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

МЕТОДИКА РОЗСЛІДУВАНЬ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У СФЕРІ ВИКОРИСТАННЯ ЕОМ, СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

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

Виконала: студентка 2 курсу 10-282 МЗ групи
Спеціальності 081 Право
Освітньо-професійної програми «Право»
Пелюховська Лідія Петрівна

Керівник: к.ю.н., доцент **Проценко М.В.**
Рецензент:
доцентка кафедри адміністративного права та адміністративного процесу
Херсонського факультету
Одеського державного університету внутрішніх справ
к.ю.н. **Шевченко Н.Л.**

Херсон – 2021

ЗМІСТ

ВСТУП

Актуальність теми. Стрімкий розвиток персональних комп’ютерів, комп’ютерних мереж та систем і, особливо глобальної комп’ютерної мережі «Інтернет» призвів до появи нових видів корисних суспільних відносин, пов’язаних з їх використанням.

Питання, пов’язані із боротьбою з кіберзлочинністю, раніше були предметом досліджень таких вчених, як В. Д. Гавловський, О. І. Гарасимів, О. М. Дуфенюк, В. А. Журавель, О. В. Захарова, А. В. Іщенко, М. І. Камлик, В. О. Коновалова, М.О. Ларкін, В. В. Пясковський, Б. В. Романюк, В. П. Сабадаш, А. В. Самодін, В. Ю. Шепітько, Ю. М. Чорноус. Однак, незважаючи на значний внесок досліджень вказаних вчених в розвиток правової науки, низка проблемних питань досліджена лише фрагментарно. До них відносяться, зокрема, проблемні питання, пов’язані з методикою розслідувань кримінальних правопорушень у сфері використання мереж електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж. Удається за необхідне провести дослідження зазначених питань.

Мета і задачі дослідження. Метою дослідження є розгляд проблемних питань, пов’язаних з методикою розслідувань кримінальних правопорушень у сфері використання мереж електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж.

Нами поставлено такі **завдання** для досягнення мети дослідження**:**

– дослідити основні етапи розвитку кіберзлочинності

– проаналізувати елементи методики розслідувань кримінальних правопорушень у сфері використання мереж електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж;

– дослідити тактичні особливості проведення оперативно-розшукових заходів при розслідуванні кримінальних правопорушень у сфері використання мереж електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж;

– розглянути тактичні особливості проведення слідчих дій при розслідуванні кримінальних правопорушень у сфері використання мереж електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж.

Об’єктом дослідження є **дослідження** корисних суспільних відносин, пов’язаних із розслідуванням кримінальних правопорушень у сфері використання мереж електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж.

Предметом дослідження є результати наукових досліджень, правові норми, за допомогою яких визначається розслідування кримінальних правопорушень у сфері використання мереж електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж.

Методи дослідження обрані, виходячи із мети і завдань роботи, а також із врахуванням об’єкта і предмета дослідження. В основу дослідження покладено метод ідеалістичної діалектики як фундаментальний (філософський) метод наукового пізнання.

При проведенні дослідження використовувались загально наукові методи: аналізу, версії, аналогії, дедукції, індукції, синтезу, описовий, формально-юридичний, експериментальний, порівняльний, порівняльно-правовий, статистичний, системно-структурний.

Наукова новизна одержаних результатів у тому, що надана робота робить спробу комплексного дослідження проблемних питань, пов’язаних із розслідуванням кримінальних правопорушень у сфері використання ЕОМ, систем та комп'ютерних мереж і мереж електрозв'язку.

Практичне значення роботи у виявленні основних проблемних питань щодо методики розслідувань кримінальних правопорушень у сфері використання ЕОМ, систем та комп'ютерних мереж і мереж електрозв'язку. У роботі сформульовані висновки, пропозиції та рекомендації можуть бути використані в подальшому дослідженні даної теми, а окремі положення та висновки роботи – в процесі підготовки і проведення практичних занять з курсу «Криміналістика», «Актуальні проблеми кримінального права».

Апробація результатів дослідження. Основні положення дослідження були представленні на ІІ-му дискусійному форумі «Сучасні проблеми державотворення та право» організованому ГО УКРАЇНСЬКО-СЛОВАЦЬКИЙ ЦЕНТР ПАРТНЕРСТВА (29 листопада 2021 р., м. Херсон).

Структура роботи обумовлена метою та завданнями дослідження і складається із вступу, двох розділів, які поділяються на чотири підрозділи, висновків, списку використаних джерел.

РОЗДІЛ 1
ЗАГАЛЬНІ ПОЛОЖЕННЯ МЕТОДИКИ РОЗСЛІДУВАНЬ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У СФЕРІ ВИКОРИСТАННЯ МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ, ЕЛЕКТРОННИХ ОБЧИСЛЮВАЛЬНИХ МАШИН, СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ

1.1. Основні етапи розвитку кіберзлочинності

Слушним, на думку автора, уявляється аналіз основних етапів розвитку кіберзлочинності.

Розвиток кіберзлочинності можна зарахувати до настання так званої комп’ютерної ери.

Історію кіберзлочинності можна розділити на дві фази:

1. Перша – від створення першого комп’ютера і до початку 90-х років 20 століття.

2. З початку 90-х років 20 століття і до теперішнього часу.

Причина саме такого розподілу полягає у тому, що з початку 90-х років комп’ютерна мережа Інтернет почала поширюватися по країнах усього світу з надзвичайною швидкістю.

Вперше застосування комп’ютеру для вчинення з кримінального правопорушення було зафіксовано у 60-х роках 20 століття, коли комп’ютери були великими за розмірами та універсальними.

Після Другої світової війни в 1946 році багато компаній почали розробляти комп’ютери, які б могли працювати в приватних підприємствах, установах та організаціях. До 1951 року розробка цих комп’ютерів була завершена і американська фірма UNIVAC випустила перший комерційний комп'ютер у Сполучених Штатах Америки. До цього комп’ютери, пристосовані для діяльності у комерційних фірмах були розроблені та випущені у Великобританії та Німеччині. Перші

американські «цивільні» комп’ютери, випущені на протязі 50-х років 20 століття, використовувались у державних установах, які працювали з великим обсягом статистичних даних, комерційними установами та вищих навчальних закладах.

Зрозуміло, що використанню комп’ютерів в якості об’єктів злочинів та засобів їх вчинення в той час заважали наступні фактори:

1. Вкрай невелика кількість комп’ютерів.

2. Використання комп’ютерів в установах, де існувала технічна можливість організувати контроль за їх використанням.

3. Занадто «скромні» характеристики комп’ютерів.

4. Обмежене коло функцій, які могли виконувати комп’ютери.

5. Відсутність мереж для зв’язку комп’ютерів.

6. Невелика кількість спеціалістів в комп’ютерній галузі, за діяльністю яких порівняно легко можна було встановити контроль.

Поступово розміри комп’ютерів зменшувались, а надійність, потужність та швидкість, навпаки, збільшувались. Суттєво збільшився також обсяг пам’яті комп’ютерів. З середині 50-х років замість електронних ламп на комп’ютерах почали використовуватись транзистори.

В 60-ті роки 20 століття для роботи комп’ютерів почали використовуватись інтегральні мікросхеми, «напівпровідникова» пам’ять (використовується і дотепер). З’явилися перші стандарти щодо будови комп’ютерів, що зробило їх сумісними один з одним.

Зазначені вдосконалення, в свою чергу, одразу призвели до наступних суттєвих змін у використанні комп’ютерів:

1. Комп’ютери стали доступними для використання невеликими підприємствами, установами, організаціями, лабораторіями.

2. Через суттєвого зменшення ціни та вдосконалення технологій виробництва значно виросли обсяги серійного виробництва комп’ютерів.

3. З’явились так звані «міні-комп’ютери», які хоч і не були занадто потужними, але їх потужності цілком вистачало для використання великою кількістю організацій, для яких велика потужність не має значення, а вирішальними факторами є доступність, помірні розміри та мінімальний набір функцій.

В 70-ті роки 20 століття з’явились вже цілком доступні для великого кола користувачів персональні комп’ютери, чим, у свою чергу, було забезпечено умови для поширення комп’ютерної злочинності. Однак, реалії розвитку комп’ютерів того часу призвели до наступних відмінностей тогочасної «комп’ютерно» злочинності від теперішньої:

1. В той час не існувало Інтернету та інших комп’ютерних мереж.

2. Комп’ютери того часу все ще залишалися порівняно дорогими.

3. Коло осіб, які мали знання і навички для роботи з комп’ютерами, все ще залишалось невеликим.

До появи та широкого розповсюдження комп’ютерних мереж об’єктивна сторона «комп’ютерних» злочинів полягала, як правило, у фінансових махінаціях, пов’язаних з їх виробництвом.

Заслуговує, на думку автора, аналіз наступних етапів розвитку злочинної діяльності у сфері використання ЕОМ, систем та комп'ютерних мереж і мереж електрозв'язку:

1. До появи та широкого розповсюдження комп’ютерної мережі «Інтернет».

1.1. 60-ті роки 20 століття. Поява групи хакерів у Массачусетському технологічному інституті з числа студентів. Зазначені особи зробили перші спроби незаконних маніпуляцій з програмним забезпеченням комп’ютерів.

1.2 70-ті роки 20 століття. Злом місцевих та міжнародних телефонних ліній для отримання можливості безкоштовного ведення телефонних розмов. злом здійснювався за допомогою пристрою зі свистком всередині, за допомогою якого генерувався сигнал на частоті,

яка співпадала із частотою електричного сигналу, який використовувався в телефонній мережі для отримання доступу до ней. Пристрій подавав штучно генерований сигнал у мікрофон телефону.

1.3. 80-ті роки 20 століття. Фрікери та хакери ведуть злочинну діяльність, спрямовану на незаконний доступ до кредитних карт, викрадаючи паролі та коди доступу до них, здійснюють «обмін досвідом». Формуються перші хакерські групи.

1.4. 1983 рік. Вперше в історії з'являється фільм про хакерів «Ігри військових», поліцією заарештовано кілька підлітків, які здійснили злом 60 комп'ютерів, зокрема комп'ютер, який належав лабораторії ядерних досліджень.

1.5 1984 рік. Починає публікуватися спеціальний журнал для хакерів «2600», а також кілька онлайн-журналів для хакерів, за допомогою яких хакерами здійснюється «обмін досвідом» та «поради».

1.6. 1986 р. Конгрес США на законодавчому рівні закріплює злом комп'ютерів як злочин.

1.7. 1988 р. Програма, розроблена студентом Корнельського університету Р. Моррісом, вивела з ладу близько 6000 на території Сполучених Штатів Америки.

2. Починаючи з середини 90-х років 20 століття. Починаючи з цього часу комп'ютерна мереж «Інтернет» отримує широке визнання та швидке розповсюдження. У грудні 1995 року, за деякими даними, зареєструвалося 16 мільйонів користувачів Інтернету у всьому світі, а до травня 2002 року ця цифра зросла до 580 мільйонів, що становить майже 10 відсотків від усього населення планети (NUA, 2003). Слід зазначити, що поширення Інтернету нерівномірне у всьому світі, наприклад, більше 95 відсотків від загальної кількості Інтернет -посилань у США, Канаді, Європі, Австралії та Японії. Цього разу в історію злочинності був внесений новий вид злочинів, який має назву «Злом» і включає поняття

злочинів кіберзлочинності. Це хакерство, яке виявляє протиправну діяльність хакерів.

2.1 1990 р. У Сполучених Штатах Америки хакери звинувачуються у крадіжці кредитів з числа кредитів та зломі телефонних дзвінків. Заарештовані свідчать один про одного про судовий імунітет. Спільноти сильно вразили хакерів.

2.2 1993 р. У вікторині розіграшу в прямому ефірі на одній з радіостанцій кур'єр ровера Кевін Полсен та двоє його друзів у мережі припинили телефонні дзвінки, щоб від них було прийнято лише радіодзвінок. Тож вони отримали два автомобілі Porsche, один тур та понад 20 000 доларів. Це був перший DefCon у Лас -Вегасі - найбільша щорічна конвенція про піратство. Спочатку DefCon планував провести разову прощальну зустріч з BBS пізніше як щорічну подію.

2.3 1994 р. Видхід браузера Netscape полегшує перегляд та зберігання інформації, ніж BBS. Хакери переміщують повідомлення з планшетів на веб -сторінки з програмним забезпеченням, утилітами, порадами та технологіями. Все це стає суспільним багатством.

2.4. 1995 р. Російський хакер - 30 -річний Володимир Левін - вкрав 10 мільйонів доларів у американського Citibank. Він був затримани та екстрадований до США. Його засудили до 3 років позбавлення волі.

2.5. 1997 р. Безкоштовно розповсюджені програми піратства під назвою "AOHell" ("America-On-Hell") кошмар для AmericaOnline-найбільшого інтернет-провайдера. За допомогою навіть недосвідченого користувача багатомегабайтові поштові бомби на AOL могли надсилати повідомлення електронної пошти та надсилати спам у свої кімнати.

2.6. 1998 р. Команда CultoftheDeadCow Pirate створює програмне забезпечення BackOrifice для відновлення Windows 95/98. Цей інструмент є потужним для виявлення потужності маси троянів за

допомогою віддаленого пристрою. Програма була запропонована на конгресі DefCon.

2.7. 2000 р. На піку популярності розповсюджені атаки через відмову в обслуговуванні або DDoS-атаки. Під їх атаку потрапляють найбільші сайти eBay, Amazon та інші. Деякі хакери крадуть із корпоративної мережі Microsoft і публікують вихідний код останньої версії Windows та Office.

2.8. 2001 р. Величезними жертвами злому DNS -серверів стають сайтами Microsoft.

2.9. 2009 р. Хакер, які навчаються за допомогою спеціальних «навчальних програм», захоплюють численні комп'ютери у всьому світі. Авторами цих програм створюють спеціальні «словники» для підбору паролів.

2.10. 2010 р. «Комп'ютерний вірус Stuxnet, вперше виявлений у 2010 р., назвали першою у світі цифровою зброєю. На відміну від інших вірусів, він був розроблений так, щоб завдати фізичної шкоди обладнанню, яке управляється комп'ютерами. Це був перший відомий випадок, коли хакери змогли завдати фізичної шкоди реальному обладнанню, зробивши його дуже складним і досить страшним. Вірус був розроблений для націлювання на системи управління, що використовуються для моніторингу промислових об'єктів, і вперше був виявлений на атомних електростанціях в Ірані після того, як велика кількість уранових центрифуг почала несподівано ламатися. Вірус, відповідальність за який ніхто не взяв, пошкодив приблизно п'яту частину центрифуг збагачення, які використовуються в іранській ядерній програмі» [1].

2.11. «Поширення соціальних мереж призвело до появи та активізації груп хакерів, метою яких є злам аккаунти у зазначених мережах. Найвідомішою з цих груп є Lulz Security, загальновідома як LulzSec. Ця група оприлюднила їх хакерські атаки в Твіттері з наміром

збентежити власників веб-сайтів і висміяти недостатні заходи безпеки. З’явившись у 2011 році з атакою на Fox.com, хакери націлилися на понад 250 державних та приватних організацій, включаючи сумнозвісну атаку на мережу Sony PlayStation Network. Злом Sony зламав конфіденційні дані 24,6 мільйонів клієнтів і призвів до того, що компанія припинила свою онлайн-мережу на 23 дні. Після арешту ФБР співзасновника LulzSec Гектора Ксав'є Монсегура, він же Сабу, у 2012 році виявилося, що хакер надавав інформацію про своїх колег під час кампанії, що призвело до п'яти арештів у Великобританії та Ірландії» [1].

Хоча це може здатися, що ворожі уряди є винуватцем номер один, коли мова йде про онлайн -атаки в Інтернеті, це не так. За оцінками експертів з кібербезпеки Організації Об’єднаних Націй, приблизно 80% усієї злочинності, що базується на кіберзлочинствах, скоюють складні угруповання злочинців, які здійснюють високоорганізовані операції. Групи діяли так само, як і законні підприємства, оскільки вони підтримують регулярний робочий час з ієрархією членів, працюючи в парі, щоб створювати, діяти та підтримувати будь -яке шахрайство, на якому вони зосереджені [2].

Слушним, на думку автора, є виділення закономірностей історичного розвитку кіберзлочинності:

1. Основною причиною розвитку вказаної злочинної діяльності є вдосконалення не тільки безпосередньо комп’ютерів, а й комп’ютерних мереж та систем.

2. Вказаний вид злочинів є надзвичайно латентним, факти виявлення вказаної злочинної діяльності у більшості випадків є випадковими.

3. Однією з розповсюджених причин латентності кіберзлочинності небажання співробітників підприємств, установ та організацій, якими були виявлені факти вчинення кіберзлочинів у відношенні них, звертатися до правоохоронних органів.

У свою чергу, причинами цього є:

3.1. Небажання нести репутаційні втрати, втрату клієнтів,

3.2. Небажання надавати приводи та підстави для виявлення власної незаконної діяльності.

3.3. Небажання співробітників підрозділів безпеки банків та комерційних фірм втрачати престижну роботи та посаду через ризик виявлення власної бездіяльності, яка стала причиною та/або умовою для вчинення кіберзлочину).

3.4. Небажання надавати доступ співробітникам правоохоронних органів до системи комп’ютерної безпеки підприємства.

3.5. Недостатня компетентність з питань протидії кіберзлочинам керівників та рядових співробітників підрозділів безпеки підприємств, установ, організацій, високий рівень правового нігілізму серед них.

1.2. Елементи методики розслідувань кримінальних правопорушень у сфері використання мереж електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж

Слушним, на думку автора, є розгляд елементів методики розслідувань кримінальних правопорушень у сфері використання ЕОМ, систем та комп'ютерних мереж і мереж електрозв'язку.

В.П. Сабадаш та М.О. Ларкін визначають методику розслідування окремих видів злочинів як «розділ криміналістики, який складається з системи наукових положень та розроблених на їх основі рекомендацій щодо процесу розкриття та розслідування злочинів» [38].

В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель зазначають, що «методика розслідування злочинів може розглядатися у двох аспектах. По-перше, це сам процес розслідування злочинів як специфічна діяльність уповноважених законом органів та осіб, що

здійснюється на підставі застосування засобів криміналістичної техніки, прийомів слідчої тактики, методів розслідування певних видів злочинів. По-друге, це розділ науки криміналістики, який містить систему комплексних криміналістичних рекомендацій щодо виявлення, розслідування та профілактики окремих видів злочинів. Саме у взаємозв'язку цих двох напрямів – практичного і теоретичного – методика розслідування злочинів виявляє своє призначення, сприяючи розробці наукових рекомендацій і запровадженню їх у практику розслідування злочинів» [33].

Вчені зазначають, що «зазвичай об'єктом дослідження криміналістики є процес розслідування злочинів. В окремих випадках, намагаючись спеціалізувати і конкретизувати цей об'єкт, надати йому суто криміналістичної спрямованості, говорять про процес розкриття злочинів. При такому підході поза об'єктом дослідження залишається найважливіша діяльність з боротьби зі злочинністю, з її найбільш небезпечною формою – організованою злочинністю – сфера виявлення злочинів. Як свідчить практика боротьби зі злочинністю останніх років та нові напрями законодавчого регулювання, об'єктом дослідження методики розслідування мають стати всі етапи, а разом з ними напрями та форми боротьби зі злочинами: виявлення, відшукання, розкриття, розслідування та попередження їх» [33].

Друге визначення удається нам більш слушним, як таке, що є більш детальним та розгорнутим.

А.В. Іщенко, В.В. Пясковський, А.В. Самодін, Ю.М. Чорноус справедливо вказують на те, що «криміналістична методика – це завершальний розділ науки криміналістики, що представляє собою систему інтегрованих наукових положень і сформованих на їх основі комплексів методичних рекомендацій, що забезпечують оптимальну організацію розслідування та попередження окремих видів кримінальних правопорушень» [32].

О. В. Федосова у науковій роботі «Становлення та перспективи розвитку криміналістичної методики розслідування злочинів» визначає криміналістичну методику як «систему інтегрованих наукових положень і сформованих на їх основі комплексів методичних рекомендацій та слідчих технологій у вигляді типових інформаційних моделей, спрямованих на оптимальне здійснення виявлення та розслідування злочинів» [41].

Розглянемо структуру криміналістичної методики.

В.П. Сабадаш та М.О. Ларкін «до елементів методики розслідування окремих видів злочинів відносять криміналістичну характеристику злочинів (на думку вчених, це типова інформаційна система, яка містить дані про ключові елементи механізму злочинної поведінки і слугує основою для планування розслідування і висування слідчих версій), а також вчення про початковий, наступний та заключний етапи розслідування злочинів» [38].

В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель зазначають, що «внутрішня система розділу методики розслідування складається з двох основних частин:

1) загальної методики розслідування злочинів (поняття, об’єкт дослідження, завдання, принципи, місце у системі криміналістики та зв’язок з іншими галузями знань);

2) окремих методик розслідування різних видів злочинів (криміналістична класифікація злочинів і методики їх розслідування, структура окремих методик розслідування)» [33].

В. Малюга у статті «Структура методики розслідування окремих видів злочинів і місце в ній взаємодії слідчого» слушно зазначає, що «система криміналістичної методики – це загальні положення методики розслідування злочинів і окремі (видові чи групові) методики розслідування певних видів чи груп злочинів. Найважливішим призначенням окремої криміналістичної методики є розроблення

типових систем дій і заходів слідчого, які сприяють обранню ним найоптимальнішої й ефективнішої лінії поведінки під час роз слідування певного виду (групи) злочинів» [34].

А.В. Іщенко, В.В. Пясковський, А.В. Самодін, Ю.М. Чорноус зазначають, що «криміналістична методика як розділ науки складається з двох частин: загальних положень та окремих (видових) методик розслідування кримінальних правопорушень. Перша частина включає загальні закономірності організації та проведення розслідування, понятійний апарат, завдання і принципи криміналістичної методики, характеристику структури окремих методик розслідування тощо. Другу частину розділу складають методики розслідування окремих видів (груп) злочинів, що розробляються на основі загальних положень криміналістичної методики відповідно до потреб слідчої практики» [32].

С.О. Книженко у статті «Структурні елементи методики розслідування окремих видів злочинів» зазначає, що «методика розслідування окремих видів злочинів, незалежно від її класифікаційного виду, повинна включати в себе наступні обов’язкові структурні елементи:

– криміналістичну характеристику злочинів певного виду чи групи;

– типові слідчі ситуації початкового етапу розслідування й відповідні їм комплекси слідчих та оперативно-розшукових заходів; - особливості тактики окремих слідчих дій;

– профілактичну діяльність слідчого» [20].

У зазначеній науковій праці вчений також слушно наголошує на тому, що «до складу криміналістичної методики окремих видів злочинів можуть входити такі додаткові елементи:

– криміналістична класифікація злочинів;

– особливості дослідчої перевірки та порушення кримінальної справи; - особливості використання спеціальних знань;

– взаємодія слідчого з іншими службами та державними органами;

– типові слідчі ситуації послідуючого, завершального етапів розслідування й відповідні їм комплекси слідчих та оперативно-розшукових заходів;

– використання допомоги громадськості» [20].

Остання позиція заслуговує на увагу з огляду на те, що підкреслює важливу роль налагодженню взаємодії органів та підрозділів досудового розслідування з представниками підприємств, установ та організацій, що є особливо важливим з огляду на зазначені вище випадки небажання керівників та рядових співробітників підприємств, установ та організації повідомляти про факти вчинення щодо них кіберзлочинів.

Розглянемо елементи методики розслідувань кримінальних правопорушень у сфері використання ЕОМ, систем та комп'ютерних мереж і мереж електрозв'язку.

О. І. Гарасимів, О. М. Дуфенюк, О. В. Захарова до елементів методики розслідування кіберзлочинів відносять:

– «криміналістичну характеристику кіберзлочинів;

– типові слідчі ситуації, слідчі версії та алгоритми дій під час розслідування;

– особливості тактики проведення окремих слідчих (розшукових) дій» [35].

Розглядаючи питання, пов’язані з криміналістичною характеристикою кіберзлочинів, автори наводять наступну класифікацію кіберзлочинів:

– «агресивні: кібертероризм, погроза фізичної розправи (наприклад, передана через електронну пошту), кіберпереслідування, кібersталкінг (протиправне сексуальне домагання та переслідування іншої особи через Інтернет), дитяча порнографія (створення порнографічних матеріалів, виготовлених із зображенням дітей, розповсюдження цих матеріалів, отримання доступу до них);

– не агресивні: кіберкрадіжки, кібервандалізм, кібершахрайство, кібершпигунство, розповсюдження спаму та вірусних програм» [35].

Вказана класифікація удається нам спірною, оскільки як перша, так і друга група вказаних злочинів має дуже високий рівень суспільної небезпечності і так чи інакше несе загрозу для життя та здоров'я осіб.

Більш слушною нам удається класифікація кіберзлочинів, наведена у «Конвенція Ради Європи про кіберзлочинність, що була відкрита для підписання у листопаді 2001 р.» [24].

З урахуванням положень вказаної конвенції слушною удається наступна класифікація кіберзлочинів:

– кримінальні правопорушення, які посягають комп'ютерні дані, а саме на їх доступність, цілісність та конфіденційність. Такі дії можуть полягати у незаконних утручаннях у роботу комп'ютерних систем, втручатися у дані, отриманні незаконного доступу до них;

– кримінальні правопорушення, які полягають у незаконному використання в якості засобів вчинення злочинів персональних комп'ютерів, зокрема, для незаконних дій з інформацією;

– кримінальні правопорушення, які полягають у незаконних діях з інформацією;

– кримінальні правопорушення, предметом посягання яких є авторське право та суміжні права;

– кримінальні правопорушення, до об'єктивної сторони яких відносяться акти ксенофобії та расизму.

Розглянемо такий обов'язковий елемент криміналістичної характеристики кіберзлочинів, як знаряддя їх вчинення.

О. І. Гарасимів, О. М. Дуфенюк, О. В. Захарова в своїй роботі «Методика розслідування злочинів» справедливо зазначають, що «знаряддями вчинення комп'ютерних злочинів виступають засоби комп'ютерної техніки, зокрема спеціальне програмне забезпечення: носії комп'ютерної інформації (лазерні диски, зовнішні жорсткі диски, flech-

накопичувачі), різноманітне периферійне устаткування (наприклад, dvd-rom-накопичувачі), електронні ключі, особисті ідентифікаційні коди, мережеве устаткування, а також засоби доступу до віддалених мереж (засоби телефонного і супутникового зв'язку, модем) тощо» [35].

О. І. Мотлях поділяє «способи, вчинення кіберзлочинів на наступні види:

– способи вчинення кібезлочинів, які полягають у діях, спрямованих на безпосереднє втручання в роботу комп'ютерів. При цьому, як зазначає вчений, комп'ютерна інформація може бути незаконно скопійована, заблокована, знищена; за допомогою незаконної видачі команд з комп'ютерного пристрою робота комп'ютерів та/або комп'ютерних мереж може бути порушена. При цьому, як вказує вчений, такі злочини вчиняють, як правило, оператори персональних комп'ютерів, спеціалісти з програмування, інженери тощо;

– способи вчинення кібезлочинів, які полягають у діях злочинців, спрямованих на видалений (опосередкований) доступ інформації, яка міститься в серверах (комп'ютерах) та до самих комп'ютерів (серверів). Як слушно зазначає вчений, без використання глобальних (зокрема, комп'ютерної мережі Інтернет) та локальних комп'ютерних мереж. Вчений наголошує на можливих способах вчинення такого підключення, а саме: коли злочинець, маючи вигляд особи, яка користується комп'ютерами та комп'ютерними мережами на законних підставах, отримує підключення до ліній електронного зв'язку власника інформації, на яку здійснюється незаконне посягання; коли злочинці використовують паролі та коди доступу до комп'ютерних мереж та комп'ютерів, якій їм не належать і незаконно проникають таким чином до пристроїв збереження даних та комп'ютерних мереж; коли особи, які вчиняють кіберзлочини, під'єднуються до пристроїв збереження даних та комп'ютерних мереж, автоматично підбирають номери засобів

комп’ютерного зв’язку, які належать особам, що користуються цими засобами та пристроями на законних підставах» [36].

Романюк Б. В., Камлик М. І., Гавловський В. Д. зазначають, що «до способів вчинення кіберзлочинів відносяться:

– способи вчинення кіберзлочинів, які полягають у розповсюдженні (виготовленні) шкідливого програмного забезпечення. Існує велика кількість зразків ті видів шкідливого програмного забезпечення. Зазначене програмне забезпечення створюється спеціально для певної, визначеної категорії осіб і може модифікуватися під конкретні потреби. Зокрема, комп’ютерні програми, які є шкідливими, можуть створюватись з використання робочого місця, яке належить злочинцю; шкідливе програмне забезпечення може створюватись за межам комп’ютерної мережі та системи, для «нападу» на який створена вказана програма; для створення шкідливого програмного забезпечення до вже існуючої програми вносяться необхідні зміни» [37].

Слушним удається розгляд питань щодо особливостей «слідової картини» кіберзлочинів.

До слідів вчинення кіберзлочинів можна віднести наступні сліди:

– сліди, які залишаються «пакетами» інформаційних даних коли останні «рухаються» глобальною комп’ютерною мережею Інтернет. При цьому кожний користувач комп’ютера при відправленні «пакетів» інформаційних даних адресу комп’ютера-адресата; при проходженні комп’ютерних даних глобальною комп’ютерною мережею Інтернет вони проходять через вузлові комп’ютери (сервери); на цих комп’ютера (серверах) залишаються відомості щодо реєстрації проходження пакетів даних. Цілком природньо, що при цьому на вузлових комп’ютерах (серверах) залишаються також сліди вчинення злочинів злочинцями;

– некоректна або уповільнена робота персональних комп’ютерів та серверів, зокрема, поява на моніторі персонального комп’ютера нехарактерних символів та написів, уповільнене зчитування пакетів

даних, некоректне або уповільнене завантаження операційної системи персонального комп’ютера або сервера;

– зміна способу взаємодії з модемами, принтерами та іншим апаратним устаткуванням; зміна назв та розташування файлів, видалення старих та поява нових мережевих пристроїв;

– зміни у роботі тестового та антивірусного програмного забезпечення, яке використовується у роботі персональних комп’ютерів;

– розмагнічення та фізичне знищення носіїв інформації, додавання або стирання файлових записів, видалення з каталогів імен файлів, поява нових файлів та каталогів, корегування стандартних реквізитів файлів, зміна змісту та розмірів файлів, перейменування окремих файлів і, навіть, цілих каталогів;

– зміна параметрів роботи пристроїв, за допомого яких персональних комп’ютер «впізнає» користувача за голосом, зміни в електронних «ключах доступу» та інші сліди, які зловмисники залишають на спеціальних засобах, призначених для захисту комп’ютерної інформації;

– рукописні записи, за допомогою яких злочинець записував таблиці шифрування, переліки паролів, коди та інші сліди, які може залишити на місці перебування особа, яка вчинила кіберзлочин;

– сліди пальців рук та ДНК, які особа, що вчинила кіберзлочин залишила на кнопках увімкнення/вимкнення комп’ютерного устаткування, клавіатурі тощо.

Проаналізуємо особу злочинців, які вчиняють кіберзлочини.

О. І. Гарасимів, О. М. Дуфенюк, О. В. Захарова слушно зазначають, що «надають класифікацію кіберзлочинців в залежності від їх віку. Вчені виділяють кіберзлочинців віком до двадцяти одного року та кіберзлочинців віком старше двадцяти одного року. Автори визначають наступні властивості вікової групи віком до двадцяти одного року: відсутність цілеспрямованої, системного планування кіберзлочину; вигадують оригінальний спосіб вчинення злочину; вказані

злочинці не вчиняють заходів, спрямованих на приховування злочинної діяльності. Кіберзлочинці віком старше двадцяти одного року, на слушну думку вчених, як правило, вже входять до організованих груп, приділяють значну увагу технічному оснащенню, ретельному плануванню злочинної діяльності. На момент досягнення зазначеного віку кіберзлочинці, як правило, вже встигають отримати вищу освіту, значний досвід роботи (у тому числі злочинної діяльності). Виходячи з перелічених властивостей, злочинці саме цієї групи, на слушну думку вчених, являють підвищену суспільну небезпеку» [35].

Слушною удається наступна загальна класифікація осіб, що вчиняють кіберзлочини:

– хакери – це загальна назва людей, які отримують несанкціонований доступ до комп'ютерних систем. Буквально, хакер – це комп’ютерний хуліган, який із задоволенням проникає у чужий комп’ютер для розваги чи розваги, зазвичай без матеріальних цілей чи шкоди. Основна мета хакерів – здобути перемогу над захистом комп’ютера, розширити відкритий кіберпростір, довести свою перевагу та силу в електронному світі. Вони здійснюють свою діяльність, заважаючи комп’ютерним системам для різних цілей. Через складність системи захисту вона приваблива для хакерів. Зазвичай вони чудово знають деякі системи захисту інформації і сприяють відкритості електронного простору та програмного забезпечення;

– крекери – люди, які завдають шкоди, крадуть інформацію, змінюють або пошкоджують файли, бухгалтери здійснюють пограбування (грошові перекази з рахунку на рахунок), прагнучі створити програму. Містить серійний номер алгоритмів, що використовуються при розробці програмного забезпечення для створення генераторів ключів. Крекери – прихильники професіоналів, які серйозно порушують безпеку, оскільки не мають моральних обмежень. Комп'ютерні злочини скоюють злочинні групи, які крадуть

гроші, найчастіше у кредитних агентств. Таким чином, вони завдають шкоди причині, тобто намагаються стерти інформацію. обробка інформації порушує будь-яку процедуру. Деякі вчені кажуть, що це технічно набагато складніше технічних операцій;

– фрікери (передатні, перетворювачі частоти) – електронні професіонали, які не звикли платити за послуги електронної пошти, використовують телефонні системи, щоб уникнути оплати телекомунікаційних послуг (переміщення облікових записів на інші), зламують таксофони, лічильники, миготливі системи супутникового телебачення та ін. Основною метою цієї групи є використання безкоштовних ресурсів Інтернету для спілкування. По -різному (програмне та апаратне забезпечення) ці типи хакерів подобаються долати технічні труднощі, іноді перешкоджаючи хакерству знаючим та кваліфікованим фахівцям. Це головним чином пов'язано з тим, що, наприклад, у випадку безкоштовного доступу до Інтернету, іноді постачальнику необхідно змінити статистику, для якої це потрібно. віддалено перевіряти або перевіряти доступ або пароль інших користувачів;

– кардери – вони крадуть гроші з банку (зазвичай зазіхаючи на зарплатні та кредитні картки);

– кіберплути – займайтеся злочинною діяльністю виключно з корисливих мотивів. Вони крадуть інформацію, включаючи різні бази даних, а потім продають цю інформацію;

– пірати – здебільшого вчиняють крадіжки, порушення безпеки та продаж нового комерційного програмного забезпечення, технічних досягнень та іншої інтелектуальної власності тощо. Така робота, звичайно, повинна бути організована за наявності реального покупця. За відсутності наказів пірат вірить у папери (так звані «картери»), банківські рахунки та телефонний зв'язок (їх називають «монстрами», «переповненими» тощо). Але якою б не була причина, це матеріальна

причина інтересу, а не цікавості чи люди цієї категорії можуть створювати шкідливі програми.

– шкідники (у тому числі вандали) страждають від нових видів психічних захворювань, «комп'ютерних манії», «комп'ютерних фобій», «комп'ютерних психозів» і намагаються реалізувати свої патологічні відхилення у кіберпросторі. Частково або повністю знищують комп'ютерні системи, намагаються знищити зламані системи. Вони часто шкодять без користі (крім морального задоволення). Часто мотивом є помста;

– «експериментатори» – це люди, які, керуючи інструментами та ресурсами мережі та власними комп'ютерами, хочуть вчитися на власній землі. власні помилки базуються на тому, «як неможливо». Основну частину цієї групи складають діти та підлітки. Основною причиною гри в цій групі часто є досвід професіоналів високого класу;

– автори шкідливого програмного забезпечення. Іншим видом комп'ютерної злочинності є незаконне пошкодження комп'ютерної системи чи мережі під час роботи комп'ютерних систем або порушення глобальної телекомунікаційної системи вірусом. Розробники такого програмного забезпечення становлять сьогодні серйозну загрозу для своїх користувачів;

– терористи та навіть цілі терористичні організації дедалі частіше використовують ресурси персональних комп'ютерів, локальних та глобальних комп'ютерних мереж для отримання коштів для подальшої злочинної діяльності, викрадення секретної інформації та ведення пропаганди;

– спецслужби країн-агресорів. Не дивно, що іноземні розвідувальні організації вже давно використовують кібермедіа як засіб спостереження для отримання належного доступу до секретної та секретної інформації. На жаль, деякі країни вже розвивають військову дисципліну за допомогою електронних засобів, створюють та

розробляють комп’ютерне програмне забезпечення. Як справедливо зазначає Д. В. Дубов у своїй роботі «Кіберпростір як новий вимір геополітичного суперництва», «поділяє умовну сукупність кіберконфліктів на наступні категорії: хактивізм, або політично вмотивовані хакерські атаки; кібершпигунські акції; кібердиверсії» [12].

Розглянемо питання щодо осіб, які найчастіше стають потерпілими від кіберзлочинів:

– до першої групи належать підприємства, установи та організації з розгалуженою бюрократичною організаційною структурою управління, де влада обмежена однією особою – керівником, але ніхто з підлеглих ні за що не відповідає. Завдяки комп’ютеризації люди все частіше залучаються до автоматизованого програмного забезпечення для управління брендом та баз даних облікових записів. Більшість акторів не мають повного уявлення про те, як працюють ці системи. Він робить це через несанкціоноване використання працівниками, які вирішили стати на злочинний шлях;

– друга група – це юридичні особи з різними властивостями. які мають велике значення для внутрішнього виробництва та технологічного розвитку відповідно до використання комп’ютерних технологій, які не встигають розробити відповідні адміністративні структури. У таких закладах їх керівники не завжди знають, які заходи слід вжити, щоб запобігти несанкціонованому доступу роботодавців і клієнтів, а також сторонніх осіб;

– третя група – це установи та організації, які, з одного боку, працюють над забезпеченням захисту інформації та конфіденційності інформації для цілей ІТ, з іншого – ще не мають належної організаційної та адміністративної структури, можливості контролювати чутливі сфери виробництва (офіси, відділи, конкретні працівники), які беруть участь у створенні цієї інформації;

– четверта група – це компанії та/або товариства, які за визначенням створюються зовнішнім капіталом або залежать від великих корпорацій. Ці правові організації представляють «сфери підвищеного ризику злочинності», оскільки вони дуже зацікавлені у кримінальних структурах та компонентах. Наприклад, коли вони відвідують національні форуми, ці фірми в першу чергу працюють, щоб відповідати своїм нормам і структурам режиму. місцеві працівники, по -друге, змінюють роботу відповідно до національного законодавства, по -третє, зменшують інформаційну систему конфіденційності під впливом національних стандартів та правил, по-четверте, для врахування конкретних програм Існуючі просторові інструменти, подалі від мереж та комп'ютерних систем, включені до цифрових телекомунікації. Все це збільшує можливості кримінального переслідування щодо такого типу жертв;

– п'яту групу складають проекти, установи та установи, в яких існують різні моральні аномалії за різних обставин. і психологічний клімат (наприклад, через: неточні міжособистісні стосунки між працівниками, між працівниками та керівниками; значні відмінності в оплаті праці працівників на тих самих посадах; управління наймом персоналу по відношенню до нижчих професійних рівнів. моральний, псевдопідприємець і для інші причини.

Оцінюючи ймовірну особу злочинця, який вчинив кіберзлочин під час встановлення його особи, надзвичайно важливо визначити його рівень компетенції ІТ. Це питання є критично важливим.

При цьому рівень володіння ним навичками із приховування та видалення комп'ютерної інформації має вирішальне значення. Коли невідомо, який рівень має підозрюваний, його слід вважати високим. Наприклад, під час вилучення увімкнутого комп'ютера технік повинен вирішити, чи використовувати звичайне вимкнення, або просто вимкнути живлення. З одного боку, певна кількість інформації, майже

нерелевантної, може зникнути, коли комп'ютер буде вимкнуто перериванням живлення. Але краще виходити з того, що серед осіб, що вчиняють кіберзлочини розповсюдженою є тактика, коли така особа залишає у ввімкненому комп'ютері комп'ютерну логічну бомбу, яка реагує на команду вимкнення. Тому існує небезпека, що всі документи будуть знищені своїми руками при нормальному вимкненні комп'ютеру. Вибір варіанту залежить від того, як ми оцінюємо вертикальну рівень власника комп'ютера. Якщо неможливо оцінити цей рівень, комп'ютер вимикається внаслідок переривання живлення, тобто слід виходити із можливої наявності логічної бомби.

Заслуговує на увагу питання щодо місця вчинення кіберзлочинів.

О. В. Мотлях з цього приводу справедливо зазначає, що «для кіберзлочинів відсутнє територіальне (просторове) обмеження. Тобто, злочин може виходити за рамки однієї держави. Але, незважаючи на віртуальність у використанні технологій, злочин є реальним і важко розслідуваним. Складність полягає у відтворенні «слідової картини» злочину, визначенні конкретного місця та часу вчинення протиправної дії. Слід зазначити, що ще на стадії підготовчих дій злочинці, з моменту виникнення свого замислу, чітко вивчають обстановку, в якій їм доведеться діяти. Збирають інформацію про об'єкт посягання; вивчають системи захисту, якими забезпечене комп'ютерне устаткування; реальний час несанкціонованого втручання в роботу інформаційних технологій, пам'ятаючи при цьому, що час не завжди пропорційний способу скоєння злочину» [36].

О. І. Гарасимів, О. М. Дуфенюк, О. В. Захарова правильно вказують на те, що «місцем скоєння комп'ютерних злочинів є і конкретні точки й ділянки території, і ті установи, організації, підприємства та системи, в яких використовується той чи інший засіб електронно-обчислювальної техніки в будь-якому технологічному процесі. Отже, місцем учинення комп'ютерного злочину можуть бути:

– місця постійного зберігання інформації;

– місця безпосередньої обробки та зберігання інформації;

– місця безпосереднього використання технічних засобів для неправомірного доступу до комп’ютерної інформації;

– місця зберігання інформації на машинних носіях;

– місця безпосереднього використання результатів неправомірного доступу до комп’ютерної інформації» [35].

На нашу думку, з появою та розвитком локальних і, особливо глобальних комп’ютерних мереж з використанням останніх для вчинення кіберзлочинів традиційне для криміналістики поняття місця вчинення злочину підлягає, на нашу думку, більш розширеному тлумаченню. При вчиненні кіберзлочинів між злочинцем та об’єктом злочинного посягання відстань може бути дуже великою – аж до тисяч кілометрів.

Аналіз проблемних питань, пов’язаних із загальними положеннями методики розслідувань кримінальних правопорушень у сфері використання ЕОМ, систем та комп'ютерних мереж і мереж електрозв'язку, слід, на нашу думку, зробити наступні висновки:

1. Існують наступні закономірності розвитку кіберзлочинності:

– основною причиною розвитку вказаної злочинної діяльності є вдосконалення не тільки безпосередньо комп’ютерів, а й комп’ютерних мереж та систем;

– із появою глобальної комп’ютерної мережі «Інтернет» кіберзлочинність «вийшла» на принципово новий рівень і набула глобального, світового характеру;

– якщо «обмін досвідом» між особами, які вчиняють кіберзлочини, і, навіть, видання ними спеціалізованої літератури та організація зустрічей з метою спілкування, «обміну досвідом» злочинної діяльності та узгодження позицій, то з появою глобальної комп’ютерної мережі

«Інтернет» особи, які вчиняють кіберзлочини, почали об’єднуватись у групи, розташовані у різних країнах світу;

– вказаний вид злочинів є надзвичайно латентним, факти виявлення вказаної злочинної діяльності у більшості випадків є випадковими;

– однією з розповсюджених причин латентності кіберзлочинності небажання співробітників підприємств, установ та організацій, якими були виявлені факти вчинення кіберзлочинів у відношенні них, звертатися до правоохоронних органів. У свою чергу, причинами цього є: небажання нести репутаційні втрати, втрату клієнтів, небажання надавати приводи та підстави для виявлення власної незаконної діяльності; небажання співробітників підрозділів безпеки банків та комерційних фірм втрачати престижну роботи та посаду через ризик виявлення власної бездіяльності, яка стала причиною та/або умовою для вчинення кіберзлочину); небажання надавати доступ співробітникам правоохоронних органів до системи комп’ютерної безпеки підприємства; недостатня компетентність з питань протидії кіберзлочинам керівників та рядових співробітників підрозділів безпеки підприємств, установ, організацій, високий рівень правового нігілізму серед них.

2. Слушною удається наступна класифікація кіберзлочинів:

– кримінальні правопорушення, які посягають комп’ютерні дані, а саме на їх доступність, цілісність та конфіденційність. Такі дії можуть полягати у незаконних втручаннях у роботу комп’ютерних систем, втручатися у дані, отриманні незаконного доступу до них;

– кримінальні правопорушення, які полягають у незаконному використання в якості засобів вчинення злочинів персональних комп’ютерів, зокрема, для незаконних дій з інформацією;

– кримінальні правопорушення, які полягають у незаконних діях з інформацією;

– кримінальні правопорушення, предметом посягання яких є авторське право та суміжні права;

кримінальні правопорушення, до об’єктивної сторони яких відносяться акти ксенофобії та расизму.

3. До слідів вчинення кіберзлочинів можна віднести наступні сліди:

– сліди, які залишаються «пакетами» інформаційних даних коли останні «рухаються» глобальною комп’ютерною мережею Інтернет. При цьому кожний користувач комп’ютера при відправленні «пакетів» інформаційних даних адресу комп’ютера-адресата; при проходженні комп’ютерних даних глобальною комп’ютерною мережею Інтернет вони проходять через вузлові комп’ютери (сервери); на цих комп’ютера (серверах) залишаються відомості щодо реєстрації проходження пакетів даних. Цілком природньо, що при цьому на вузлових комп’ютерах (серверах) залишаються також сліди вчинення злочинів злочинцями;

– некоректна або уповільнена робота персональних комп’ютерів та серверів, зокрема, поява на моніторі персонального комп’ютера нехарактерних символів та написів, уповільнене зчитування пакетів даних, некоректне або уповільнене завантаження операційної системи персонального комп’ютера або сервера;

– зміна способу взаємодії з модемами, принтерами та іншим апаратним устаткуванням; зміна назв та розташування файлів, видалення старих та поява нових мережевих пристроїв;

– зміни у роботі тестового та антивірусного програмного забезпечення, яке використовується у роботі персональних комп’ютерів;

– розмагнічення та фізичне знищення носіїв інформації, додавання або стирання файлових записів, видалення з каталогів імен файлів, поява нових файлів та каталогів, корегування стандартних реквізитів файлів, зміна змісту та розмірів файлів, перейменування окремих файлів і, навіть, цілих каталогів;

– зміна параметрів роботи пристроїв, за допомого яких персональних комп’ютер «впізнає» користувача за голосом, зміни в електронних «ключах доступу» та інші сліди, які зловмисники залишають на спеціальних засобах, призначених для захисту комп’ютерної інформації;

– рукописні записи, за допомогою яких злочинець записував таблиці шифрування, переліки паролів, коди та інші сліди, які може залишити на місці перебування особа, яка вчинила кіберзлочин;

сліди пальців рук та ДНК, які особа, що вчинила кіберзлочин залишила на кнопках увімкнення/вимкнення комп’ютерного устаткування, клавіатурі тощо.

4. Розглянемо питання щодо осіб, які найчастіше стають потерпілими від кіберзлочинів:

– до першої групи належать підприємства, установи та організації з розгалуженою бюрократичною організаційною структурою управління, де влада обмежена однією особою – керівником, але ніхто з підлеглих ні за що не відповідає. Завдяки комп’ютеризації люди все частіше залучаються до автоматизованого програмного забезпечення для управління брендом та баз даних облікових записів. Більшість акторів не мають повного уявлення про те, як працюють ці системи. Він робить це через несанкціоноване використання працівниками, які вирішили стати на злочинний шлях;

– друга група – це юридичні особи з різними властивостями. які мають велике значення для внутрішнього виробництва та технологічного розвитку відповідно до використання комп’ютерних технологій, які не встигають розробити відповідні адміністративні структури. У таких закладах їх керівники не завжди знають, які заходи слід вжити, щоб запобігти несанкціонованому доступу роботодавців і клієнтів, а також сторонніх осіб;

– третя група – це установи та організації, які, з одного боку, працюють над забезпеченням захисту інформації та конфіденційності

інформації для цілей ІТ, з іншого – ще не мають належної організаційної та адміністративної структури, можливості контролювати чутливі сфери виробництва (офіси, відділи, конкретні працівники), які беруть участь у створенні цієї інформації;

– четверта група – це компанії та/або товариства, які за визначенням створюються зовнішнім капіталом або залежать від великих корпорацій. Ці правові організації представляють «сфери підвищеного ризику злочинності», оскільки вони дуже зацікавлені у кримінальних структурах та компонентах. Наприклад, коли вони відвідують національні форуми, ці фірми в першу чергу працюють, щоб відповідати своїм нормам і структурам режиму. місцеві працівники, по -друге, змінюють роботу відповідно до національного законодавства, по -третє, зменшують інформаційну систему конфіденційності під впливом національних стандартів та правил, по-четверте, для врахування конкретних програм Існуючі просторові інструменти, подалі від мереж та комп'ютерних систем, включені до цифрових телекомунікації. Все це збільшує можливості кримінального переслідування щодо такого типу жертв;

– п'яту групу складають проекти, установи та установи, в яких існують різні моральні аномалії за різних обставин. і психологічний клімат (наприклад, через: неточні міжособистісні стосунки між працівниками, між працівниками та керівниками; значні відмінності в оплаті праці працівників на тих самих посадах; управління наймом персоналу по відношенню до нижчих професійних рівнів. моральний, псевдопідприємець і для інші причини.

5. Оцінюючи ймовірну особу злочинця, який вчинив кіберзлочин під час встановлення його особи, надзвичайно важливо визначити його рівень компетенції ІТ. Це питання є критично важливим. При цьому рівень володіння ним навичками із приховування та видалення комп'ютерної інформації має вирішальне значення. Коли невідомо, який

рівень має підозрюваний, його слід вважати високим. Наприклад, під час вилучення увімкнутого комп’ютера технік повинен вирішити, чи використовувати звичайне вимкнення, або просто вимкнути живлення. З одного боку, певна кількість інформації, майже нерелевантної, може зникнути, коли комп’ютер буде вимкнуто перериванням живлення. Але краще виходити з того, що серед осіб, що вчиняють кіберзлочини розповсюдженою є тактика, коли така особа залишає у ввімкненому комп’ютері комп’ютерну логічну бомбу, яка реагує на команду вимкнення. Тому існує небезпека, що всі документи будуть знищені своїми руками при нормальному вимкненні комп’ютеру. Вибір варіанту залежить від того, як ми оцінюємо вертикальну рівень власника комп’ютера. Якщо неможливо оцінити цей рівень, комп’ютер вимикається внаслідок переривання живлення, тобто слід виходити із можливої наявності логічної бомби.

РОЗДІЛ 2
ОСОБЛИВОСТІ ПРОВЕДЕННЯ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ ТА СЛІДЧИХ ДІЙ ПРИ РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У СФЕРІ ВИКОРИСТАННЯ МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ, ЕЛЕКТРОННИХ ОБЧИСЛЮВАЛЬНИХ МАШИН, СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ

2.1. Тактичні особливості проведення оперативно-розшукових заходів при розслідуванні кримінальних правопорушень у сфері використання мереж електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж

Слушним удається розгляд тактичних особливостей проведення оперативно-розшукових заходів при розслідуванні кримінальних правопорушень у сфері використання ЕОМ, систем та комп'ютерних мереж і мереж електрозв'язку.

О. А. Самойленко, виділяє наступні «суб’єкти оперативно-розшукової діяльності, котрі прямо або опосередковано здійснюють виявлення злочинів, вчинених у сфері ІТ-технологій:

– Національна поліція України, а саме підрозділи Департаменту кіберполіції (ДКП), інші оперативні підрозділи НП (зокрема, департамент карного розшуку;

– підрозділи контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, захисту національної державності Служби безпеки (ДКІБ СБ України). До завдань СБ України також входить попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, тероризму, корупції та організованої злочинної діяльності у сфері управління і економіки та інших протиправних дій,

які безпосередньо створюють загрозу життєво важливим інтересам України» [39].

Під час ведення оперативно-розшукової діяльності при розкриття та розслідування кіберзлочинів надзвичайно важливим є налагодження взаємодії між співробітниками оперативних підрозділів зі спеціалістами. Адже спеціальні знання в галузі ІТ, захисту інформації, програмування та телекомунікації необхідні на всіх етапах розслідування і, навіть, судового розгляду кримінальних проваджень.

До недоліків існуючої взаємодії між оперативними співробітниками правоохоронних органів та спеціалістами в галузі ІТ, захисту інформації, програмування та телекомунікацій слід, на нашу думку, віднести наступні:

– переоцінка оперативними співробітниками правоохоронних органів власних знань та досвіду роботи у відповідній галузі;

– залучення спеціаліста лише на окремих стадіях розслідування кримінального провадження (наприклад, при проведенні огляду місця події та обшуку по кримінальних провадженнях за фактами вчинення кіберзлочинів, під час призначення комп’ютерно-технічної експертизи).

Натомість, оперативні співробітники правоохоронних органів повинні залучати спеціаліста для надання допомоги значно раніше: наприклад, при проведенні оперативно-розшукових заходів при виявленні комп’ютерних злочинів.

Важливою при проведенні оперативно-розшукових заходів при виявленні комп’ютерних злочинів є також взаємодія з провайдерами (операторами зв’язку).

2.2. Тактичні особливості проведення слідчих дій при розслідуванні кримінальних правопорушень у сфері використання мереж електрозв'язку, електронних обчислювальних машин, систем та комп'ютерних мереж

Слушним удається аналіз тактичних особливостей проведення слідчих дій при розслідуванні кримінальних правопорушень у сфері використання ЕОМ, систем та комп'ютерних мереж і мереж електрозв'язку.

Розглянемо тактичні особливості проведення обшуку при розслідуванні кримінальних правопорушень у сфері використання ЕОМ, систем та комп'ютерних мереж і мереж електрозв'язку.

Предметом обшуку при розслідуванні є носії комп’ютерної інформації, до яких, в свою чергу, відносяться:

- зйомні магнітні диски;
- незйомні магнітні диски;
- оптичні диски;
- магнітні карти;
- цифрові касети;
- персональні комп’ютери;
- сервери;
- комунікаційне обладнання;
- комунікатори;
- смартфони;
- мобільні телефони;
- цифрові фотоапарати;
- цифрові відеокамери;
- інші предмети.

При проведенні обшуку ті види електронної техніки, які не містять носії комп’ютерної інформації, не підлягають вилученню з тактичних міркувань. До таких пристроїв відносяться:

– принтери;
– сканери;
– факси;
– клавіатури;
– монітори;
– маніпулятори «миша»;
– джойстики;
– звукові колонки.

Виходячи із законодавчих, а також тактичних вимог до проведення обшуку, під час вилучення не повинна змінюватись будь-яка інформація, що міститься на носіях комп’ютерної інформації, що вилучаються. Особа, яка керує обшуком, а також інші особи, які під час обшуку їй підпорядковуються, зобов’язані забезпечити такі умови проведення обшуку, за яких вилучена при проведенні обшуку комп’ютерна інформація, яка потім буде надана експерту та суду, жодним чином не змінювалась.

Доступ до комп’ютерної інформації та її дослідження «на місці» здійснюється лише у виключних випадках і за наступних умов:

– коли неможливо вилучити носій комп’ютерної інформації та направити його на експертне дослідження до спеціалізованих експертних установ;
– доступ та дослідження «на місці» проведення обшуку повинні здійснюватись компетентними спеціалістами, які за своїм кваліфікаційним рівнем здатні зрозуміти та пояснити зміст такої інформації, зміст та послідовність дій, що здійснюються ними при її дослідженні.

Всі дії з комп’ютерною технікою, яка є джерелом комп’ютерної інформації, повинні бути занесені до протоколу обшуку з метою забезпечення можливості подальшого їх повторення незалежними спеціалістами для отримання тих самих результатів.

Існують наступні загальні тактичні вимоги до проведення обшуку, метою якого є виявлення, вилучення та фіксація комп’ютерної інформації по кримінальних провадженнях за фактами вчинення кіберзлочинів:

– слідчий та/або прокурор, які здійснюють керівництво проведенням обшуку, одразу повинні взяти під контроль все приміщення, в якому проводиться обшук, а також прилади контролю за електроживленням цього приміщення. При цьому важливо не переплутати комп’ютерну техніку, яка вимкнена та комп’ютерну техніку, яка знаходиться у стані гібернації («сну»): на панелі техніки, яка знаходиться у стані гібернації («сну»), «горить» індикатор живлення;

– упакування та опечатування вилученої комп’ютерної техніки слід здійснювати таким чином, щоб виключити можливість несанкціонованих фізичного доступу в середину корпусу, а також увімкнення електроживлення (обов’язковим відображенням цього у протоколі слідчої дії);

– вилучена техніка упаковується таким чином, щоб виключити можливість пошкодження. Жорсткі магнітні диски через їх особливу чутливість до механічних пошкоджень через сильні удари або вібрацію можуть повністю втратити наявну на них комп’ютерну інформацію;

– усіх співробітників підприємства, установи, організації, в якій проводиться обшук, слід опитати на предмет паролів усіх користувачів. Вони повинні бути зареєстровані письмово, звертаючи увагу на алфавіт та великі літери кожного символу та перевіряючи джерело. Ви не можете вводити паролі або журнал запитів, лише писати на карті. Їх доказове значення не зменшується.

Інформацію, яка підходить для комп'ютера та інших цифрових даних про злочинну діяльність, можна знайти на різноманітних цифрових носіях та носіях інформації. В ході обшуку слідчий має знайти всілякі прилади та інструменти, швидко визначити, чи можуть вони містити цікаву інформацію, і, якщо це можливо, зрозуміти їх. Для цього під час обшуку потрібно залучати спеціаліста.

Розглянемо тактичні особливості проведення огляду комп'ютерів на предмет виявлення доказової інформації про вчинення кіберзлочинів.

А. Старушкевич справедливо зазначає: «при розслідуванні комп'ютерних злочинів слідчий огляд проводитися на місці:

– збереження й обробки комп'ютерної інформації, підданої злочинному впливу (наприклад, у разі незаконного втручання у роботу ЕОМ (комп'ютерів), їх систем чи комп'ютерних мереж);

– знаходження комп'ютерного обладнання, яке використовувалося при вчиненні злочину (наприклад, у разі розповсюдження комп'ютерного вірусу після незаконного проникнення у комп'ютерну мережу);

– збереження інформації, отриманої злочинним шляхом (наприклад, у разі заволодіння комп'ютерною інформацією шляхом викрадення, привласнення, вимагання, шахрайства чи зловживання службовим становищем);

– порушення правил експлуатації ЕОМ, комп'ютерної системи або мережі;

– настання шкідливих наслідків (знищення, блокування, модифікації, копіювання комп'ютерної інформації, порушення роботи комп'ютера, комп'ютерної системи або мережі» [40].

Як правильно зазначає О. І. Мотлях, «Особливу увагу необхідно звертати на локальне з'єднання (об'єднання кількох комп'ютерних систем у межах одного чи кількох приміщень, що становлять єдине ціле) та розподільне (кілька комп'ютерних систем, розкиданих у межах

визначеної території (кварталу, району, міста, області тощо), що об’єднані в одну телекомунікаційну систему. З метою належного функціонування зазначеного технічного комплексу та збереження конфіденційної інформації при непередбачуваних випадках, створюються один чи кілька центральних комп’ютерів, так званих серверів, на яких зберігається основна базова інформація, а всі інші мережеві комп’ютери, відносно названих, є робочими станціями» [36].

На відміну від багатьох інших видів доказів, комп'ютерна інформація не може сприйматися людиною безпосередньо за допомогою органів відчуття. Сприймати її можна тільки за посередництвом технічних апаратних і програмних засобів. До того ж, кількість і складність цих технічних посередників настільки великі, що зв'язок між вихідною інформацією і тим, що ми бачимо не екрані, не надто прямий і далеко не завжди очевидний. А часом цей зв'язок і зовсім умовний і хисткий. Слід визнати, що огляд комп'ютерної інформації – це не цілком огляд (від слова «дивитися»), а скоріше інструментальна перевірка, яка вимагає певних знань про використовувані технічних засобах, принцип дії яких не завжди є очевидним. Ймовірність помилитися і побачити не те, що є насправді, при цьому підвищена, навіть за відсутності цілеспрямованого впливу злочинця, спрямованого на приховування злочинів. Тому для отримання та фіксації доказової інформації при розслідуванні кіберзлочинів призначення комп’ютерно-технічної експертизи може бути більш корисним, ніж огляд.

Розглянемо особливості огляду та вилучення ноутбуків. Якщо ноутбук включений на момент початку обшуку або огляду, то перш за все слід сфотографувати або іншим чином зафіксувати вміст його екрану.

Щоб вимкнути ноутбук, недостатньо витягнути з нього шнур живлення, адже при цьому ноутбук перейде на живлення від акумулятора. Для знеструмлення ноутбука треба витягти акумулятор.

При цьому не слід закривати кришку ноутбука, складати його. При складанні ноутбука зазвичай активізується функція глибокого сну («засинання»), а це означає внесення змін до інформації на його «жорсткому» диску.

Розглянемо особливості огляду принтерів. Сучасні принтери (за дуже рідкісним винятком) не мають доступних користувачеві носіїв комп'ютерної інформації. Тому вилучати принтери під час огляду та обшуку немає необхідності. Треба тільки вилучити всі друковані документи, виявлені в вихідному лотку принтера або біля нього, оскільки такі роздруківки також містять комп'ютерну інформацію. Крім того, деякі фотопринтери мають роз'єм для безпосереднього підключення носіїв інформації типу флеш-накопичувачів. Якщо такий накопичувач залишений в роз'ємі принтера, його потрібно вилучити, а принтер можна не чіпати. При проведенні огляду чи обшуку слід відобразити в протоколі наявність принтера і спосіб його підключення до комп'ютера. З цього правила є один виняток – справи про підробку документів. Принтери дуже часто використовуються для виготовлення підроблених документів, оскільки їх роздільна здатність (від 600 точок на дюйм і більше) перевищує роздільну здатність людського ока. Тобто підроблений документ, надрукований на сучасному принтері, відрізнити візуально неможливо.

За допомогою експертизи слідчий може встановити, що підроблений документ був надрукований саме на цьому конкретному принтері або з використанням конкретного картриджа.

Коли у кримінальному провадженні фігурують підроблені документи, то крім комп'ютерів і машинних носіїв інформації слід також вилучати:

– принтери;
– картриджі для принтерів (крім, може бути, нових в упаковці);
– інші витратні матеріали (тонер, стрічки, чорнило);

– всі виявлені роздруківки;
– чистий папір і плівку, приготовані для використання в принтері.

Принтер слід опечатати так, щоб унеможливити підключення електроживлення і доступ до друкувального вузла без порушення упаковки. Цей факт відобразити в протоколі. Інші вилучені матеріали також слід опечатати.

Розглянемо особливості огляду та вилучення мобільних телефонів. Перед тим, як прийняти рішення про вилучення мобільного телефон та використання його в якості носія комп'ютерної інформації про вчинення кіберзлочину, слід вирішити, чи потрібно отримати з нього матеріальні сліди – відбитки пальців, сліди наркотиків, інші. Слід пам'ятати, що деякі методи зняття відбитків можуть привести телефон у стан, непридатний для зчитування з нього комп’ютерної інформації. У більшості випадків при вилученні потрібно вимкнути мобільний телефон, щоб виключити втрату наявних даних внаслідок надходження нових викликів і нових SMS. Акумулятор виймати не слід. Однак в деяких випадках керівник слідчої дії може вирішити, що контролювати виклики важливіше. Тоді телефон треба залишити включеним і заряджати його в міру необхідності. Виключений телефон упаковується в жорстку упаковку і опечатується так, щоб виключити доступ до органів його управління. Це зазначається в протоколі. У разі вимкнення телефону не треба турбуватися про PIN-коді на доступ до даних в SIM-карті телефону. У оператора зв'язку в будь-який момент можна дізнатися PUK (PIN unlock key) і з його допомогою отримати доступ до SIM-карти.

Під час проведення слідчих дій з комп’ютерами та іншими носіями комп’ютерної інформації слідчими на увазі, що низка комп’ютерних даних зберігається на електронному пристрої лише під час підключення його до живлення, зокрема:

– вміст ОЗУ, тобто всі виконувані в поточний момент програми (завдання, процеси), системні та прикладні (призначені для користувача);

– колишній уміст ОЗУ в областях оперативної пам'яті, які на поточний момент вважаються вільними;

– список відкритих файлів з відомостями, який процес яким файлом користується;

– інформація про користувацькі сесії, тобто вхід до системи (користувачів які мають логін та пароль);

– мережева конфігурація – динамічно надана IP-адреса, маска підмережі, ARP-таблиця, лічильники мережевих інтерфейсів, таблиця маршрутизації;

– мережеві з'єднання – інформація про поточні з'єднаннях (коннекції) з використанням різних протоколів, про відповідні динамічні налаштування брандмауера або пакетного фільтра;

– поточний системний час;

– список призначених завдань;

– кеш доменних імен і NETBIOS-імен;

– завантажені модулі ядра (LKM);

– монтовані файлові системи, підключені мережеві диски

– файл або область підкачки на диску – інформація про поточний стан віртуальної частини ОЗУ, а також дані, які раніше перебували там;

– тимчасові файли, які автоматично стираються при штатному завершення роботи ОС або при завантаженні ОС.

Більшість зазначені даних можна зняти лише з комп’ютера, який працює. Після його вимкнення або перезавантаження вони будуть втрачені. Вилучити ці відомості під час проведення комп’ютерно-технічно експертизи неможливо і тому у випадку, коли комп’ютер вилучається у вимкненому стані, вони повинні бути вилучені (за

потреби) спеціалістом, якого залучено для проведення слідчої дії. Питання про доцільність вилучення зазначених даних під час огляду/обшуку вирішується слідчим за участі спеціаліста виходячи з наступного:

– ці дані можуть містити корисну доказову інформацію (наприклад, запис поточної TCP-сесії з вузлом, який «атаковано», або ключ для доступу до криптодиска;

– при знятті вмісту ОЗП неможливо не змінити інформацію на комп'ютері, у тому числі на його диску, що може негативно вплинути на оцінку достовірності результатів висновку комп'ютерно-технічної експертизи, яку ймовірно буде призначено у подальшому;

Тому питання про доцільність вилучення цих даних спеціалістом повинно вирішуватись слідчим виходячи з обставин справи (для вирішення цього питання слідчий повинен чітко уявляти, що для нього важливіше: збереження вмісту «жорсткого» диск чи можливість вилучення інформації з оперативної пам'яті).

Розглянемо питання щодо правильного вимкнення комп'ютера під час проведення слідчих дій, спрямованих на пошук комп'ютерної доказової інформації. Існують наступні способи вимкнення комп'ютера:

– за допомогою штатної команди;

– перериванням електроживлення.

Під час процедури завершення роботи комп'ютера закриваються всі відкриті файли, у деяких випадках очищується область підкачки (своп). Всім працюючим програмам надсилається сигнал про завершення роботи при цьому низка шкідливих програми після отримання такого сигналу можуть знищити «сліди» своєї роботи. В такому випадку спеціаліст при проведенні слідчих дій повинен скопіювати вміст ОЗП.

У разі переривання електроживлення всі тимчасові файли залишаються недоторканими. Але зате може бути порушена цілісність

файлової системи, якщо переривання електроживлення застане комп'ютер в момент проведення файлової операції. Зіпсована файлова система в більшості випадків може бути потім відновлена, але не всі експертні системи підтримують таку операцію, а експертне вивчення зіпсованої файлової системи ускладнено. Крім того, можуть з'явитися локальні дефекти в деяких відкритих на запис файлах, наприклад лог-файлах. При цьому обраний слідчим метод вимкнення комп’ютера повинен бути відображений у протоколі слідчої дії.

Розгляд проблемних питань, пов’язаних з особливостями проведення оперативно-розшукових заходів та слідчих дій при розслідуванні кримінальних правопорушень у сфері використання ЕОМ, систем та комп'ютерних мереж і мереж електрозв'язку, дозволяє зробити наступні висновки:

1. До недоліків існуючої взаємодії між оперативними співробітниками правоохоронних органів та спеціалістами в галузі ІТ, захисту інформації, програмування та телекомунікацій слід, на нашу думку, віднести наступні:

– переоцінка оперативними співробітниками правоохоронних органів власних знань та досвіду роботи у відповідній галузі;

– залучення спеціаліста лише на окремих стадіях розслідування кримінального провадження (наприклад, при проведенні огляду місця події та обшуку по кримінальних провадженнях за фактами вчинення кіберзлочинів, під час призначення комп’ютерно-технічної експертизи).

2. Предметом обшуку при розслідуванні є носії комп’ютерної інформації, до яких, в свою чергу, відносяться: зйомні магнітні диски; незйомні магнітні диски; оптичні диски; магнітні карти; цифрові касети; персональні комп’ютери; сервери; комунікаційне обладнання; комунікатори; смартфони; мобільні телефони; цифрові фотоапарати; цифрові відеокамери; інші предмети.

3. При проведенні обшуку ті види електронної техніки, які не містять носії комп’ютерної інформації, не підлягають вилученню з тактичних міркувань. До таких пристроїв відносяться: принтери; сканери; факси; клавіатури; монітори; маніпулятори «миша»; джойстики; звукові колонки.

4. Виходячи із законодавчих, а також тактичних вимог до проведення обшуку, під час вилучення не повинна змінюватись будь-яка інформація, що міститься на носіях комп’ютерної інформації, що вилучаються. Особа, яка керує обшуком, а також інші особи, які під час обшуку їй підпорядковуються, зобов’язані забезпечити такі умови проведення обшуку, за яких вилучена при проведенні обшуку комп’ютерна інформація, яка потім буде надана експерту та суду, жодним чином не змінювалась.

5. На відміну від багатьох інших видів доказів, комп'ютерна інформація не може сприйматися людиною безпосередньо за допомогою органів відчуття.

6. Сприймати комп'ютерну інформацію можна тільки за посередництвом технічних апаратних і програмних засобів. До того ж, кількість і складність цих технічних посередників настільки великі, що зв'язок між вихідною інформацією і тим, що ми бачимо не екрані, не надто прямий і далеко не завжди очевидний. А часом цей зв'язок і зовсім умовний і хисткий.

7. Огляд джерел комп'ютерної інформації – це не цілком огляд (від слова «дивитися»), а скоріше інструментальна перевірка, яка вимагає певних знань про використовувані технічних засобах, принцип дії яких не завжди є очевидним. Ймовірність помилитися і побачити не те, що є насправді, при цьому підвищена, навіть за відсутності цілеспрямованого впливу злочинця, спрямованого на приховування злочинів. Тому для отримання та фіксації доказової інформації при

розслідуванні кіберзлочинів призначення комп’ютерно-технічної експертизи може бути більш корисним, ніж огляд.

ВИСНОВКИ

Розгляд проблемних питань, пов’язаних із методикою розслідувань кримінальних правопорушень у сфері використання ЕОМ, систем та комп'ютерних мереж і мереж електрозв'язку, дає можливість зробити наступні висновки:

1. Існують наступні закономірності розвитку кіберзлочинності:

– основною причиною розвитку вказаної злочинної діяльності є вдосконалення не тільки безпосередньо комп’ютерів, а й комп’ютерних мереж та систем;

– із появою глобальної комп’ютерної мережі «Інтернет» кіберзлочинність «вийшла» на принципово новий рівень і набула глобального, світового характеру;

– якщо «обмін досвідом» між особами, які вчиняють кіберзлочини, і, навіть, видання ними спеціалізованої літератури та організація зустрічей з метою спілкування, «обміну досвідом» злочинної діяльності та узгодження позицій, то з появою глобальної комп’ютерної мережі «Інтернет» особи, які вчиняють кіберзлочини, почали об’єднуватись у групи, розташовані у різних країнах світу;

– вказаний вид злочинів є надзвичайно латентним, факти виявлення вказаної злочинної діяльності у більшості випадків є випадковими;

– однією з розповсюджених причин латентності кіберзлочинності небажання співробітників підприємств, установ та організацій, якими були виявлені факти вчинення кіберзлочинів у відношенні них, звертатися до правоохоронних органів. У свою чергу, причинами цього є: небажання нести репутаційні втрати, втрату клієнтів, небажання надавати приводи та підстави для виявлення власної незаконної діяльності; небажання співробітників підрозділів безпеки банків та комерційних фірм втрачати престижну роботи та посаду через ризик виявлення власної бездіяльності, яка стала причиною та/або умовою для

вчинення кіберзлочину); небажання надавати доступ співробітникам правоохоронних органів до системи комп'ютерної безпеки підприємства; недостатня компетентність з питань протидії кіберзлочинам керівників та рядових співробітників підрозділів безпеки підприємств, установ, організацій, високий рівень правового нігілізму серед них.

2. Слушною удається наступна класифікація кіберзлочинів:

– кримінальні правопорушення, які посягають комп'ютерні дані, а саме на їх доступність, цілісність та конфіденційність. Такі дії можуть полягати у незаконних втручаннях у роботу комп'ютерних систем, втручатися у дані, отриманні незаконного доступу до них;

– кримінальні правопорушення, які полягають у незаконному використання в якості засобів вчинення злочинів персональних комп'ютерів, зокрема, для незаконних дій з інформацією;

– кримінальні правопорушення, які полягають у незаконних діях з інформацією;

– кримінальні правопорушення, предметом посягання яких є авторське право та суміжні права;

кримінальні правопорушення, до об'єктивної сторони яких відносяться акти ксенофобії та расизму.

3. До слідів вчинення кіберзлочинів можна віднести наступні сліди:

– сліди, які залишаються «пакетами» інформаційних даних коли останні «рухаються» глобальною комп'ютерною мережею Інтернет. При цьому кожний користувач комп'ютера при відправленні «пакетів» інформаційних даних адресу комп'ютера-адресата; при проходженні комп'ютерних даних глобальною комп'ютерною мережею Інтернет вони проходять через вузлові комп'ютери (сервери); на цих комп'ютера (серверах) залишаються відомості щодо реєстрації проходження пакетів

даних. Цілком природньо, що при цьому на вузлових комп'ютерах (серверах) залишаються також сліди вчинення злочинів злочинцями;

– некоректна або уповільнена робота персональних комп'ютерів та серверів, зокрема, поява на моніторі персонального комп'ютера нехарактерних символів та написів, уповільнене зчитування пакетів даних, некоректне або уповільнене завантаження операційної системи персонального комп'ютера або сервера;

– зміна способу взаємодії з модемами, принтерами та іншим апаратним устаткуванням; зміна назв та розташування файлів, видалення старих та поява нових мережевих пристроїв;

– зміни у роботі тестового та антивірусного програмного забезпечення, яке використовується у роботі персональних комп'ютерів;

– розмагнічення та фізичне знищення носіїв інформації, додавання або стирання файлових записів, видалення з каталогів імен файлів, поява нових файлів та каталогів, корегування стандартних реквізитів файлів, зміна змісту та розмірів файлів, перейменування окремих файлів і, навіть, цілих каталогів;

– зміна параметрів роботи пристроїв, за допомого яких персональних комп'ютер «впізнає» користувача за голосом, зміни в електронних «ключах доступу» та інші сліди, які зловмисники залишають на спеціальних засобах, призначених для захисту комп'ютерної інформації;

– рукописні записи, за допомогою яких злочинець записував таблиці шифрування, переліки паролів, коди та інші сліди, які може залишити на місці перебування особа, яка вчинила кіберзлочин;

сліди пальців рук та ДНК, які особа, що вчинила кіберзлочин залишила на кнопках увімкнення/вимкнення комп'ютерного устаткування, клавіатурі тощо.

4. Розглянемо питання щодо осіб, які найчастіше стають потерпілими від кіберзлочинів:

– до першої групи належать підприємства, установи та організації з розгалуженою бюрократичною організаційною структурою управління, де влада обмежена однією особою – керівником, але ніхто з підлеглих ні за що не відповідає. Завдяки комп'ютеризації люди все частіше залучаються до автоматизованого програмного забезпечення для управління брендом та баз даних облікових записів. Більшість акторів не мають повного уявлення про те, як працюють ці системи. Він робить це через несанкціоноване використання працівниками, які вирішили стати на злочинний шлях;

– друга група – це юридичні особи з різними властивостями. які мають велике значення для внутрішнього виробництва та технологічного розвитку відповідно до використання комп'ютерних технологій, які не встигають розробити відповідні адміністративні структури. У таких закладах їх керівники не завжди знають, які заходи слід вжити, щоб запобігти несанкціонованому доступу роботодавців і клієнтів, а також сторонніх осіб;

– третя група – це установи та організації, які, з одного боку, працюють над забезпеченням захисту інформації та конфіденційності інформації для цілей ІТ, з іншого – ще не мають належної організаційної та адміністративної структури, можливості контролювати чутливі сфери виробництва (офіси, відділи, конкретні працівники), які беруть участь у створенні цієї інформації;

– четверта група – це компанії та/або товариства, які за визначенням створюються зовнішнім капіталом або залежать від великих корпорацій. Ці правові організації представляють «сфери підвищеного ризику злочинності», оскільки вони дуже зацікавлені у кримінальних структурах та компонентах. Наприклад, коли вони відвідують національні форуми, ці фірми в першу чергу працюють, щоб відповідати своїм нормам і структурам режиму. місцеві працівники, по -друге, змінюють роботу відповідно до національного законодавства, по -третє,

зменшують інформаційну систему конфіденційності під впливом національних стандартів та правил, по-четверте, для врахування конкретних програм Існуючі просторові інструменти, подалі від мереж та комп'ютерних систем, включені до цифрових телекомунікації. Все це збільшує можливості кримінального переслідування щодо такого типу жертв;

– п'яту групу складають проекти, установи та установи, в яких існують різні моральні аномалії за різних обставин. і психологічний клімат (наприклад, через: неточні міжособистісні стосунки між працівниками, між працівниками та керівниками; значні відмінності в оплаті праці працівників на тих самих посадах; управління наймом персоналу по відношенню до нижчих професійних рівнів. моральний, псевдопідприємець і для інші причини.

5. Оцінюючи ймовірну особу злочинця, який вчинив кіберзлочин під час встановлення його особи, надзвичайно важливо визначити його рівень компетенції ІТ. Це питання є критично важливим. При цьому рівень володіння ним навичками із приховування та видалення комп'ютерної інформації має вирішальне значення. Коли невідомо, який рівень має підозрюваний, його слід вважати високим. Наприклад, під час вилучення увімкнутого комп'ютера технік повинен вирішити, чи використовувати звичайне вимкнення, або просто вимкнути живлення. З одного боку, певна кількість інформації, майже нерелевантної, може зникнути, коли комп'ютер буде вимкнуто перериванням живлення. Але краще виходити з того, що серед осіб, що вчиняють кіберзлочини розповсюдженою є тактика, коли така особа залишає у ввімкненому комп'ютері комп'ютерну логічну бомбу, яка реагує на команду вимкнення. Тому існує небезпека, що всі документи будуть знищені своїми руками при нормальному вимкненні комп'ютеру. Вибір варіанту залежить від того, як ми оцінюємо вертикальну рівень власника комп'ютера. Якщо неможливо оцінити цей рівень, комп'ютер

вимикається внаслідок переривання живлення, тобто слід виходити із можливої наявності логічної бомби.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cyber crime is often thought of as a type of modern warfare, but hacking practices have been around longer than you might expect. URL: https://www.pdaa.edu.ua/sites/default/files/node/4518/pravylaoformlennyaspyskuvykorystanyhdzherel.pdf (дата звернення: 1.10.2021).

2. Where does cybercrime come from? The origin & evolution of cybercrime. URL: https://www.le-vpn.com/history-cyber-crime-origin-evolution/ (дата звернення: 1.10.2021).

3. Абрамова В.М. Криміналістика : [навч. посіб. для дистанційного навчання] / [В.М. Абрамова, А.О. Ляш]; за наук. ред. А.В. Іщенка. - К. : Університет "Україна", 2007. - 557 с.

4. Алексеев О.О. Розслідування окремих видів злочинів : навч. посіб. 2-ге вид. перероб. та доп. / О.О. Алексеев, В.К. Весельський, В.В. Пясковський - К. : "Центр учбової літератури", 2014. - 320 с.

5. Бахін В.П. Взаємодія слідчого з фахівцями під час огляду місця події (збір інформації про особу, що скоїла злочин) : Науково-практичні рекомендації / В.П. Бахін, О.О. Волобуєва. - Донецьк : ДЮІ, 2005. - 72 с.

6. Бишовець О.В. Психологічний вплив у кримінальному провадженні: теорія і практика : [монографія] / О.В. Бишовець. - К. : Істина, 2013. -152 с.

7. Біленчук П.Д. Документування результатів слідчої дії: методи фіксації доказової інформації : [монографія] / П.Д. Біленчук, А.В. Кофанов, О.Л. Кобилянський, Л.Д. Скільська ; [за ред. П.Д. Біленчука]. - Київ : ННІПСК КНУВС, 2009. - 96 с.

8. Бірюков В.В. Теоретичні основи інформаційно-довідкового забезпечення розслідування злочинів : [монографія] / Бірюков Валерій Васильович / Луган. держ. ун-т внутр. справ ім. Е.О Дідоренка. - Луганськ : РВВ ЛДУВС їм. Е. О. Дідоренка, 2009. - 664 с.

9. Бутузов В.М. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток : Навчальний посібник / В.М. Бутузов, В.І. Василинчук, В.П. Шеломенцев. - К. : Типографія ТОВ "СТ-Стиль". - 2006. - 139 с.

10. Волобуєв А.Ф. Про методи криміналістики / А.Ф. Волобуєв // Про печення розкриття та розслідування злочинів : 36. матеріалів міжнарод. на-ук.-практ. конф. - К., 2010. - С. 28-29.

11. Гора І.В. Криміналістика : [навч. посібник] / І.В. Гора, А.В. Іщенко, В.А. Колесник. - [4-те вид]. - К. : Вид. ПАЛИВОДА А.В., 2007 - 236 с.

12. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. : НІСД, 2014. – 328 с.

13. Енциклопедія судової експертизи / [Клименко Н.І., Бахін В.П., Будко Т.В., Цимбал П.В]. - Ірпінь : Національний університет ДПС України, 2013. - 184 с.

14. Іщенко А.В. Методологічні проблеми криміналістичних наукових досліджень : [монографія] / А.В. Іщенко ; за ред. LH Красюка. - К. : Нац. акад. внутр. справ України, 2003. - 359 с.

15. Іщенко А.В. Наукове забезпечення протидії злочинності / [Іщенко А.В., Карпов НС, Кондратьев Я.Ю.]. - К., 2001. - 223 с.

16. Керівництво з розслідування злочинів : наук.-практ. посіб. / [кол. авт. : В.К). Шепітько, В.О Коновалова, В.А. Журавель та ін.] ; за ред. В.Ю. ГДепітька. - Х. : Одіссей, 2009. - 960 с.

17. Клименко НІ. Інтеграційна функція експертології // Теорія та практика судової експертизи і криміналістики : 36. наук.-практ. матер. - Х. : Право, 2006. - Вип. 6. - С. 117-124.

18. Клименко НІ. Судова експертиза в розслідуванні комп'ютерних злочинів як форма використання спеціальних знань / НІ. Клименко, П.Д. Біленчук // Теорія та практика судової експертизи і криміналістики : 36. матер. міжнар. наук.-практ. конф. - Х. : Право, 2002. - Вип. 2. - С. 62-66.

19. Клименко НІ. Судова експертологія: курс лекцій : навч. посіб. для студ. юрид. спец. вищ. навч. закл. / НІ. Клименко. - К. : Видавничий Дім "Ін Юре", 2007. - 528 с.

20. Книженко, С. О. Структурні елементи методики розслідування окремих видів злочинів [Електронний ресурс] // Форум права. - 2008. - № 2. – С. 227-230. URL: http://www.nbuv.gov.ua/e-journals/FP/2008-2/08ksoonz.pdf. (дата звернення: 1.10.2021).

21. Кобилянський О.Л. Методика дослідження документів, які мають захисні засоби : [метод. рек.] / О.Л. Кобилянський. - К. : Нац. акад. внутр. справ України, 2005. - 36 с.

22. Когутич І.І. Криміналістика : [курс лекцій] / І.І. Когутич. - К. : Атіка, 2008. - 888 с.

23. Когутич І.І. Криміналістичні знання, їх сутність і потреба розширення меж використання : монографія / І.І. Когутич. - Львів : "Тріада плюс", 2008. - 420 с.

24. Конвенція Ради Європи про кіберзлочинність: від 23.11.2001 р. URL: http://zakon2.rada.gov.ua/laws/show/994_575 (дата звернення 1.10.2021).

25. Коросташова Т.О. Основи слідознавства : [курс лекцій з криміналістики] / Т.О. Коросташова, Ю.О Ланцедова, ОС. Тунтула ; [за наук. ред. О.А. Кириченка]. - Миколаїв : ЧДУ ім. Петра Могили, 2012. - 48 с.

26. Котюк І.І. Теоретичні аспекти криміналістичної ідентифікації : [монографія] / І.І. Котюк. - К. : ВПЦ "Київський університет", 2004. - 208 с.

27. Кофанов А.В. Криміналістика: питання і відповіді : [навчальний посібник] / А.В. Кофанов, О.Л. Кобилянський, Я.В. Кузьмічов та ін. - К. : Центр учбової літератури, 2011. - 280 с.

28. Криміналістика (криміналістична техніка) : [курс лекцій] / П.Д. Біленчук, А.П. Гель, М.В. Салтевський, Г.С. Семаков. - К. : МАУП, 2001. - 216 с.

29. Криміналістика : [електронний ресурс] / В.І. Перкін, П.Д. Біленчук, В.К. Весельський, В.Б. Школьний, Ю.Б. Комаринська ; під. ред. П.Д. Біленчука. (Мультимедійний підручник). - Київ : Київський національний університет внутрішніх справ, 2008. - 1 електрон. опт. Диск (CD-ROM); 12 см. - Назва з титул. екрану.

30. Криміналістика : [навч.-метод. посібник] / В.В. Тіщенко, Л.І. Аркуша, В.М. Плахотіна. - [4-те вид., випр.]. - Одеса : Фенікс, 2013. - 338 с.

31. Криміналістика в тестах : [навч. посібник] / І.І. Когутич, (D.M. Колужна, І.В. Жолнович та ін. ; [за заг. ред. І.І. Когутича]. - К. : Але-рта, 2013. - 534 с.

32. Криміналістика у питаннях і відповідях : Навчальний посібник [Текст] К 82 / [А.В. Іщенко, В.В. Пясковський, А.В. Самодін, Ю.М. Чорноус та ін.] – К. : ТОВ "Видавництво "Центр учбової літератури" , 2016. – 118 с.

33. Криміналістика: Підручник / Кол. авт.: В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін. / За ред. проф. В. Ю. Шепітька. – 4-е вид., перероб. і доп. – Х.: Право, 2008. – 464 с.

34. Малюга В. Структура методики розслідування окремих видів злочинів і місце в ній взаємодії слідчого / В. Малюга // Підприємництво, господарство і право. – 2015. – № 8. – С. 61-65.

35. Методика розслідування окремих видів злочинів: навч. посібник / О. І. Гарасимів, О. М. Дуфенюк, О. В. Захарова та ін.; за заг. ред. Є. В. Пряхіна. 2-ге вид., перероб. та допов. Львів: ЛьвДУВС, 2019. 312 с.

36. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп’ютерних технологій : автореф. дис. ... канд. юрид.

наук : 12.00.09 / О. І. Мотлях ; Академія адвокатури України. – Київ, 2005. – 20 с.

37. Романюк Б. В., Камлик М. І., Гавловський В. Д. Виявлення та розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій: Посіб. / За заг. ред. проф. Я. Ю. Кондратьєва. – К.: Національна академія внутрішніх справ України, 2000. – 64 с.

38. Сабадаш В. П. Криміналістика [текст] : навч. посіб./ В. П. Сабадаш, М. О. Ларкін - К. : «Центр учбової літератури», 2013. - 228 с.

39. Самойленко О. А. Виявлення та розслідування злочинів в сфері ІТ-технологій [Текст] : навчальнометодичний посібник / О. А. Самойленко. Одеса : , 2020. 133 с.

40. Старушкевич А. Організація огляду місця події. Аналіз криміналістично- значимої інформації при розслідуванні злочинів у сфері комп'ютерної інформації // Вісник прокуратури. – 2003. – № 12. – С. 77 – 86.

41. Федосова, О. В. Становлення та перспективи розвитку криміналістичної методики розслідування злочинів / Федосова О. В. // Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція. – 2020. – Вип. 46. – С. 174-178.