ВИКОРИСТАННЯ КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ ДЛЯ ЕФЕКТИВНОГО РОЗСЛІДУВАННЯ КІБЕРБЗЛОЧИНІВ

Чукалов Кирило Едуардович
курсант групи Ф4-202 факультету № 4
Харківський національний університет внутрішніх справ

Жмуровська Катерина Романівна
курсант групи Ф4-202 факультету № 4
Харківський національний університет внутрішніх справ

Товстик Вадим Олександрович
курсант групи Ф4-203 факультету № 4
Харківський національний університет внутрішніх справ

Цуркан Іван Олексійович
курсант групи Ф4-102 факультету № 4
Харківський національний університет внутрішніх справ

Онищенко Юрій Миколайович
кандидат наук з державного управління, доцент,
заступник декана факультету з навчально-методичної роботи факультету № 4
Харківський національний університет внутрішніх справ

З розвитком інформаційно-комунікаційних технологій виник та масштабується новий тип злочинів, пов'язаних з порушеннями інформаційної безпеки, компрометацією інформаційних систем, персональних комп'ютерів, систем автоматизації, комп'ютерних мереж, несанкціонованим доступом до інформації, порушенням прав на неї та функціонуванню телекомунікаційних мереж – кримінальні вторгнення. Окрім терміну "кіберзлочинність" активно використовуються такі терміни, як "комп'ютерна злочинність", "IT-злочинність", "злочинність у сфері інформаційних відносин", "віртуальна злочинність". Нові загрози вимагають розробки сучасних мтодів захисту та постійного оновлення знань і навичок фахівців у сфері забезпечення кібербезпеки. Важливим напрямком діяльності у цій сфері є співпраця на міжнародному рівні для ефективної боротьби з такими злочинами та захисту критичної інфраструктури [1].

Комп'ютерна криміналістика є однією з галузей криміналістики, яка спеціалізується на розслідуванні злочинів і доказах, пов'язаних із комп'ютерами та іншими цифровими пристроями, зокрема мобільними телефонами та ігровими консолями, підключеними до мережі Інтернет. Комп'ютерна криміналістика – це процес збору, вилучення, зберігання, аналізу та

представлення електронних доказів для отримання інформації та розслідування різних видів злочинів, включаючи кіберзлочини та інциденти, пов'язані з інформаційною та кібербезпекою. З технічного аспекту, цей процес включає використання спеціалізованих інструментів та програмного забезпечення для відновлення видалених файлів, декодування зашифрованих даних, аналізу мережевих трафіків, а також відстеження діяльності користувачів у цифровому середовищі. Фахівці у цій галузі повинні мати глибокі знання у сферах програмування, системного адміністрування та мережевих технологій для ефективного виконання своїх завдань [2].

Комп’ютерна (цифрова) криміналістика (форензика) – це судова наука практичного спрямування, започаткована у 1970-80-х рр., яка вивчає відновлення та дослідження у цифрових пристроях даних, пов’язаних з кіберзлочинністю. Комп’ютерна криміналістика традиційно охоплює не лише рекомендації, прийоми і засоби викриття та розслідування інцидентів інформаційної та кібербезпеки, а й рекомендації щодо їх запобігання. Крім цього, закономірності розслідування кіберзлочинів використовуються й у спорах між компаніями та/або фізичними особами, коли цифрового спеціаліста залучають до пошуку інформації про особу чи компанію. Для опису цього типу розслідувань використовується спеціальний термін «eDiscovery». Кібербезпека і кіберрозслідування тісно взаємопов’язані, проте суттєво відрізняються. Кіберрозслідування досліджує незаконну та/або шкідливу поведінку в Інтернеті, її рушійні сили, а кібербезпека – прогнозування, уникнення та реагування на ці дії [3].

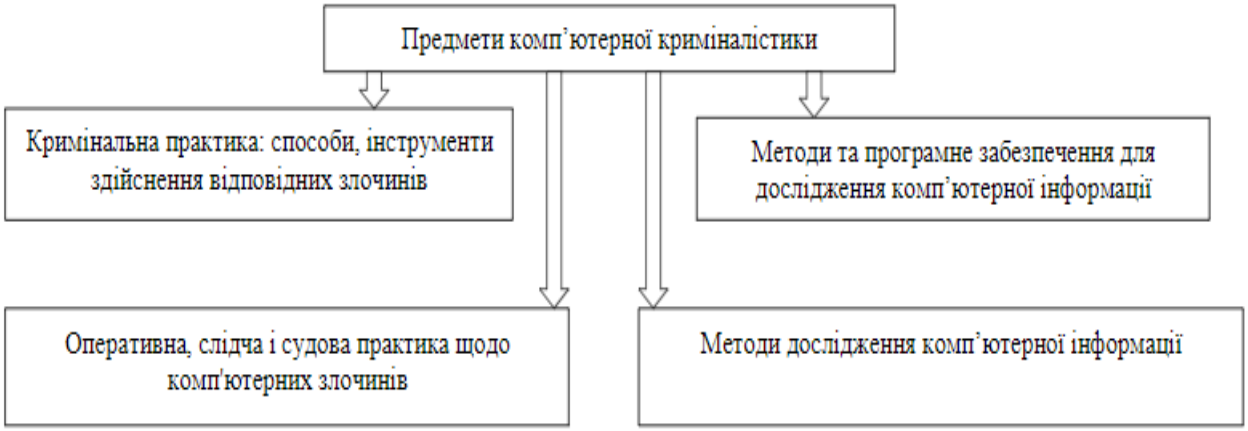

Рисунок1 – Предмет комп’ютерної криміналістики

Майже всі сліди, що вказують на інциденти інформаційної та кібербезпеки, з якими доводиться працювати спеціалісту з комп'ютерної криміналістики, представлені у вигляді комп'ютерної інформації, як регулярної, так і побічної. Їх досить легко знищити – як навмисно, так і випадково. Часто їх можна підробити, оскільки підроблений байт не відрізняється від справжнього. Фальсифікація електронних (цифрових) доказів виявляється або за інформаційним змістом, або за іншими цифровими та інформаційними слідами, які залишені в інших місцях.

Цифрові докази не можна сприйняти безпосередньо органами чуттів

людини, а лише за допомогою складних апаратно-програмних засобів. Тому ці сліди важко продемонструвати іншим особам – свідкам, прокурору, судді. Не завжди легко забезпечити незмінність слідів під час зберігання. І не лише забезпечити, а й довести цю незмінність у суді. Види комп'ютерної криміналістики залежать від типу проблем і належать до певної частини персонального комп'ютера.

Комп'ютерну криміналістику умовно можна поділити на розділи:

- Дискова криміналістика.
- Мережева криміналістика.
- Криміналістика шкідливих програм.
- Криміналістика баз даних.
- Криміналістика електронної пошти.

Дискова криміналістика займається витягуванням даних із комп'ютерних носіїв; мережева криміналістика дозволяє відстежувати та аналізувати мережевий трафік комп'ютера; криміналістика баз даних передбачає вивчення та перевірку баз даних і їхніх метаданих; криміналістика шкідливих програм дає можливість ідентифікувати шкідливий код для аналізу його функціоналу, вірусів, хробаків тощо; криміналістика електронної пошти допомагає відновлювати електронні листи, включаючи видалені листи, календарі та контакти. Комп'ютерна криміналістика базується на загальних принципах, одним з яких є принцип обміну Едмона Локарда: коли об'єкти і поверхні контактують один з одним, відбувається взаємне перенесення матеріалів. У контексті комп'ютерної криміналістики люди, використовуючи інформаційно-комунікаційні технології (далі – ІКТ), залишають цифрові сліди. Зокрема, особа, яка використовує ІКТ, може залишати "цифрові відбитки" або, як їх ще називають, "віртуальні, цифрові сліди".

Комп'ютерна криміналістика в розвинутих країнах розвивається стрімкими темпами і ефективно блокує поширення кіберзлочинності та появу інцидентів інформаційної та кібербезпеки. В Україні аналогічна ситуація. Зокрема, Національна поліція має в своєму складі структурний підрозділ, що опікується питаннями боротьби з кіберзлочинністю – Департамент кіберполіції. Також існує ряд приватних компаній, які мають ліцензію на здійснення діяльності, пов'язаної з криміналістичним розслідуванням інцидентів інформаційної та кібербезпеки. На основі викладеної вище інформації можна стверджувати, що комп'ютерні дані безперечно можуть виконувати роль джерел криміналістичної інформації відносно інцидентів інформаційної та кібербезпеки у сфері використання сучасних ІКТ та інших злочинів, в яких вони присутні. Інциденти інформаційної та кібербезпеки мають певні особливості, які мають бути враховані у кожному окремому випадку з урахуванням особливостей застосування певних програмних продуктів та утиліт, арсенал яких постійно збільшується та вдосконалюється, що дає змогу виявляти порушників інформаційної безпеки та запобігати виникненню інцидентів інформаційної й кібербезпеки та комп'ютерних злочинів, що викликають порушення конфіденційності, цілісності та доступності інформації та

порушують інформаційну безпеку загалом.

Список літератури

1. Загуменний О.О. Співвідношення понять «кіберзлочинність» і «комп'ютерні злочини». Процесуальне та техніко-криміналістичне забезпечення досудового розслідування. Харків, 2019. С. 67 - 70.

2. Колодіна А.С., Федорова Т.С. Цифрова криміналістика: проблеми теорії і практики. Електронне наукове фахове видання «Юридичний науковий електронний журнал ». Запоріжжя, 2022. No4. С. 378 - 380.

3. Комп'ютерна криміналістика URL: https://law.lnu.edu.ua/course/digitalforensics (дата звернення 15.06.2024).

4. Гуцалюк М., Гавловський В., Хахановський В. та ін. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком. / за заг. Ред. О.В. Корнейка. Вид. 2-ге, доп. Київ: Вид-во Нац. акад. внутр. справ, 2020. 104 с.

5. Колодіна А., Федорова Т. Цифрова криміналістка: проблеми теорії і практики. Київський часопис права. 2022. № 4. С. 176–180.