мережевого обслуговування [58, с. 124];

є) суттєвою особливістю обшуку мобільного телефону є те, що слідчий, як правило, не завжди може оцінити на місці значення інформації, що виявляється, оскільки по-перше, він зіштовхується з великим об'ємом персональних даних і технічних налаштувань, і, по-друге, вона представлена в спеціальному вигляді, для сприйняття якого необхідні певні спеціальні знання, а іноді спеціальні апаратні і програмні засоби[60, с. 159].

ж) обшук (виїмка), зняття копій і роздруківка із затриманих телекомунікаційних повідомлень проводиться у присутності представника оператора мобільного зв'язку (або тієї організації, яка здійснює доступ в Інтернет), понятих з числа працівників даної організації. Крім того, поняті розписуються на всіх роздруківках інформації, отриманих під час обшуку (виїмки), які оформляються як додатки до протоколу слідчої дії;

з) залежно від змісту затриманих повідомлень, вони можуть бути вилучені шляхом копіювання змісту на магнітні носії комп'ютерної інформації. У даному випадку ще на підготовчій стадії огляду, обшуку (виїмки) варто підготувати апаратно-технічні засоби зчитування і зберігання інформації, що вилучається, набір яких варто заздалегідь погодити зі спеціалістом, а також переносні накопичувачі інформації (флеш пам'ять, змінні та зовнішні жорстки диски, диски щільного запису Zip, DVD і таке інше).

і) у випадках, коли планується огляд вилучених повідомлень, у протоколі виїмки доцільно наголосити перші слова тексту, останні фрази, номер (та інші дані, які дозволяють проводити ідентифікацію) абонента, який послав повідомлення. Також наголошується, що дане повідомлення скопійоване на електронний носій, вказуються зовнішній вигляд, спосіб упаковки, вигляд і текст відтиснення друку.

Висновки до Розділу ІІІ

До групи ситуацій, у яких повідомлення про злочин і матеріали, що додаються, містять дані для внесення відомостей до ЄРДР відносять наступні: а) заявники (оператор мобільного зв'язку) власними силами виявили факт кримінального доступу до мережі мобільного зв'язку і користування її ресурсами, інші ознаки злочинів, які вчинюються у мережах мобільних телекомунікацій, встановили дані підозрюваної особи і заявили про це у правоохоронні органи; б) заявники (оператор мобільного зв'язку) власними силами виявили факт кримінального доступу до мережі мобільного зв'язку і користування її ресурсами та інші ознаки злочинів, які вчинюються у мережах мобільних телекомунікацій, проте не змогли самі встановити вину особи, зважаючи на це звернулися у правоохоронні органи із заявою; заявники (потерпілі користувачі).

З метою підвищення ролі понятих у провадженні слідчих дій по даній категорії справ доцільно, при вирішенні питання про їх залучення, орієнтуватися на студентів останніх курсів вищих навчальних закладів радіотехнічних спеціальностей, а також співробітників науково-дослідних інститутів подібного профілю.

Об'єкти обшуку, які можуть мати значення при розслідуванні злочинів у сфері мобільних телекомунікацій можуть бути умовно розподілені на такі три групи: а) апаратно-технічні засоби (мобільний телефон, скануючи технічні пристрої, монітори мобільного зв'язку, засоби комп'ютерної техніки і т. ін.); б) комп'ютерна інформація, яка має відношення до розслідуваних злочинів; в) паперові носії.

ВИСНОВКИ

Аналіз ситуації свідчить, що поява і зростання кримінальних проявів в мережах мобільного зв'язку українських операторів прямо залежить від ряду чинників, серед яких, передусім, варто відзначити: швидкі темпи розвитку бездротових засобів зв'язку; прогалини правового регулювання у сфері інформаційної безпеки; недосконалість засобів інформаційної безпеки сфер мобільного зв'язку та активне використання кримінальним світом сучасних досягнень науки і техніки.

Дані, що характеризують стан і динаміку злочинів у сфері мобільних телекомунікацій, та збитки від них неоднозначні й уривчасті. Потерпіла сторона (оператор мобільного зв'язку), бажаючи зберегти професійний імідж і конфіденційність відомостей, що стосуються її діяльності, рідко звертається в правоохоронні органи із заявою про факт вчинення злочинів у їх мережі і вважає за краще не публікувати дані про заподіяний їм збиток і кількість зафіксованих службою безпеки випадків неправомірного доступу до мережі і користування її ресурсами.

Накопичення такої інформації в правоохоронних органах теж має ряд труднощів, зокрема: відсутність відповідних криміналістичних обліків; внутрівідомча роз'єднаність слідчих і оперативних апаратів; закритий характер ряду відомостей і їх джерел; пасивність низових підрозділів у наповненні баз даних інформацією. Цим зумовлюється високий рівень латентності даного виду злочинів.

Специфіка середовища, та обумовлені нею кримінальні дії в мережах мобільного зв'язку призвели до того, що сучасна система окремих криміналістичних методик не може задовольнити потреби практики боротьби з даним видом злочинів та вимагає розробки самостійної криміналістичної методики розслідування злочинів у сфері мобільних телекомунікацій.

При виділенні загальних ознак, які дозволяють віднести злочини у сфері мобільних телекомунікацій до певної класифікаційної групи

встановлено, що дії злочинця, спрямовані на отримання доступу до системи мобільного зв'язку залежать від даної системи і здійснюються «ззовні» або «всередині неї». Тим самим, загальні принципи технічної побудови системи мобільного зв'язку в цілому індукують свої властивості і визначають типові дії різного рівня, які виступають підставою для розробки криміналістичної класифікації злочинів у сфері мобільних телекомунікацій:

І. Дії спрямовані на доступ до системи мобільного зв'язку:

а) доступ до апаратно-технічних засобів підтримки системи мобільного зв'язку:

- незаконне заволодіння мобільним телефоном (ст. 185 – 187 КК України і інші способи заволодіння чужим майном, передбачені Особливою частиною КК України);

- створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361^1 КК України);

б) доступ за допомогою підключення мобільного телефону через допоміжні засоби підтримки системи мобільного зв'язку (центри роботи з клієнтами, дилери та ін.):

- умисне надання невірних даних шляхом представлення підроблених документів, що засвідчують особу, при укладенні договору на надання послуг мобільного зв'язку (ст. 358 КК України);

- створення фіктивної організації з метою неправомірного користування ресурсами (послугами) мобільного зв'язку і отримання майнової вигоди (ст. 205 КК України);

- здійснення без державної реєстрації, як суб'єкта підприємницької діяльності, що містить ознаки підприємницької та яка підлягає ліцензуванню, або здійснення без одержання ліцензії видів господарської діяльності, що підлягають ліцензуванню відповідно до законодавства, чи здійснення таких видів господарської діяльності з порушенням умов ліцензування, якщо це було пов'язано з отриманням доходу у великих розмірах (ст. 202 КК України,

на даний момент не є кримінально карним діянням, проте, такий вид порушень існує);

в) доступ до інформаційних засобів підтримки системи мобільного зв'язку – програмного забезпечення, даних і баз даних, що дозволяють системі мобільного зв'язку здійснювати свої функціональні можливості:

- несанкціоноване отримання ідентифікаційних даних користувачів за допомогою засобів комп'ютерної техніки, перепрограмування ідентифікаційних даних легальних користувачів, проникнення в комп'ютерну систему захисту для видалення механізмів захисту або переконфігурації системи базових станцій з метою використання (або подальшої реалізації) наявних в системі функціональних можливостей або з метою користування ресурсами мобільного зв'язку (ст. 362 КК України).

II. Дії спрямовані на користування ресурсами мобільного зв'язку (кримінальна абонентська активність): а) користування ресурсами мобільного зв'язку без її належної оплати і (або) реєстрації (ст. 190, 192 КК України).

Під злочинами у сфері мобільних телекомунікацій пропонується розуміти злочинну діяльність, до якої включається комплекс (система) не тільки кримінальних дій з користування ресурсами (послугами) системи мобільного зв'язку, а також і кримінальні дії щодо доступу до даної системи, передбачені самостійними складами Кримінального кодексу України.

На основі аналізу наукових концепцій сформульовано визначення способу вчинення злочинів у сфері мобільних телекомунікацій, під яким розуміється система дій з підготовки, вчинення і приховування даної категорії злочинів, що виражаються у несанкціонованому доступі до системи мобільного зв'язку, користуванні її ресурсами і (чи) наданні такої можливості іншим особам, об'єднаних загальною цільовою спрямованістю – несанкціоноване користування ресурсами системи мобільного зв'язку без їх належної оплати і (чи) реєстрації, мотивованих суб'єктивними і об'єктивними чинниками.

Для забезпечення якісного розслідування злочинів у сфері мобільних телекомунікацій слід конкретизувати дані про способи їх вчинення, типові мотиви і мету, обстановку і місце злочину, а також розробити теоретичні положення, що розкривають механізм слідоутворення у мережах мобільного зв'язку та виявлені його особливості.

Існують типові приводи і підстави відкриття кримінального провадження про злочини у сфері мобільних телекомунікацій. За критерієм інформаційної визначеності, виділяють групи типових ситуацій, що виникають в стадії початку досудового розслідування злочинів у сфері мобільних телекомунікацій, зокрема:

І. Ситуації, в яких повідомлення про злочин і матеріали, що додаються до них, містять достатні дані для відкриття провадження:

- заявники (оператор мобільного зв'язку) власними силами виявили факт кримінального доступу до мережі мобільного зв'язку і користування її ресурсами, інші ознаки злочинів у сфері мобільних телекомунікацій, виявили дані про підозрювану особу і заявили про це у правоохоронні органи;

- заявники (оператор мобільного зв'язку) власними силами виявили факт кримінального доступу до мережі мобільного зв'язку і користування її ресурсами і (чи) інші ознаки злочинів у сфері мобільних телекомунікацій, але не змогли самі встановити винну особу (осіб), зважаючи на це звернулися у правоохоронні органи із заявою;

- факт кримінального доступу до мережі мобільного зв'язку і користування ресурсами і (чи) інші ознаки злочинів у сфері мобільних телекомунікацій, винна особа (особи), були встановлені під час проведення оперативно-розшукових заходів.

В ході дослідження також виявлені характерні особливості підготовки і тактики проведення окремих слідчих дій, а також досліджено криміналістичні рекомендації з використання спеціальних знань у процесі розслідування злочинів у сфері мобільних телекомунікацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України від 28.06.1996 № 254к/96-ВР. [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

2. Про телекомунікації [Електронний ресурс]: закон України від 24.06.2004 – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1280-15

3. Про збір на обов'язкове державне пенсійне страхування [Електронний ресурс]: закон України від 26.06.1997 року – Режим доступу: http://zakon.rada.gov.ua/cgi-in/laws/main.cgi?nreg=1740-98-%EF

4. Про невідкладні заходи щодо забезпечення інформаційної безпеки України [Електронний ресурс] : указ Президента України від 21 березня 2008 року. Про рішення Ради національної безпеки і оборони України № 377/2008 – Режим доступу: http://www.crime-research.ru/library/UKAZ_P.htm

5. Правила надання та отримання телекомунікаційних послуг [Електронний ресурс] : затверджені постановою Кабінету Міністрів України від 11.04.2012. №295 – Режим доступу : http://zakon5.rada.gov.ua/laws/show/295-2012-%D0%BF

6. Про призначення та проведення судових експертиз та експертних досліджень : інструкція затв. наказ. №.1950/5 Мін'юсту України від 26 грудня 2012 [нова редакція] // Офіційний вісник України. – 2012. – №12. – Ст. 325.

7. Про встановлення одиниць обліку часу телефонних розмов абонентів стаціонарної телефонної мережі з абонентами мереж операторів стільникового рухомого зв'язку [Електронний ресурс] : наказ № 50 від 17.03.2004 Державного комітету зв'язку та інформатизації України – Режим доступу : http://www.ucrf.gov.ua/uk/doc/dkzi/1238058903/

8. «АМКУ визнав низку компаній монополістами на ринку

завершення телефонних з`єднання на мережі рухомого мобільного зв`язку» // газета «Хрещатик», [Електронний ресурс] : – Режим доступу: www.kreschatic.kiev.ua

9. Бахін В. П. Актуальні проблеми способу вчинення злочинів за умов істотної зміни характеру злочинної діяльності / В. П. Бахін, С. М. Зав'ялов // Науковий вісник НАВСУ. – К., 2015. – №2 – С. 178–182.

10. Бахін В. П. Взаємодія слідчого з фахівцями під час огляду місця події (збірник інформації про особу, що скоїла злочин) : [наук. – практ. рек.] / В. П. Бахін, О. О. Волобуєва – Донецьк, 2015. – 71 с.

11. Бахін В. П. Як розкриваються злочини [Криміналістика у питаннях та відповідях] / В. П. Бахін, В. Г. Гончаренко ; Ун-т ім. Т. Г. Шевченка. Юрид. фак-т. – К., 2006. – 198 с.

12. Бєляков К. І. Інформація в праві : теорія і практика : [монографія] / Бєляков К. І. ; Держ. наук.-досл. ін-т МВС України. – Київ : КВІЦ, 2016. – 117 с.

13. Близнюк І. Л. Інформаційна безпека України та заходи її забезпечення / І.Л. Близнюк // Науковий вісник НАВСУ. – 2003. – №5. – С. 206–214.

14. Близнюк І. Л. Способи вчинення злочинів з використанням комп'ютерних систем та мереж / І. Л. Близнюк, В. В. Шорошев // Науковий вісник НАВСУ. – К., 2014. – № 6. – С. 118–132.

15. Бондарчук М. Ринкові позиції телекомунікаційників ДК [Електронний ресурс] / М. Барчук // Зв'язок. – 2015. – 24 листопада. – №45. – Режим доступу: http://www.ucrf.gov.ua/ru/press/71/1138260941/

16. Боротьба з телефонним піратством : [методи, схеми, рекомендації] / І. Н. Балахничев, А. В. Дрик, А. І. Крупа. – Минск, 2008. – 322 с.

17. Ботвінкін О. В. Інформація з обмеженим доступом, що не є державною таємницею, в законодавстві України : [аналітичний огляд] / О. В. Ботвінкін, В. П. Ворожко / Нац. акад. СБ України. Ін-т захисту інформації з

обмеженим доступом. – К.: Нац. акад. СБ України, 2006. – 96 с.

18. Веліканов С. В. Класифікація слідчих ситуацій в криміналістичній методиці : автореф. дис. на здобуття наук. степеню канд. юрид. наук : спец. 12.00.09 «Кримінальний процес, криміналістика; судова експертиза» / С. В. Веліканов – Харків, 2002. – 19 с.

19. Весельський В. К. Криміналістична характеристика злочинів / В. К. Весельський // Право України. – 2014. – №5. – С. 112–114.

20. Виявлення та розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій : [посібник] / Коорд. комітет по боротьбі з корупцією при Президентові України. Міжвід. НДЦ з проблем боротьби з організ. Злочинністю ; НАВСУ; [за за. ред. Я. Ю. Кондратьєва, Б. В. Романюк, М. І. Камлик, Г. Д. Гавловський, В. Г. Хахановський, В. С. Цимбалюк]. – К. : НАВСУ, 2013. – 62 с.

21. Виявлення та розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій : [посібник] / Коорд. комітет по боротьбі з корупцією при Президентові України. Міжвід. НДЦ з проблем боротьби з організ. Злочинністю ; НАВСУ; [за за. ред. Я. Ю. Кондратьєва, Б. В. Романюк, М. І. Камлик, Г. Д. Гавловський, В. Г. Хахановський, В. С. Цимбалюк]. – К. : НАВСУ, 2012. – 62 с.

22. Вісім найпопулярніших способів обману абонентів мобільного зв'язку // Український діловий тижневик «Контракти» / № 19 від 12.05.2017 [Електронний ресурс]. – Режим доступу : http://www.kontrakty.com.ua/show/ukr/print_article/42/19200810414.html

23. Гавловський В. Д. Проблеми організації боротьби з правопорушеннями, що вчиняються з використанням сучасних інформаційних технологій / В. Д. Гавловський, Б. В. Романюк, В. С. Цимбалюк // Боротьба з організованою злочинністю і корупцією (теорія і практика). – К., 2005. – №3. – С. 163–169.

24. Галаган В. І. Засоби збирання доказів на стадії досудового розмлідування / В. І. Галаган, О. І. Галаган, Ж. В. Удовенко // Науковий

вісник КНУВС. – К., 2014. – Вип.4. – С. 111–120.

25. Галаган В. І. Проблеми вдосконалення кримінально-процесуальної діяльності органів внутрішніх справ України : [монографія] / Галаган В.І. ; НАВСУ. – Київ: НАВСУ, 2012. – 299 с.

26. Головкін С. В. Поняття слідчих ситуацій, їх формування і класифікація / С. В. Голокін // Вісник Луганської академії внутрішніх справ. – Луганськ, 2005. – Спец. вип. – Ч. 2. – С. 40–45.

27. Гурджи Ю. А. Процессуальное обеспечение прав личности : вопросы теории : [монография] / Гурджи Ю. А. – Одесса, 2006. – 265 с.

28. Дізнайся, чи відключать тобі мобільник. Як перевірити свій IMEI-код [Електронний ресурс]. – Режим доступу : http://ukr.dozor.kharkov.ua/hi-tech/1039359.html

29. Дослідження документів, виконаних за допомогою комп'ютерних технологій : [методичні рекомендації] / МВС України. НАВСУ. ННІПСК. Каф. криміналістич. Експертиз ; [уклад., за ред. О. В. Шведової]. – К. : НАВСУ, 2015. – 41 с.

30. Дрьомов С. Комп'ютерна інформація як предмет злочину, передбаченного статтею 362 Кримінального кодексу України / С. Дрьомов // Підприємництво, господарство і право. – 2005. – №4. – С. 129–132.

31. Егорова Н. К вопросу о новых мотивах совершения пре ступлений / Н. Егорова //Уголовное право. – 2008. – №1. – С. 41–44.

32. Європейське законодавство з телекомунікацій : [аналітичний матеріал; порівняльний аналіз]. – Київ, 2009. – 225 с.

33. Жуков С. Хакинг мобильных телефонов / Сергей Жуков. – М.: Бук-пресс, 2015. – 224 с.

34. Зав'ялов С. М. Спосіб вчинення злочину : сучасні проблеми вивчення та використання у боротьбі зі злочинністю : автор. дис. канд. юрид. наук : 12.00.09 / Зав'ялов Сергій Михайлович. – К., 2005. – 232 с.

35. Завидов Б. Д. Мошенничество в сфере высоких технологий / Б. Д. Завидов, З. А. Ибрагимова // Современное право. – 2001. – №4. – С. 41–

44.

36. Закон Великобританії «Про телекомунікації» (Telecommunication Act) та «О защите данных»[Електронний ресурс], 12.07.84 р. – Режим доступу:http://www.pdp.org.ua/index.php?option=com_content&view=article&id=887:212-3-visnyk-&catid=44:--i&Itemid=120

37. Закон Венгрии «О защите информации о лице и доступе к информации, представляющей общественній интерес» от 06.11.1992 [Електронний ресурс],– Режим доступу : http://www.pdp.org.ua/index.php?option=com_content&view=article&id=887:212-3-visnyk-&catid=44:--i&Itemid=118

38. Занюк С. С. Психологія мотивації : [навч. посібник для студентів вищих навч. закладів] / С. С. Занюк – Київ : Либідь, 2002 р. – 303 с.

39. Иванов П. Досье на телефонного мошенника / А. Иванов // Сети. – 2000. – №12. – С. 52–61.

40. Использование эмуляторов таксофонных чип-карт наносит значительный экономический ущерб государству [Електронний ресурс] – Режим доступу : http://www.kmv.gov.ua/news.asp?IdType=1&Id=56686

41. Історія виникнення субкультури «Хакерів» [Електронний ресурс]. – Режим доступу : http://pibhe.org.ua/readarticle.php?article_id=20

42. Іщенко А. В. Наукове забезпечення протидії злочинності : [посібник] / Іщенко А. В., Карпов Н. С., Кондратьєв Я. Ю. – Київ : Просвіта, 2002. – 221 с.

43. Іщенко А. В. Теорія і практика криміналістичного забезпечення процесу доказування в розслідуванні злочинів / Іщенко А. В., Ієрусалимов І. О., Удовенко Ж. В. ; [за ред. А. В. Іщенко] ; М-во освіти і науки України ; МВС України. КНУВС. – К. : КНУВС, 2017. – 158 с.

44. Карпов Н. С. Виникнення знань про криміналістичні засоби і методи слідчої діяльності : [історичний аспект дослідження проблеми] / Н. С. Карпов // Науковий вісник НАВСУ. – К., 2010. – №2. – С. 200–206.

45. Карпов Н. С. Злочинна діяльність : [монографія] / Карпов Н. С. ; МВС України. НАВСУ. – Київ : НАВСУ, 2015. – 307с.

46. Карпов Н. С. Злочинна діяльність у сфері телекомунікаційних засобів стільникового зв'язку : проблеми та шляхи протидії / Н. С. Карпов, Г. В. Семенов // Науковий вісник НАВСУ. – К., 2014. – № 5. – С.72–81.

47. Карпов Н. Система сотовой связи как основополагающий фактор, детерминирующий способы совершения мошенничества в системе сотовой связи./ Н. Карпов, Г. Семенов // Закон и жизнь. – 2009. – № 3. – С. 20–24.

48. Кашинцева О. Перспективи розвитку національного законодавства у сфері телекомунікацій / О. Кашинцева // Законодавство України. – К., 2016. – № 6. – С. 56–60.

49. Коваленко Є. Г. Теорія доказів у кримінальному процесі України : [підручник] / Є. Г. Коваленко ; М-во освіти і науки України. – К. : ЮрІнком Інтер, 2015. – 631 с.

50. Коваленко П. Ретроспективний аналіз українського та світового досвіду боротьби з шахрайством з фінансовими ресурсами на транснаціональному рівні / П. Коваленко // Підприємництво, господарство і право. – 2017. – №6. – С. 79–83.

51. Кодекс України про адміністративні правопорушення : науково-практичний коментар / [Р. А. Калюжний, О. О. Погрібний та ін.]. – К. : Правова єдність, 2016. – 781 с.

52. Козак І. А. Телекомунікації в бізнесі : [навчальний посібник] / Козак І. А. — К. : КНЕУ , 2014. — 367 с.

53. Комп'ютерно-технічна експертиза. Загальна частина : [методика] / МВС України. ДНДЕКЦ ; [уклад. К. М. Ковальов, С. М. Корнійко, В. О. Княждвірський]. – К., 2013. – 24 с.

54. Користін О. Є. Відмивання коштів : теоретико-правові засади протидії та запобігання в Україні : [монографія] / Користін О. Є. ; КНУВС. – К. : Поліграфкнига, 2015. – 447 с.

55. Кримінальне право України. Загальна частина : [підручник для

вузів] / за ред. В. В. Сташиса, В. Я. Тація ; Ю. В. Баулін, В. І. Борисов, Л. М. Кривоченко. – К. : ЮрІнком Інтер, 2014. – 495 с.

56. Кримінальне право України. Загальна частина : [підручник] / за ред. М. І. Мельника, В. А. Клименка. – К. : Атіка, 2013. – 375 с.

57. Кримінальне право України. Особлива частина : [підручник] / М-во освіти і науки України ; за ред. В. В. Сташиса, В. Я. Тація ; [авт. : Ю.В. Баулін, В.І. Борисов, С.Б. Гавриш та ін.]. – К. : ЮрІнком Інтер, 2007. – 622 с.

58. Лук'янчиков Б. Є. Вимоги до спеціаліста у кримінальному судочинстві / Б. Є. Лук'янчиков // Науковий вісник КНУВС. – К., 2017. – Вип.4. – С. 121–126.

59. Лук'янчиков Б. Є. Напрями вдосконалення правових норм, що регулюють процесуальні засоби збирання криміналістичної інформації / Б. Є. Лук'янчиков, Є. Д. Лук'янчиков // Науковий вісник НАВСУ. – К., 2011. – №1. – С. 50–54.

60. Лук'янчиков Є. Д. Методологічні засади інформаційного забезпечення розслідування злочинів : [монографія] / Є. Д. Лук'янчиков ; МВС України. НАВСУ. – Київ: НАВСУ, 2015. – 359 с.

61. Лукашевич В. Г. Розвиток доказування як форми пізнання в сучасному кримінальному процесі / В. Г. Лукашевич // Науковий вісник НАВСУ. – К., 2004. – №4. – С. 205–211.

62. Мобільні оператори України [Електронний ресурс]. – Режим доступу :http://mobilnik.ua/info/operators/

63. Невловимі «трубки». Боротьба з крадіжками мобільних телефонів зайшла в глухий кут. Потрібні радикальні заходи. // Дзеркало тижня./ [Електронний ресурс] 25.02.2016. – №7. – Режим доступу: http://www.dt.ua/2000/2675/52691/

64. Некоторые данные по защите от несанкционированного доступа [Електронний ресурс]. – Режим доступу : http: // www.sotovik.com =172

65. Несанкціонований доступ до послуг сотового зв'язку [Електронний ресурс]. – Режим доступу :http: // www.sotovik. com.

66. Огляд місця події при розслідуванні окремих видів злочинів : [науково-практичний посібник] / [В. П. Бахін, В. К. Весельський, Н. І. Клименко, І. І. Котюк, В. К. Лисиченко, Є. Д. Лукьянчиков, В. С. Мацишин, М. В. Перебитюк, В. Л. Перебитюк, В. Л. Підпалий, А. В. Старушкевич, В. В. Циркаль] ; за ред. П. В. Коляди. – К. : ЮрІнком Інтер, 2015. – 215 с.

67. Орлов Ю. Ю. Особливості експертного дослідження спеціальних технічних засобів на сучасному етапі / Ю. Ю. Орлов // Науковий вісник КНУВС. – К., 2017. – Вип.2. – С. 102–113.

68. Орлов Ю. Ю. Питання законодавчого забезпечення ефективності оперативно-розшукових заходів із застосуванням технічних засобів / Ю. Ю. Орлов // Науковий вісник КНУВС. – К., 2016. – Вип. 6. – С. 45–57.

69. Орлов Ю. Ю. Стан дослідженості проблем застосування технічних засобів в оперативно-розшуковій діяльності / Ю. Ю. Орлов // Науковий вісник КНУВС. – К., 2013. – Вип.6. – С. 73–78.

70. Пазиніч В. І. Генезис злочинів у сфері мобільних телекомунікацій / В. І.Пазиніч // Науковий вісник НАВСУ. –К., 2005. – № 2. – С. 226–231.

71. Пазиніч В. І. Криміналістична класифікація способів здійснення шахрайства в системі мобільного зв'язку / В. І. Пазиніч // Підприємництво, господарство і право. – 2007. – №7. – С. 146–161.

72. Погорецький М. А. Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі : [монографія] / Погорецький М. А. ; РНБО України. МНДЦ ПБОЗ. Акад. прав. наук України. Ін-т вивчення проблем злочинності. – Харків : Арсіс, ЛТД, 2007. – 575 с.

73. Романюк Б. В. Сучасні теоретичні та правові проблеми використання спеціальних знань у досудовому слідстві : [монографія] / Романюк Б. В. – Київ : НАВСУ, 2012. – 195 с.

74. Рудик М. В. Незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.08 «Кримінальне право ; кримінологія ; кримінально-виконавче право» / М. В. Рудик. – Одеса, 2007. – 19 с.

75. Самойленко О. Особливості предмета корисливих злочинів, вчинений з використанням комп'ютерних технологій / О. Самойленко // Підприємництво, господарство і право. – 2015 – №8. – С. 153–155.

76. Сахарук Д. В. Електронний документ як засіб доказування у цивільному процесі України / Д. В. Сахарук // Проблеми правознавства та правоохоронної діяльності. – Донецьк, 2013. – Вип. 2. – С. 307–312.

77. Служба безпеки знешкодила телефонного «пірата» – Режим доступу: http://ssu.kmu.gov.ua/sbu/control/uk/publish/article;jsessionid=9D3AD5E2F52EF39CB36F83BC27BF5387.app2?art_id=53415&cat_id=51966

78. Смирнов М. Процесуальні особливості проведення трансграничних обшуків і вилучення інформації, переданої через телекомунікаційні мережі / М. Смирнов // Підприємництво, господарство і право. – 2013. – №10. – С. 133–136.

79. Стратонов В. М. Слідча дія як криміналістичний метод отримання інформації / В. М. Стратонов // Вісник Луганської академії внутрішніх справ. – Луганськ, 2015. – Спец. вип. – Ч. 2. – С. 21–35.

80. Судово-експертна діяльність : довідник для експертів / [Н. М. Дяченко, В. С. Пєчніков, О. Р. Рувін та інші] ; під ред. І. П. Красюк. – Київ, 2012 . – 319 с.

81. Телефонні пірати знову виходять на «стежку війни». Останнім часом СБУ ліквідувала кілька підпільних «переговорних станцій» [Електронний ресурс]. – Режим доступу: http://ua.glavred.info/archive/2007/11/12/173705-1.html

82. Телефонні терористи. // Український діловий тижневик «Контракти» / № 19 від 12.05.2008. – С. 7–9.

83. Тихомиров А. М. Способ совершения и сокрытия преступления, как элементы криминалистической характеристики нарушения авторских прав / А. М. Тихомиров // Вісник Луганської академії внутрішніх справ. – Луганськ, 2005. – Спец. вип. – Ч. 2. – С. 130–133.

84. Удалова Л. Д. Кримінальний процес України. Загальна частина : [підручник] / Удалова Л. Д. – К. : Кондор, 2014 . – 151 с.

85. Узагальнення практики Верховного суду розгляду судами справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. – К., 2017. – 19 с.

86. Умови користування мережами мобільного зв'язку ЗАТ «Український мобільний зв'язок» / [Електронний ресурс] від 29.09.2016 – Режим доступу: http://www.mts.com.ua/ukr/rules.php

87. Хараберюш І. Ф. Використання оперативно-технічних засобів у протидії злочинам, що вчиняються у сфері нових інформаційних технологій : [монографія] / [І. Ф.Хараберюш, В. Я. Мацюк, В. А. Некрасов, О. І. Хараберюш]. – К. : КНТ, 2015. – 195 с.

88. Центр дослідження комп`ютерної злочинності [Електронний ресурс]. – Режим доступу : http://oaau.info/crime/?nid=17

89. Шведова О. В. Комплексне криміналістичне дослідження документів, виконаних за допомогою комп'ютерних технологій : автор. дис. канд. юрид. наук : 12.00.09 / Шведова Олена Вікторівна. – К., 2005. – 259 с.

90. Шило О. Обшук житла чи іншого володіння особи : проблеми правової регламентації / О. Шило, О. Капліна // Вісник Академії правових наук України. – Х., 2015. – Вип.2(41). – С. 192–200.

91. Шумило М. Є. Поняття, сутність і критерії незаконних процесуальних дій і рішень / М. Є Шумило // Науковий вісник НАВСУ. – К., 2014. – Вип.1. – С. 39–49.

92. Щепельков В. Соотношение мотива и цели преступления / В. Щепельков // Законность. –2001. – №4. – С. 39–40.

93. Щербакова Г. В. Проблема класифікації слідчих ситуацій / Г. В. Щербакова //Науковий вісник НАВСУ. – 2014. – №3 – С. 143–150.

94. CNews: Итоги 2016: Лидеры и новые технологии года [Електронний ресурс]. – Режим доступу : http://www.cnews.ua

http://www.dp.ukrtelecom.ua/presscenter/news/official?id=42010

95. Jos Dumortier, Mark Hyland, Diana Alonso Blas. Legal aspects of fraud detection. – Leuven, 2014. – P. 5–9.

96. Phil Gosset. Classification, Detection and Prosecution of Fraud on Mobile Networks / Grosset Phill, Hyland Mark // Presented at ACTS Mobile Communications International. – 2016. – №1. – P. 14–18.