МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХЕРСОНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ БІЗНЕСУ І ПРАВА
КАФЕДРА НАЦІОНАЛЬНОГО, МІЖНАРОДНОГО ПРАВА ТА ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА ЗЛОЧИНІВ ПОВ'ЯЗАНИХ З КОМП'ЮТЕРНОЮ ТЕХНІКОЮ ТА ІНФОРМАЦІЙНИМИ СИСТЕМАМИ

Кваліфікаційна робота (проєкт)
на здобуття ступеня вищої освіти «магістр»

Виконала: студентка 2 курсу 10-281М групи
Спеціальності 081 Право
Освітньо-професійної програми «Право»
Федак Інна Валеріївна

Керівник: д.ю.н., професор **Стратонов В.М.**
Рецензент:
завідувач кафедри спеціальних та професійних дисциплін Херсонського факультету Одеського державного університету внутрішніх справ
д.ю.н., професор **Шкута О.О.**

Херсон – 2021

ЗМІСТ

ВСТУП

Актуальність теми. В сучасних умовах розвитку суспільства, кожна сфера функціонування будь-якої системи практично неможлива без використання комп'ютерних технологій, комп'ютерної техніки, інформаційних систем, мережі Інтернет. Суцільна інтеграція перелічених складових інформаційного життя поступово призвела до того, що виник новий вид злочинів, а саме злочинів пов'язаних з комп'ютерною технікою та інформаційними системами.

З кожним роком кількість злочинів пов'язаних з комп'ютерною технікою та інформаційними системами зростає. Варто відзначити, що кожного року зростає професійна майстерність злочинців, що здійснюють такі злочини.

Отже, виникає необхідність розслідування злочинів пов'язаних з комп'ютерною технікою та інформаційними системами. Скоєння нових та більш досконалих злочинів пов'язаних з комп'ютерною технікою та інформаційними системами вимагає появу інноваційних метод розслідування.

У методиці розслідування злочинів криміналістична характеристика злочину займає особливе місце. Криміналістична характеристика злочинів пов'язаних з комп'ютерною технікою та інформаційними системами покликана виявити та надати основні характерні риси злочину, допомогти розслідуванню злочину. Вона включає в себе різні складові, так й на даний момент серед науковців не існує єдиної думки щодо структури криміналістичної характеристики злочинів пов'язаних з комп'ютерною технікою та інформаційними системами

Все це підтверджує складність теми обраного дослідження, його важливість та високу актуальність.

Дослідженню криміналістичної характеристики злочинів пов’язаних з комп’ютерною технікою та інформаційними системами присвячено велику кількість праць учених. Серед них слід виділити: Г.К. Авдєєва, А.І. Баянова, Р.С. Бєлкіна, І. І. Васильковського, О.М. Миколенка, В.М. Стратонова, В.Г. Танасевича, В.І. Чванкіна, М.П. Яблокова тощо. Проте, враховуючи постійний розвиток інформаційних систем та комп’ютерної техніки, залишається велика необхідність визначення та вивчення суттєвих розбіжностей у визначенні структури криміналістичної характеристики злочинів пов’язаних з комп’ютерною технікою та інформаційними системами.

Зв'язок теми з питаннями які розглядаються в роботі зумовлюється тим, що аналіз криміналістичної характеристики злочинів пов’язаних з комп’ютерною технікою та інформаційними системами дозволить практично сформувати та реалізувати заходи з підвищення ефективності розслідування таких злочинів.

Об’єкт дослідження – суспільні відносини пов’язані з злочинами вчиненими за допомогою комп’ютерної техніки та інформаційних системами.

Предмет дослідження – криміналістична характеристика злочинів пов’язаних з комп’ютерною технікою та інформаційними системами, а також методи їх розслідування.

Мета дослідження – деталізований аналіз теоретичних та практичних даних у сфері розслідування злочинів, пов’язаних з комп’ютерною технікою та інформаційними системами.

Відповідно до мети роботи слід вирішити наступні завдання:

– визначити поняття злочинів пов’язаних з комп’ютерною технікою та інформаційними системами, їх характерні ознаки;

– обґрунтувати способи вчинення злочинів пов’язаних з комп’ютерною технікою та інформаційними системами;

– розкрити генезис в формуванні основних методів розслідування;

– провести дослідження злочинів пов’язаних з комп’ютерною технікою та інформаційними системами;

– винайти шляхи підвищення ефективності розслідування злочинів пов’язаних з комп’ютерною технікою та інформаційними системами.

В роботі використані наступні методи дослідження: діалектичний метод, метод якісного аналізу і синтезу, системного підходу, спостереження, графічний метод, кількісний аналіз, метод вибіркового спостереження, табличний, порівняння, структурний метод, групування, узагальнення.

Науковою новизною роботи слід виділити те, що було розглянуто теоретичні й практичні питання криміналістичної характеристики злочинів пов’язаних з комп’ютерною технікою та інформаційними системами, а також методи їх розслідування. На основі отриманих з теоретичних, практичних джерел інформації: доповнено, введено нові визначення щодо питання криміналістичної характеристики злочинів пов’язаних з комп’ютерною технікою та інформаційними системами, систематизовано заходи підвищення ефективності розслідування злочинів.

Теоретичне і практичне значення результатів дослідження роботи підтверджується тим, що згруповано основні положення щодо криміналістичної характеристики злочинів пов’язаних з комп’ютерною технікою та інформаційними системами, методики розслідування таких злочинів. Отримана інформація може бути використана для поглиблення знань студентів вищих навчальних закладах.

Апробацію результатів дослідження здійснено в збірнику міжнародної науково-практичної конференції «Стратегічні пріоритети розвитку економіки, менеджменту, сфери обслуговування та права в умовах інтеграційних процесів» (17 листопада 2021 року, м. Херсон)

Публікація: Федак І.В. Криміналістична характеристика злочинів

пов’язаних з комп'ютерною технікою та інформаційними системами. *Стратегічні пріоритети розвитку економіки, менеджменту, сфери обслуговування та права в умовах інтеграційних процесів.*

Структура кваліфікаційної роботи визначена у відповідності до мети та завдань кваліфікаційної роботи та включає вступ, два розділи, висновки, список використаних джерел та додатки.

РОЗДІЛ 1
ЗАГАЛЬНО-ТЕОРЕТИЧНА ХАРАКТЕРИСТИКА ЗЛОЧИНІВ ПОВ'ЯЗАНИХ З КОМП'ЮТЕРНОЮ ТЕХНІКОЮ ТА ІНФОРМАЦІЙНИМИ СИСТЕМАМИ

1.1 Поняття злочинів пов'язаних з комп'ютерною технікою та інформаційними системами, їх характерні ознаки

Стрімкий розвиток сучасного суспільства, передових технологій, науково-технічний прогрес призвели до суцільної інтеграції комп'ютерної техніки у повсякденне життя населення, у всі сфери діяльності суб'єктів підприємництва (юридичних осіб та фізичних осіб-підприємців), функціонування держави (всі галузі) тощо. Тобто використання комп'ютерної техніки та інформаційних систем має велику кількість позитивних рис. В той же час, як зазначає В.М. Стратонов, інформатизація, як і будь-яке соціальне явище, має і негативні прояви: можливість використання комп'ютерних технологій для вчинення правопорушень, зокрема злочинів, у т. ч. організованими злочинними формуваннями [40, с. 84].

Комп'ютерні системи містять в собі нові досконалі можливості скоєння правопорушень, а також дозволяють вчиняти традиційні злочини нетрадиційними засобами [41, с. 56].

Саме тому протиправне використання комп'ютерної техніки та інформаційних систем, мереж передачі такої інформації й становить потенційну суспільну небезпеку [13].

М.В. Старічков суспільну небезпеку злочинів у сфері комп'ютерної техніки та інформаційних систем вбачав у неправомірному доступі до даних, що знаходились в техніці чи зміна її складових. Науковець зазначав, що злочинці здійснюючи злочини у

сфері комп'ютерної техніки та інформаційних систем можуть здійснювати їх з метою порушення діяльності різних систем. Наприклад, в державному управлінні це може бути сфера оборони, управління міських та обласних рад, сфера енергетики. Він звертав увагу, що заподіяння цих злочинів призводить не лише до матеріальних збитків, а й до людських жертв [1, с. 109].

Злочинність з комп'ютерною технікою та інформаційними системами – це специфічний вид злочинів, пов'язаних із протизаконним використовуванням комп'ютерної техніки та інформаційних систем з корисною метою.

Поняття «комп'ютерне шахрайство» з'явилося ще в 70 –ті рр. минулого століття, коли в розвинених країнах зріс рівень економічних злочинів, що зумовило потребу реформування законодавства. Але позиція законодавчих органів була спочатку дещо розмитою, адже, на перший погляд, могло б здатися, що треба тільки об'єднати низку кваліфікуючих ознак та чинних норм законодавства, проте під час ретельнішого вивчення конструкції таких злочинів стало очевидно, що тут можна твердити про появу нового способу й нового предмету посягань, що спричинило потребу введення нових складів у Кримінальний кодекс України, котрі містять відповідальність за такі види злочинів [15].

На думку Л. Кривоченка, конструкція «шахрайство, учинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки», свідчить про специфічний спосіб учинення цього злочину, до того ж його небезпечність полягає в тому, що ця техніка значно полегшує вчинення шахрайства, дає змогу заволодівати значними коштами, завдаючи непоправної шкоди власникам [7, с. 160].

В. Бутузов також розглядав питання злочинів пов'язаних з комп'ютерною технікою та інформаційними системами. Він вважає, що цей вид злочинів дещо відрізняється від кіберзлочинності, адже вони

відносяться до різних видів злочинів, пов'язаних з інформаційними технологіями. Останні він рекомендував класифікувати за наступними ознаками:

– злочини пов'язані з комп'ютерною технікою та інформаційними системами пов'язані з відповідним знаряддям здійснення злочину, а саме комп'ютерної техніки;

– інформація інформаційних систем та суспільні відносини є об'єктом посягання таких злочинів;

– кіберзлочинність має мати специфічне середовище, в якому здійснюється вчинення злочину, а саме кіберпростір, до яких відносяться комп'ютерні системи та мережі [28, с. 48] .

М. Погорецький та Шеломенцев В. зауважують, що Конвенцією та Додатковим протоколом до Конвенції, визначено, що універсальною ознакою злочинів пов'язаних з комп'ютерною технікою та інформаційними системами є те, що вони вчинюються з безпосереднім використанням комп'ютерної техніки або комп'ютерних систем, які є середовищем здійснення таких злочинів. Такі злочини вони відносять до кіберзлочинів. Так вони стверджують, що до кіберзлочинів слід відносити всі види злочинів, які здійснюються з використанням пристроїв, що отримують, обробляють та зберігають дані [29, с.89-96].

Багато науковців розглядають кіберзлочини з різних сторін. Так Є. Скулишин із О. Копатіним вважають, що до кіберзлочинів слід відносити такі злочини, які безпосередньо пов'язані з використанням комп'ютерних систем та мереж. Вони вважають, що такі злочини здійснюються у кіберпросторі та є найбільш небезпечними. Крім того, здійснення таких злочинів несе за собою кримінальну відповідальність [30].

Наступна група науковців, а саме В. Болгов, Н.М. Гадіон та О.З. Гладун у кіберзлочинах вбачають сукупність небезпечної діяльності (бездіяльності), яка направлена на несанкціонований доступ до даних, їх

поширення, розповсюдження або використання, які призводять до негативних наслідків та порушують права власності, за що відповідно до чинного законодавства передбачена кримінальна відповідальність [31].

Кіберзлочини характеризуються певними ознаками та рисами, так вони мають латентний характер, тобто часто потерпіли не повідомляють про здійсненні злочини проти них, адже впевнені у неможливості розкриття злочину та покарання злочинця. Крім того, користувачі Інтернету проти яких скоєно злочин, як правило, не хочуть публічно визнавати, що їх дані було викрадено, через можливе засудження їх з боку близьких та знайомих людей. Отже, протидія кбірзлочинам має починатися з їх профілактики та включати цілий комплекс заходів по усуненню таких злочинів.

М.О. Гвоздецька та К.Ю. Ісмайлов у злочинах пов'язаних з комп'ютерною технікою та інформаційними системами виділяють наступні характерні ознаки:

– високий рівень латентності, який викликаний суцільної інформатизацією та комп'ютеризацією, крім того можливістю здійснення злочинів з закордону;

– порівняльна простота вчинення злочинів, яка обумовлена використанням комп'ютерної техніки великою кількістю людей, постійними змінами програмного забезпечення, вдосконалення шахрайських програм [2, с. 53].

Крім того, слід додати, що злочини пов'язані з комп'ютерною технікою та інформаційними системами мають й наступні ознаки:

– інтелектуальний характер злочину, який вимагає від злочинця специфічних знань;

– кіберзлочини не вимагають від злочинця високого соціального статусу;

– не має вікових обмежень;

– можливість видавати себе за іншу особу тощо.

Слід виділити наступні негативні чинники розповсюдження злочинів пов’язаних з комп’ютерною технікою та інформаційними системами:

– низький рівень контролю за безпекою комп’ютерного простору;

– висока латентність злочинів, необхідність замовчування злочинів через негативний вплив на репутацію;

– недостатність практичних навичок розслідування злочинів пов’язаних з комп’ютерною технікою та інформаційними системами;

– постійні зміни та оновлення програмного забезпечення;

– важкість розслідування та доведення до суду порушених кримінальних справ цієї категорії.

Таким чином, злочини пов’язані з комп’ютерною технікою та інформаційними системами – це правопорушення, які тягнуть за собою кримінальну відповідальність, що здійснюються за допомогою комп’ютерної техніки та посягають на конфіденційні дані, чим порушують право власності на інформацію чи інформаційні системи, здійснюючи на них негативний вплив.

1.2 Способи вчинення злочинів пов’язаних з комп’ютерною технікою та інформаційними системами

Одним із важливих складових криміналістичної характеристики злочинів пов’язаних з комп’ютерною технікою та інформаційними системами є спосіб вчинення злочину, а іноді саме він служить й кваліфікуючою обставиною.

Якщо за основу класифікації способів вчинення злочинів пов’язаних з комп’ютерною технікою та інформаційними системами використовувати методи, якими злочинці отримують доступ до комп’ютерної техніки та інформаційних систем, отримуємо наступні

групи:

– вилучення комп’ютеру, або його складової частини для здійснення злочину;

– перехват інформації та даних;

– несанкціоноване втручання в роботу комп’ютеру або інформаційної системи;

– маніпуляція даними, їх підміна або підробка;

– комплекс методів.

Перша група способів скоєння злочинів пов’язаних з комп’ютерною технікою та інформаційними системами характеризується тим, що в таких видах злочинів комп’ютерна техніка завжди виступає лише предметом злочинного посягання, проте інші технічні інструменти виступають знаряддям скоєння злочину (або без їх використання), які не є засобами комп’ютерної техніки.

Друга група способів скоєння злочинів пов’язаних з комп’ютерною технікою та інформаційними системами включає такі злочини, коли злочинці використовують різні засоби перехоплення інформації.

При здійсненні злочинів пов’язаних з комп’ютерною технікою та інформаційними системами перехват інформації здійснюється різними методами:

– безпосередній перехват (активний);

– електромагнітний перехват (пасивний);

– перехват аудіо даних;

– перехват відео даних;

– використання інформаційних відходів («прибирання сміття»).

При активному перехопленні для підключення з метою отримання необхідного паролю чи іншої важливої інформації використовуються кабель чи перехват мікроволн від супутника та наземних радіостанцій.

При пасивному перехопленні сигнали з електронно-лучової трубки

дисплея приймаються, записуються і аналізуються навіть, коли обладнання знаходиться більш ніж на 1 кілометр.

Захистити інформацію при аудіоперехопленні досить складно, перехват аудіо даних, як правило, реалізується з використанням підслуховуючого пристрою, це так звані таблетки, клопи, жучки. Крім того, злочинці часто використовують різні акустичні та вібраційні датчики, які також дозволяють перехоплювати інформацію.

Слід звернути увагу, що лише перша група способів скоєння злочинів пов'язаних з комп'ютерною технікою та інформаційними системами характеризується тим, що комп'ютер становиться предметом злочинів, в той час як в інших групах таких злочинів комп'ютер виступає і предметом і знаряддям злочину.

Третя група способів скоєння злочинів пов'язаних з комп'ютерною технікою та інформаційними системами включає такі злочини, в яких дії злочинця спрямовуються на отримання несанкціонованого доступу до засобів комп'ютерів та інформаційних систем (мереж). До них слід враховувати: «за дурнем» – проникнення злочинця в заборонні зони за іншими людьми; «за хвіст» – підключення злочинця до зв'язку певної людини з метою перехоплення сигналу в кінці бесіди для доступу до системи; «комп'ютерний абордаж» – підбір злочинцем паролю; «неспішний вибір» та «пролом» - пошук вразливих місць в системі безпеки інформаційних систем; «маскарад» – злочинець видає себе за законного користувача проникає у комп'ютерну систему; «містифікація» – підключення користувача персонального комп'ютера до чиєїсь системи, злочинець формує правдоподібні відповіді на запити володаря інформаційної системи; «аварійний» – злочинець використовує засоби та програми, які дозволяють обійти системи безпеки інформації; «склад без стін» –використання поломок в системі захисту.

Четверта групи способів скоєння злочинів пов'язаних з комп'ютерною технікою та інформаційними системами включає в себе

різну злочинну діяльність злочинців, яка направлена на маніпуляцію даними, їх підробку, підміну, заміну, введення нових даних, з злочинними намірами.

Злочини пов’язані з комп’ютерною технікою та інформаційними системами поділяють на:

1. Злочини, в яких об’єктом скоєння є електронно-обчислювальні машини, вони включають злочини, де відбулось втручання в комп’ютерну техніку та інформаційні системи (мережі). Скоєння цих видів злочинів включає в себе наступні противоправні дії: викрадення даних або програмного забезпечення, що зберігається на комп’ютері, їх перехват, зіпсування, заміна, розповсюдження, продаж та інше. Метою таких видів злочину може бути як користь (матеріальна зацікавленість), так і шпигунство, викрадення даних з комерційною таємницею.

2. Злочини, в яких комп’ютерна техніка є знаряддям злочину. До таких видів злочинів відносяться: комп’ютерний саботаж; вимагання даних; шпигунство; викрадення коштів та їх розтрата; навмисне обдурення.

Сьогодні злочини пов’язані з комп’ютерною технікою та інформаційними системами найчастіше скоються з матеріальних міркувань, тобто з метою наживи, викрадення коштів, незаконного збагачення. Так злочинці вимагають коди та паролі даних, під видом робітників банку, а потім знімають грошові кошти з їх карток.

Наступним значним мотивом скоєння злочинів пов’язаних з комп’ютерною технікою та інформаційними системами є комерційне шпигунство, яке передбачає отримання даних, що носять комерційну таємницю та мають особливе значення для суб’єктів господарювання. Наприклад, даними комерційної таємниці можуть стати дані щодо секретів виробництва, розробки тощо.

Злочини пов’язані з комп’ютерною технікою та інформаційними системами є дуже розповсюдженими, адже створюють відчуття

безкарності, адже встановлення місця знаходження злочинця кіберзлочинів є дуже складним. Крім того, кіберзлочини можуть здійснюватися в будь-якій точці світу, так злочинець може перебувати в Австралії, а викрадати дані фірми, що знаходиться в Україні. Ці фактори підвищують суспільну небезпеку злочинів пов'язаних з комп'ютерною технікою та інформаційними системами висувають вимогу постійного пошуку актуальних заходів розслідування таких злочинів.

П.В. Берназ зазначає, що велика частина злочинів пов'язаних з комп'ютерною технікою та інформаційними системами відбувається в інформаційних мережах. Тобто місце вчинення злочину і місце настання негативних наслідків, як правило, дуже відрізняються та можуть знаходиться в тисячі кілометрів один від одного, в різних державах, і навіть на різних континентах [3, с. 14].

Варто також звернути увагу, що злочини пов'язані з комп'ютерною технікою та інформаційними системами можуть мати різний час скоєння злочину та настання наслідків. Так шкідливі програми можуть бути занесені до комп'ютерної техніки в один час, а руйнівні дії відбуватися в зовсім інший.

Як правило, при здійсненні злочинів пов'язаних з комп'ютерною технікою та інформаційними системами йдеться справа з комплексом злочинів, вираженими у незаконному втручанні в комп'ютерну техніку, інформаційні системи, мережі та противоправному доступу до конфіденційної інформації, її викрадення, зміна, перехоплення, викрадення коштів з карткових рахунків.

Тож під способом здійснення злочинів пов'язаних з комп'ютерною технікою та інформаційними системами розуміють певну сукупність прийомів і засобів, які забезпечують навмисний доступ несанкціонованим шляхом до інформаційних даних і систем, з корисною метою, яка виражається у порушені прав власності, наприклад, викрадення коштів з карткових рахунків однієї особи на рахунки іншої.

Таким чином, способи вчинення злочинів пов’язаних з комп’ютерною технікою та інформаційними системами дуже різноманітні і постійно змінюються. Визначення способів здійснення цих злочинів має велике значення, адже їх усунення дозволяє захистити від порушення прав власності, махінацій із грошовими коштами, втручання в дані підприємства чи фізичних осіб, несанкціоноване поширення інформації, що має комерційний інтерес, персональні дані.

1.3 Генезис в формуванні основних методів розслідування

Науковці активно розробляють питання, пов’язані з методикою розслідування шахрайств, учинених із використанням ЕОТ. Під криміналістичною методикою розкриття та розслідування комп’ютерних злочинів В. Голубєв розуміє всі наукові положення і розроблені на їх основі рекомендацій щодо розкриття та розслідування таких злочинів [17, с. 65].

Вчений О. Мотлях, досліджуючи основні аспекти методик розслідування та розкриття злочинів пов’язаних з комп’ютерною технікою та інформаційними системами, детально проаналізував криміналістичну характеристику злочинів цієї категорії як інформаційну модель, що представляє собою систематизований набір типових ознак скоєння кіберзлочинів, які мають важливе значення для розслідування та розкриття протиправних дій осіб у сфері комп’ютерних технологій [18, с. 13].

У методиці розслідування злочинів криміналістична характеристика злочину займає особливе становище, адже допомагає розкривати та розслідувати злочини пов’язані з комп’ютерною технікою та інформаційними системами.

Для широкого та повного аналізу криміналістичної характеристики злочинів пов’язаних з комп’ютерною технікою та

інформаційними системами необхідно розглянути визначення поняття «криміналістична характеристика» науковцями.

На даний момент, існують різні визначення поняття «криміналістична характеристика», єдине визначення відсутнє. Слід додати, що становлення криміналістичної характеристики відбувалось поступово та цей процес був тривалий.

Р.С. Бєлкін під криміналістичною характеристикою злочинів вбачав абстрактне наукове поняття, яке дозволяє слідчому зорієнтуватися в характеристиці злочину, розглянути всі типові питання скоєння злочину, проаналізувати способи та мету скоєння злочину, його наслідків [42, с. 305].

Криміналістична характеристика злочинів включає в себе типову структуру певних елементів, що характеризують все, що пов'язано із певним злочином. Криміналістична характеристика злочинів мала декілька етапів становлення та розвитку а саме:

– перший етап – радянський;

– другий етап – сучасний.

Представником радянського етапу становлення криміналістичної характеристики злочинів можна вважати А.І. Баянова, він виділяв наступні її елементи:

– спосіб підготовки, вчинення і приховання злочину;

– предмет замаху;

– наслідки злочину;

– характеристика особи, що скоїла злочин;

– характеристика потерпілого

– мотивація вчинення злочину [43, с. 107].

Також до представників радянського етапу становлення криміналістичної характеристики злочинів слід віднести О.М. Колесніченка, на його думку до її елементів входить:

1) спосіб підготовки, вчинення і приховання злочинів;

2) місце злочину, час скоєння, в якій обстановці, за допомогою якого знаряддя і засобів;

3) предмет замаху;

4) характеристика особи, що скоїла злочин;

5) характеристика потерпілого;

6) сліди злочину [44, с. 34].

Отже, радянський етап розвитку структури криміналістичної характеристики злочинів є базовим, адже на його основі відбувалось становлення і розвиток її структурних елементів.

Наступним та сучасним етапом у розвитку криміналістичної характеристики злочинів слід вважати ті розробки, які відбуваються в умовах сьогодення. Нині, як і раніше, відсутній єдиний підхід до визначення структурних елементів криміналістичної характеристики злочинів.

Так В.І. Гончаренко, Н.І. Клименко, В.К. Лисиченко, Г.А. Матусовський та Н.А. Сенчик рекомендують наступні структурні елементи криміналістичної характеристики злочину:

1) спосіб приготування, вчинення і приховання злочину;

2) обставини скоєння злочину (в якому місце знаходився злочинець, де знаходився комп'ютер, час скоєння злочину, засоби скоєння злочину та інше);

3) предмет злочину;

4) характеристика особи, що є потерпілою стороною;

5) характеристика особи злочинця;

6) сліди злочину (в широкому розумінні) [45, с. 22].

Криміналістична характеристика злочинів пов'язаних з комп'ютерною технікою та інформаційними системами не є уніфікованою, до неї не входять обов'язковий набір елементів. Кожний вид злочинів має свій комплекс елементів, що входять до криміналістичної характеристики.

Таким чином, криміналістична характеристика злочинів пов’язаних з комп’ютерною технікою та інформаційними системами займає значне місце для ефективного розслідування та розкриття злочинів цього види, саме вона визначає необхідні прийоми та засоби, що мають використовуватися під час розслідування. Структура криміналістичної характеристики злочинів пов’язаних з комп’ютерною технікою та інформаційними системами включає в себе сукупність найбільш важливих структурних елементів, що характеризують весь процес скоєння злочину від початку до настання негативних наслідків від таких видів злочинів. Ці структурні елементи характеризують небезпечні діяння, які було скоєно, особу потерпілого та злочинця, мету злочину та мотиви злочинця, місце, час скоєння злочину та іншу. Все це є ефективним інструментом розслідування злочинів пов’язаних з комп’ютерною технікою та інформаційними системами та інструментом висування версій.

Варто звернути увагу, що криміналістична характеристика злочинів пов’язаних з комп’ютерною технікою та інформаційними системами не є універсальною, кожна група злочинів та й кожний окремий злочин може мати різну структуру криміналістичної характеристики.

Серед основних структурних елементів криміналістичної характеристики злочинів пов’язаних з комп’ютерною технікою та інформаційними системами О. Мотлях пропонує розглянути такі:

– способи скоєння злочинів цієї категорії (як було отримано доступ до комп’ютеру або інформаційної системи, а відповідно й до даних, що в них зберігаються; види віддаленого доступу; яким шляхом виготовлялась, розповсюджувалась, реалізувалась інформація);

– слідова картина цих злочинів, а саме втручання в комп’ютер, інформаційні системи, перехват даних, їх розповсюдження, продаж;

– всі дані щодо особи, яка скоїла злочин пов’язаних з

комп’ютерною технікою та інформаційними системами, мета та мотиви скоєння таких злочинів. Як правило, відповідно до міжнародної та вітчизняної статистики, вік злочинців, що здійснюють злочині пов’язані з комп’ютерною технікою та інформаційними системами від 15 до 40 років. Крім того, варто відзначити, що щороку вік злочинців зменшується, й все частіше найбільшу питому вагу займають злочинці до 25 років;

– будь-які інші обставини здійснення злочинів пов’язаних з комп’ютерною технікою та інформаційними системами, які не були враховані раніше [18, с. 13].

Подані елементи криміналістичної характеристики, як зауважує автор, перебувають у взаємозв’язку, взаємодоповнюють один одного й виступають логічним продовженням попереднього структурного елементу.

Виходячи з аналізу світової та вітчизняної практик, О. Мотлях пропонує розподіляти їх за наступною питомою вагою здійснення:

– злочини з корисною метою – 66%;

– злочини з політичними мотивами – 17%;

– злочини через інтерес – 7%;

– злочини з хуліганськими намірами – 5%;

– через помсту – 5% [18, с. 13].

Тоді як А.С. Білоусов, здійснюючи криміналістичний аналіз об’єктів комп’ютерних злочинів у межах учення про криміналістичну характеристику злочинів, обґрунтував необхідність розробки криміналістичної характеристики злочинів пов’язаних з комп’ютерною технікою та інформаційними системами [26].

Методи розслідування кіберзлочинів суттєво відрізняються від загальних принципів проведення слідчих і розшукових дій. Фіксація злочинної діяльності та розкриття злочину вимагають застосування спеціального обладнання, яке не використовується у звичайному обігу

та не доступне. До того ж така діяльність є транснаціональною, тобто вона не обмежується територією однієї держави, а тому потребує міжнародної правової допомоги для її документування та розкриття злочинів.

За визначенням О.В. Голубєва, криміналістична методика розкриття злочинів пов'язаних з комп'ютерною технікою та інформаційними системами – це певна сукупність нормативно-методологічних положень, які практично підтвердили свою ефективність при розслідуванні кібезлочинів та рекомендацій, які можуть бути використанні при розкритті подобних видів злочинів [17, с. 65].

Розслідування злочинів, учинених у сфері інформаційних технологій, ускладняється тим, що органам розслідування важко виявити та зафіксувати сліди, які залишаються після вчинення комп'ютерного злочину, оскільки досвідчений «хакер» залишає за собою їх невелику кількість. Щоб його вирахувати і затримати, потрібна допомога провайдерів і обмін технічною інформацією з їх закордонними партнерами та міжнародними правоохоронними органами. Криміналістична особливість кіберзлочинів характеризується тим, що виявлення та розслідування злочинів пов'язаних з комп'ютерною технікою та інформаційними системами неможливе без комп'ютерів та інших приладів, адже потрібне вилучення доказів, їх обробка та фіксування.

Саме наявність відповідних вмінь і навичок у сфері інформаційних технологій надають можливість прокурору забезпечити дієве процесуальне керівництво розслідуванням слідчими органів внутрішніх справ кіберзлочинів, зібрати належні докази та усунути процесуальні недоліки під час розслідування.

Розслідування злочинів пов'язаних з комп'ютерною технікою та інформаційними системами на думку О.М. Моїсева вимагає:

– використання криміналістичних лабораторій оснащених необхідними технічними засобами;

– високого рівня професійного підготовки спеціалістів, що здійснюють експертизи [35, с. 81 – 85].

Як стверджує О.М. Миколенко де-юре слід констатувати відсутність вимог чинного законодавства щодо проведення обов'язкових експертиз в злочинах пов'язаних з комп'ютерною технікою та інформаційними системами. Проте фактично експертиза надає можливість ефективно розслідувати такі злочини, тобто без її використання розкриття справи практично неможливе [34, с.155-157].

Розслідування злочинів пов'язаних з комп'ютерною технікою та інформаційними системами вимагає проведення окремих та негласних слідчих дій. Ці дії мають здійснюватися у рамках досудового розслідування та значно впливають на результат пошуку винуватців. Так розслідування злочинів пов'язаних з комп'ютерною технікою та інформаційними системами вимагає від оперативних спеціалістів, що здійснюють слідчі дії, специфічних глибоких знань технічних засобів, комп'ютерної техніки, а також розуміти механізм за яким здійснюються злочини такого виду. Тобто виникає необхідність комплексної підготовки фахівців високого професійного рівня не лише за напрямом юриспруденції, а й програмування, адміністрування комп'ютерів, інформаційних систем та багато іншого.

Водночас дослідник акцентує увагу на потребі використання спеціальних знань у розслідуванні комп'ютерних злочинів, а також проведенні комплексних досліджень комп'ютерних об'єктів. Науковець доповнив перелік основних завдань, що висуваються перед спеціалістом у разі його участі в проведені слідчих дій у справах цієї категорії. Розмірковуючи далі, учений стверджує, що розслідування злочинів пов'язаних з комп'ютерною технікою та інформаційними системами вимагає використання міжвидової криміналістичної характеристики, яка

відображатиме певні закономірності здійснення таких кіберзлочинів.

А.С. Білоусов пропонує до основних елементів криміналістичної характеристики злочинів пов’язаних з комп’ютерною технікою та інформаційними системами відносити наступні особливості:

– використання злочинів пов’язане з комп’ютерною технікою та інформаційними системами, які є об’єктом злочину;

– специфічність віртуальної слідової картини (апаратні, програмні чи інформаційні елементи комп’ютерних об’єктів);

– істотні особливості слідів злочинів пов’язаних з комп’ютерною технікою та інформаційними системами (вплив на комп’ютерну інформацію);

– використання різних носіїв інформацію (віртуальна пам'ять, флешки, жорсткий диск, оперативна пам'ять, роздруковані матеріали);

– необхідність мати специфічні знання для скоєння злочину [26, с. 5].

Слушною вважаємо думку О. Моїсеєва, що під час розслідування шахрайств, учинених із використанням ЕОТ, зокрема й кіберзлочинів дослідження засобів злочину необхідно проводити в відповідних криміналістичних лабораторіях. Відповідні фахівці мають провести всі необхідні дії, пов’язані з отриманням максимальної кількості доказів саме в умовах лабораторії, де все має фіксуватися на камеру та буде відсутня можливість змінити, викривити дані [19].

Ще одним науковим напрямом досліджень проблем розслідування шахрайств, учинених із використанням ЕОТ, є визначення організаційних заходів, що являють собою ефективний спосіб захисту інформації та реальний фундамент, на якому будується вся система захисту.

Отже, апелюючи до наукової позиції С. Чернявського [21], уважаємо, що аналіз стану наукового забезпечення розслідування шахрайств, учинених із використанням електронно-обчислювальної

техніки, дає змогу говорити про дві тенденції, що визначають перспективи формування окремих методик, – деталізацію та інтеграцію. Потребу деталізації методик визначають особливості слідчих ситуацій, що складаються, та інші обставини злочинної діяльності [22; 23].

Поряд із процесом деталізації розгорнувся процес інтеграції методик, коли почали створювати міжвидові групи злочинів, що відбивають особливості розслідування споріднених видів (комплексів) злочинів. Водночас сучасні науковці (А. Білоусов, О. Мусієнко, С. Самойлов, В. Тіщенко, С. Чернявський та ін.) наголошують на потребі розробки комплексної методики розслідування шахрайств, учинених із використанням ЕОТ, оскільки практика розслідування свідчить, що в кримінальному середовищі складаються складні схеми злочинної діяльності. Це положення створює потребу розробки загальних методико-криміналістичних рекомендацій із розслідування цих злочинів на основі їх узагальнених криміналістичних характеристик [24; 25, с. 64].

Скажімо, вивчаючи обстановку скоєння злочину, треба обов’язково звернути увагу на наявність і спосіб підключення електронно-обчислювальної техніки (ЕОТ), у роботу якої було здійснено несанкціоноване втручання до комп’ютерних мереж і мереж електрозв’язку. Відразу ж можна виділити три основні ситуації:

1) ЕОТ не підключена до будь-яких мереж;

2) ЕОТ підключена до локальної мережі;

3) ЕОТ підключена до глобальної мережі Інтернет.

Відштовхуючись від цих відомостей, можна в деяких випадках істотно звузити коло можливих підозрюваних і виділити типи осіб злочинців за способом здійснення несанкціонованого втручання:

1. Злочинець мав безпосередній (фізичний) доступ до ЕОТ. Тоді доцільно було б визначити коло осіб, які могли мати доступ до ЕОТ з урахуванням установлених часу та місця скоєння злочину (прикладом

може бути ситуація, коли співробітник підприємства, якого, на його думку, незаслужено звільняють, проникає в дата –центр і, з помсти, використовуючи шкідливе програмне забезпечення, маючи безпосередній доступ до ЕОТ, знищує всю інформацію на серверах компанії).

2. Злочинець мав доступ до ЕОТ у локальній мережі і з її допомогою здійснив несанкціоноване втручання в роботу ЕОТ, що міститься в тій само локальній мережі. У цьому випадку є можливість з'ясувати в адміністратора локальної мережі обмежений список точок підключення ЕОТ, які входять у мережу, а також фізичні (реальні) і IP – адреси точок підключення до мережі. Маючи таку інформацію, можна встановити обмежене коло осіб, які працюють у локальній мережі (прикладом може послужити ситуація, коли комірник на підприємстві, де комп'ютери об'єднані в закриту локальну мережу, для приховування нестачі товару підключається за допомогою одного з комп'ютерів у цій мережі до сервера із системою обліку товарообігу, за допомогою шкідливого програмного забезпечення зламує її захист і змінює дані про кількість товару на складі).

3. Злочинець здійснив несанкціонований доступ та втручання в роботу ЕОТ, що підключена до глобальної мережі Інтернет, за допомогою невстановленої ЕОТ, яка також підключена до глобальної мережі Інтернет. Така ситуація є найскладнішою для вирішення, оскільки в теорії несанкціонований доступ та втручання в роботу ЕОТ мало змогу здійснити необмежене коло осіб по всьому світу при наявності підключення до глобальної мережі Інтернет (прикладом може послужити ситуація, коли хакер розіслав електронною поштою шкідливе програмне забезпечення, що здійснило шифрування даних на жорстких дисках комп'ютерів підприємства, призвело до блокування інформації, після чого вимагає гроші за відновлення можливості доступу до цієї інформації). Зіткнувшись з останньою ситуацією, треба розглянути

особу злочинця в прив’язці до слідової картини й способу вчинення злочину. Потрібно з’ясувати, чи використовував злочинець шкідливе програмне забезпечення, бекдори (з англ. backdoor – чорний хід, тобто уразливості в коді програмного забезпечення) або ж несанкціоноване втручання здійснили потерпілі чи користувачі ЕОТ через недотримання елементарних правил забезпечення кібербезпеки.

Для цього під час огляду ЕОТ за участю фахівця крім іншої інформації, яка має значення для проведення розслідування, треба встановити також, чи залишилися на зламаній ЕОТ сліди шкідливого програмного забезпечення, чи не пошкоджений реєстр з інформацією щодо останніх дій користувача, чи здійснювалося підключення ЕОТ до мережі безпосередньо або через маршрутизатор, чи використовується в маршрутизаторі стандартний логін і пароль або вони змінені, чи присвоєно точці підключення до мережі статичну або динамічну IP – адресу, а також які налаштування підключення до мережі використовуються; яку MAC –адресу має мережеве обладнання користувача, чи був злочинцем проведений повний вайп (від англ. wipe – стирати, знищувати, видаляти) інформації на носіях, вайп операційної системи або її часткове пошкодження, а також чи можливо відновити дані.

Завершення розслідування злочинів пов’язаних з комп’ютерною технікою та інформаційними системами залежить від своєчасного і грамотного проведення необхідних експертиз. Використовують наступні традиційні експертизи: дактилоскопічні, трасологічні, фоноскопічні, фінансово-економічні, техніко-криміналістичні експертизи документів тощо.

Крім того, слід здійснювати судову комп’ютерно-технічну експертизу, різні інженерно-технічні експертизи. Вони основуються на необхідності діагностичних та ідентифікаційних процедур, які має здійснити експерт. Вони покликані вирішити наступні завдання:

– встановити факт здійснення злочину;

– встановити факт викрадення даних на технічних носіях;

– отримати дані про професійні якості злочинця.

Для порушення кримінальної справи за скоєння злочинів пов'язаних з комп'ютерною технікою та інформаційними системами мають бути підстави. До них відносяться достатність даних, які підтверджують скоєння злочину та мають наявність ознак складу злочину.

Зміст криміналістичної характеристики злочинів пов'язаних з комп'ютерною технікою та інформаційними системами визначає, що комп'ютерна техніка може бути предметом злочину, а також його засобом, що дозволяє злочинцю здійснити злочин.

Таким чином, наразі є об'єктивна потреба в узагальненні та впорядкуванні наявних методичних рекомендацій розслідування виявів шахрайств, учинених із використанням ЕОТ, для формування комплексної криміналістичної методики. Об'єднані в єдиній класифікаційній групі ідеї та теоретичні положення стають цілісною теоретичною концепцією, в основі якої – характеристика різних видів злочинів, урахування якої дає змогу об'єднати окремі рекомендації в єдину методику. До допоміжних компонентів цієї концепції належать положення криміналістичної класифікації злочинів, криміналістична характеристика злочинів, теорія криміналістичного прогнозування та ін. [12, с. 290 –291].

Ми можемо виділити наступні особливості у методиці розкриття і розслідування злочинів пов'язаних з комп'ютерною технікою та інформаційними системами:

– застарілість та неефективність традиційних методик розслідування злочинів, адже кіберзлочини мають значні особливості, що передбачають використання новітніх технологій;

– методики розслідування злочинів пов'язаних з комп'ютерною

технікою та інформаційними системами мають постійно змінюватися, адже щодня оновлюються бази даних вірусів, з'являються нові пристрої зчитування інформації, її викрадення, перехвату;

– необхідність підготовки спеціалістів за різними напрямами: юриспруденція, програмування, адміністрування мереж та інше;

– впровадження та розробка нових технічних засобів, які допомогли проведенню експертиз;

– нормативне регулювання використання мобільного інтернету, стаціонарного інтернету, закріплення IP-адрес за паспортами;

– постійний аналіз та використання досвіду розвинутих країн у боротьбі із кіберзлочинністю.

Отже, сучасний стан боротьби з шахрайствами, учиненими з використанням ЕОТ, визначив для криміналістики низку невирішених завдань. Найбільш суттєві з них – у галузі криміналістичної методики, оскільки саме тут прослідковується основне відставання рівня науково – методичних рекомендацій від потреб практики. Ідеться не лише про відсутність методик розслідування «нових» злочинів, а й про застарілість підходів до розслідування тих діянь (зокрема, шахрайства), що, зберігаючи стару кримінально-правову форму, значно змінилися змістовно. Нині розробка окремих методик у криміналістиці ведеться за шаблоном, у якому практичний аспект незрідка загалом відсутній, тоді як їх основою мають бути саме методи, адаптовані до рівня сприйняття конкретним користувачем.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ ЗЛОЧИНІВ ПОВ'ЯЗАНИХ З КОМП'ЮТЕРНОЮ ТЕХНІКОЮ ТА ІНФОРМАЦІЙНИМИ СИСТЕМАМИ І ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЇХ РОЗСЛІДУВАННЯ

2.1 Дослідження злочинів пов'язаних з комп'ютерною технікою та інформаційними системами

Сучасний етап технологізації суспільства характеризується переходом від простих поодиноких злочинів пов'язаних з комп'ютерною технікою та інформаційними системами до складної, а саме організованої злочинності.

М.О. Гвоздецька та К.Ю.Ісмайлов вважають, що щорічне зростання злочинів пов'язаних з комп'ютерною технікою та інформаційними системами пов'язане з активним застосування комп'ютерів у всіх значимих сферах життя суспільства, які є невід'ємною частиною сучасного миру [2, с. 52].

Водночас із позитивним впливом впровадження комп'ютерної техніки та інформаційних систем, цей процес супроводжується побічним негативним явищем криміногенного характеру, до якого належать злочини у сфері електронно –обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж або ж «комп'ютерна злочинність» (скорочена назва цього виду злочинів) [12, с. 287].

Поняття «злочини пов'язані з комп'ютерною технікою та інформаційними системами» передбачає противоправні незаконні дії з використанням комп'ютерної техніки з метою збагачення, наживи, нанесення моральної шкоди, власних інтересів, які передбачають викрадення даних, їх обробку, розповсюдження, перехват, продаж,

видалення або інші дії, які порушують право власності особистості на таку інформацію.

В.М. Стратонов влучно зазначає, що об'єктом посягання у злочинах пов'язаних з комп'ютерною технікою та інформаційними системами є інформація, оброблювана в комп'ютерній системі, а комп'ютер є знаряддям посягання [40, с. 87].

Цим видам злочинів присвячений XVI Розділ Кримінального Кодексу України, який регламентує кримінальні правопорушення, що здійсненні з використанням комп'ютерної техніки та інформаційних систем.

До кримінальних правопорушень у сфері використання електронно –обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку відповідно до чинного законодавства слід віднести:

– противоправний доступ до комп'ютерної техніки та інформаційних системам;

– розробка шкідливих програм, які дозволяють перехвачувати, використовувати, розповсюджувати, продавати отриману, за допомогою них, інформацію;

– противоправний незаконний продаж та розповсюдження викраденої інформації, яка зберігалась в комп'ютерній техніці та інформаційних системах, та мала обмежений до неї доступ, особами, що мали до неї офіційний доступ;

– противоправний незаконний продаж та розповсюдження викраденої інформації, яка зберігалась в комп'ютерній техніці та інформаційних системах, та мала обмежений до неї доступ, з використанням будь-яких засобів іншими особами;

– використання комп'ютерної техніки, інформаційних систем, інформаційних мереж, у способах, які порушують правила їх експлуатації;

– перешкода використання комп’ютерної техніки, інформаційних систем, інформаційних мереж, через розповсюдження вірусних повідомлень.

Відповідно до Кримінального кодексу України кожний з перелічених злочинів несе за собою відповідальність у вигляді штрафу зазначеного розміру, обмеження волі, або її позбавлення, заборона займати певні посади, обтяження виправними роботами, заборона певного види діяльності, яким не може займати особистість на визначений час.

За повторне здійснення будь-якого виду злочину пов’язаного з комп’ютерною технікою та інформаційними системами відповідальність посилюється. Крім того, на рівень відповідальності впливає розмір заподіяної шкоди. Так Кримінальний кодекс України визначає таке поняття, як значна шкода, вона полягає у заподіянні матеріальних збитків, які в 100 і більше разів вище ніж неоподатковуваний мінімум доходів, визначений законодавством на певну дату.

Нині шахрайство з використанням можливостей мережі «Інтернет» зберігає сталу тенденцію до еволюціонування, з’являються нові його види чи вдосконалюються вже відомі, зокрема:

– у сфері дистанційного банківського обслуговування, з електронними платіжними системами й швидкими системами оплати товарів: жебракування, розробка незаконних інтернет сторінок існуючих банків, їх маскування під офіційні сторінки, пропозиції щодо роботи, віртуальні гаманці, листування від імені інших осіб з вимаганням, проханням грошових коштів, шантажування з використанням фотографій, які відредактовано у фотошопі, різноманітні казино);

– шахрайство з вимаганням та списанням кредитних коштів (шпигунські програми, надання неіснуючих продуктів у кредит, креммінг, розробка Інтернет сторінок, які схожі на вже популярні, проте мають відмінності в одній букві, перепис вже існуючих сторінок з

використанням рерайтінгу та інше [16, с. 145].

Важливого значення в розкритті та розслідуванні злочинів пов'язаних з комп'ютерною технікою та інформаційними системами набрала Конвенція про кіберзлочиність від 01.07.2006 року. Вона включає в себе класифікацію злочинів пов'язаних з комп'ютерною технікою та інформаційними системами.

Конвенція про кіберзлочиність злочини пов'язані з комп'ютерною технікою та інформаційними системами розподіляє на три категорії:

– злочини пов'язані з комп'ютерною технікою та інформаційними системами що порушують конфіденційність, цілісність і працездатність комп'ютерів, даних, що в них зберігаються (викрадення даних, їх обробку, розповсюдження, незаконний перехват, продаж, видалення або інші дії, які порушують право власності особистості на таку інформацію);

– злочини пов'язані з комп'ютерною технікою та інформаційними системами що передбачають фальсифікацію і підробку;

– злочини пов'язані з комп'ютерною технікою та інформаційними системами щодо виробництва та розповсюдження дитячої порнографії [37].

Отже, прикладами злочинів пов'язаних з комп'ютерною технікою та інформаційними системами є: розробка та поширення програм-вірусів, шпигунство, перехват інформації, фармінг, підробка даних для заволодіння іншою інформацією, жебракування, розробка незаконних інтернет сторінок існуючих банків, їх маскування під офіційні сторінки, пропозиції щодо роботи, віртуальні гаманці, листування від імені інших осіб з вимаганням, проханням грошових коштів, шантажування з використанням фотографій, які відредактовано у фотошопі.

Тобто, злочини пов'язані з комп'ютерною технікою та інформаційними системами, як правило, здійснюються у мережі Інтернет та з використанням комп'ютерної техніки.

Слід виділити наступні специфічні особливості комп’ютерної інформації, яка використовується у злочинах пов’язаних з комп’ютерною технікою та інформаційними системами:

– обов’язковий зв'язок з фактичним носієм відсутній, тобто дані можуть зберігатися в мережі Інтернет;

– наявність можливості здійснення злочину фактично не знаходячись поряд з комп’ютером;

– можливість здійснення противоправних дій з великою кількістю інформації за короткий проміжок часу;

– необхідність розробки нових методів розслідування кіберзлочинів, адже традиційні методи мають дуже низьку ефективність, тобто практично не працюють.

Залежно від мотивів виділяють наступні види злочинів пов’язаних з комп’ютерною технікою та інформаційними системами:

– кіберзлочини, спрямовані на заволодіння коштами;

– кіберзлочини, спрямовані на захват інформації, як для власних потреб, так із метою подальшого розповсюдження, або продажу даних зацікавленим особам;

– втручання в роботу комп’ютерної техніки, інформаційних систем або інформаційних мереж задля отримання доступу до автоматичних систем управління (з метою навмисного пошкодження за винагороду або для нанесення шкоди конкурентам);

– всі інші злочини, що не враховані.

На думку фахівця Васильковського І. І, існує п’ять основних типів злочинів пов’язаних з комп’ютерною технікою та інформаційними системами, які мають подібні цілі та методи:

– злочини пов’язані з комп’ютерною технікою та інформаційними системами з метою фінансової наживи, які здійснюються однією особою або організованим приступним угрупуванням з метою заволодіння грошовими коштами населення, юридичних осіб;

– злочини пов’язані з комп’ютерною технікою та інформаційними системами направлені на шкоду інтелектуальній власності, вони здійснюються однією особою або організованим приступним угрупуванням з метою викрадення, розповсюдження матеріалів, які відносяться до комерційної таємниці та є інтелектуальною власністю. Найчастіше такі злочини проявляються у виробництві піратських копій відомих виконувачів музики, фільмів, мультфільмів та інше;

– злочини пов’язані з комп’ютерною технікою та інформаційними системами направлені на шкоду воєнної сфери держави, вони здійснюються однією особою або, як правило, на замовлення представників інших держав з метою викрадення, ознайомлення з даними, які відносяться до воєнної таємниці та належать певній державі. Такі злочини здійснюються, як правило, при військових конфліктах між державами. Вони передбачають злочини національного масштабу та можуть бути направлені на порушення всіх галузей діяльності держави (енергетична, транспортна, фінансова та інші);

– злочини пов’язані з комп’ютерною технікою та інформаційними системами направлені на тероризм. Ця група злочинів є однією із найнебезпечніших та може перекликатися із злочинами військового напряму. Як правило, такі злочини здійснюються терористичними угрупуваннями, з метою захвату найбільш важливих та стратегічних об’єктів державного або приватного призначення;

– злочини пов’язані з комп’ютерною технікою та інформаційними системами направлені на активізм. Як правило, такі види злочинів здійснюються ідейними активістами [39, с. 278].

Криміналістична характеристика будь-якого злочину передбачає наявність певних елементів, одним з яких є особа злочинця. Криміналістичне вивчення стосовно особи злочинця в кримінальних провадженнях полягає як у встановленні даних, що відображають сутність особи, яка вчинила злочин, у розрізі до вимог чинного

кримінального та кримінально-процесуального законодавства, так і у виявленні комплексу значущих ознак цієї особи, які можуть бути використані для її встановлення, розшуку та викриття. Зміст особи злочинця як елементу криміналістичної характеристики полягає у визначенні особи як певної системи, властивості та ознаки якої знаходять відображення в навколишньому середовищі та використовуються під час розслідування злочинів [6, с. 213].

Аналізуючи вивчення криміналістичної характеристики особи злочинця в контексті розслідування кіберзлочинів, наведемо деяку класифікацію. Скажімо, О. А. Самойленко пропонує такі типи особи злочинця, що вчиняє злочин з використанням обстановки кіберпростору:

1) злочинець-користувач з початковим рівнем знань;

2) злочинець-користувач;

3) злочинець-упевнений користувач;

4) злочинець-досвідчений користувач;

5) злочинець-користувач професіонал [8, с. 200].

О. В. Курман виділяє декілька груп осіб, які здійснюють незаконне втручання в роботу комп'ютерної техніки та інформаційних систем (мереж):

1) працівники будь-яких інших підприємств, установ, організацій – конкурентів;

2) працівники, які вчиняють незаконні дії з інформацією на замовлення, перебуваючи з її власником (уповноваженим органом) у трудових відносинах;

3) працівники, які збирають інформацію для себе (про всяк випадок);

4) особи, професійна або службова діяльність яких чи інші законні підстави обумовлюють виникнення певних правовідносин цивільно – правового характеру з власником інформації;

5) особи, які не перебувають у жодних цивільно-правових чи

трудових відносинах з власником, але вчиняють незаконні дії через «спортивний інтерес», бажання заявити про себе, прорекламувати свої можливості та уміння, на замовлення сторонніх осіб (для передачі конкурентам чи вчинення шантажу) [7, с. 130].

Така класифікація особи злочинця може мати місце при розслідуванні несанкціонованого втручання в роботу комп'ютерної техніки, інформаційних систем, комп'ютерних мереж, де іншими елементами криміналістичної характеристики зазначеного злочину виступають: виток, втрата, підробка, блокування інформації, спотворення процесу обробки інформації та порушення встановленого порядку маршрутизації інформації, а також обстановка, сліди, способи вчинення злочину і його приховування. У зв'язку з цим було б неправильним при розслідуванні цієї категорії злочинів розглядати криміналістичний аспект особи злочинця у відриві від вищевказаних елементів криміналістичної характеристики, оскільки саме вони дають змогу в багатьох ситуаціях істотно обмежити та звузити коло осіб, які можуть бути причетні до вчинення злочину.

Таким чином, дослідження злочинів пов'язаних з комп'ютерною технікою та інформаційними системами показало, що це особливий вид злочинів, що включають дії, спрямовані на заволодіння коштами, викрадення інформації, втручання в роботу комп'ютерної техніки з метою викрадення даних, доступу до інформаційних систем, або інші злочини, за які передбачено кримінальну відповідальність та певні заходи покарання. Злочини пов'язані з комп'ютерною технікою та інформаційними системами здійснюють різні груп осіб, які здійснюють несанкціоноване втручання в роботу електронно-обчислювальних машин, вони не мають вікових, соціальних обмежень та мають різні мотиви.

2.2 Шляхи підвищення ефективності розслідування злочинів пов'язаних з комп'ютерною технікою та інформаційними системами

Нині в Україні намагаються протидіяти злочинам пов'язаним з комп'ютерною технікою та інформаційними системами, задля забезпечення конституційних прав населення, забезпечення їх прав власності, інформаційної безпеки. Проте слід визнати, що традиційні методи розслідування злочинів пов'язаних з комп'ютерною технікою та інформаційними системами неефективні.

Розповсюдження злочинів пов'язаних з комп'ютерною технікою та інформаційними системами призводить до необхідності постійного пошуку шляхів підвищення ефективності розслідування та розкриття таких видів злочинів. Розробка шляхів підвищення ефективності розслідування злочинів пов'язаних з комп'ютерною технікою та інформаційними системами здійснюється за різними напрямками. Одним із таких напрямків є практично-науковий, який передбачає детальне дослідження таких злочинів. Так для визначення сутності та механізму розвитку феномена злочинів пов'язаних з комп'ютерною технікою та інформаційними системами немаловажне значення має аналіз кримінологічних характеристик, які, доцільно, розкривати за наступними групами ознак:

– кримінально-правова;

– кримінологічна;

– соціально-демографічна.

Соціально-демографічна кримінологічна характеристика передбачає дослідження особистості потерпілого та злочинця.

Підвищення ефективності розслідування злочинів пов'язаних з комп'ютерною технікою та інформаційними системами має передбачати впровадження оптимальних засобів протидії таким злочинам,

впровадження новітніх засобів їх розслідування, звертання до найбільших професіоналів у сфері комп'ютерної техніки, інформаційних систем, програмування для співпраці у розробки ефективних заходів розслідування.

Окрім вищепереліченого має постійно здійснюватися профілактика таких злочинів.

Підвищення ефективності розслідування злочинів пов'язаних з комп'ютерною технікою та інформаційними системами можливе за рахунок:

– розробка шляхів попередження злочинів пов'язаних з комп'ютерною технікою та інформаційними системами;

– розробка та посилення нормативно-правового регулювання відповідальності за скоєння злочинів пов'язаних з комп'ютерною технікою та інформаційними системами;

– розробка організаційно-адміністративних заходів розкриття злочинів пов'язаних з комп'ютерною технікою та інформаційними системами;

– розробка шляхів захисту інформації, що зберігається в комп'ютерній техніці та інформаційних системах;

– підготовка висококваліфікованих кадрів розслідування злочинів пов'язаних з комп'ютерною технікою та інформаційними системами.

Для розробки шляхів підвищення ефективності розслідування злочинів пов'язаних з комп'ютерною технікою та інформаційними системами необхідно визначити проблемні питання щодо розслідування таких злочинів. Так В.М. Стратонов звертає увагу на те, що основна проблема сучасного етапу, полягає в рівні спеціальної підготовки посадових осіб правоохоронних органів, котрі мають втілювати в життя вимоги нових законів. Надаючи криміналістичні рекомендації у сфері інформаційних правовідносин, варто враховувати різнорідність складу й освітній рівень нашого слідчо-судового апарату. Ясно, що є вже і добре

підготовлені фахівці. Але багато співробітників органів слідства і дотепер не тільки не використовують технічні засоби й інформаційні технології у своїй діяльності, але і недостатньо інформовані про них [40, с. 86].

Нині актуальним в процесі проведення розслідування кіберзлочинів є питання швидкого обміну інформацією, покращення якості розслідування за допомогою налагодження активної взаємодії між прокурорами і органами досудового розслідування для встановлення користувачів послуг зв‘язку, збору відомостей про рух інформації та інших технічних під час проведення перевірки за заявами та повідомленнями, що внесені до Єдиного реєстру досудового розслідування, а також створення та використання спеціальних банків зберігання електронних доказів, проведення належного розслідування кримінальних проваджень про кіберзлочини.

В.М. Стратонов вважає, що розслідування комп’ютерних злочинів істотно відрізняється від розслідувань інших «традиційних» злочинів, однією з істотних причин низької якості слідства є відсутність систематизованих і відпрацьованих методів розслідування комп’ютерних злочинів, а також помилки при проведенні слідчих дій щодо комп’ютерної інформації або самих комп’ютерів. Саме тому науковець рекомендує ввести змішану класифікацію інформаційних злочинів, яка б враховувала й особливості злочинів скоєних за допомогою засобів ЕОТ і цифрового зв’язку, й особливості родових об’єктів інформаційних злочинів (додаток А) [40, с. 87].

Подібна класифікація дозволить поглянути на інформаційні злочини як на цілісну взаємопов’язану систему, а не набір окремих злочинів, пов’язаних із явищем інформації [40, с. 87].

Сучасне українське законодавство, що закріплює порядок розслідування злочинів пов’язаних з комп’ютерною технікою та інформаційними системами є недосконалим та потребує уточнення,

виконання вимог міжнародних співтовариств, тобто уніфікації.

Невдовзі Україна може опинитися в ситуації, коли рівень знань злочинців може значно перевищити рівень знань фахівців, що мають їх розслідувати. Така ситуація в умовах повсякденного розповсюдження комп'ютерної техніки та інформаційних систем є критичною. Наразі велика кількість злочинів залишається нерозкритою.

Як влучно зазначає К.Ю. Ісмайлов, кількість злочинів пов'язаних з комп'ютерною технікою та інформаційними системами постійно зростає, тож у правоохоронних органах виникає необхідність адекватно на них реагувати та розслідувати. Адже злочинність у кіберпросторі має зустріти протидію, що можливе лише за умови належного правового та фінансового забезпечення правоохоронної діяльності. Держава має здійснювати підготовку висококваліфікованих спеціалістів, тож потребує коригування система навчання у вищих навчальних закладах за напрямком юриспруденція, захисту інформації, зв'язок з громадськістю, журналістський напрямок [5, с. 215].

Аналіз практичних даних розслідування злочинів пов'язаних з комп'ютерною технікою та інформаційними системами показав, що існує нагальна потреба розробки нових підходів та заходів розслідування таких злочинів, адже статистика розслідування таких злочинів свідчить про низький рівень розкриття таких злочинів. Постійні зміни у програмному забезпеченні, появи нових вірусів, розростання мережі Інтернет, збільшення кількості користувачів, поява нових гаджетів підтверджують необхідність підвищення кваліфікації та професійного рівня всіх посадових осіб, що здійснюють розслідування таких злочинів. Недостатність досвіду та знань призводить до помилок при розслідуванні, відсутності додаткової інформації, що підтверджує здійснення злочинів, отримання доказів та інше [47, с.136].

Відсутність необхідного досвіду та знань в органах прокуратури та внутрішніх справ, які займаються розслідуванням злочинів пов'язаних з

комп’ютерною технікою та інформаційними системами ускладнює прийняття швидких і оперативних рішень у кримінальних провадженнях про такі види злочинів. Крім того, слід виділити наступні проблемні питання при розслідуванні злочинів пов’язаних з комп’ютерною технікою та інформаційними системами:

– перехід більшої частини користувачів мережі Інтернет від використання комп’ютерів до гаджетів, а саме мобільного Інтернету, що ускладнює визначення IP-адреси злочинця;

– використання членами міжнародних злочинних організацій закритих TOR-мереж, що унеможливлює отримання відповідних результатів шляхом проведення негласних слідчих (розшукових) дій;

– відсутності міжнародної бази даних про вчинені злочини пов’язані з комп’ютерною технікою та інформаційними системами;

– високої латентністю вказаних видів злочинів, оскільки фінансові установи (банки) не бажають афішувати факти незаконного втручання в роботу їхньої установи з метою збереження власного іміджу;

– недостатньої кількості державних експертів в області комп'ютерно-технічної експертизи.

Таким чином, злочини пов’язані з комп’ютерною технікою та інформаційними системами є особливо важливими для розслідування, адже є суспільно-небезпечними та протиправними діями, направленими на завдання шкоди населенню, юридичним особам, корпораціям, брендам. Саме тому постає актуальне питання розробки шляхів попередження та підвищення ефективності розслідування злочинів пов’язаних з комп’ютерною технікою та інформаційними системами.

ВИСНОВКИ

Таким чином, злочини пов’язані з комп’ютерною технікою та інформаційними системами – це правопорушення, які тягнуть за собою кримінальну відповідальність, що здійснюються за допомогою комп’ютерної техніки та посягають на конфіденційні дані, чим порушують право власності на інформацію чи інформаційні системи, здійснюючи на них негативний вплив.

Способи вчинення злочинів пов’язаних з комп’ютерною технікою та інформаційними системами дуже різноманітні і постійно змінюються. Визначення способів здійснення цих злочинів має велике значення, адже їх усунення дозволяє захистити від порушення прав власності, махінацій із грошовими коштами, втручання в дані підприємства чи фізичних осіб, несанкціоноване поширення інформації, що має комерційний інтерес, персональні дані.

Сучасний стан боротьби з шахрайствами, учиненими з використанням ЕОТ, визначив для криміналістики низку невирішених завдань. Найбільш суттєві з них – у галузі криміналістичної методики, оскільки саме тут прослідковується основне відставання рівня науково-методичних рекомендацій від потреб практики. Ідеться не лише про відсутність методик розслідування «нових» злочинів, а й про застарілість підходів до розслідування тих діянь (зокрема, шахрайства), що, зберігаючи стару кримінально-правову форму, значно змінилися змістовно. Нині розробка окремих методик у криміналістиці ведеться за шаблоном, у якому практичний аспект незрідка загалом відсутній, тоді як їх основою мають бути саме методи, адаптовані до рівня сприйняття конкретним користувачем.

Дослідження злочинів пов’язаних з комп’ютерною технікою та інформаційними системами показало, що це особливий вид злочинів, що

включають дії, спрямовані на заволодіння коштами, викрадення інформації, втручання в персональні дані, розповсюдження даних інформаційних систем, або інші злочини, за які передбачено кримінальну відповідальність та певні заходи покарання. Злочини пов'язані з комп'ютерною технікою та інформаційними системами здійснюють різні груп осіб, які здійснюють несанкціоноване втручання в роботу електронно-обчислювальних машин, вони не мають вікових, соціальних обмежень та мають різні мотиви.

Аналіз практичних даних розслідування злочинів пов'язаних з комп'ютерною технікою та інформаційними системами показав, що існує нагальна потреба розробки нових підходів та заходів розслідування таких злочинів, адже статистика розслідування таких злочинів свідчить про низький рівень розкриття таких злочинів. Постійні зміни у програмному забезпеченні, появи нових вірусів, розростання мережі Інтернет, збільшення кількості користувачів, поява нових гаджетів підтверджують необхідність підвищення кваліфікації та професійного рівня всіх посадових осіб, що здійснюють розслідування таких злочинів. Недостатність досвіду та знань призводить до помилок при розслідуванні, відсутності додаткової інформації, що підтверджує здійснення злочинів, отримання доказів та інше.

Таким чином, злочини пов'язані з комп'ютерною технікою та інформаційними системами є особливо важливими для розслідування, адже є суспільно-небезпечними та протиправними діями, направленими на завдання шкоди населенню, юридичним особам, корпораціям, брендам. Саме тому постає актуальне питання розробки шляхів попередження та підвищення ефективності розслідування злочинів пов'язаних з комп'ютерною технікою та інформаційними системами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики: дис. ... канд. юрид. наук: 12.00.08. Иркутск, 2008. С. 269.

2. Гвоздецька М.О., Ісмайлов К.Ю. Кримінологічна характеристика кіберзлочинності: сучасний стан, структура та специфіка вчинення. *Актуальні задачі та досягнення у галузі кібербезпеки.* Матеріали Всеукраїнської науково-практичної конференції 23–25 листопада 2016 року, м. Кропивницький. 2016. С.52-53.

3. Берназ П.В. Структура криміналістичної характеристики злочину. *Південноукраїнський правничий часопис*. 2017. № 3. С. 11-14.

4. Конвенція Ради Європи «Про кіберзлочинність». URL: http://zakon2.rada.gov.ua/laws/show/994_575 (звернення від 06.10.2021) .

5. Ісмайлов К.Ю. Прорахунки в інформаційно-правовій підготовці фахівців. *Роль та місце правоохоронних органів у розбудові демократичної правової*: Матеріали VIII Міжнародної науково-практичної конференції (м. Одеса, 25 березня 2016 р.). Одеса: Одеський державний університет внутрішніх справ, 2016. С. 215-216.

6. Бородай О. В. Особа злочинця як елемент криміналістичної характеристики несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка, 2018. №4(84). С. 212-220. URL: https://doi.org/10.33766/2524-0323.84.212-220 (звернення від 08.10.2021)

7. Курман О. В. Криміналістична характеристика несанкціонованого втручання в роботу електронно-обчислювальних

машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Науковий вісник Херсонського державного університету. Серія «Юридичні науки». №4. Том 2. 2017. С. 127-130.

8. Самойленко О. А. Типизація особи, що вчиняє злочин, пов'язаний із використанням обстановки кіберпростору (з позицій криміналістичної науки). Підприємництво, господарство і право. 2018. № 8. С. 195-201.

9. Кримінальний кодекс України: Закон від 05.04.2001 № 2341-III. Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст. 131. (із поточними змінами). URL : http://zakon3.rada.gov.ua/laws/show/2341-14 (дата звернення: 19.10.2021).

10. Кримінальний процесуальний кодекс України : Закон від 13.04.2012 № 4651-VI. Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11- 12, № 13, ст.88. (із поточними змінами). URL: http://zakon2.rada.gov.ua/ laws/show/4651-17 (дата звернення: 19.10.2021).

11. Джеймс Л. Фишинг. Техника компьютерных преступлений (пер. с англ. Р. В. Гадицкого). Москва: НТ Пресс, 2008. 320 с.

12. Романенко Т. В. Стан наукових досліджень проблем розслідування шахрайств, учинених із використанням електронно-обчислювальної техніки. Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. 2020. №3(91). С.286-294. URL: https://doi.org/10.33766/2524-0323.91.286-294 (дата звернення 16.10.2021)

13. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469- VIII. URL:https://zakon.rada.gov.ua/laws/show/2469-19#n355. (дата звернення 16.10.2021)

14. Баулін Ю. В., Борисов В. І., Тютюгін В. І. та ін. Кримінальне право України: *Особлива частина: підручник*; за ред. В. В. Сташиса, В. Я. Тація; 4-те вид, переробл. і допов. Харків: Право, 2010. 608 с.

15. Susan H. Nycum. The Criminal Law Aspects of Computer Abuse: *Applicability ofthe State Penal Laws to Computer Abuse (Menlo Park,*

California, Stanford Research Institute, 1976). Ulrich Sieber, Computerkriminalität und Strafrecht (Cologne, Karl Heymanns Verlag, 1977). URL:http:// www.worldcat.org/title/criminal-law- aspects-of-computer- abuse- applicability-of-the- state-pe nal-laws-to-computerabuse/oclc/654145221/editions?referer=di&editionsView=true.

16. Шапочка С. В. До питання запобігання окремим видам шахрайства, яке вчиняється з використанням можливостей мережі Інтернет. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2014. № 1. С. 145–149.

17. Голубєв В. О. Розслідування комп'ютерних злочинів: монографія. Запоріжжя: Гуманітарний університет «ЗІДМУ», 2003. 296 с.

18. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2005. 20 с.

19. Моїсеєв О. М. Залучення спеціаліста до розслідування комп'ютерних злочинів. *Правові основи захисту комп'ютерної інформації від протиправних посягань: матеріали міжвузівської наук.-практ. конф.* (м. Донецьк, 22 грудня 2000 р.). Донецький інститут внутрішніх справ, 2001. С. 81–85.

20. Миколенко О. М. Деякі особливості розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Кібербезпека в Україні: правові та організаційні питання*: матеріали Всеукр. наук.-практ. конф. (м. Одеса, 21 жовтня 2016 р.). Одеса: ОДУВС, 2016. с. 155–157.

21. Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування: монографія. Київ, 2010. 624 с.

22. Анапольська А. І., Коваленко В. В., Корякін Р. В. та ін. Особливості розслідування шахрайств, учинених у сфері

функціонування електронних розрахунків: метод. рек. Луганськ, 2010. 56 с.

23. Користін О. Є., Бутузов В. М., Василевич В. В. та ін. Протидія кіберзлочинності в Україні: правові та організаційні засади: навч. посіб. Київ: Видавничий дім «Скіф», 2012. 728 с.

24. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет»: дис. канд. юрид. наук: 12.00.09. Донецьк, 2014. 100 с.

25. Тіщенко В. В. Теоретичні і практичні основи методики розслідування злочинів: монографія. Одеса: Фенікс, 2007. 260 с.

26. Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів: автореф. дис. ... канд. юрид. наук: 12.00.09. Київ, 2008. 20 с.

27. Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф., м. Одеса, 17 листопада 2017 р. Одеса: ОДУВС, 2017. 204 с.

28. Бутузов В. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз). К. : КИТ, 2010. 148 с.

29. Погорецький М., Шеломенцев В. Кіберзлочини: до визначення поняття. Вісник прокуратури. 2012. № 8. С. 89–96.

30. Словник термінів з кібербезпеки / за заг. ред. О. Копатіна, Є. Скулишина. К. : Аванпост - Прим, 2012. 214 с.

31. Болгов В., Гадіон Н.М., Гладун О.З. та ін. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій. К.: Національна академія прокуратури України, 2015. 202 с.

34. Миколенко О.М. Деякі особливості розслідування злочинів у сфері використання електроннообчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Кібербезпека в Україні: правові та організаційні питання* : матеріали Всеукр. наук.-практ. конф. (м. Одеса, 21 жовтня 2016 р.). Одеса : ОДУВС, 2016. 233 с.

35. Моїсеєв О. М. Залучення спеціаліста до розслідування комп'ютерних злочинів. *Правові основи захисту комп'ютерної інформації від протиправних посягань:* матеріали міжвузівської науково-практичної конференції (м. Донецьк, 22 грудня 2000 р.). Донецький інститут внутрішніх справ, 2001. С. 81–85.

36. Мухин Г. Н. Структура и содержание методики расследования преступлений, связанных с посягательством на информационные ресурсы. Управление защитой информации. 1999. Т. 3, № 3. С. 315.

37. Конвенція про кіберзлочинність від 01.07.2006 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення 02.10.2021)

38. Авдєєва Г. К. Використання спеціальних знань у боротьбі з комп'ютерною злочинністю. Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка: матеріали. 2016. №1. С. 268-277.

39. Васильковський І. І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика). 2018. №1–2 (10–11). С. 276-282.

40. Стратонов В. М. Інформація та інформаційні відносини як новий криміналістичний об'єкт. *Правова система: теорія і практика.* 2019. №2. С. 84-88.

41. Стратонов В. М. Інформаційно-пізнавальні можливості криміналістичної техніки. Вісник Національного університету внутрішніх справ. 2002. №20. С. 56-58.

42. Белкин Р.С. Курс криминалистики. В. 3 т. Т. 3 *Криминалистические средства, приемы и рекомендации.* М. Юристь, 1997. 480 с.

43. Советская криминалистика. *Методика расследования отдельных видов преступлений*. Киев, 1988. 405 с.

44. Старушкевич А.В. Криміналістична характеристика злочинів: Навчальний посібник. Київ: НВТ «Правник» – НАВС, 1997. 44 с.

45. Криминалистика / Под ред. И.Ф. Герасимова, Л.Я. Драпкина. М., 1994. С. 330 –333.

46. Чванкин В.И. Криминалистическая структура преступлений, нарушающих смежные и авторские права оборотом контрафактной продукции. Вестник Полоцкого государственногоуниверситета. 2014. № 5. С. 146 –152.

47. Проблеми забезпечення ефективності діяльності органів кримінального переслідування в Україні: монографія / кол. авт. ; за заг. ред. В.І. Борисов, В.С. Зеленецький. Х. : Право, 2010. 400 с.

Додаток А

Змішана класифікація інформаційних злочинів за В.М. Стратоновим