**Криміналістична інформатика в оперативнорозшуковій роботі при розслідуванні злочинів за колабораційну діяльність та пособництво державі-агресору**

1. Криміналістичну інформатику можна розглядати як криміналістичну теорію про закономірності та особливості інформаційних процесів у сфері розслідування злочинів, про їх автоматизацію, принципи побудови і методи використання автоматизованих систем, створюваних для підвищення ефективності слідчої та експертної практики на базі комплексного використання теорії та методології криміналістики, засобів та методів математики й інформатики.

В умовах побудови інформаційного суспільства одною з головних категорій криміналістичної інформатики як наукового напряму є категорія «інформація». Одною з категорій криміналістичної інформатики можна розглядати моделювання як метод наукового пізнання.

В основі криміналістичної діяльності лежать процеси збирання, переробки та використання інформації про злочинну подію і злочинця. Тому для підвищення ефективності цієї діяльності, насамперед необхідно підвищити ефективність інформаційних процесів, чому сприяє новий науковий напрям – криміналістична інформатика.

Серед відомого сьогодні програмного забезпечення для криміналістичної підготовки заслуговують на увагу такі комп’ютерні програми – «Розбій», «Слідчий», «Убивство», «Дізнання», «Пошук зниклого», «Крадіжка» тощо.

Інформаційні процеси при розслідуванні злочинів відрізняються значною складністю і специфічністю, які обумовлені:

- неочевидністю джерел інформації;

- фрагментарністю інформації щодо конкретного злочину;

- навмисними діями осіб, які маскують джерела інформації та перешкоджають її виявленню й адекватному сприйняттю;

- перекрученням чи знищенням інформації про обставини події, що виникає випадково або умисно;

- складністю у вилученні (декодуванні) отриманої інформації;

- труднощами, пов’язаними з правовим оформленням виявлення інформації та її джерел, посвідченням, фіксацією інформації, отриманням її в результаті оперативно-розшукових заходів і використанням в кримінальному судочинстві;

- складністю у встановленні зв’язків і відносин між обставинами події.

Повне сприйняття інформаційних процесів та процесів інформатизації, розуміння можливостей використання сучасних інформаційних технологій і програмного забезпечення, що нині використовується в органах внутрішніх справ, можливе лише за умови комплексного, системного підходу шляхом впровадження і створення навчально-практичних полігонів інформатизації органів внутрішніх справ, що дозволить відтворити інформаційні процеси.

Важливе значення для розкриття та розслідування злочинів мають автоматизовані інформаційні системи оперативно-розшукового і профілактичного призначення, де накопичується інформація про осіб, факти і предмети, що являють оперативний інтерес.

Разом з тим, одною з проблем інформаційного забезпечення органів внутрішніх справ є інтеграція та систематизація обліків, яка може бути вирішена шляхом створення дійсно інтегрованого банку даних, який би містив різну (криміналістичну, кримінологічну, статистичну, оперативно-розшукову) інформацію, яка необхідна у боротьбі зі злочинністю.

2. На сьогоднішній при розслідуванні злочинів за колабораційну діяльність та пособництво державі-агресору 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,

Злочинці комп’ютерної мережі умовно поділяються на декілька груп:

1. 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, які без дозволу проникають у чужі інформаційні мережі для забави.

2. Крекери – 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.

3. Фріки – спеціалізуються на використанні телефонних систем з метою уникнення від оплати телекомунікаційних послуг.

4. 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.

5. Кіберплути – це злочинці, які спеціалізуються на розрахункових рахунках. Вони використовують комп’ютери для крадіжки грошей, отримання номерів кредитних карток та іншої цінної інформації.

Всіх їх єднає те, що вони працюють з інформацією незаконними методами, які нині віднесені до злочинних посягань (статті 361-3631 КК України). 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.

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.

3. 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, при розслідуванні злочинів за колабораційну діяльність та пособництво державі-агресору, 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.

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.

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.

Мобільний комплект (такий комплект можна повністю розмістити у звичайній валізі) науково-технічних засобів, до складу якого входять:

1) портативний комп’ютер;

2) цифровий фотоапарат;

3) відеокамера;

4) мікрофон;

5) портативний принтер;

6) радіотелефон.