Вісник ЛДУБЖД
Bulletin of Lviv State University of Life Safety
https://journal.ldubgd.edu.ua/index.php/Visnuk
ISSN 2078-4643 (print), ISSN 2708-1389 (online)

UDC 349.3
DOI: 10.32447/20784643.28.2023.07

О. І. Полотай
Львівський державний університет безпеки життєдіяльності, м. Львів, Україна
ORCID: https://orcid.org/0000-0003-4593-8601 – О. І. Полотай
orest.polotaj@gmail.com

ВИКОРИСТАННЯ КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОГО РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ

Постановка проблеми. Враховуючи сучасні тенденції розвитку інформаційного суспільства та суспільства знань, все більшого розвитку набувають інноваційно-комунікаційні технології (ІКТ), які все частіше впроваджуються в різні сфери життя суспільства. Разом с тим, удосконалення комп'ютерних технологій призвело до появи нових видів злочинів, так званих "комп'ютерних злочинів". За своїм механізмом, способами вчинення та укриття ці злочини мають певну специфіку, характеризуються підвищеним рівнем латентності та низьким рівнем розкриття [11]. Це в свою чергу змусило розвиватись і галузь криміналістики та методи розслідування комп'ютерних злочинів, яка в умовах розвитку сучасних ІКТ досягла нового етапу свого розвитку. Зокрема, завдяки новітнім технологіям з'явилася нова галузь криміналістики – цифрова криміналістика.

Мета. Метою статті є дослідження нової галузі розслідування інцидентів інформаційної та кібербезпеки – комп'ютерної криміналістики.

Результати. У статті проаналізовано складові частини комп'ютерної криміналістики, оцінено основні тенденції розвитку цієї науки на сучасному етапі. Комп'ютерна криміналістика включає процеси виявлення, отримання, накопичення, зберігання, аналізу, дослідження та представлення цифрових доказів. Криміналістичні докази та методи криміналістичної експертизи залежать від операційної системи технічного пристрою, ефективності реалізації його функцій безпеки. Також в статті детально описано предмети та принципи комп'ютерної криміналістики, основні сфери її застосування а також наведено перелік методів дослідження, які властиві тільки їй. Особливу увагу у статті приділено поняттю «цифрові, віртуальні» сліди, на зборі та дослідженні яких, побудована вся суть комп'ютерної криміналістики. Зокрема, наводиться класифікація цифрових слідів за формою, місцем зберігання тощо. Описано основні місця зберігання доказів наявності інцидентів інформаційної та кібербезпеки. У статті описані чотири основні етапи робіт з цифровими слідами інцидентів інформаційної та кібербезпеки, а власне кажучи, комп'ютерною інформацією та даними. Також описані основні проблеми фахівців з комп'ютерної криміналістики, а саме: технічні проблеми та адміністративні. Описані основні перспективи розвитку комп'ютерної криміналістики.

Висновки. Комп'ютерна (цифрова) криміналістика – це прикладна наука про розкриття та розслідування інцидентів інформаційної та кібербезпеки, пов'язаних з комп'ютерною інформацією, про використання методів отримання і дослідження доказів факту інцидентів інформаційної та кібербезпеки у вигляді комп'ютерної інформації (цифрових слідів) та технічними засобами, що використовуються для цього. Це дає змогу швидко виявляти порушників інформаційної безпеки та запобігати виникненню інцидентів інформаційної і кібербезпеки та комп'ютерних злочинів, що викликають порушення конфіденційності, цілісності та доступності інформації та порушують інформаційну безпеку загалом.

Ключові слова: комп'ютерна криміналістика, криміналістика, цифрові сліди, кібербезпека, інформаційна безпека, кіберзлочинність.

O. I. Polotai
Lviv State University of Life Safety, Lviv, Ukraine

USE OF COMPUTER FORENSICS TO ENSURE EFFECTIVE INVESTIGATION OF INFORMATION AND CYBER SECURITY INCIDENTS

Introduction. Taking into account the current trends in the development of the information society and the knowledge society, innovative communication technologies (ICT) are gaining more and more development, which are increasingly being introduced into various spheres of society. At the same time, the improvement of computer technologies led to the emergence of new types of crimes, the so-called "computer crimes". According to their mechanism,

methods of committing and hiding, these crimes have a certain specificity, they are characterized by a high level of latency and a low level of disclosure [11]. This, in turn, forced the development of the field of criminology and computer crime investigation methods, which in the conditions of the development of modern ICT reached a new stage of its development. In particular, thanks to the latest technologies, a new branch of forensics has appeared - digital forensics.

Purpose. The purpose of the article is to research a new field of investigation of information and cyber security incidents - computer forensics.

Results. The article analyzes the components of computer forensics, assesses the main trends in the development of this science at the current stage. Computer forensics includes the processes of detecting, obtaining, accumulating, storing, analyzing, examining and presenting digital evidence. Forensic evidence and methods of forensic examination depend on the operating system of the technical device, the effectiveness of its security functions. The article also describes in detail the subjects and principles of computer forensics, the main areas of its application, as well as a list of research methods that are unique to it. The article pays special attention to the concept of "digital, virtual" traces, on the collection and study of which the entire essence of computer forensics is built. In particular, the classification of digital traces is given, such as by form, place of storage, etc. The main storage locations for evidence of information and cyber security incidents are described. The article describes four main stages of work with digital traces of information and cyber security incidents, or rather computer information and data. Also described are the main problems faced by computer forensics specialists, namely technical and administrative problems. The main prospects for the development of computer forensics are described.

Conclusion. Computer (digital) forensics is an applied science of uncovering and investigating information and cyber security incidents related to computer information, of using methods of obtaining and investigating evidence of information and cyber security incidents in the form of computer information (digital traces) and technical means used for this. This allows you to quickly identify violators of information security and prevent the occurrence of information and cyber security incidents and computer crimes that cause violations of confidentiality, integrity and availability of information and violate information security in general.

Keywords: computer forensics, forensics, digital traces, cyber security, information security, cybercrime.

Вступ. З розвитком ІКТ з'являється новий вид злочинів, предметом яких є інформаційна безпека, персональні комп'ютери, системи автоматизації, комп'ютерні мережі, комп'ютерна інформація, права на неї і нормальне функціонування телекомунікаційних мереж – злочинне вторгнення. Крім поняття "кіберзлочинність", активно використовуються такі поняття, як "комп'ютерна злочинність", "ІТ-злочинність", "злочинність у сфері інформаційних відносин", "віртуальна злочинність" [1].

Питання протидії та розслідування інцидентів інформаційної та кібербезпеки, які здійснені з використанням сучасник ІКТ, розглядали такі вчені, як Біленчук П.Д., Волеводза А.Г., Гаврилін Ю.В., Голубєва В.О., Романюк Б.В., Козлов В.В., Паламарчук В.П., Цимбалюк В.С. та ін. Дослідженням комп'ютерної криміналістики в Україні займаються такі вчені, як Бутузов В. М., Власова С. В., Іщенко Є. П., Нечаєва Н. Б. та інші. Серед іноземних вчених, які займаються питаннями комп'ютерної криміналістики варто виділити Marie-Helen Maras. Проте дослідження цього питання ще перебуває в початковому етапі та потребує подальшого вивчення.

Комп'ютерна криміналістика – це "одна з областей криміналістики, яка зосереджується на кримінальному провадженні та доказах, пов'язаних з комп'ютерами та пов'язаними з ними пристроями", включаючи мобільні пристрої та ігрові консолі, що працюють в мережі Інтернет. Зокрема, комп'ютерна криміналістика – це по суті, процес збору, отримання, зберігання, аналізу та подання електронних доказів для отримання слідчої інформації, а також розслідування та переслідування різних видів злочинів, включаючи кіберзлочини та інциденти інформаційної і кібербезпеки. [5].

Методи досліджень. Методологічну основу дослідження становлять принципи та основні категорії діалектичного пізнання соціальних явищ і процесів, розвитку та взаємозв’язку об’єктів реальної дійсності, система загальнонаукових та спеціальних методів, які є засобами наукового пошуку в арсеналі гуманітарних, у тому числі й юридичних наук. Поряд із загальновідомими науковими та іншими методами дослідження, у статті були використані такі: структурно-системний метод для дослідження взаємозв'язків між елементами механізму комп'ютерного злочину як системи джерел бази інформаційних доказів про факт наявності інцидентів інформаційної та кібербезпеки. Формально-логічні методи дали змогу визначити поняття і характеристики окремих даних предмета дослідження і дати їм криміналістичну оцінку.

Результати досліджень. 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 [6].

Комп’ютерна криміналістика традиційно охоплює не лише рекомендації, прийоми і засоби викриття та розслідування інцидентів інформаційної та кібербезпеки а також інших

цифрових зловживань, а й рекомендації щодо їх запобігання – тобто кібербезпеку. Крім цього, закономірності розслідування кіберзлочинів однаково використовуються й у спорах між компаніями та/або фізичними особами, коли цифрового спеціаліста залучають до відшукання інформації про особу чи компанію, перевіривши їхній комп'ютер. 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 [6].

На рисунку 1 показано, на що спрямована комп'ютерна криміналістика:

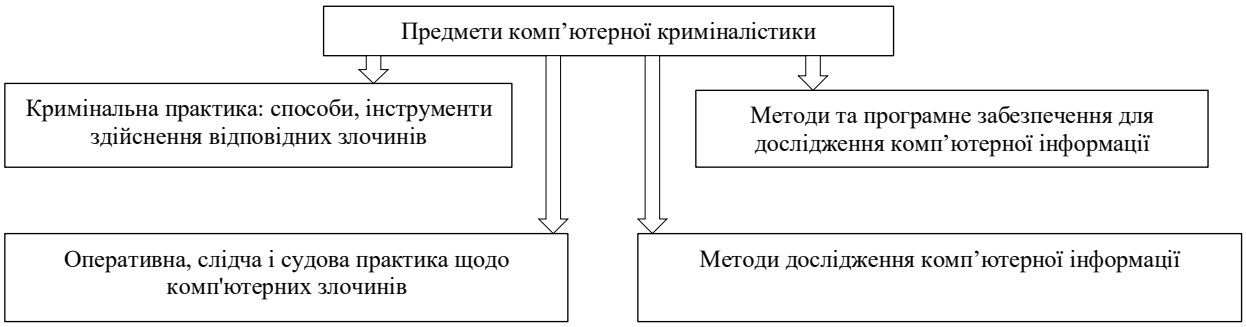

Рисунок 1 – Предмет комп'ютерної криміналістики

Майже всі сліди, які вказують на наявність інцидентів інформаційної та кібербезпеки, та з якими доводиться працювати фахівцю з комп'ютерної криміналістики, мають вигляд комп'ютерної інформації, регулярної чи побічної. Їх досить легко знищити – як навмисне, так і випадково. Часто їх легко підробити, бо підроблений байт нічим не відрізняється від справжнього. Фальсифікація електронних (цифрових) доказів виявляється або за змістовим інформаційним наповненням, або за іншими цифровими та інформаційними слідами, які були залишені в інших місцях. Цифрові докази не можна сприйняти безпосередньо органами почуттів людини, але лише за допомогою складних апаратно-програмних засобів. Тому ці сліди складно продемонструвати іншим особам – понятим, прокурору, судді. Не завжди легко забезпечити незмінність слідів під час зберіганні. І не лише забезпечити, а й довести суду цю незмінність.

Сфери застосування комп'ютерної криміналістики представлені на рисунку 2:

Рисунок 2 – Сфери застосування комп'ютерної криміналістики

Комп'ютерна криміналістика використовує спеціальні методи дослідження, властиві тільки їй. Серед цих методів можна виділити такі (рисунок 3):

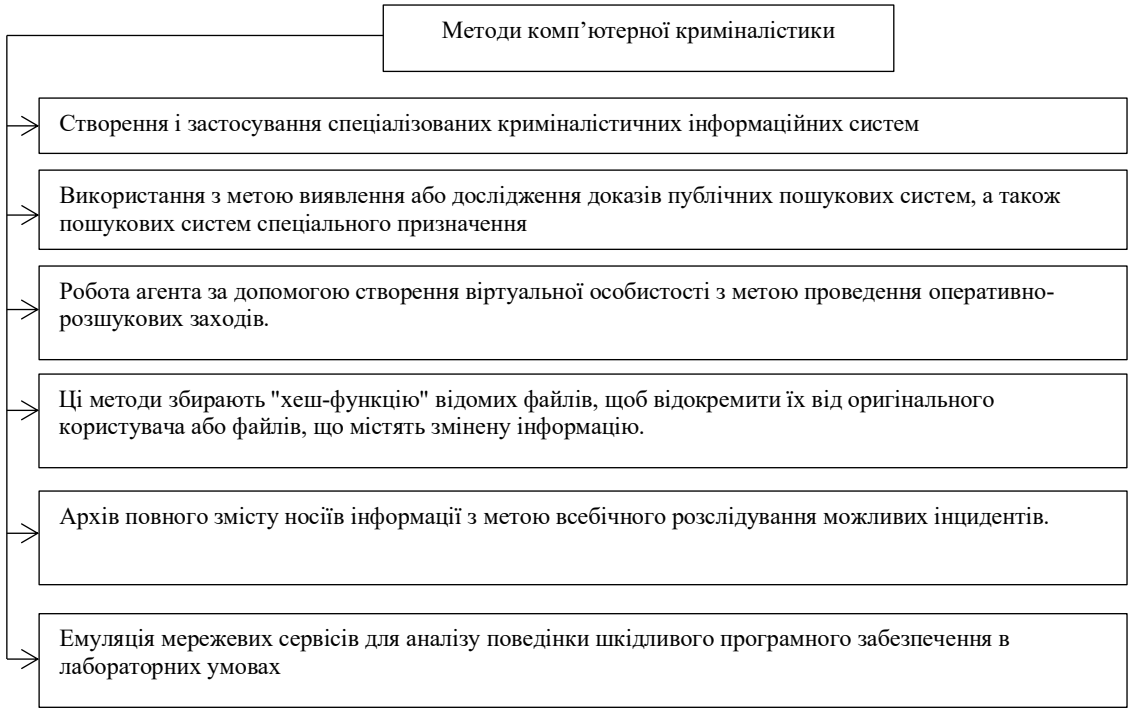

Рисунок 3 – Основні методи комп'ютерної криміналістики

Види комп'ютерної криміналістики залежать від типу проблем і належать до певної частини персонального комп'ютера. На рисунку 4 наведені різні види комп'ютерної криміналістики [12]:

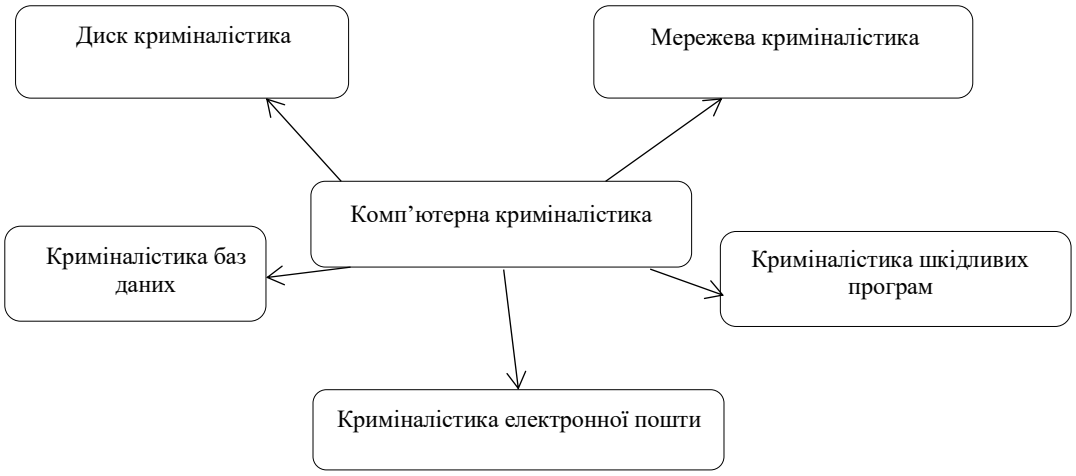

Рисунок 4 – Види комп'ютерної криміналістики

Диск-криміналістика займається вилученням даних із носія даних комп'ютера; мережева криміналістика дає змогу відслідковувати та аналізувати мережевий трафік комп'ютера; криміналістика бази даних визначає вивчення та перевірку відповідних баз даних та їх збережених метаданих; криміналістика шкідливих програм дає змогу ідентифікувати шкідливий код для виконання роботи над їх корисним навантаженням, вірусами, хробаками тощо; криміналістика електронною поштою допомагає перевірити відновлення електронних листів, охоплюючи всі видалені листи, календарі та контакти.

Комп'ютерна криміналістика ґрунтується на загальних принципах де одним із головних є принцип обміну Едмона Локара: коли об'єкти і поверхні вступають в контакт один з одним, відбувається перехресне перенесення матеріалів. У контексті комп'ютерної криміналістики люди, після використання ІКТ, залишають цифрові сліди. Зокрема, особа, яка використовує ІКТ, може залишити «цифрові відбитки» або, як ще їх називають «віртуальні, цифрові сліди».

Концепція "віртуальних слідів" в кримінології заснованана вперше Мещеряковим В.О. Під віртуальними слідами він розуміє "зміни

в стані автоматизованих інформаційних систем, які пов'язані з кримінальними подіями і зафіксовані у вигляді комп'ютерної інформації". Такі сліди займають умовне проміжне положення між матеріальним і ідеальним слідом. "Комп'ютерні сліди залишаються в пам'яті як комп'ютерів, так і інших цифрових пристроїв. Науковець, Агібалов В.Ю. підтримуючи висновок Мещерякова, відносить віртуальні сліди до незалежних груп, які рівні ідеальним і матеріальним. Він вважає, що зображення фіксується з цифрових значень параметрів формальної математичної моделі спостережуваних реальних фізичних явищ в результаті електронного цифрового відображення на матеріальному носії.

Можна навести певну класифікацію віртуальних слідів (рисунок 5):

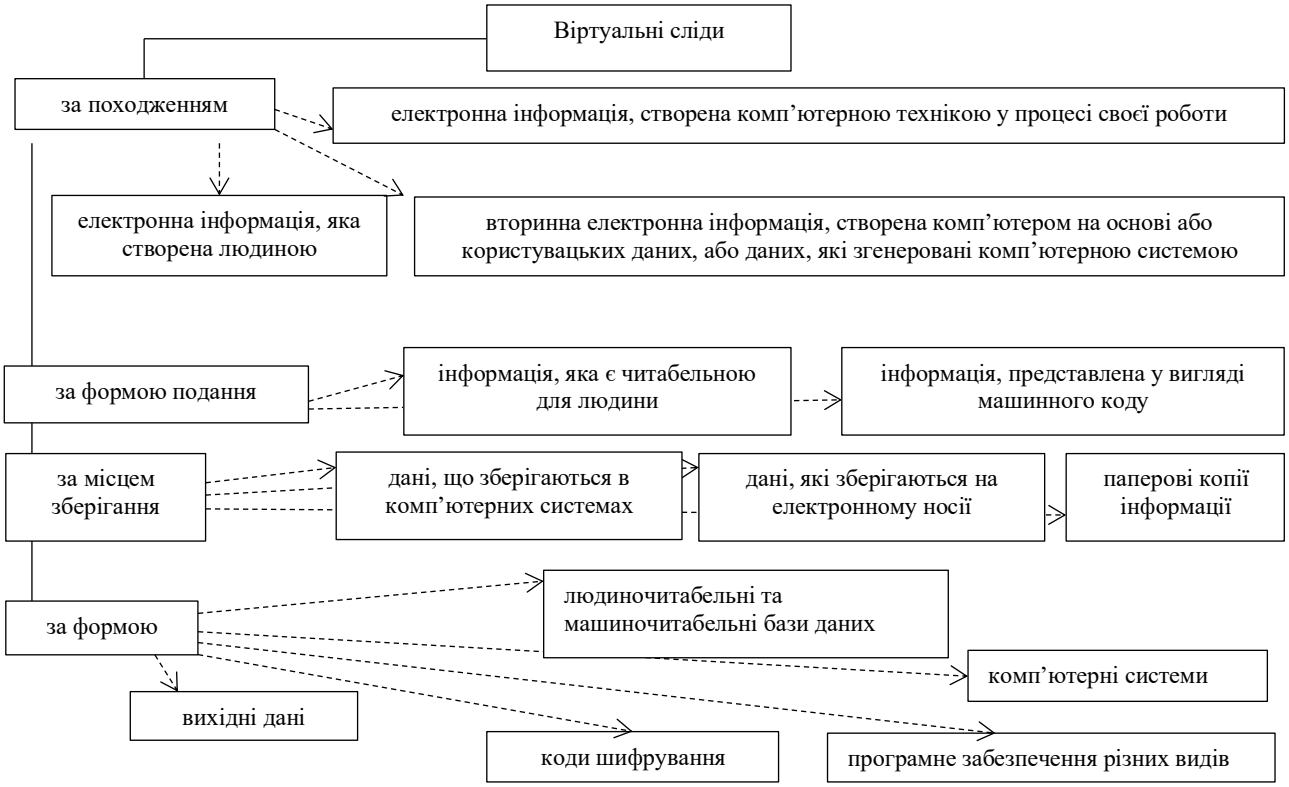

Рисунок 5 – Класифікація віртуальних слідів інцидентів інформаційної та кібербезпеки

Для розкриття інцидентів інформаційної та кібербезпеки можливе застосування таких видів цифрових (віртуальних) слідів:

1. Електронна поштова скринька;
2. Інтернет сайт;
3. Профіль у соціальних мережах;
4. Рахунок в електронних платіжних системах;
5. База даних;
6. Локальна обчислювальна мережа;
7. Персональний комп'ютер та його жорсткі диски;
8. Файли логування подій та журнали подій операційних систем.

Саме в цих місцях присутня значна кількість цифрових слідів, аналіз яких дасть змогу полегшити процес розслідування інцидентів інформаційної та кібербезпеки.

Термін "інформаційний слід" також використовується Гавриліним Ю.В., який зазначав, що ця категорія злочинів найчастіше пов'язана з незаконним доступом злочинців до комп'ютерної інформації, а відстеження засноване на традиційних методах, що вивчаються трасологією.

Дані, залишені користувачами ІКТ, можуть розкривати інформацію про них, включаючи інформацію про вік, стать, расу та етнічну належність, громадянство, сексуальну орієнтацію, думки, уподобання, звички, хобі, історію хвороб та проблеми зі здоров'ям, психологічні розлади, статус, зайнятість, спільноту, особисті стосунки, географічне розташування, повсякденне життя та іншу діяльність. За допомогою таких слідів можна побудувати цифровий портрет зловмисника, а в деяких випадках – його фоторобот. Такі цифрові сліди можуть бути активними або пасивними.

Активні цифрові сліди створюються на основі даних, наданих користувачем, таких як персональні дані, відео, зображення та коментарі, розміщені в додатках, веб-сайтах, електронних рекламних щитах, соціальних мережах та інших онлайн-форумах.

Пасивні цифрові сліди – це дані, ненавмисно залишені людьми, які використовують мережу Інтернет або цифрові технології. Дані, які є частиною активних та пасивних цифрових відбитків, можуть бути використані як докази інцидентів інформаційної та кібербезпеки, включаючи кіберзлочинність. Такі дані також можуть бути використані для доведення або спростування тверджень про факти. Встановити причетність або непричетність підозрюваного до скоєння злочину, підтвердити або спростувати показання потерпілих, свідківі підозрюваних. Дані можуть зберігатися на цифрових пристроях (наприклад, комп'ютерах, смартфонах, планшетах, телефонах, принтерах, смарт-телевізорах та інших пристроях з цифровою пам'яттю), зовнішніх запам'ятовуючих пристроях (наприклад, зовнішніх жорстких дисках і флеш-накопичувачах USB), мережевих компонентах (маршрутизаторах) та інших пристроях. Дані зберігаються в мережі та на пристрої, сервері або у хмарному сховищі (де дані зберігаються в декількох центрах обробки даних, розташованих у різних географічних місцях).

Оскільки комп’ютерна криміналістика – це наука, яка вивчає цифрові сліди, то логічно зробити висновок, що весь процес побудований на роботі з даними та інформацією. На законодавчому рівні поняття інформації формулюється таким чином: інформація – це документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі [3]. Відносно інформації, яка обробляється в електронно-обчислюваних машинах, таке визначення не в повному обсязі відповідає дійсності та звужує зміст такої інформації. Особливість комп'ютерної інформації полягає в тому, що вона виступає в якості засобу управління електронно-обчислювальними машинами або їх окремими частинами і у вигляді комп'ютерних програм і файлів не містить інформації про події або явища. Якби беручи до уваги ці відмінності, законодавець у 1994 році керувався статтею 2 Закону України "Про захист інформації в автоматизованих системах", то він би закріпив такі поняття, як інформація в автоматизованих системах – сукупність всіх даних і програм, що використовуються в автоматизованих системах, незалежно від засобів їх фізичного і логічного представлення [2]. Згідно з цим визначенням, дані – це інформація у форматі, придатному для автоматичної обробки за допомогою обчислювальної технології, програма – це набір інструкцій, команда для виконання певного процесу, надана в такому форматі, який може бути виконаний персональним комп'ютером або перетворений в такий формат. Після обробки даних, тобто накопичення, систематизації, сортування та аналізу, дані перетворюються на інформацію. А досвід роботи з інформацією перетворює її в знання. Виходячи з наведеного вище визначення, комп'ютерні дані, поряд з комп'ютерними програмами, є невід'ємною частиною комп'ютерної інформації і співвідносяться один з одним частково і в цілому, але існують дещо інші погляди на природу комп'ютерних даних, зазначені в міжнародних документах – Конвенції про кіберзлочинність. Відповідно до цієї угоди, комп'ютерні дані зберігаються в комп'ютерній системі, включаючи програми, придатні для забезпечення виконання комп'ютерною системою певних функцій.

Існує чотири основних етапи робіт з цифровими слідами інцидентів інформаційної та кібербезпеки, а власне кажучи комп’ютерною інформацією та даними (рисунок 6):

Рисунок 6 – Етапи робіт з цифровими слідами інцидентів інформаційної та кібербезпеки

Обговорення результатів досліджень. Таким чином, комп'ютерна криміналістика включає процес ідентифікації, отримання, накопичення та зберігання, аналізу та представлення цифрових слідів інцидентів інформаційної та кібербезпеки. Цифрові докази факту наявності інцидентів інформаційної та кібербезпеки повинні бути виявлені та пройти ідентифікацію, щоб забезпечити їх прийнятність у суді. Зрештою, факти, зібрані для криміналістичного аналізу, та використовувані криміналістичні методи (наприклад, статичний або динамічний збір даних у режимі реального часу) залежать від пристрою, його операційної системи та засобів захисту.

Поряд з цим, експерти з комп'ютерної криміналістики зустрічаються з певним рядом проблем, які можна розбити на такі категорії: технічні та адміністративні [9].

До технічних питань відносять шифрування, збільшення простору зберігання даних та нові технології.

Шифрування – зашифровані дані може бути неможливо переглянути без правильної клавіші або пароля. Експерти криміналісти повинні враховувати, що ключ або пароль можуть зберігатися в іншому місці на комп'ютері або на іншому комп'ютері, до якого підозрюваний має доступ.

Збільшення простору зберігання даних – носії зберігають все більшу кількість даних, що для експерта означає, що для їх аналізу комп'ютери повинні мати достатню потужність обробки та доступну ємність для зберігання даних, щоб ефективно працювати з пошуком та аналізом великої кількості даних.

Нові технології – обчислювальна техніка – це напрям, що постійно розвивається, де завжди з'являються нові апаратні засоби, програмне забезпечення та операційні системи. Жоден криміналіст не може бути експертом у всіх областях, хоча вони часто аналізують предметну область, з якою раніше не працювали.

Щодо адміністративних питань, то в комп'ютерній криміналістиці є безліч стандартів і правил, деякі з яких, є загальноприйнятими. Причини цього включають: установи, що встановлюють стандарти, прив'язані до окремих законодавчих актів; стандарти спрямовані як на правоохоронну, так і на комерційну криміналістику. У багатьох юрисдикціях немає кваліфікаційного органу для перевірки компетенції експертів криміналістів. У таких випадках кожен може представити себе як комп'ютерний судово-медичний експерт, а це може призвести до комп'ютерної криміналістичної експертизи сумнівної якості та негативного уявлення про професію в цілому.

Операційні системи, які є запатентованими, але фахівцям з комп'ютерної криміналістики вони можуть бути не відомі, та функції безпеки (наприклад, шифрування) можуть стати перешкодою для проведення цифрової криміналістичної експертизи, і наприклад, шифрування, що блокує доступ третіх сторін до інформації та повідомлень користувачів, може завадити правоохоронним органам отримати доступ до даних, що містяться в технічних пристроях, таких, наприклад, як смартфони [5].

Висновки. 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 спеціальний підрозділ боротьби з кіберзлочинністю. Також існує ряд приватних фірм, 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 повинні бути враховані під час їх отримання, збирання, накопичення та аналізу. У зв'язку з цим існує необхідність у подальшому дослідженні кримінально-процесуальних властивостей комп'ютерної інформації та впровадженні його результатів в практичну діяльність правоохоронних органів.

Отже, комп'ютерна криміналістика, якщо враховувати всі вище описані її особливості, дає змогу ефективно, в найкоротші терміни виявляти кіберпорушників та запобігати факту вчинення комп'ютерного правопорушення, що позитивно вплине на стан інформаційної та кібербезпеки в майбутньому.

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. Закон України "Про захист інформації в автоматизованих системах" // Відомості Верховної Ради України. 1994. № 31. С. 2.

3. Закон України "Про інформацію" // Відомості Верховної Ради України. 1992. № 48. С. 3.

4. Іванченко О. М. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. *Актуальні проблеми вітчизняної юриспруденції*. 2016. № 3. С. 172–177.

5. Колодіна А.С., Федорова Т.С. Цифрова криміналістика: проблеми теорії і практики. Електронне наукове фахове видання «*Юридичний науковий електронний журнал*». Запоріжжя, 2022. №4. С. 378-380.

6. Комп'ютерна криміналістика URL: https://law.lnu.edu.ua/course/digitalforensics

7. Конвенція про кіберзлочинність: від 23.11.2001. URL: http://zakon0.rada.gov.ua.

8. Криміналістика: підручник: у 2 т. / за заг. ред. А. Ф. Волобуєва, Р. Л. Степанюка, В. О. Малярової; МВС України, Харків. нац. ун-т внутр. справ. Харків, 2018. Т. 2. 312 с.

9. Полотай О.І. Комп'ютерна криміналістика: основні завдання та проблеми. *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення*: матеріали міжнар. наук. інтернет-конф. Тернопіль, 2022. Вип. 68. С. 29-30.

10. Полотай О.І. *Роль комп'ютерної криміналістики у забезпеченні інформаційної безпеки.* Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення: матеріали Міжнародної наукової інтернет-конференції. Тернопіль, 2022. Вип. 67. С. 41-43.

11. Ращенко. Є. Комп'ютерні дані як носій криміналістичної інформації про злочини у сфері комп'ютерних технологій. *Правова інформатика*, № 1(13). 2007. С. 74-78.

12. Що таке комп'ютерна криміналістика? - Підказка щодо Linux URL: https://ciksiti.com/uk/chapters/4152-what-is-computer-forensics---linux-hint

References:

1. Zagumenny O.O. (2019). Correlation between the concepts of "cybercrime" and "computer crimes". *Procedural and technical forensic support of pre-trial investigation*, 67-70.

2. On information protection in automated systems (Law of Ukraine). №. 31 (1994).

3. About information (Law of Ukraine). № 48 (1992)

4. Ivanchenko O. M. (2016). Criminological characteristics of cybercrime, prevention of cybercrime at the national level. *Actual problems of domestic jurisprudence*. (3), 172–177.

5. Kolodina A.S., Fedorova T.S. (2022). Digital forensics: problems of theory and practice. Electronic scientific specialist publication "*Legal Scientific Electronic Journal*". (4), 378-380.

6. Computer forensics. Removed from https://law.lnu.edu.ua/course/digitalforensics

7. Convention on cybercrime: (2001). Removed from http://zakon0.rada.gov.ua.

8. Volobueva A. F., Stepaniuk R. L., Malyarova V. O. (2018). Criminology (T.2). Kharkiv: National University of Internal Affairs affairs.

9. Polotai O.I. (2022). Computer forensics: main tasks and problems. Information Society: *Technological, Economic and Technical Aspects of Formation: Proceedings of the International Scientific Internet Conference,* (68), 29-30.

10.Polotai O.I. (2022). The role of computer forensics in ensuring information security. *Information Society: Technological, Economic and Technical Aspects of Formation: Proceedings of the International Scientific Internet Conference*, (67), 41-43.

11.Rashchenko. E. (2007). Computer data as a carrier of forensic information about crimes in the field of computer technologies. *Legal Informatics*, (1-13), 74-78.

12.What is computer forensics? - A hint about Linux. Removed from: https://ciksiti.com/uk/chapters/4152-what-is-computer-forensics---linux-hint

Оглядова.
Надійшла до редакції 10.10.2023.
Прийнято до публікації 01.12.2023.