Внаслідок описаних дій можливо оптимізувати процес дослідження, оскільки порівняння проводиться на екрані та дозволяє одночасно переглядати, наприклад, досліджуваний відбиток та відбиток-зразок або 3 відбитки зразки, їх окремі ділянки, збільшуючи масштаб за допомогою комп'ютерного маніпулятора типу «миша» та одразу ж отримувати зображення для ілюстрацій.

Таким чином в даній роботі ми розглянули способи отримання більш наглядних та доступних для сприйняття ілюстрацій, дещо відступаючи від алгоритму, визначеного в п. 4 розділу VI Інструкції [2].

Разом з цим, подібний відступ лише розширює можливості відображення ходу дослідження, у т.ч. деталізації виявлених в процесі дослідження окремих ознак, які в свою чергу лише поліпшують розуміння описаних фактів сторонами кримінального чи інших проваджень, іншими замовниками досліджень.

Слід зазначити, що подібну форму ілюстрування процесу порівняльного дослідження можливо використовувати як під час проведення технічного дослідження документів, так і почеркознавчих досліджень.

Список використаних джерел

1. Методика технічної експертизи відбитків печаток та штампів / Уклад.: К.М. Ковальов, В.В. Коваленко. – К.: ДНДЕКЦ МВС України, 2009. – 19 с.

2. Про затвердження Інструкції з організації проведення та оформлення експертних проваджень у підрозділах Експертної служби Міністерства внутрішніх справ України / Наказ МВС №591 від 17.07.2017. – Офіційний вісник України від 19.09.2017 – 2017 р., № 73, стор. 24, стаття 2254, код акта 87219/2017.

Вінтула Богдан Анатолійович
здобувач ступеня вищої освіти «бакалавр» Національної к академії внутрішніх справ

Волошин Олексій Гнатович,
старший викладач кафедри криміналістичного забезпечення та судових експертиз ННІ №2 НАВС

КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ

На відміну від традиційних видів злочинів, таких як вбивство або крадіжка, історія яких налічує століття, кіберзлочинність явище відносне молоде, яке виникло з появою та розвитком всесвітньої мережі Інтернет.

Під кіберзлочинністю розуміється сукупність злочинів, що вчинюються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних.

Кіберзлочинність – явище новітньої, цифрової доби, тому слід зазначити, що сама природа мережі Інтернет є достатньо сприятливою для вчинення комп'ютерних злочинів. Такі її властивості, як глобальність, трансграничність, анонімність користувачів, охоплення широкої аудиторії, розподіл основних вузлів мережі і їх взаємозамінність створюють кіберзлочинцям, які використовують Інтернет, переваги на всіх етапах вчинення злочину, а також дозволяють ефективно переховуватися від правоохоронних органів. В даний час практично будь-який військовий або політичний конфлікт супроводжується організованим протиборством в мережі Інтернет. Для досягнення своїх політичних цілей все частіше стали використовуватися методи інформаційної війни.

Таким чином, на теперішній момент можна виділити 4 етапи в розвитку кіберзлочинності:

1. Поява кіберзлочинності і субкультури хакерів.

2. Розповсюдження кіберзлочинності, поява спеціалізацій кіберзлочинності і національних груп хакерів.

3. Набуття транснаціонального характеру у всіх сферах кіберзлочинності.

4. Використання Інтернету в політичних цілях, виникнення таких явищ, як Інтернет-страйк та Інтернет-війна, цілеспрямоване використання кібератак проти урядів окремих держав.

У листопаді 2001 року країнами Європейського союзу була ратифікована Конвенцією Ради Європи про кіберзлочинність, в якій виділяються наступні *групи кіберзлочинів*:

1) злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему);

2) злочини, пов'язані з використанням комп'ютера як засобу вчинення злочинів, а саме – для маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерні підроблення);

3) злочини, пов'язані з контентом (змістом даних);

4) злочини, пов'язані з порушенням авторського права і суміжних прав;

5) акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж.

Сучасна компютерна злочинність – це явище властиве всім державам, які в силу свого наукового прогресу вступили у період широкої комп'ютеризації своєї діяльності. В науковому середовищі існує дві думки щодо сутності комп'ютерних злочинів: перша відносить до комп'ютерних злочинів дії, в яких комп'ютерна система є або об'єктом, або знаряддям

посягань; друга базується на тому, що об'єктом посягання є інформація, яка обробляється в комп'ютерній системі, а комп'ютер служить знаряддям посягання.

На сьогодні *комп'ютерні злочини* – це одна з найдинамічніших груп суспільно небезпечних посягань. Швидко збільшуються показники поширення цих злочинів, а також постійно зростає їх суспільна небезпечність. Це зумовлене прискореним розвитком науки й технологій у сфері комп'ютеризації.

Аналіз наукової літератури дозволяє розділити комп'ютерні злочини на *два види*:

– традиційні злочини, що вчиняються за допомогою комп'ютерних технологій та Інтернету (шахрайство з використанням комп'ютерної техніки, незаконне збирання відомостей, що становлять комерційну таємницю, шляхом несанкціонованого доступу до комп'ютерної інформації тощо);

– злочини, що стали можливі завдяки новітнім комп'ютерним технологіям (злочини передбачені Розділом XVI Кримінального кодексу України).

Як різновид шахрайства в банківській системі є *кардінг* – незаконні фінансові операції з використанням платіжної картки або її реквізитів, що не ініційовані або не підтверджені її держателем. Реквізити платіжних карт, як правило, беруть зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також з персональних комп'ютерів (або безпосередньо, або через програми віддаленого доступу, так звані «трояни»).

У сфері електронної комерції та господарської діяльності, *фішинг* – виманювання у користувачів Інтернету їх логінів та паролів до електронних гаманців, сервісів онлайн аукціонів, переказування або обміну валюти, тощо. Шахраї найчастіше змушують користувачів самостійно розкрити конфіденційні дані - наприклад, посилаючи електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в Інтернеті, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів.

Серед комп'ютерних злочинів проти державної безпеки слід виділити такі суспільно небезпечні діяння, як неправомірний доступ до державної таємниці на машинному носії, і диверсію у сфері комп'ютерної інформації, комп'ютерне шпигунство.

Щоб не стати жертвою шахраїв і уникнути матеріальних втрат, необхідно слідувати декільком правилам:

1. Переконайтеся, що на вашому комп'ютері встановлено хороший антивірус, який здатний виявляти спам. У цьому випадку багато з повідомлень шахраїв будуть знайдені і класифіковані як спам.

2. Прислухайтеся до своєї інтуїції. Вона – ваш кращий союзник в боротьбі з такими видами шахрайства. Ніхто нічого не віддає просто так.

3. Завжди з обережністю починайте нові віртуальні знайомства.

5 листопада 2015 року була створена нова Кіберполіція, як структурний підрозділ Національної поліції України. Основною метою створення кіберполіції було реформування та розвиток підрозділів МВС України, що забезпечить підготовку та функціонування висококваліфікованих фахівців задіяних у протидії кіберзлочинності, та здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності.

До основних завдань Кіберполіції відносять:

1. Реалізація державної політики у сфері протидії кіберзлочинності.

2. Протидія кіберзлочинам:

3. Завчасне інформування населення про появу новітніх кіберзлочинів.

4. Впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини.

5. Реагування на запити закордонних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів.

6.Участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності.

7. Участь у міжнародних операціях та співпраця в режимі реального часу.

8. Забезпечення діяльності мережі контактних пунктів між 90 країнами світу.

Отже, загроза кіберзлочинності на сьогодні є дуже серйозною проблемою, причому її актуальність збільшується по мірі розвитку та розповсюдження інформаційно-телекомунікаційних технологій. Кіберзлочинність надає методи для захоплення інформації, а збиток, який вони можуть нанести визначається ціною цієї інформації. Так як сучасне суспільство не може обходитися без електронних носіїв інформації і цифрових методів її зберігання і обробки, кіберзлочинність представляє одну з найбільших загроз існуванню та регулювання соціальних процесів.

Список використаних джерел

1. Кримінальний кодекс України: Закон від 05.04.2001 р. // Редакція від 18.10.2019 // Офіційний сайт Верховної Ради України [Електронний ресурс]. – Режим доступу

http://zakon2.rada.gov.ua/laws/show/2341-14/page10

2. Поява і розвиток кіберзлочинності [Електронний ресурс]. – Режим доступу: http://www.kbuapa.kharkov.ua/e-book/db/2013-1/doc/1/01.pdf

3. Поняття та кримінологічна характеристика кіберзлочинності [Електронний ресурс]. Режимдоступу: http://libnet.com/content/9684_Ponyattya_ta_kriminologichna_harakteristika_kiberzloch innosti.html.