ТЕМА 23

ОСОБЛИВОСТІ МЕТОДИКИ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, СКОЄНИХ У СФЕРІ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ

§ 1. Поняття і розвиток комп'ютерної інформації та характеристика злочинних груп у цій сфері. Основні комплектуючі частини комп'ютера і їх призначення.
§ 2. Основи комп'ютерної злочинності, види комп'ютерних злочинів і основні напрямки комп'ютерних посягань.
§ 3. Криміналістична характеристика комп'ютерних злочинців.
§ 4. Особливості методики слідчих дій при розслідуванні комп'ютерних злочинів.
§ 5. Сучасні можливості використання мобільних комплектуючих науково-технічних засобів при розслідуванні та розкритті злочинів.

§1. Поняття і розвиток комп'ютерної інформації та характеристика злочинних груп у цій сфері. Основні комплектуючі частини комп'ютера і їх призначення

На сучасному етапі розвитку цивілізації інформація відіграє ключову роль у функціонуванні суспільних і державних інститутів і в житті кожної людини. Водночас з активною інформатизацією усіх сторін життєдіяльності суспільства, розширенням сфери застосування інформаційних технологій, входженням до світового інформаційного простору набувають поширення і правопорушення в цій сфері, зокрема злочини, пов'язані з використанням технічних засобів проникнення і вилучення інформації та впливу на неї.

В Україні комп'ютерна злочинність лише починає набирати силу і потребує наукового дослідження. Стосовно дослідження окремих галузей, що відносяться до юридичної науки, то тут пріоритетними напрямками є: для науки кримінального права – деякі особливості кваліфікації злочинів, що

мають комп'ютерні аспекти; для криміналістики – засоби, методи, способи і прийоми розкриття, розслідування і попередження злочинів; для судової психіатрії – діагностування комп'ютерних фобій та їх зв'язок з проблемами неосудності. Тому саме зараз в Україні ми можемо і повинні говорити про актуальність цієї теми, адже процес комп'ютеризації в нашій державі набув дуже широкого розмаху. Це вимагає забезпечення належного рівня інформаційної безпеки, яка становить підсистему в системі національної безпеки України. Комп'ютерні системи містять у собі нові, дуже досконалі можливості для невідомих раніше правопорушень, а також для скоєння традиційних злочинів, але нетрадиційними засобами. Безумовно, найбільше від комп'ютерних злочинів страждають розвинуті в технологічному відношенні країни, однак і в інших країнах з початком процесу масової комп'ютеризації з'явилось те ж саме міжнародне явище, пов'язане з криміналізацією у сфері обороту комп'ютерної інформації, назва якого – комп'ютерні злочини.

Масова комп'ютеризація в Україні почалася в кінці 80-х – на початку 90-х років XX (набагато пізніше, ніж в США та Західній Європі). Це призвело до розвитку ринку комп'ютерів та програмного забезпечення. Саме розвиток цієї сфери діяльності в Україні проходив не так швидко, як в деяких цивілізованих країнах, оскільки до комп'ютера ставились з недовірою і взагалі всю цю сферу діяльності вважали «лженаукою». Але згодом суспільство почало розуміти, що це дуже корисна річ, яка нині впевнено увійшла в інтер'єр офісів та кабінетів. «Безпаперова» технологія активно впроваджується в автоматизовану обробку бухгалтерської та іншої виробничої документації. У процесі розвитку виникла комп'ютерна мережа, до якої почали під'єднуватися майже всі компанії, організації, фірми, різного роду товариства тощо.

Звісно, коли з'явилася нова сфера діяльності – почали з'являтися правопорушники правил експлуатації ЕОМ (електронно-обчислювальних машин), тобто суб'єкти злочину в цій сфері діяльності. Саме тому в ККУ з'явився новий розділ XVI «Злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж». Для того, щоб характеризувати таких порушників потрібно знати, що собою являє комп'ютер та вміти користуватися ним.

Комп'ютер призначений для сприймання, обробки, зберігання та видачі необхідної інформації за командою людини. Він складається з основних та допоміжних частин. До основних частин комп'ютера належать:

- системний блок;
- монітор (дисплей);
- клавіатура.

Системний блок складається з різних електронних компонентів, таких як мікропроцесор, материнська плата, вінчестер, CD-ROM, дисковод та інші складові. Він виконує роботу по прийому, обробці, збереженню, виводу не-

обхідної інформації на екран монітора, або на друкуючі пристрої, такі як принтер. Системний блок – це головна частина, яка регулює всю роботу комп'ютера.

Монітор (дисплей) є другим важливим компонентом комп'ютера. Він являє собою пристрій, призначений для виведення інформації у візуальному режимі у вигляді тексту, графіків чи малюнків на екрані.

Клавіатура є стандартним пристроєм вводу інформації або команд в комп'ютер. Тобто, за допомогою клавіатури відбувається спілкування між людиною та комп'ютером.

Комп'ютер також може мати допоміжні компоненти, такі як:

- маніпулятор – «миша»;
- принтер;
- сканер;
- модем;
- зовнішні чи внутрішні динаміки.

Маніпулятор («миша») призначений для виділення, переміщення об'єктів на екрані монітора, та здійснення підтверджень на запити комп'ютера.

Принтер відтворює відображення інформації на екрані монітора в друкованій копії з виведенням її на папір.

Сканер утворює в комп'ютері (на екрані монітору) електронну копію зображення тексту, малюнка, фотографій, які були відображені на папері, тобто зчитує інформацію.

Модем – це пристрій, призначений для вводу, виводу та передачі інформації на далекі відстані за допомогою телефонної мережі. Модем використовується для «спілкування» в електронній мережі Інтернет.

Динаміки (зовнішні чи внутрішні) призначені для відтворення звуку.

Так, з появою ЕОМ, знайшлися «умільці», які почали використовувати ком'ютери в злочинних цілях (підробка цінних паперів, підробка грошей, незаконне копіювання секретної інформації, незаконне проникнення в комп'ютерну мережу та безліч злочинів, пов'язаних з Інтернетом).

Злочинці комп'ютерної мережі умовно поділяються на декілька груп: хакери, крекери, фріки, колекціонери та кіберплути. Всіх їх єднає те, що вони працюють з інформацією незаконними методами, які нині віднесені до злочинних посягань (див. ККУ ст.ст. 361–363). Незаконне втручання в роботу автоматизованих ЕОМ призводить до перекручення, викрадання або знищення комп'ютерної інформації чи носіїв такої інформації, а отже, є суспільно небезпечним діянням, тобто злочином. Зупинимось на характеристиці кожної із цих груп.

Хакери характеризуються тим, що вони здійснюють злочини «заради інтересу», тобто з метою показати іншим свої «супернавички» в цьому напрямку.

Хакери отримують задоволення від вторгнення та вивчення великих ЕОМ за допомогою телефонних ліній та комп'ютерних мереж. Це комп'ютерні хулігани, електронні корсари, які без дозволу проникають у чужі інформаційні мережі для забави. У значній мірі їх тягне до себе подолання труднощів. Чим складніша система, тим привабливіша вона для хакера. Вони чудові знавці інформаційної техніки. За допомогою телефонних ліній і персональних комп'ютерів вони підключаються до мереж, які пов'язані з державними та банківськими установами, науково-дослідницькими та університетськими центрами, військовими об'єктами. Хакери, як правило, не роблять шкоди системі та, заволодівши інформацією, вони отримують лише насолоду від почуття своєї влади над комп'ютерною системою. Наприклад, був зламаний сайт в Інтернеті Оксфордської бібліотеки хакером лише для того, щоб показати, що захисна система недосконала, тобто з часом її потрібно вдосконалювати. Вони у змозі розробити вірус, який негативно може вплинути на всі комп'ютерні системи, що підключені до мережі та ін.

Крекери, на відміну від хакерів, характеризуються тим, що вони працюють з комп'ютерами не просто в особистих інтересах, а заради наживи. Для їх дій характерні фальсифікація цінних паперів та документів, кредитних карток, злами кодів банку та переведення грошових рахунків на свій фіктивний рахунок, встановлення жучків у комп'ютерах для отримання секретної інформації та використання її в особистих цілях. Крекери – це більш серйозні порушники, здатні спричинити будь-яку шкоду системі. Вони викрадають інформацію, викачуючи за допомогою комп'ютера інформаційні блоки даних, змінюють та псують файли. З технічного боку їх злочинна діяльність набагато складніша від того, що роблять хакери. Це може бути викликано помстою, психічним захворюванням або іншими причинами і виконуватись шляхом закладання вибухівки, заливання фарбою, або підпаленням комп'ютерів. Наприклад, методом зламу та таємного проникнення в інший комп'ютер крекер оволодіває секретною інформацією та продає її за значну суму людям, які її потребують. За допомогою комп'ютерної мережі можна отримати програму будівництва ядерного реактора чи спричинити аварійну ситуацію на АЕС і, таким чином (методом шантажу), заробити велику суму грошей .

Фріки спеціалізуються на використанні телефонних систем з метою уникнення від оплати телекомунікаційних послуг. Вони також отримують насолоду від подолання труднощів технічного плану. У своїй діяльності фріки використовують спеціальне обладнання («чорні» та «блакитні» ящики), яке генерує та посилає змінені спеціальні тони виклику до телефонних мереж.

Нині фріки в основному орієнтуються на отримання кодів доступу, крадіжках телефонних карток та номерів доступу з метою уникнути платні за те-

лефонні розмови за рахунок іншого абонента. Досить часто вони займаються прослуховуванням телефонних розмов.

Колекціонери – колекціонують та використовують програми, які мають цінну інформацію, перехоплюють різні паролі, а також коди телефонного виклику та номери приватних телефонних компаній, які мають вихід до загальної мережі. Вони в основному обмінюються паролями, програмним забезпеченням, номерами, але не торгують ними.

Кіберплути – це злочинці, які спеціалізуються на розрахункових рахунках. Вони використовують комп'ютери для крадіжки грошей, отримання номерів кредитних карток та іншої цінної інформації. Цю закодовану інформацію потім продають іншим особам, при цьому досить часто контактують з організованою злочинністю, отримуючи за це досить великі грошові суми. Популярним товаром є кредитна інформація, інформаційні бази правоохоронних органів та інших державних установ.

Великі організації, компанії, фірми чи товариства, які потерпіли від такого злочину, не особливо поспішають розголошувати інформацію про скоєння злочину відносно них, оскільки це може призвести до повторного злочину іншими злочинцями такого роду або ж падіння авторитету серед конкуруючих організацій, компаній, фірм та товариств. Наприклад, якщо з певного авторитетного банку була вкрадена важлива інформація або велика кількість грошей, цінні папери, то внаслідок злочину клієнти банку втрачають довіру до нього і звертаються за послугами до інших банків з більш надійною охоронною системою комп'ютерної мережі .

Для зменшення ризику бути потерпілим від комп'ютерного злочину, потрібно приділяти певну увагу системі захисту комп'ютерних мереж та вміти попереджувати злочини такого роду. З такими злочинцями потрібно не конкурувати, а вести постійну і наполеглеву боротьбу, удосконалювати свої методи і способи з виявлення і розкриття злочинів у сфері комп'ютерної техніки.

Як відомо, особа злочинця досліджується різними науками: психологією, психіатрією, судовою медициною, кримінологією та іншими науками, в тому числі і криміналістикою, але криміналістика, в першу чергу, звертає увагу на так звані «професійні» звички та «почерк» злочинців, тобто на характерні сліди злочину, які і є джерелом інформації про скоєний злочин, про це буде сказано нижче.

§2. Основи комп'ютерної злочинності, види комп'ютерних злочинів і основні напрямки комп'ютерних посягань

Тенденція росту комп'ютерних злочинів у сфері застосування електронно-обчислювальної техніки, про що свідчить аналіз вітчизняної і особливо зарубіжної практики, вивчення наукової літератури дозволяє звернути увагу громадськості і, зокрема, юристів на те, що в світовій практиці з'явились якісно нові, юридично і психологічно оригінальні технічні види злочинів (див. ст. 361–363 ККУ). З подібним явищем суспільство раніше не мало справи.

Протягом 1990–1997 років науковцями вивчались проблеми, пов'язані з бурхливим розвитком феномена, відомого в усьому світі під назвою **«комп'ютерна злочинність».** На сьогоднішній день це поняття включає всі протизаконні дії, при яких електронне опрацювання інформації було знаряддям їх учинення або їх об'єктом .Таким чином, у це коло проблем потрапили не лише злочини, безпосередньо пов'язані з комп'ютерами, але й такі як шахрайство з магнітними кредитними картками, злочини у галузі телекомунікацій (шахрайство з оплатою міжнародних телефонних переговорів), незаконне використання банківської мережі електронних платежів, програмне «піратство», шахрайство з використанням ігрових автоматів та багато інших злочинів.

Характерні риси комп'ютерної злочинності:

- має міжнародний характер злочину (виходить за рамки кордону однієї держави);
- труднощі у визначенні «місцезнаходження злочину»;
- слабкість зв'язку між ланками в системі доказів;
- неможливість спостерігати і фіксувати докази візуально;
- широке використання злочинцями засобів шифрованої інформації.

У нашій країні комп'ютерна злочинність – поняття досить маловідоме і маловивчене. Але світовій практиці (кримінальній статистиці) це явище знайоме вже близько 50 років. Практично із застосуванням комп'ютерної техніки в різних сферах діяльності людини з'явилась фальсифікація даних, які вводились в ЕОМ. За даними американського криміналіста О. Б. Паркера злочинність, «пов'язана з системою електронної обробки даних, виникла одночасно з появою комп'ютерної техніки близько 1940 року». Поки що не має єдиної згоди у визначенні цього нового міжнародного явища, назва якого – комп'ютерна злочинність.

У системі кримінальної поліції ФРН за декілька останніх років було запропоновано ряд кримінально-правових визначень комп'ютерної злочинності. Наприклад, деякі фахівці вважають, що комп'ютерні злочини – це всі злочинні дії, при яких комп'ютер є знаряддям, засобом чи метою їх здійснення. Друге визначення об'єднує під цим терміном всі протизаконні дії, які завда-

ють збитки майну і пов'язані з електронним опрацюванням даних. Третє визначення комп'ютерної злочинності окреслює три основні види протизаконних дій:

1. Комп'ютерні майнові злочини (наприклад, комп'ютерне шахрайство, саботаж, промисловий шпіонаж);

2. Комп'ютерні злочини проти прав особи;

3. Правопорушення проти громадських і суспільних-правових цінностей (наприклад, проти національної безпеки).

Під комп'ютерною злочинністю більшість криміналістів розуміють суспільно небезпечну діяльність чи бездіяльність, яка здійснюється з використанням сучасних інформаційних технологій і засобів комп'ютерної техніки з метою спричинити збитки майновим або суспільним інтересам держави, підприємствам, відомствам, організаціям, кооперативам і громадянам, а також правам окремої особи.

Сформульоване визначення комп'ютерної злочинності дозволяє зробити висновок, що це складне нове явище в кримінально-правовій практиці, яке потребує більш досконалого спеціального і систематичного вивчення.

Комп'ютерні злочини – це якісно новий вид злочинності в нашій країні, їх діапазон у світовій практиці надзвичайно широкий. Практично навіть злочинці-дилетанти, як і досвідчені злочинці, сьогодні можуть проникати в різноманітні комп'ютерні системи і автоматизовані банки даних. Цей вид суспільно небезпечного діяння поки що залишається недостатньо вивченим. Тому попереду велика науково-дослідна робота з вивчення цього явища і розробка на цьому ґрунті відповідних законодавчих положень.

Аналізуючи цей вид злочинів, дослідники зробили висновок, що **основними видами комп'ютерних злочинів є:**

- крадіжка або маніпуляція даними машинної інформації (крадіжка, зміна або знищення даних з метою вчинення злочину);
- крадіжка машинного часу;
- несанкціоноване використання системи;
- крадіжка речей;
- шпіонаж (політичний та промисловий);
- саботаж;
- вандалізм;
- руйнування устаткування ЕОМ;
- введення в ЕОМ неправдивих відомостей;
- продовження виплат після смерті клієнта;
- зміна введеної програми;
- введення і виведення даних ЕОМ та ін.

Найпоширенішим злочином є крадіжка грошей, особливо в місцях, де погано налагоджена система комп'ютерної безпеки (ст. 362–363 ККУ). На другому місці стоїть крадіжка речей (приладів, електронного устаткування, товарів) та ін. Крадіжка машинної інформації існує двох видів:

- крадіжка інформації (ділової, фінансової, результатів наукових досліджень, конструкторських робіт тощо), що зберігається в пам'яті ЕОМ;
- крадіжка комп'ютерних програм.

Крадіжка машинного часу не у всіх країнах розглядається як злочин. Деякі відомства навіть заохочують сторонні заняття своїх співробітників з комп'ютерною службою, вважаючи, що саме цим вони стимулюють науковий пошук.

Ще одна категорія комп'ютерних злочинів – несанкціоноване використання системи, куди входить також крадіжка різних послуг (ст. 361 ККУ).

Що стосується саботажу, то він в основному викликаний економічною конкуренцією, рідше політичними міркуваннями.

Відносно вандалізму, то він зазвичай набуває форм фізичного руйнування або знищення комп'ютерних систем та їх складових. Ці дії, як правило, вчиняють «крекери» – це комп'ютерні злочинці, які є різновидом хакерів. Але якщо **хакери** отримують задоволення від вторгнення та вивчення великих ЕОМ за допомогою телефонних ліній та комп'ютерних мереж, то крекери – це більш серйозні порушники, здатні спричинити будь-яку шкоду системі.

Згідно з дослідженнями, що проводились у США, переважна більшість комп'ютерних посягань спрямована на несанкціоновану передачу та зміну комп'ютерних даних. Аналізуючи таке становище, слід зауважити, що для того, щоб запобігти цим посяганням необхідно переглянути, а можливо й розробити відповідні законопроекти, які б регламентували діяльність правоохоронних органів у цій області. Наприклад, на думку американських вчених, незаконне копіювання інформації з автоматизованих банків даних та інших компонентів програмних засобів ЕОМ, як відзначалося в журналі «Мінімікр Системс», щорічно обходиться видавцям і торгівельним фірмам в декілька мільярдів доларів.

Збитки, що виникають внаслідок комп'ютерних злочинів, приводять до наступних наслідків:

1. Порушення функціонування комп'ютерної системи (часові порушення, що ведуть до плутанини в графіках роботи, розкладах тих чи інших дій; недоступності системи для користувачів, пошкодження апаратури (такі, що можуть бути усунуті і такі, що не можна усунути; пошкодження програмного забезпечення (що можуть бути усунуті, і такі, що не можна усунути);

2. Втрати значних ресурсів (грошей, речей, устаткування, послуг, інформації);

3. Втрати монопольного використання (закупівельних цін, потенційних покупців тощо);

4. Порушення прав через стандартні комп'ютерні технології.

До категорії злочинів, пов'язаних з втручанням в роботу комп'ютерів і комп'ютерних мереж, належать:

1) несанкціонований доступ до інформації, що зберігається в комп'ютері;

2) розробка і розведення комп'ютерних вірусів;

3) введення в програмне забезпечення комп'ютерних вірусів, які частково або повністю виводять з ладу комп'ютерну систему;

4) злочинна необережність при розробці, виготовленні і експлуатації програмно-обчислювальних комплексів, що призводить до тяжких наслідків;

5) підробка комп'ютерної інформації;

6) викрадення комп'ютерної інформації та ін.

Так, наприклад, нині ЕОМ використовують з метою присвоєння власності, крадіжок програм і математичного забезпечення із автоматизованих систем проектування, фінансування, шантажу, великих вимагань (електронний рекет) та ін. Статистика США свідчить про бурхливе зростання так званих «електронних пограбувань», що здійснюються «електронними злочинцями».

Наприклад, за допомогою електронного рекету, електронного грабежу було здійснено найбільше за всю історію Америки пограбування банку. Так, фахівець, що обслуговував ЕОМ (електронний злодій) розшифрував код, за допомогою якого здійснювалось управління електронною системою банку «Сек'юріті Песіфік Нейшнл Банк» у Лос-Анджелесі, дав команду ЕОМ про перерахування 10 мільйонів доларів на його поточний рахунок. Оскільки щоденно цей банк проводить більше 1500 операцій на суму біля 4 мільярдів доларів, то така «невелика» сума як 10 мільйонів доларів виявилась непомітною. Цей електронний злочинець був затриманий лише тому, що спекулював алмазами, які придбав на викрадені гроші.

Необхідно відзначити також, що звичайні гангстери не можуть зрівнятися з грабіжниками, що мають електронні відмички. Доходи тривіальних гангстерів значно менші, ніж електронних злодіїв. Крім того, статистика свідчить, що «левова частка» комп'ютерних злочинів в основному скоюється вдень (на роботі), під час виконання електронними злодіями їх безпосередньої службової професійної діяльності, тому затримати їх в цей час практично неможливо, а імовірність пошуку і встановлення злочинця надзвичайно мала. Згідно з оцінками експертів – один випадок на 25 тисяч.

Розкриваючи соціально-правову і криміналістичну характеристику цього виду злочину, необхідно відзначити, що більшість провідних фахівців у цій галузі вважають, що електронна відмичка стане багатообіцяючим знаряддям

різних комп'ютерних злочинів майбутнього. Вже нині в річному огляді Американської асоціації адвокатів вказується, що половина злочинів у діловому світі пов'язана з використанням комп'ютерів.

Крім електронних крадіжок, в Західній Європі спостерігається зростання електронного хуліганства, вандалізму і тероризму. Типовими представниками злочинного середовища цього напрямку є так звані **хакери** – одержимі програмісти. Про цих осіб ми вже дещо говорили вище. Слід зауважити, що мета їх злочинної діяльності – несанкціонований доступ, проникнення в автоматизовані банки даних (АБД), крадіжки, рекет, різні електронні маніпуляції або просто знищення (стирання) інформації, що знаходиться в банках даних.

По суті, масштаб небезпеки**,** яка загрожує життєдіяльності суспільства з боку різного роду комп'ютерних злочинців, рекетирів, диверсантів, хуліганів, терористів та подібних їм, з розвитком національних інфраструктур важко передбачити, адже абсолютно надійного гарантованого захисту від несанкціонованого доступу і проникнення в життєво важливі АБД, АСУ на сьогоднішній день майже немає.

Як вже зазначалось, комп'ютерні злочини здійснюються не лише з метою матеріальної винагороди, а й з політичних мотивів. Прикладом цього є активність екстремістських і терористичних організацій у таких країнах, як США, Іспанія, Німеччина, Франція, Австрія, де здійснюються напади на комп'ютерні центри з політичних мотивів. Так, наприклад, 11.09.2001 р. скоєна терористична атака на «вежі-близнюки» Всесвітнього торгового центру у Нью-Йорку і на Пентагон у Вашингтоні із застосуванням авіатарану, де загинули не тільки вся комп'ютерна інформація, а і декілька тисяч людей.

Помітно зростає тенденція, коли окремі ентузіасти-зловмисники з числа досвідчених математиків-програмістів та спеціалістів у галузі електроніки почали виготовляти так звані **комп'ютерні віруси,** тобто такі програми, які вступають у дію через певний проміжок часу і руйнують всі інші програми, що зберігаються в пам'яті ЕОМ. Так, 16 листопада 2001р. була здійснена вірусна атака на комп'ютерну систему ВАТ «Укртелеком», якій було завдано збитку на суму понад 1 млн грн.

Ще у 1988 році одна з зарубіжних промислових комп'ютерних асоціацій зафіксувала більше 90 тисяч вірусних атак на персональні комп'ютери. Зрозуміло, що ця цифра в дійсності значно вища, оскільки багато фірм, побоюючись за свій рейтинг і репутацію на світовому ринку просто приховують такі злочини, що робить їх латентними. Таке становище, звичайно, лише на руку електронному злочинному світові.

Виведення з ладу ЕОМ у системах керування, зв'язку чи розвідки засобами електронної боротьби в сучасній війні може забезпечити перемогу над

противником. Враховуючи реалії, в США, де комп'ютеризація сфери охорони і безпеки досить висока, вірусній проблемі надається належна увага.

Для захисту від зловмисників, які без дозволу проникають у мережу ЕОМ у Великобританії, де комп'ютерне піратство виливається у багатомільйонні збитки для корпорацій і банків, за пошук рецепта взялася спеціальна парламентська комісія. Досконально вивчивши це питання, законодавці запропонували прирівняти електронні правопорушення до тяжких карних злочинів. Для електронних «піратів» запроваджені суворі покарання. Так, за підключення до чужого комп'ютера без дозволу можна отримати 3 місяці тюремного ув'знення. Якщо ж таке підключення здійснене з метою завдання шкоди ЕОМ, строк позбавлення волі може бути збільшений до 5 років. Стільки ж проведе за гратами і той, хто порушить або знищить програму комп'ютера, в тому числі за допомогою так званого електронного вірусу.

Для того, щоб чітко з'ясувати характер комп'ютерних злочинів, необхідно з'ясувати, ким саме створюються ці злочини.

Відомо, що особа злочинця досліджується різними науками. Кримінологічні дослідження обмежуються головним чином тими особливостями людини, які необхідні для використання кримінальної профілактики попередження злочинів.

Що стосується криміналістики, то, в першу чергу, вона вивчає «професійні» звички злочинців, які проявляються в основному в застосуванні способів, методів і прийомів вчинення злочинів, що залишають після себе на місці вчинення злочинів характерний «почерк» злочинця, оскільки результатами кожної злочинної діяльності є сліди людини, яка їх залишила. Виявлення речових доказів проливає світло як на відомості про деякі його особисті соціально-психологічні ознаки, так і на відомості про досвід, професію, соціальне заняття, стать, вік, особливості взаємовідносин з потерпілим тощо.

§3. Криміналістична характеристика комп'ютерних злочинців

Криміналістична характеристика злочинця складається із 2-х інформаційних груп.

Перша група включає в себе дані про особу невідомого злочинця по залишених ним слідах, як на місці події, в пам'яті очевидців, свідків, так і за іншими джерелами з метою встановлення напрямку і прийомів його розшуку і затримання. Така інформація дає уявлення про загальні ознаки певної групи осіб, серед яких може бути злочинець. Такі відомості слід співставляти з наявними криміналістичними даними про особу, яка швидше за все вчиняє злочини того типу, що розслідується.

Друга група об'єднує інформацію, яка отримана за допомогою вивчення затриманого, підозрюваного чи обвинуваченого, тобто отримана у конкретної особи – суб'єкта злочину. З цією метою збираються відомості не лише про ціннісні орієнтації, особливості антисуспільних поглядів, але і про те, яка інформація найбільше характеризує особу – суб'єкта злочину, його зв'язки, особливості поведінки до, під час і після вчинення злочину. Все це може допомогти слідчому чи оперативному працівнику встановити зі злочинцем психологічний контакт, отримати правдиві свідчення, а також обрати найбільш дієві способи профілактичного впливу на нього.

Вважається, що ця інформація з урахуванням відомостей про злочинців, які відображаються в інших елементах криміналістичної характеристики, може бути покладена в основу типізації злочинців. Формування банку типових моделей різних категорій злочинців, вивчення загальних рис цих людей дозволяє оптимізувати процес виявлення кола осіб, серед яких потрібно вести пошук злочинця.

Характеризуючи окремі особи комп'ютерних злочинців, необхідно відмітити, що для них **основною ознакою є те,** що в електронну злочинність, як правило, втягнуте широке коло осіб, від висококваліфікованих фахівців до дилетантів, оскільки правопорушники приходять з усіх сфер життя, мають різний досвід і різний рівень освіти.

З метою глибшого вивчення цієї проблеми необхідно чітко з'ясувати і знати: «хто ж вони, комп'ютерні злочинці?» Вітчизняні та зарубіжні дослідження дають змогу намалювати типовий портрет комп'ютерного злодія, тобто портрет конкретного соціального типу.

У своєму підручнику «Криміналістика» П. Д. Біленчук виділив загальні характерні риси комп'ютерного злочинця. За його словами *«це особа, для якої комп'ютерна система – це таємниця, яку необхідно дослідити і ефективно використовувати»*. Вже у школі, і особливо у вищих навчальних закладах, студенти вивчають основи комп'ютерної науки. Тому у більшості випадків злочинці набувають знань у коледжі або університеті. Самостійне вивчення ЕОМ також може бути фундаментом майбутньої злочинної діяльності.

Аналіз вітчизняної і зарубіжної практики та вивчення літературних джерел показує, що вік комп'ютерних правопорушників коливається в досить широких межах (у середньому 15-45 років). Дослідження показують, що на момент вчинення злочину у 33% злочинців вік не перевищував 20 років, 13% були старші 40 років і 54% – мали вік від 20 до 40 років. Таким чином, хакери – це не завжди молоденькі хлопчаки.

Біля 83% осіб цієї категорії – чоловіки, але слід зауважити, що відсоток участі жінок швидко зростає через професійну орієнтацію деяких спеціальностей та посад, які заповнюють в основному жінки (секретар, бухгалтер, еко-

номіст, менеджер, касир, контролер, ділознавець тощо). При цьому розмір збитків від злочинів, які вчиняють чоловіки, у 4 рази більший, ніж від злочинів, вчинюваних жінками. За даними соціологів США приблизно третину комп'ютерних злочинців становлять жінки.

Більшість комп'ютерних злочинців у віці від 14 до 21 років навчаються у коледжі або інституті. Про це свідчить той факт, що більшість вірусів виникає у період літніх або зимових канікул. Вони добре розуміються в ряді дисциплін, але можуть відставати з інших. Наприклад, значна частка програмістів погано пише документацію або має слабко розвинуті мовні навички. Зате вони мають коефіцієнт інтелекту вищий за середній, оскільки високий рівень інтелекту необхідний для написання компактної програми. Цікаво, що 77% злочинців, які вчинили комп'ютерний злочин, мали середній рівень інтелектуального розвитку; 21% – вище середнього і лише 2 % – нижче середнього. При цьому 20% злочинців мали середню освіту, 20% – середню спеціальну і 40% – вищу.

Характерні особливості особи комп'ютерного злочинця: активна життєва позиція, оригінальність (нестандартність) мислення і поведінки, обережність, уважність, зосередженість уваги на розумінні, передбаченні і управлінні процесами, це є основою їх компетенції та майстерності, до того ж вони відзначаються уважністю і пильністю, їх дії витончені, хитромудрі, супроводжуються відмінним маскуванням.

З точки зору людських психофізіологічних характеристик – це, як правило, яскрава, мисляча і творча особистість, великий професіонал своєї справи, здатний іти на технічний виклик, бажаний працівник. Водночас це людина, яка боїться втратити свій авторитет або статус у рамках якоїсь соціальної групи, або ж вона боїться на роботі сторонніх зневажань. Зовні їх поведінка майже не відрізняється від встановлених у суспільстві норм поведінки. Крім того, практика свідчить, що комп'ютерні злочинці у своїй більшості не мають кримінального минулого.

Значна частина комп'ютерних злочинів здійснюється індивідуально, але нині має місце тенденція співучасті у групових посяганнях. Кримінальна практика свідчить, що 38% злочинців діяли без співучасників, тоді як 62% вчиняли злочини в складі організованих злочинних груп і співтовариств.

Деякі з правопорушників цієї категорії технічно оснащені досить слабко, але більшість мають дорогі, престижні, науково-місткі й могутні комп'ютерні системи.

Велика кількість комп'ютерних злочинців – це посадові керівники всіх рангів (більше 25%). Це обумовлено тим, що керівником є, як правило, спеціаліст більш високого класу, який володіє достатніми професійними знаннями, має доступ до широкого кола інформації, може давати відповідні вказ-

івки та розпорядження і безпосередньо не відповідає за роботу комп'ютерної техніки.

Особи, схильні до вчинення комп'ютерних злочинів, поділяються на 3 групи:

1. До першої групи комп'ютерних злочинців слід віднести осіб, які характеризуються сталим поєднанням професіоналізму в галузі комп'ютерної техніки і програмування з елементами своєрідного фанатизму і винахідливості. На думку інших дослідників, ці суб'єкти сприймають засоби комп'ютерної техніки як своєрідний виклик їхнім творчим і професійним знанням, умінням і навичкам. Саме це є у соціально-психологічному плані стимулюючим фактором для вчинення різних дій, більшість з яких мають яскраво виражений злочинний характер. За наявними у МВС, НБР, ФБР, ФСБ та інших спецслужбах світу даними, хакерів широко використовують організовані злочинні групи для проникнення у закордонні та вітчизняні комп'ютерні системи.

Під впливом вказаного вище фактору особи цієї групи розробляють і вишукують різні методи несанкціонованого проникнення в комп'ютерні мережі, увесь час працюють над тим, як обійти, перехитрити з кожним разом все більш досконалі системи захисту. Це, в свою чергу, призводить до збільшення алгоритму злочинних дій, що об'єктивно сприяє удосконаленню і нарощуванню банку даних про способи вчинення комп'ютерних злочинів. Слід підкреслити, що характерною особливістю злочинців цієї групи є відсутність у них чітко визначених протиправних намірів. Практика свідчить, що всі дії вчиняються ними з метою реалізації своїх інтелектуальних і професійних здібностей.

Ситуацію тут умовно можна порівняти з тією, яка виникає при різного роду іграх, які стимулюють розумову активність гравців, зокрема при грі в шахи, карти тощо. Однак насправді у житті в ролі одного гравця виступає гіпотетичний злочинець, а в ролі його противника – узагальнений образ комп'ютерної системи та інтелект розробників засобів захисту від несанкціонованого доступу. Детально такі ситуації досліджуються в теорії ігор, математичній науці. У цьому випадку дослідники вивчають моделі поведінки двох протилежних сторін.

Особливий інтерес (у першій групі вивчення особи злочинця) представляють спеціалісти-професіонали у галузі комп'ютерної техніки. Представники цієї спеціальності, як правило, достатньо фахово підготовлені, майстри своєї справи, мають достатні розумові здібності. При цьому вони не позбавлені деякого своєрідного азарту і фанатизму. Тому нові заходи по забезпеченню безпеки комп'ютерних систем і мереж ними сприймаються у психофізіологічному плані як виклик особистості, внаслідок цього вони намагаються будь-якою ціною знайти ефективний підхід, розробити оптимальні методи втручання в банк даних, чим довести свою неперевершеність. Таким чином, комп'ютерну зло-

чинність підштовхують реальні соціально-економічні фактори, фактичні умови, адже спеціалістам-професіоналам добре платять за їх роботу.

Причому це може проявлятися у злочинців як у відкритій формі (при спілкування зі знайомими, товаришами, рідними, співробітниками), так і у прихованій (у формі думок, роздумів, переживань, без будь-яких зовнішніх проявів), останнє характерно для людей замкнутих. Усе це характеризує основні етапи появи, розвитку і переродження «аматора-програміста» у досвідченого, професійно орієнтованого комп'ютерного злочинця.

2. До другої групи комп'ютерних злочинців слід віднести осіб, які страждають новим видом психічних захворювань – інформаційними хворобами, комп'ютерними фобіями. Дослідники на основі всебічного аналізу емпіричних даних підкреслюють, що комп'ютерні злочини, які вчиняються злочинцями цієї групи, в основному пов'язані зі злочинними діями, які спрямовані на фізичне знешкодження або пошкодження засобів комп'ютерної техніки без наявності злочинного умислу, з частковою або повною втратою контролю над своїми діями.

3. До третьої і найбільш небезпечної групи відносяться комп'ютерні злочинці з яскраво вираженою корисливою метою, так звані «профі». На відміну від першої групи «аматорів» і другої специфічної групи «хворих», злочинці третьої групи характеризуються систематичним багаторазовим вчиненням комп'ютерних злочинів з обов'язковим виконанням дій, які спрямовані на підготовку та їх приховування. Слідча практика показує, що на долю цих злочинців припадає максимальна кількість особливо небезпечних посягань, наприклад, до 79% розкрадань грошових коштів у великих та особливо великих розмірах і різного роду посадових злочинів, які вчиняються з використанням засобів комп'ютерної техніки.

Таким чином, для представників третьої групи притаманні наступні риси:

- вони спеціалісти вищого класу;
- мають сучасне технічне та програмне забезпечення;
- добре організовані;
- мають чітко налагоджений порядок обміну інформацією;
- добре законспіровані;
- мають високий рівень взаємодії та кооперації.

Підсумовуючи викладені вище дослідження, можна зробити висновок, що комп'ютерна злочинність та комп'ютерні злочини – це принципово нове явище в науці кримінального права. Ці злочини вчиняються особами, які, як ми бачимо, належать до різних верств населення, кожен з типів цих осіб має свої особливості, і для того, щоб боротися з цими злочинами, необхідно досконало знати всі ці особливості, а для того, щоб юридично грамотно кваліфікувати такі злочини, необхідно чітко і обґрунтовано визначати склад злочину.

§4. Особливості методики слідчих дій при розслідуванні комп'ютерних злочинів

Науково-технічний прогрес висунув на передній план проблему використання комп'ютерних технологій, що проникла у найрізноманітніші галузі народного господарства та науки. Від ефекту її практичного застосування стали безпосередньо залежати успіхи розвитку цих найважливіших галузей.

Але розбудова незалежної держави України супроводжується низкою негативних явищ, таких як загострення криміногенної ситуації, зростання рівня злочинності та появою нових форм, у тому числі організованої, зокрема, у сфері економіки, приватизації, зовнішньоекономічних відносин, кредитно-фінансовій і банківській системах. Як відомо, в цих сферах діяльності переважно використовуються технічні засоби інформації, а тому саме тут скоюються злочини, які нині стали відомі в усьому світі під назвою комп'ютерна злочинність.

Комп'ютерна злочинність – це нове міжнародне явище, рівень якого тісно пов'язаний з економічним рівнем розвитку суспільства у різних державах та регіонах.

У більшості країн Європи під комп'ютерною злочинністю розуміють протизаконні дії, що несуть за собою великі майнові збитки, де об'єктом злочину є електронне опрацювання інформації.

При підготовці до огляду, обшуку або виїмки комп'ютерної техніки, слідчий, перш за все, вирішує питання про необхідність вилучення комп'ютерної інформації. На цю необхідність, крім ознак складу злочину у сфері руху комп'ютерної інформації, можуть вказувати:

- наявність у підозрюваного (обвинуваченого), потерпілого, свідка спеціальної освіти в галузі обчислювальної техніки та інформації, а також комп'ютерної техніки в особистому користуванні;
- наявність у матеріалах справи документів, виготовлених машинописним способом (отримані від обвинуваченої або потерпілої сторони);
- розкрадання носіїв комп'ютерної інформації;
- дані про захоплення або зацікавленість вказаних вище осіб обчислювальною технікою, інформатикою та програмуванням або про їх постійні контакти з людьми, які мають такі захоплення.

На підготовчому етапі огляду або обшуку необхідно:

- отримати достовірні дані про вид та конфігурацію ЕОМ, що використовувалася;
- встановити чи підключена вона до локальної або глобальної мережі;
- визначити наявність служби інформаційної безпеки та захисту від несанкціонованого доступу;

• виявити системне електроспоживання приміщень, де встановлена обчислювальна техніка;

• встановити кваліфікацію споживачів;

• зібрати відомості про співробітників, які обслуговують обчислювальну техніку (взаємовідносини в колективі, його можливої криміналізації та ін.).

Володіння такою інформацією полегшить слідчому доступ до інформації, яка зберігається в комп'ютері, та максимально підвищить її доказову силу.

Дуже часто вирішальне значення має раптовість обшуку (невідкладність огляду), оскільки комп'ютерну інформацію можна швидко знищити. Якщо отримані відомості про те, що комп'ютери організовані і підключені в локальну мережу, слід заздалегідь встановити місце знаходження всіх засобів комп'ютерної техніки, які підключені до цієї мережі, та організувати груповий обшук одночасно у всіх приміщеннях, де встановлені ЕОМ.

Перед початком обшуку вживають заходів, що спрямовані на попередження можливого пошкодження або знищення інформації. Для цього потрібно забезпечити контроль за безперервним електропостачанням ЕОМ. У момент обшуку вивести всіх сторонніх осіб з території, на якій проводиться огляд або обшук, вжити заходів, щоб особи, які залишилися в приміщенні, не мали можливості доторкатися до засобів обчислювальної техніки та до джерел електроспоживання.

Якщо на об'єкті огляду знаходяться вибухові, швидкозаймисті, їдкі речовини, сторонні джерела електромагнітного випромінювання та інші предмети та апаратура, яка здатна призвести до виведення з ладу ЕОМ, то необхідно евакуювати їх. Огляд або обшук необхідно проводити за участю спеціаліста в галузі інформатики та обчислювальної техніки. Бажано і в якості понятих запрошувати осіб, знайомих з роботою ЕОМ.

Не можна обмежуватись пошуком інформації лише в комп'ютері. Необхідно уважно вивчати документацію, навіть записи на клаптиках паперу, оскільки програмісти досить часто залишають записи про свій пароль, зміни конфігурації системи, особливості побудови інформаційної бази комп'ютера та ін. Багато користувачів зберігають копії своїх файлів на дискетах, щоб уникнути втрати їх при виході комп'ютера з ладу. Тому будь-які виявлені носії інформації повинні бути вилучені та вивчені.

Лише після перерахованих підготовчих засобів слід приступати до робочого етапу слідчої дії. Вивчення практики показує, що недотримання елементарних правил призводить до того, що діяльність слідчого по збору комп'ютерної інформації не досягає своєї мети. Так, якщо присутній при обшуку підозрюваний непомітно від членів слідчо-оперативної групи всього-навсього змінить положення тумблера перемикача робочої напруги, який розташований на задній стороні системного блока, з 220 на 115 вольт, то при вми-

канні, блок живлення тут же вийде з ладу, що в результаті призведе до несправності всього комп'ютера.

Захист комп'ютерної інформації здійснюється шляхом ідентифікації, тобто користувач повідомляє своє ім'я іншій стороні, яка після перевірки переконується в автентичності, що суб'єкт дійсно той, за кого себе видає. Справжність підтверджується знанням паролю, особистого ідентифікаційного номера, криптографічного ключа, а також особистою карткою, голосом, відбитками пальців рук та іншими способами.

Необхідно пам'ятати, що навіть у тому випадку, коли в розпорядженні слідчого є комп'ютер або магнітний носій, але електронний ключ не виявлений, то прочитати інформацію та ідентифікувати її автора (власника) не можливо.

Електронний ключ – це пристрій, який має пам'ять та виконаний на спеціалізованій мікросхемі розміром не більше сірникової коробки. Якщо при огляді комп'ютера запустити захищену програму, то вона перевірить наявність свого ключа. Коли такий ключ знайдений – програма виконується, в інших випадках видається інформація про помилку і робота на цьому припиняється.

У випадку, якщо при огляді апаратних засобів виявлені невідомі пристрої (додаткові плати, нестандартні з'єднання та ін.), комп'ютер необхідно відразу вимкнути. При цьому не слід відключати тумблер блока живлення, а висмикнути вилку з розетки. Далі (до роз'єднання проводів) необхідно промаркувати всю систему підключення, всі розйоми, щоб в подальшому можна було здійснити точну реконструкцію розташування кабелів, плат та інших пристроїв.

Присутнім при огляді (обшуку) необхідно роз'яснити всі дії слідчого і спеціаліста в ході маніпуляцій з ЕОМ. Не дозволяється будь-яке вторгнення в інформаційну базу без наочного, доступного і зрозумілого коментаря своїх дій. Повинно роз'яснюватися будь-яке натискання на клавіатуру, переміщення «миші» та ін.

Вмикати та вимикати комп'ютери, виконувати з ними будь-які маніпуляції може лише спеціаліст у галузі обчислювальної техніки. Якщо на об'єкті, де проводиться обшук, було вимкнуте електропостачання, наприклад, в зв'язку з пожежею або вибухом, до його вмикання слід перевірити, чи знаходяться всі комп'ютери і периферійні пристрої у відключеному стані. Вилучати необхідно відразу всі комп'ютери, які є в наявності, а також блоки живлення і магнітні носії. Не можна залишати їх на відповідальне зберігання на самому об'єкті або в іншому місці, де до них можуть мати доступ сторонні особи. Інформація, що міститься на магнітних носіях може бути легко знищена злочинцем, наприклад, за допомогою джерела електромагнітного випромінювання. При цьому візуально визначити це неможливо.

Комп'ютери та їх комплектуючі опечатуються. Магнітні носії запаковуються, зберігаються і перевозяться в спеціальних екранованих контейнерах або в стандартних дискетних, або інших футлярах з алюмінію заводського виготовлення, щоб не допустити руйнуючий вплив різноманітних електромагнітних і магнітних полів, а також направлених випромінювань. У протоколі слідчої дії описуються основні фізичні характеристики вилучених пристроїв, магнітних та інших постійних носіїв інформації, серійні номери апаратури, їх видимі індивідуальні ознаки.

Оскільки, крім інформаційних носіїв, на апаратних засобах часто виявляються традиційні для криміналістики сліди, то в таких випадках доцільно залучати експерта-криміналіста. Із слідчої практики відомі випадки виявлення слідів пальців рук при огляді зовнішніх і внутрішніх комплектуючих частин комп'ютера.

Під час проведення допиту свідків і потерпілих необхідно з'ясувати призначення і функції комп'ютерної системи, хто мав доступ до неї, де розташовувалась комп'ютерна техніка, чи не з'являлися там сторонні особи, які засоби захисту використовувались. Якщо частина інформації була закритою, то хто санкціонував доступ до неї і хто реально був допущений. Яка шкода (майнова, немайнова) спричинена злочином і чи є способи для її зменшення та ін.

При здійсненні допиту підозрюваних і обвинувачених необхідно враховувати дані криміналістичної характеристики кожної особи окремо. Важливою є підготовка до допиту, в процесі якої необхідно намагатися хоча б умовно вибрати, до якої групи належить підозрюваний чи обвинувачений, і на цій основі проводити тактику допиту. При початковому допиті потрібно спонукати особу до каяття, з'ясувати, які вже зміни внесені в роботу, які віруси використовувалися, чи є, з точки зору підозрюваного (обвинуваченого), можливість швидко усунути або зменшити шкоду, спричинену несанкціонованим проникненням у систему. Які відомості і кому передавалися і цілий ряд інших питань на розсуд слідчого.

§5. Сучасні можливості використання мобільних комплектуючих науково-технічних засобів при розслідуванні та розкритті злочинів

Нині питання про можливість використання науково-технічних засобів для пошуку, фіксації та обробки інформації, потрібної для встановлення істини при розслідуванні злочинів, постійно привертають до себе увагу вчених-криміналістів та практиків.

Під впливом науково-технічного прогресу постійно розширюється коло науково-технічних засобів, які дозволяють удосконалити процес пошуку, виявлення, фіксації і вилучення криміналістично значущої інформації. До них, насам-

перед, належать комп'ютерні технології, за допомогою яких обробляється різноманітна інформація. При цьому інформація може бути зафіксована у вигляді графічних зображень, письмових текстів, аудіо- і відео- повідомлень-записів.

Протягом останнього десятиріччя ці технології набули поширення в слідчій практиці при складанні протоколів та інших письмових документів, а пізніше для фіксації інформації в графічній формі (цифрова фотографія). Перспективним у своєму розвитку є цифровий звуко- та відеозапис.

Водночас, перехід на якісно новий рівень обробки криміналістично значущої інформації вимагає глибокого наукового усвідомлення практичних напрацювань, підготування більш досконалих методик для застосування цих технологій у процесі розслідування, а також вирішення низки питань, пов'язаних із процесуальним статусом інформації, зафіксованої та обробленої з їх використанням.

Питання використання комп'ютерних технологій для збирання й обробки криміналістично значущої інформації останнім часом все частіше привертає увагу вчених криміналістів. Вже нині запропонована нова концепція щодо проблеми забезпечення науково-технічними засобами осіб, які здійснюють безпосередню фіксацію криміналістично значущої інформації при проведенні слідчих дій. Розв'язання цієї проблеми вимагає комплексного підходу, що включає визначення необхідного комплекту науково-технічних засобів, а також вирішення деяких організаційних, правових і тактичних питань, пов'язаних з їх застосуванням.

Серед тактико-технічних характеристик, які слід враховувати при використанні мобільних комплектуючих засобів комп'ютерної техніки, найважливішими залишаються якість і швидкість обробки інформації, можливість її передавання по каналам зв'язку та забезпечення процесуальної форми їх отримання і використання.

Інакше кажучи, мобільний комплект комп'ютерної техніки має включати в себе науково-технічні засоби, призначені для пошуку, виявлення, фіксації і попереднього дослідження доказів на місці їхнього виявлення.

Засоби й методи, що застосовуються при провадженні слідчих дій, деякі криміналісти (В. К. Лисиченко і З. Т. Гулькевич) поділяють на дві групи:

1) призначені для пошуку, виявлення і вивчення різноманітних слідів та об'єктів;

2) призначені для фіксації фактичних даних та проведення слідчих дій.

Перші сприяють вирішенню завдань щодо пошуку, виявлення і консервації об'єктів-носіїв криміналістично значущої інформації. Ці засоби забезпечують так звану технічну сторону фіксації.

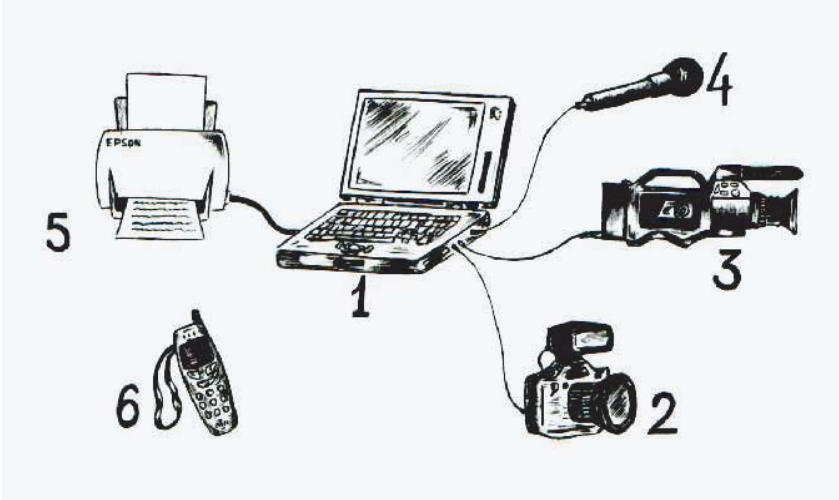
Другі – це засоби й матеріали, призначені для створення умов підготовки до фіксації у вигляді моделей, зліпків, протоколів, схем і додатків до них, які забезпечують так звану процесуальну сторону фіксації.

Перша група науково-технічних засобів на сучасному етапі продовжує найповніше задовольняти потреби слідчої практики, хоча, звичайно, деякі науково-технічні засоби та матеріали потребують вдосконалення.

Що стосується другої групи науково-технічних засобів, то вона за весь час існування зазнала найменшого розвитку в області новітніх розробок і технологій науково-технічного прогресу. В основному для складання протоколу або інших документів слідчий і сьогодні використовує звичайні бланки, лінійку, ручку, олівець і в кращому випадку друкарську машинку.

Але настав час, коли вирішення завдань удосконалення другої групи технічних засобів стає реальністю. Воно можливе при використанні сучасної комп'ютерної техніки і відповідних технологій. Використання комп'ютерних технологій дозволяє скоротити час підготування документів, а інформацію, що фіксується в графічній або вербальній формі, розміщувати як в окремих документах, так і комбіновано як складові частини одного документа.

А тому як приклад пропонується схематичне зображення зразкового мобільного комплекту комп'ютерної техніки для забезпечення швидкої оперативної фіксації та обробки інформації в «польових» умовах.



Мал.63. Схематичне зображення зразкового мобільного комплекту науково-технічних засобів

На малюнку(див.мал.63) схематично зображений і відмічений цифрами 1–6 зразковий мобільний комплект науково-технічних засобів, до складу якого входять:

1) портативний комп'ютер;
2) цифровий фотоапарат;
3) відеокамера;
4) мікрофон;
5) портативний принтер;
6) радіотелефон.

Такий комплект можна повністю розмістити у звичайній валізі. Радіотелефон (радіомодем) дозволить здійснювати оперативний зв'язок, підтримувати постійний контакт з керівником слідчого підрозділу, іншими службами, вчасно одержувати консультації і відправляти їх для перевірки, а також отримувати інформацію про різноманітні об'єкти – речові докази.

Комп'ютер, укомплектований звуковою картою, може за необхідності формувати звукові файли, виконуючи при цьому функції магнітофону, що інколи необхідно при провадженні слідчих дій. У цьому випадку вже можна говорити не про уніфікований комплект для проведення огляду місця події, а про мобільне автоматизоване робоче місце слідчого, а якщо точніше – оперативної групи.

Використовуючи такий комплект технічних засобів, особа, яка проводить огляд, формує протокол у вигляді тексту в комп'ютері, а схеми, графічні зображення (цифрові фотознімки) може включати безпосередньо до текстової частини протоколу в тому місці, де описує сфотографовані об'єкти. Підготовлені документи друкуються та розглядаються безпосередньо на місці події за допомогою мобільного принтера і тут же засвідчуються підписами понятих, слідчого та інших учасників слідчої дії.

Описаний метод фіксації, по-перше, забезпечує високий рівень інформативності зафіксованого матеріалу, по-друге, створює умови, що гарантують дотримання процесуальної форми.

Таким чином, використання та подальше вдосконалення комплектів науково-технічних засобів фіксації та обробки криміналістично значущої інформації є не тільки своєчасним, але й достатньо доцільним. Застосування комп'ютерної технології дозволяє не тільки забезпечити оперативність і якість обробки отриманої інформації, але швидко й успішно провести розслідування і розкриття злочинів. Саме тому нині у Державному науково-дослідному експертно-криміналістичному центрі МВС України запроваджений і функціонує новий вид експертиз – комп'ютерно-технічна експертиза.

Об'єктами комп'ютерно-технічних досліджень є комп'ютерні носії (накопичувачі на гнучких магнітних дисках, накопичувачі на жорстких магнітних дисках, CD-ROM тощо), комп'ютер, його окремі блоки та пристрої, комп'ютерні комплекси, програмні продукти.

Основні завдання комп'ютерно-технічної експертизи:

встановлення технічного стану комп'ютерної техніки;

виявлення інформації, що міститься на комп'ютерних носіях, та визначення її цільового призначення;

встановлення відповідності програмних продуктів певним параметрам;

визначення вартості програмного продукту;

визначення вартості комп'ютерної техніки та ін.

Перелік основних питань, які вирішує КТЕ (комп'ютерно-технічна експертиза).

Наведемо орієнтовний перелік об'єктів дослідження та питань, які може вирішувати комп'ютерно-технічна експертиза.

1. Технічні засоби:

1. Чи належить наданий на дослідження пристрій до апаратних комп'ютерних засобів?

2. До якого типу (марки, моделі) належить апаратний засіб? Вказати його параметри і дати характеристику?

3. Яке функціональне призначення наданого на дослідження апаратного засобу?

4. Яка роль і функціональні можливості даного апаратного засобу в конкретній комп'ютерній системі?

5. Чи використовується цей апаратний засіб для вирішення конкретного функціонального завдання?

6. Який фактично-технічний стан (справний, несправний) наданого на дослідження апаратного засобу?

7. Чи є наданий на дослідження апаратний засіб носієм інформації?

8. Який вид (тип, модель, марку) має наданий на дослідження носій інформації?

9. Який пристрій використовується для роботи з цим носієм інформації?

10. Чи входить до складу наданої на дослідження комп'ютерної системи пристрій для роботи із вказаним носієм інформації, або його аналогами?

11. Які параметри (об'єм, середній час читання даних, швидкість передачі даних тощо) має носій інформації?

12. Чи можливо прочитати інформацію з даного носія інформації?

13. Яка вартість комп'ютерно-технічних засобів (окремих комплектуючих) на момент їх придбання (вилучення, проведення експертизи тощо)?

2. Програмні продукти:

1. Яка загальна характеристика наданого на дослідження програмного забезпечення, з яких компонентів (програмних засобів) воно складається?

2. Яку класифікацію мають конкретні програмні засоби (системну або прикладну) наданого на дослідження програмного забезпечення?

3. Які найменування, тип, версію, вид представлення (явний, прихований, видалений) має програмний засіб?

4. Який зміст файлів програмного забезпечення, які їхні параметри (об'єм, дата створення, атрибути)?

5. Яке загальне функціональне призначення має програмний засіб?

6. Чи можна за допомогою даного програмного продукту реалізувати функції, передбачені технічним завданням на його розробку?

7. Чи є на цих носіях інформації окремі програмні засоби для реалізації певного функціонального завдання?

8. Які вимоги має цей програмний засіб до апаратних засобів комп'ютерної системи?

9. Яка сумісність конкретного програмного засобу із програмним й апаратним забезпеченням комп'ютерної системи;

10. Чи можливе використання цього програмного засобу для вирішення конкретного функціонального завдання?

11. Який фактичний стан програмного засобу, яка його працездатність щодо реалізації окремих функцій?

12. Яким шляхом організовано введення вхідних даних та виведення результатів роботи у наданому на дослідження програмному засобі?

13. Чи є в програмному засобі відхилення від нормальних параметрів (наприклад, властивості інфікування, приховані функції тощо)?

14. Чи має програмний засіб захисні можливості (програмні, апаратно-програмні) від несанкціонованого доступу та копіювання?

15. Яким шляхом організовані захисні можливості програмного засобу?

16. Який загальний алгоритм цього програмного засобу?

17. Чи містить програмний засіб функції, які можуть призводити до знищення, блокування, модифікації або копіювання інформації, порушення роботи комп'ютерної системи?

18. Яка вартість програмного продукту на момент його придбання (вилучення, проведення експертизи)? Для вирішення цього питання, тобто встановлення вартості програмного продукту, експертові надається носій з копією досліджуваного програмного продукту і еталонна (дистрибютивна) копія програмного продукту, що реалізується на вітчизняному ринку програмних засобів.

3. Інформація, яка зберігається та обробляється за допомогою програмно-технічних засобів:

1. Чи містить конкретний носій будь-яку інформацію і якщо так, то яке її цільове призначення? Для дослідження інформації, що міститься на комп'ютерних носіях, експертові надається сам комп'ютерний носій, а також комп'ютерний комплекс, до складу якого входить досліджуваний носій. У деяких випадках можна обмежитися наданням тільки комп'ютерного носія. Щодо можливості проведення такого дослідження слід попередньо проконсультуватися з експертом (спеціалістом);

2. Які властивості, характеристики й параметри (об'єм, дата створення та редагування, атрибути та ін.) мають дані на носії інформації?

3. В якому вигляді (явному, прихованому, видаленому) міститься інформація на носії?

4. До якого типу належать виявлені дані (текстові, графічні, бази даних, електронні таблиці, мультимедійні, запис пластикової карти тощо) і які програмні засоби для їх обробки присутні на носії інформації?

5. Яким чином організований доступ (вільний, обмежений та ін.) до даних на носії інформації і які його характеристики?

6. Які властивості та характеристики мають виявлені засоби захисту даних і які можливі шляхи їх подолання?

7. Які ознаки подолання захисту (або спроб несанкціонованого доступу) містить носій інформації?

8. Який зміст захищених даних?

9. Які дані для вирішення конкретного функціонального завдання містить носій інформації?

10. Які дані з фактами й обставинами конкретної справи містить наданий на дослідження носій інформації?

11. Які дані про власника (користувача) комп'ютерної системи (у т.ч. імена, паролі, права доступу та ін.) містить носій інформації?

12. Які текстові дані із наданих на дослідження документів (зразків) і в якому вигляді (цілісному, фрагментному) містить носій інформації?

13. Чи містить носій інформацію, яка була видалена, і чи можна її відновити?

14. В якому вигляді, якого змісту та з якими характеристиками і атрибутами перебували конкретні дані на цьому носії інформації до їхнього видалення або модифікації? та ін.

4. Комп'ютерні мережі:

1. Чи є надане на дослідження устаткування комп'ютерною мережею?

2. Надане на дослідження устаткування є цілісною комп'ютерною мережею чи являється якоюсь її частиною?

3. До якого типу відноситься комп'ютерна мережа?

4. Який склад і характеристики має комп'ютерна мережа?

5. Яи перебуває комп'ютерна мережа в робочому стані?

6. Яка система захисту інформації реалізована в наданій комп'ютерній мережі?

7. Які характеристики цієї системи захисту?

8. Чи існують можливості для її подолання та ін?

Наведений вище перелік питань не є остаточним, він може бути розширений, виходячи з обставин конкретної кримінальної справи. А в необхідних

ситуаціях, що викликають труднощі при формулюванні запитань, необхідно завчасно консультуватись з експертом.

Тепер наведемо приклади з наочною ілюстрацією, взятою із практики комп'ютерно-технічних досліджень, які проводяться у відділенні технічної експертизи документів та почерку в Державному науково-дослідному експертно-криміналістичному центрі МВС України.

На експертизу надійшов:

• Системний блок комп'ютера сірого кольору з CD-ROM x 48 max, вилучений під час проведення обшуку за місцем проживання Сидоренка А. Ю.

На вирішення експерта поставлені питання:

1. Чи можливо за допомогою наданого на дослідження комп'ютерного обладнання виготовити підроблені грошові купюри?

2. Якщо так, то які саме підроблені грошові купюри були виготовлені на представленому комп'ютерному обладнанні? Які характерні ознаки їх виготовлення, що відрізняють їх від інших купюр?

Ці ж питання переопрацьовані в редакції експерта та погоджені зі слідчим наступним чином:

1. Чи містить жорсткий диск системного блоку файли із зображенням грошових знаків?

2. Чи містить жорсткий диск системного блоку програмне забезпечення, за допомогою якого можна отримати зображення грошових знаків?

ДОСЛІДЖЕННЯ

Системний блок комп'ютера доставлений до Державного науково-дослідного експертно-криміналістичного центру в неупакованому вигляді (мал.64). На тильній стороні системного блоку до блоку живлення білими нитками прив'язаний відрізок паперового аркуша білого кольору розмірами 150х205 мм, на якому барвником чорного кольору нанесено рукописний текст: «Системний блок вилучений при обшуку за місцем проживання Сидоренка А. Ю. 26.05.2004 р. Поняті: (два підписи). Ст. слідчий А. М.Петренко». На зворотному боці вказаного аркушу приклеєний відрізок паперового аркуша білого кольору розмірами 40х40 мм, на якому барвником чорного кольору нанесено підпис ст. слідчого А. М. Петренка та відбиток печатки синього кольору з текстом: «МВС України. Придунайський міськрайвідділ УМВС України в Одеській області. Для пакетів № 1». Порти блоку живлення та бічні кришки корпусу на тильній стороні системного блоку, а також кнопка вмикання живлення і кришка дисководу CD-ROM на передній панелі системного блоку заклеєні шістьма відрізками паперового аркуша білого кольору розмірами 40х40 мм, на кожному з яких розміщений відтиск печатки синього кольору з текстом: «МВС України. Придунайський міськрайвідділ УМВС України в Одеській області. Для пакетів № 1». Цілісність всіх відрізків не порушена.

Наданий на дослідження системний блок комп'ютера прямокутної форми розмірами 410х200х340 мм.

Мал.64. Зовнішній вигляд системного блоку, наданого на дослідження

Системний блок складається з таких основних частин:

металевого корпусу типу «Tower» та металевих кришок з покриттям світло-сірого кольору;

передньої панелі, що виготовлена з пластмаси світло-сірого кольору. На передній панелі розташований один отвір під дисковод для накопичувачів на CD-ROM і один отвір під дисковод для накопичувачів на гнучких магнітних дисках діаметром 3,5 дюйми. Справа на передній панелі розміщені вертикально одна під однією три полімерні вставки синьо-зеленого кольору;

тильної сторони корпусу, виготовленої з металу сірого кольору, з отворами для всіх портів системної плати комп'ютера, одного порту відеоплати, чотирьох портів внутрішнього модему;

системної плати Manli (чіпсет i815) з процесором Intel Pentium III 733 МГц та кулером.

До системної плати приєднані:

модуль оперативної пам'яті IBM об'ємом 128 Мб, на якому знаходяться: чорно-біла наклейка з написом «IBM 0111 128MB 16MX64 N B3N16644NCB-75AT ASSEMBLED IN ITALY», чорно-біла наклейка із штрих-кодом та написом «WUANL023830 19L7354 UANL», чорно-біла наклейка з написом «PC133U 333-542-B1»;

відеоплата ATI-RADEON RV100 об'ємом 64 Мб, на якій знаходиться чорно-біла наклейка із штрих-кодом та написом «ATI Radeon VE 64MB P/N: PM8912-970-1400 891202042000618». Відеоплата підключена до шини AGP;

внутрішній модем Motorola, на якому знаходиться чорно-біла наклейка із штрих-кодом та написом «P/N:C1010312-HPI56M 0114132024». Модем підключений до шини PCI;

блок живлення комп'ютера LPF2 (серійний номер: 0102132711);

дисковод MITSUMI D359M3D (серійний номер: 1A08QN0439) для накопичувачів на гнучких магнітних дисках діаметром 3,5 дюйми та місткістю 1,44 Мб;

дисковод SAMSUNG SC-148 для накопичувачів на CDROM (серійний номер: 6RCR306041);

накопичувач на жорсткому магнітному диску Quantum Fireball™ lct (серійний номер: 052108583172, об'єм 20,4 Гб) з габаритними розмірами 146x102x25 мм (далі – жорсткий диск).

З метою дослідження інформації, яка знаходиться на жорсткому диску, він був підключений до робочої станції експерта. Жорсткий диск був розпізнаний системою BIOS, інформація з диску вільно читалась.

Дослідженням встановлено, що фізичний жорсткий диск поділений на два логічні диски: диск без помітки місткістю 9,49 Гб (далі – диск С) та диск з поміткою «WORK» місткістю 9,49 Гб (далі – диск D). На диску С встановлено операційну систему «Microsoft Windows XP Professional».

При дослідженні диску D в папці **D:\Games\Cossacks\Missions\Russia\ \Missru01\vr** виявлено сім файлів із зображеннями грошових знаків Національного банку України (мал.65-71). Назви файлів, дати їх створення, останніх змін, останнього доступу, а також номінал, серія та номер на зображеннях грошових купюр наведено в таблиці 1.

Файл «Doc1.doc» містить чотири зображення лицьової сторони грошового знаку номіналом 100 гривень (мал.70), розташованих вертикально один під одним на сторінці формату 210x297 мм. Файл «Doc2.doc» містить чотири зображення зворотної сторони грошового знаку номіналом 100 гривень (мал.71), розташованих вертикально один під одним на сторінці формату 210x297 мм.

Таблиця 1

№ п/п	Назва файлу	Дата створення	Дата останніх змін	Дата останнього доступу	Номінал на зображенні грошової купюри	Серія та номер на зображенні грошової купюри
1	1.JPG	21.05.2004	21.05. 2004	20.06.2004	50 гривень	АЛ7442710
2	2.JPG	21.05.2004	21.05. 2004	20.06.2004	50 гривень	відсутні
3	22.JPG	10.04.2004	10.04. 2004	20.06.2004	100 гривень	АБ5572410
4	222.JPG	12.04.2004	12.04. 2004	20.06.2004	100 гривень	АБ5572410
5	33.JPG	10.04.2004	10.04.2004	20.06.2004	100 гривень	відсутні
6	Doc1.doc	02.04.2004	12.04.2004	20.06.2004	100 гривень	АБ5572410
7	Doc2.doc	02.04.2004	12.04.2004	20.06.2004	100 гривень	відсутні

Мал.65. Файл «1.jpg»

Мал.66. Файл «2.jpg»

Мал.67. Файл «22.jpg»

Мал.68. Файл «222.jpg»

Мал.69. Файл «33.jpg»

Мал.70. Файл «Doc1.doc»

Мал. 71. Файл «Doc2.doc»

Отже, жорсткий диск системного блоку містить сім файлів із зображенням грошових знаків Національного банку України.

При подальшому дослідженні встановлено, що на диску С міститься програмне забезпечення сканера Mustek 1200 UB Plus та програмний пакет для сканування текстів та зображень, їх розпізнання і обробки – ABBYY FineReader 4.0 Sprint.

Отож, жорсткий диск наданого на дослідження системного блоку містить програмне забезпечення, за допомогою якого можна отримати зображення грошових знаків.

ВИСНОВКИ

1. Жорсткий диск системного блоку містить сім файлів із зображенням грошових знаків Національного банку України. Всі зображення наведені в дослідницькій частині.

2. Жорсткий диск наданого на дослідження системного блоку містить програмне забезпечення, за допомогою якого можна отримати зображення грошових знаків Національного банку України.

Контрольні запитання та завдання для самоперевірки

• Розкрийте поняття і прослідкуйте історію розвитку комп'ютерно-технічної інформації.

• Назвіть основні комплектуючі частини комп'ютера і дайте їм характеристику.

• Назвіть злочинні групи комп'ютерної мережі. Дайте характеристику кожній із них.

• Які Ви знаєте характерні риси комп'ютерної злочинності?

• Назвіть види комп'ютерних злочинів. Дайте їм характеристику.

• Які дії, пов'язані з втручанням у роботу комп'ютерів і ком'ютерних мереж, відносяться до категорії злочинів?

• Дайте криміналістичну характеристику ком'ютерним злочинам.

• Назвіть основні групи людей, які схильні до вчинення комп'ютерних злочинів.

• Які Ви знаєте характерні особливості з тактики слідчих дій при розслідуванні комп'ютерних злочинів?

• Що необхідно розуміти під сучасним використанням мобільного комплекту науково-технічних засобів?

Література до теми: див. список рекомендованої літератури за п./№ (1, 2, 3, 8, 9, 12, 13, 15, 16, 18, 20, 33, 48, 49).