Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: *«Використання системи для розподіленого зберігання інформації в анти-форензиці»*

Виконав: студент (ка)
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Дячун В.П.
підпис (прізвище та ініціали)

Керівник *Марценюк В.П.*
підпис (прізвище та ініціали)

Нормоконтроль *Лобур Т.Б.*
підпис (прізвище та ініціали)

Завідувач кафедри *Загородна Н.В.*
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«19» __червня__ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Дячуну Всеволоду Петровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Використання системи для розподіленого зберігання інформації в анти-форензиці

Керівник роботи Марценюк Василь Петрович, д.т.н., проф.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 03 » 04 2023 року № 4/7-349

2. Термін подання студентом завершеної роботи 17.06.2023

3. Вихідні дані до роботи Вимоги до програмного забезпечення

4. Зміст роботи (перелік питань, які потрібно розробити)

Безпека життєдіяльності, основи охорони праці

Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Пилипець.М.І., проф. кафедри МТ		

7. Дата видачі завдання 16.01.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	16.01 – 19.01	*Виконано*
2.	Підбір джерел про принципи побудови та методи забезпечення безпеки в децентралізованих системах	20.01 – 05.02	*Виконано*
3.	Опрацювання джерел в галузі дослідження	06.02 – 22.02	*Виконано*
4.	Розроблення програмного коду	23.02 – 20.03	*Виконано*
5.	Тестування роботи програми та верифікація результатів	21.03-05.04	*Виконано*
6.	Оформлення розділу «Аналіз безпеки децентралізованих систем»	06.03 – 17.04	*Виконано*
7.	Оформлення розділу «Аналіз механізмів забезпечення конфіденційності та автентичності в децентралізованих системах»	18.04 – 29.04	*Виконано*
8.	Оформлення розділу «Реалізація створення та використання криптовалют на основі децентралізованих систем»	30.04 – 13.05	*Виконано*
9.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	14.05 – 21.05	*Виконано*
10.	Оформлення кваліфікаційної роботи	22.05 – 05.06	*Виконано*
11.	Нормоконтроль	06.06 – 11.06	*Виконано*
12.	Перевірка на плагіат	12.06 – 15.06	*Виконано*
13.	Попередній захист кваліфікаційної роботи	16.06 – 19.06	*Виконано*
14.	Захист кваліфікаційної роботи	22.06.2023	

Студент _____ *Дячун В.П.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Марценюк В.П.*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Використання системи для розподіленого зберігання інформації в анти-форензиці // Кваліфікаційна робота ОР «Бакалавр» // Дячун Всеволод Петрович// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-41 // Тернопіль, 2023 // С. __ , рис. – 50, табл. – 1, кресл. – , додат. –

Ключові слова: КІБЕРБЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА, БЕЗПЕКА ІНФОРМАЦІЇ, ЦИФРОВА КРИМІНАЛІСТИКА, КРИПТОГРАФІЧНІ МЕТОДИ, РОЗДІЛЕННЯ СЕКРЕТІВ

Метою роботи є розробка системи для розподіленого зберігання інформації в анти-форензиці, яка грунтується на генеруванні часток секретних даних на основі першого порогового значення кількості часткок, які дозволяють підвищити рівень безпеки при зберіганні та передачи секретних даних.

Об'єкт дослідження – процес розподіленого зберігання інформації в анти-форензиці з використанням методів генерування часток секретних даних для отримання відповідного рівня надійності та безпеки зберегання та передачи секретних даних, а також проведення аналізу та порівняння інструментів і криптографічних методів за допомогою яких можливо маскувати передані дані для протидії цифровий криміналістики.

Предмет дослідження – методи зберігання та алгоритми розподілу секретних даних на необхідну кількість часток, що забезпечує необхідний рівень секретності та безпеки зберігання, обробки та передачи секретних даних на основі цифрової криміналістики і її підрозділу – антіфорензікі, формування ознак для класифікації рішень в сфері цифрової криміналістики.

Методи дослідження – теорія захисту інформації, експертного оцінювання.

У результаті дослідження було проаналізовано сучасний стан загроз на інформаційні ресурси, визначені основні інструменти та методи, що

використовуються в протидії цифровий криміналістиці та було запропоновано концепцію захисту та маскування інформації за допомогою схеми спільного використання секрету, криптографічного методу підвищення безпеки критично важливих даних.

ABSTRACT

Using a distributed information storage system in anti-forensics // Thesis of educational level "Bachelor" // Diachun Vsevolod Petrovych // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, СБс-41 group // Ternopil, 2023 // P. ___ , fig. -____, table. - __ , chair. - ___ , added. -___.

Keywords: CYBER SECURITY, INFORMATION SECURITY, INFORMATION SECURITY, DIGITAL CRIMINAL SCIENCE, CRYPTOGRAPHIC METHODS, SECRET SEPARATION

The purpose of the thesis is to develop a system for distributed storage of information in anti-forensics, which is based on the generation of particles of classified data based on the first threshold value of the number of particles that increase security during storage and transmission of classified data.

The object of research – the process of distributed storage of information in anti-forensics using methods of generating particles of classified data to obtain the appropriate level of reliability and security of storage and transmission of classified data, as well as analysis and comparison of tools and cryptographic methods to mask transmitted data to counter digital forensics.

The subject of research – storage methods and algorithms for dividing classified data into the required number of particles, which provides the required level of secrecy and security of storage, processing and transmission of classified data on the basis of digital forensics and its unit – antiphorenics.

Research methods – information protection theory, expert evaluation.

The study analyzed the current state of threats to information resources, identified the main tools and methods used in combating digital forensics and proposed the concept of protection and masking of information using a scheme of sharing secrets, a cryptographic method of improving the security of critical data.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

АФ – антифорензіка;

ІС – інформаційна система;

КБ – кібербезпека;

НС – національна система;

СІ – соціальна інженерія:

СРС – схема розділення секретів;

ЦК – цифрова криміналістика;

MDS – distance matrix;

OSINT – open source intelligence.

ВСТУП

За останнє десятиліття Інтернет став свідком величезного зростання обсягу, характеру та збільшення каналів обміну інформацією між декількома засобами масової інформації незалежно від відстані та місцезнаходження. Протягом останнього десятиліття цифрова криміналістика набула великого розголосу. Науково обґрунтоване та законне судово-комп’ютерне розслідування цифрових доказів має на меті виявити та розпізнати їх значення, де докази повинні бути надійними, точними та повними.

Актуальність роботи полягає в порівняльному аналізу методів захисту секретних даних, і зокрема ключів, різноманітних програмно-апаратних комплексів із розподіленою структурою доступу, таких як удосконалення центрів та апаратних модулів захисту конфіденційної інформації. Серед яких розглядаються різні методи підвищення секретності ключів і можна виділити метод, заснований на застосуванні схеми розділення секретів (СРС).

Метою даної роботи є дослідження методів та інструментів комп'ютерної криміналістики та антикриміналістики з точки зору комп'ютерної безпеки, що дозволить оприділяти засекречену інформацію. Щоб надати безпеку вихідними даними, вони поділяються на кілька «фрагментів» або підмножин даних. Обсяг даних в кожному зрізі менш придатний для використання або менш розпізнається, або повністю непридатний для використання.

1 ОГЛЯД ФОРЕНЗІКИ ЯК НАУКИ ПРО РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

1.1 Аналіз сучасних загроз інформаційним системам

Під погрозами безпеки ІС розуміється спільність умов і факторів, які створюють потенційну або реально загрозу, пов'язану з витоком інформації або несанкціонованими, ненавмисними діями на неї (рис. 1.1).

Інформаційна безпека визначається як захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення, зміни або знищення з метою забезпечення конфіденційності, цілісності та доступності. Відповідно до Міжнародної організації зі стандартизації (ISO), модель, зазвичай іменована «7 принципів ISO», складається з семи принципів (рис. 1.2).

Спектр інтересів суб'єктів, пов'язаних з використанням інформаційних систем, можна розділити на наступні категорії: забезпечення доступності, цілісності і конфіденційності інформаційних ресурсів і підтримуючої інфраструктури (рис. 1.3) [1].

Кіберзлочинність охоплює злочинні дії, пов'язані з комп'ютерами та мережами, від електронного злому до атак типу «відмова в обслуговуванні», в результаті яких веб-сайти електронного бізнесу втрачають гроші. Кіберзлочини здійснюються шляхом незаконного доступу до баз даних, незаконного перехоплення, втручання в дані, втручання в систему, неправомірного використання пристроїв, підробки та електронного шахрайства (рис. 1.4).

У складі загроз інформаційній безпеці інформаційних ресурсів, які впливають на інформаційну систему, а також на економічну складову відносяться внутрішні і зовнішні загрози. За характером і спрямованості впливу на діяльність певних суб'єктів і об'єктів поділяються на економічні, фізичні та інтелектуальні (рис. 1.5).

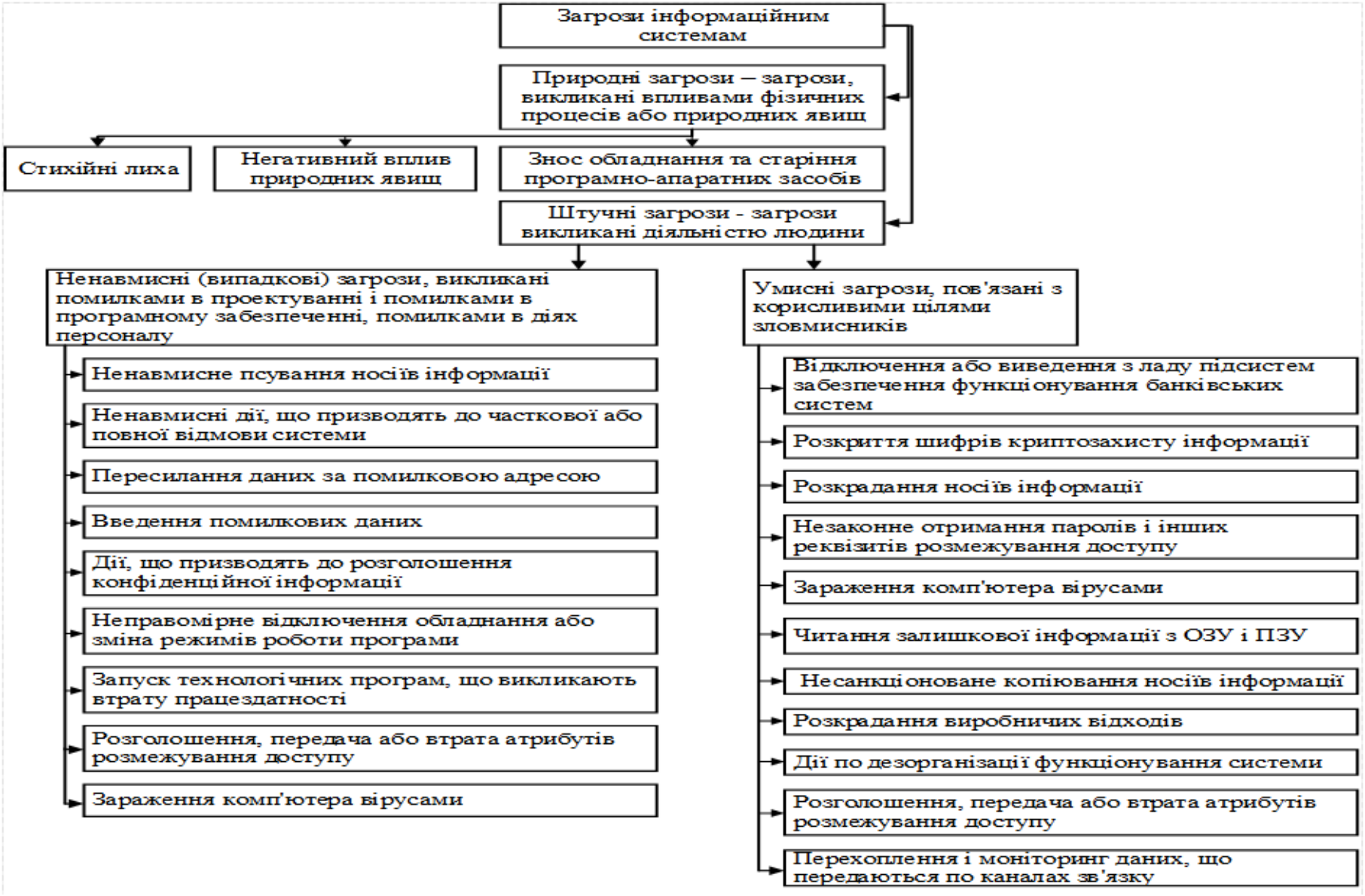

Рисунок 1.1 – Класифікація причин основних загроз для інформаційних систем

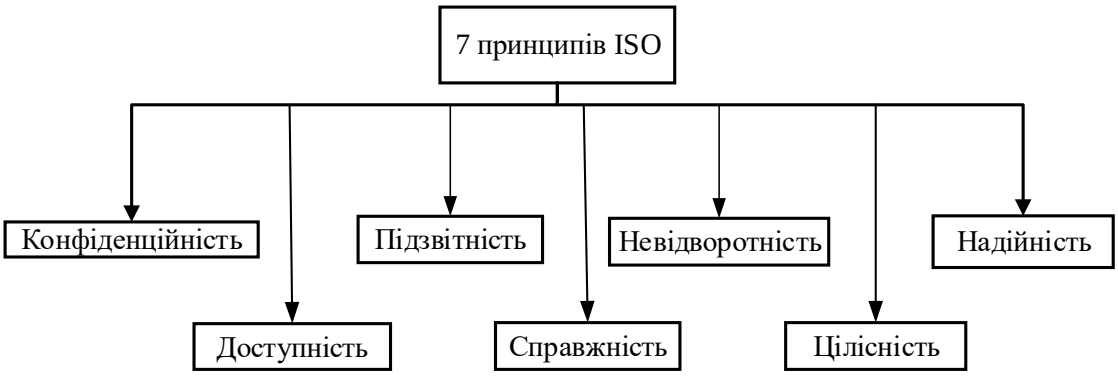

Рисунок 1.2 – Принципи ISO

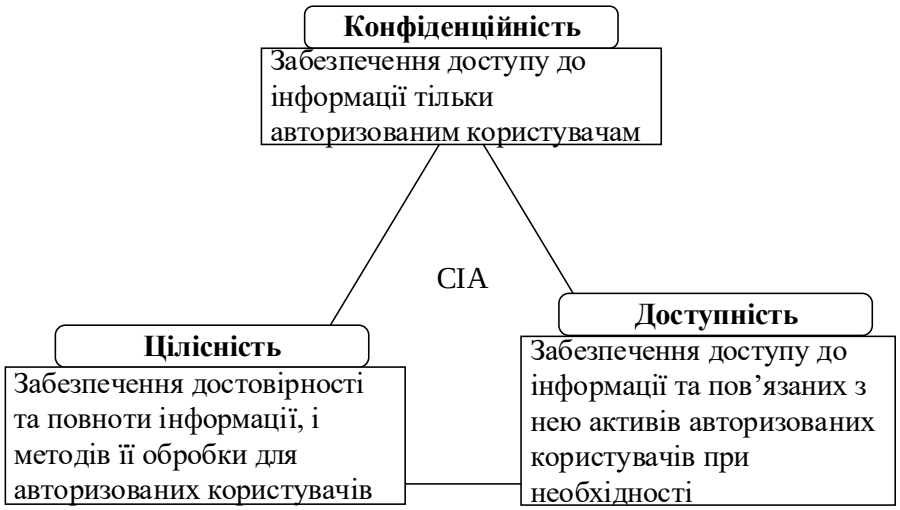

Рисунок 1.3 – Модель тріади CIA

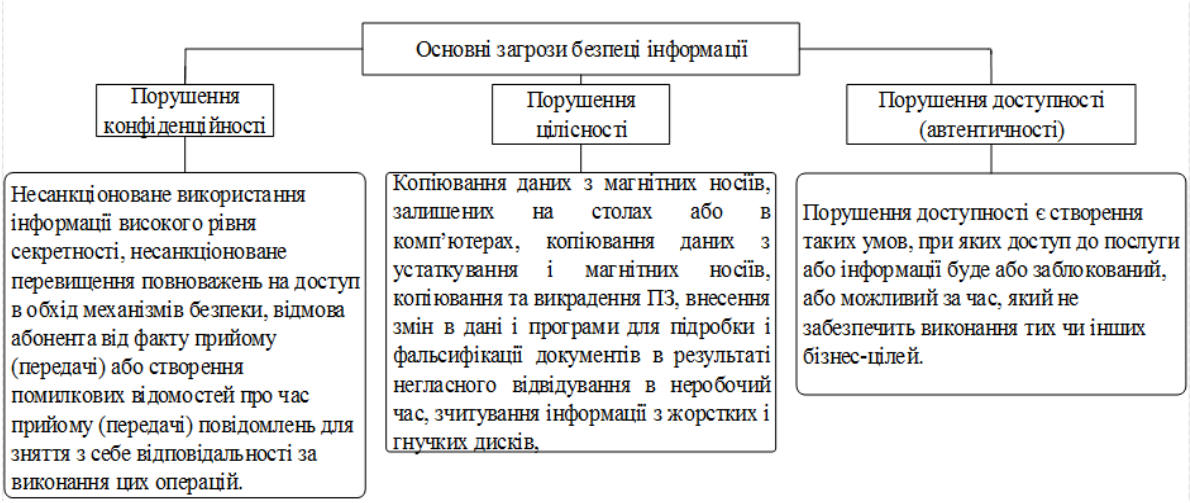

Рисунок 1.4 – Загрози безпеці інформації

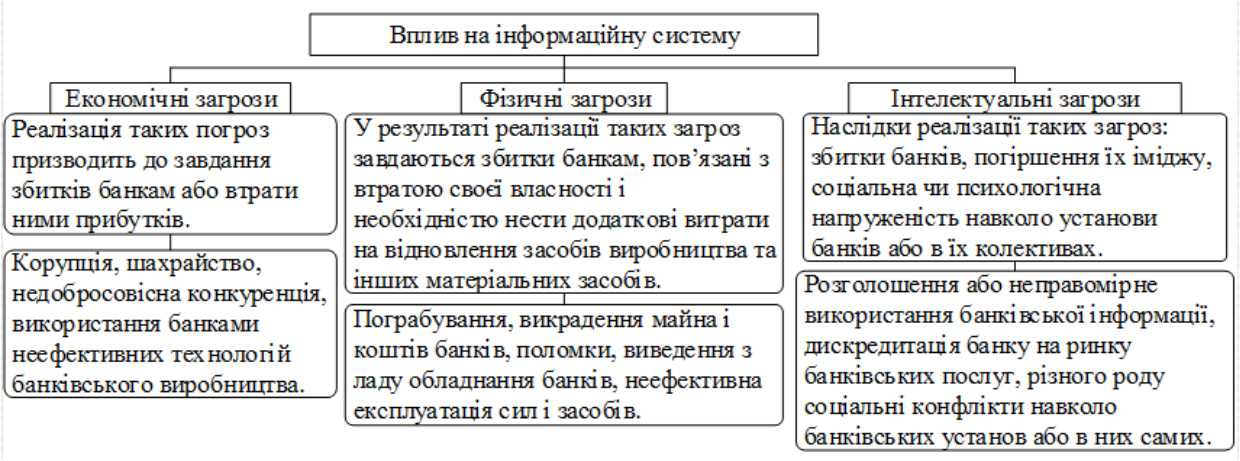

Рисунок 1.5 – Враження ІС

Основними загрозами КБ, спрямованими на зрив процесів управління або взяття їх під контроль, є кібератаки, які можна винести в чотири основні класи, сутність яких розкрита на рис. 1.6 [2].

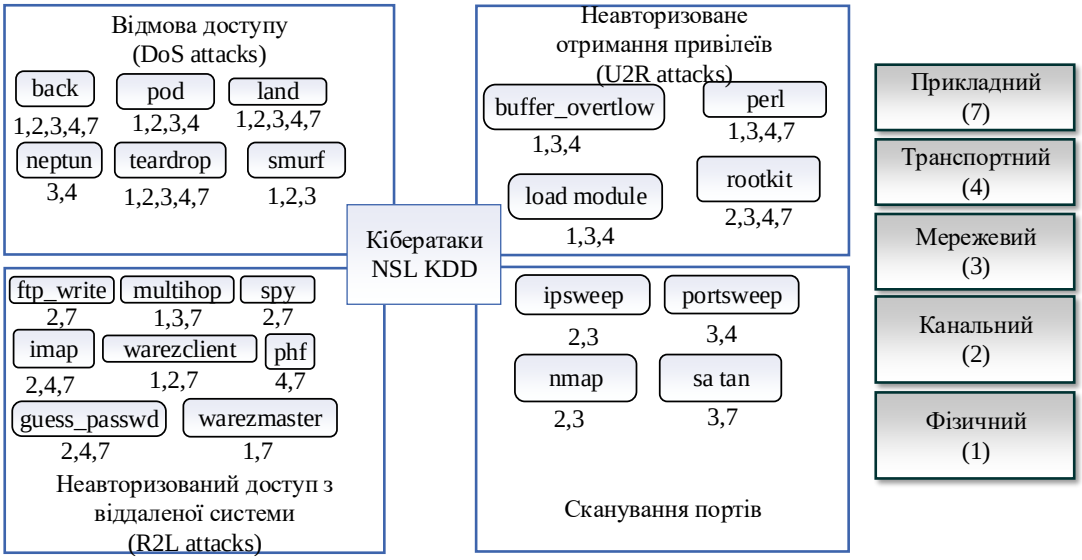

Рисунок 1.6 – Класифікація кібератак з прив'язкою до моделі OSI

Дана класифікація (рис. 1.6) показує, що різноманітні кібератаки мають важливе значення на різноманітних моделях взаємодії відкритих систем OSI.

Одна з провідних міжнародних компаній щодо запобігання та розслідування кіберзлочинів Group-IB в своїх дослідженнях за 2020 звітує про наступні кіберкримінальних тенденції і виділяє наступні напрямки в злочинності, які зображені на рис. 1.7.

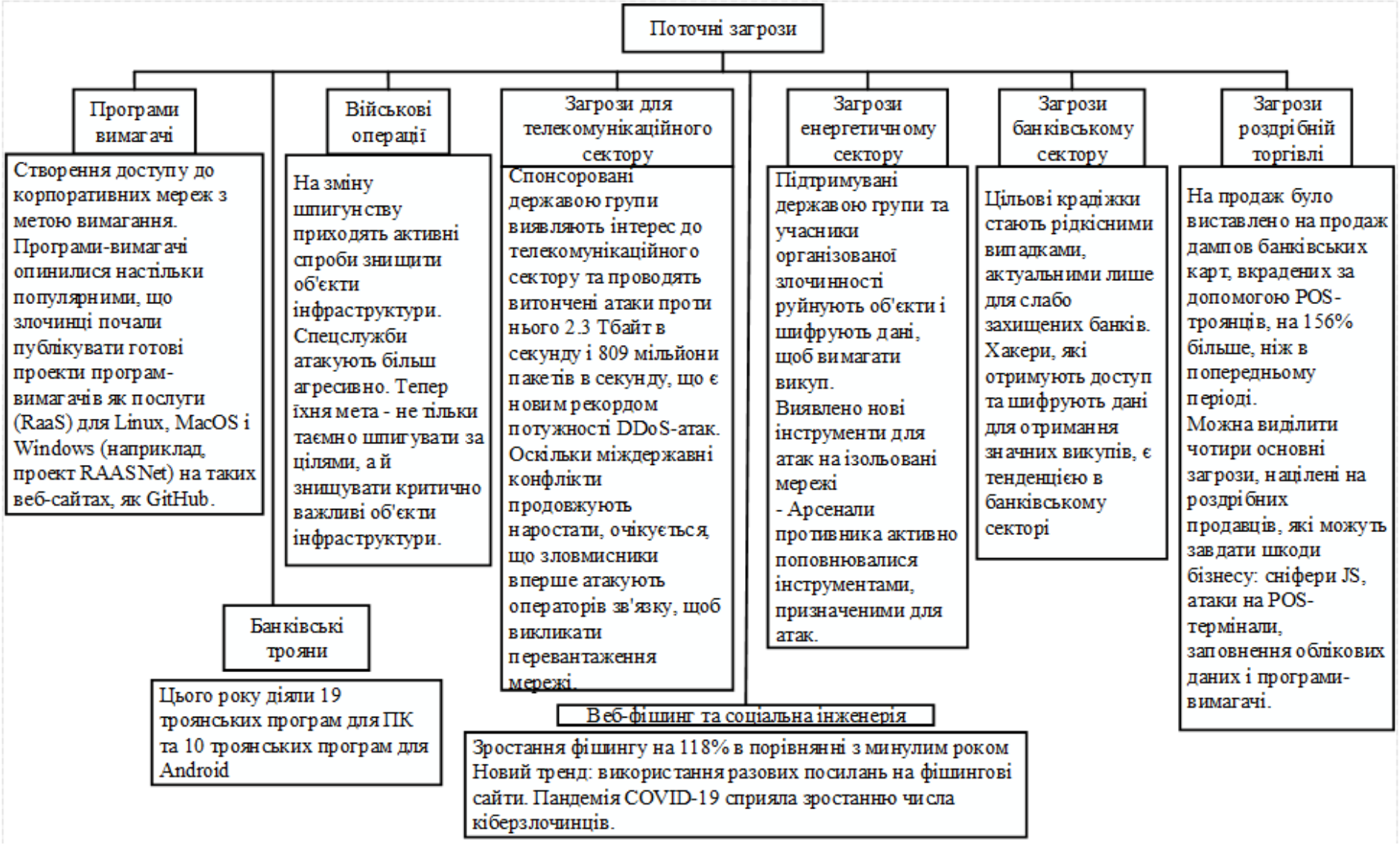

Рисунок 1.7 – Поточні загрози

У період з 2019 по 2020 р.р. кількість скарг в Центр прийому скарг на шахрайство в Інтернеті при ФБР збільшилася майже на 70%. У травні 2021 р. відмітка досягла 6 мільйонів скарг. Трьома основними типами злочинів, про які повідомляють потерпілі в 2020 р. стали фішинг, вимагання та шахрайство з платіжками і доставкою.

У зв'язку з новим витком холодної війни, в світі все частіше спостерігаються атаки на оборонну промисловість. Як приклад однієї з таких атак, на основі доповіді фахівців Лабораторії Касперського, коротко розберемо як хакерське угруповання Lazarus, яку пов'язують зі спецслужбами КНДР, провела хакерську атаку на одне з оборонних підприємств Російської Федерації. На етапі початкового зараження була використана цілеспрямована розсилка фішингових листів. Перед початком атаки зловмисники вивчили публічну інформацію про атакується організації і встановили адреси електронної пошти, що належать різним підрозділам атакується. Шкідливий код, призначений для завантаження і запуску, містився у вигляді макросу всередині документа Microsoft Word (рис. 1.8).

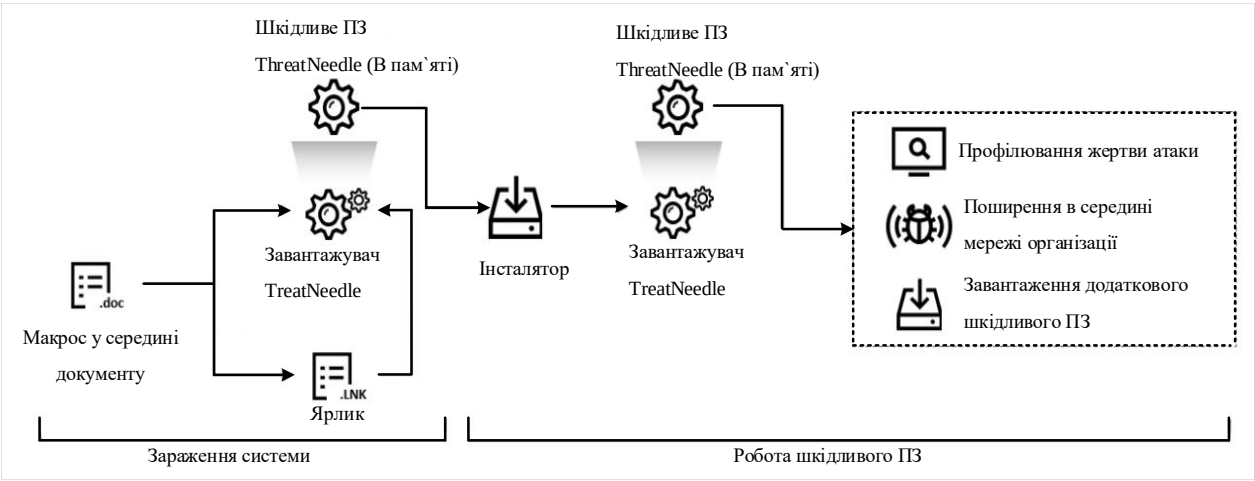

Рисунок 1.8 – Принцип роботи шкідливого ПЗ, яке застосовувалося угрупованням Lazarus

В результаті процедури розгортання завантажувач ThreatNeedle розпаковує і запускає в ураженій системі бекдор знаходиться тільки в оперативної пам'яті і

використовується для прихованого віддаленого управління зараженої системою. З його допомогою зловмисники виконують первинну розвідку і розгортають додаткове шкідливе ПЗ для зараження інших комп'ютерів в мережі підприємства. Для зараження інших комп'ютерів в мережі зловмисники застосовують інший компонент шкідливого ПО ThreatNeedle – інсталятор. Інсталятор відповідає за установку вже згаданого раніше завантажувача ThreatNeedle і його реєстрацію в автозапуску для закріплення в системі [3].

Стандарти ISO/IEC 27032:2012 «Інформаційні технології. Методи забезпечення безпеки. Настанови щодо кібербезпеки», на рисунку 1.9.

Рисунок 1.9 – Логічні взаємозв’язки кібербезпеки та інших доменів безпеки згідно зі стандартом ISO/IEC 27032:2012

Варто брати до уваги зростання атак пов'язаних з соціальною інженерією. Зловмисники змогли завдати величезної шкоди, використовуючи прості атаки соціальної інженерії. У 2015 році компанія Ubiquiti Networks, що виробляє мережеве обладнання, була вражена методом соціальної інженерії. Злочинці змогли зібрати інформацію про генерального директора і видати його особистість за свою, щоб дати вказівку фінансовому відділу направити величезні суми грошей якийсь зарубіжної компанії, яка проінформувала його про зміну своїх платіжних переваг. Стандартний цикл соціальної інженерії показаний на наступному рисунку [6] (рис. 1.11).

В тіньовій мережі зафіксовано різке зростання оголошень від фахівців, які шукають нелегальну роботу. Це пов'язано з важкою економічною ситуацією, нинішня економічна система не може впоратися з раптовою небезпекою, через пандемію і відтоком частини користувачів з сайтів для фрілансерів ряди хакерів стають ширшими, тим самим погіршуючи обстановку в кіберпросторі.

Методи, якими користуються кіберзлочинці для отримання прибутку з пандемії, залишилися колишніми. CI стала ще більш ефективною. В сучасних умовах організаціям необхідно приділяти особливу увагу навчанню віддалених користувачів безпечній поведінці (рис. 1.12).

Ландшафт кіберзагроз в Україні

Перед тим як розібратися з ландшафтом кіберзагроз, спочатку необхідно визначити категорії кіберекосистеми. У цьому нам допоможуть дані, які надали компанії CyberLands і Cyber Unit Technologies під час свого дослідження ринку кібербезпеки України в 2021 р.:

Рисунок 1.10 – Дані досліджень CyberLands і Cyber Unit Technologies

Рисунок 1.11 – Цикл соціальної інженерії

Україна часто піддається кібератакам не тільки через політичні мотиви, а й у зв'язку з низьким рівнем кібербезпеки в країні. Також діють наступні закони щодо забезпечення кібербезпеки, зображені на рис.1.13.

Закон про кібербезпеку встановлює особливий режим для операторів критичних інфраструктур. Закон про кібербезпеки виділяє такі галузі: хімічна промисловість, енергетика, комунальні послуги, транспорт, інформаційні технології, електронні комунікації, банківська справа і фінанси, охорона здоров'я, виробництво продуктів харчування і сільське господарство. Виділяються наступні проблеми кібербезпеки в Україні [7] (рис. 1.14).

Інформаційна війна є найбільш небезпечним інструментом зовнішньої і внутрішньої політики, так як надає можливість таємно і ефективно реалізовувати соціально-економічні, військово-політичні та інші інтереси шляхом комплексного застосування сучасних методів і засобів негативного інформаційного впливу. Інформаційна війна включає в себе наступні елементи (рис. 1.15).

Конфлікт на сході України призвів до численних кібератак високого рівня, тобто складової інформаційної війни, в зв'язку з цим було прийнято рішення про створення Національної системи кібербезпеки. Роботу даної системи забезпечує співробітництво в області кібербезпеки між усіма державними установами, місцевими органами влади, військовими частинами, правоохоронними органами, дослідними установами, освітніми установами, громадськими групами, підприємствами і організаціями, незалежно від їх форми власності, які займаються електронним зв'язком та інформацією безпеки або є власниками критичної інформаційної інфраструктури (рис. 1.16).

Рисунок 1.12 – Категорії екосистеми кібербезпеки в Україні

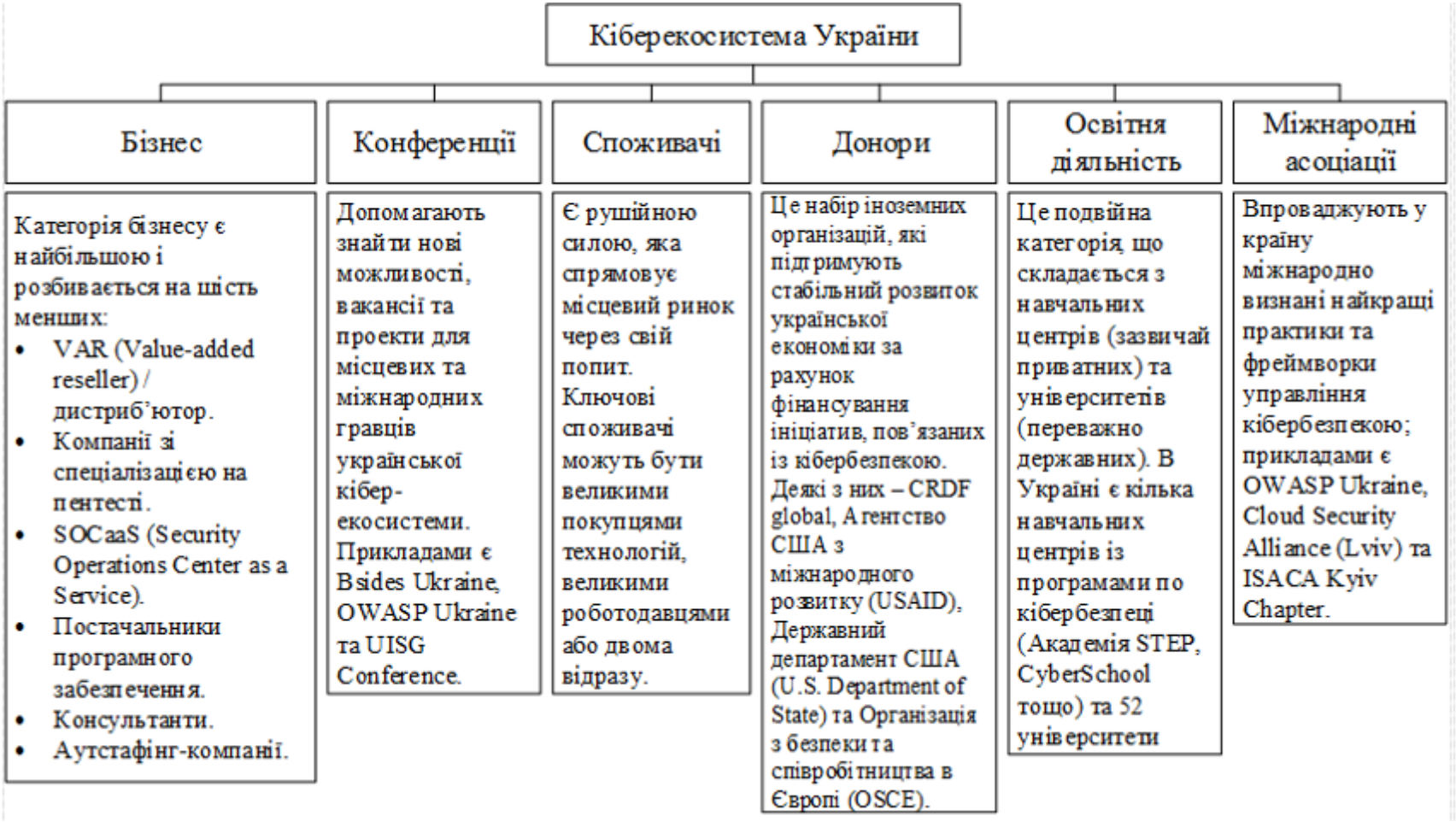

Рисунок 1.13 – Закони щодо забезпечення КБ

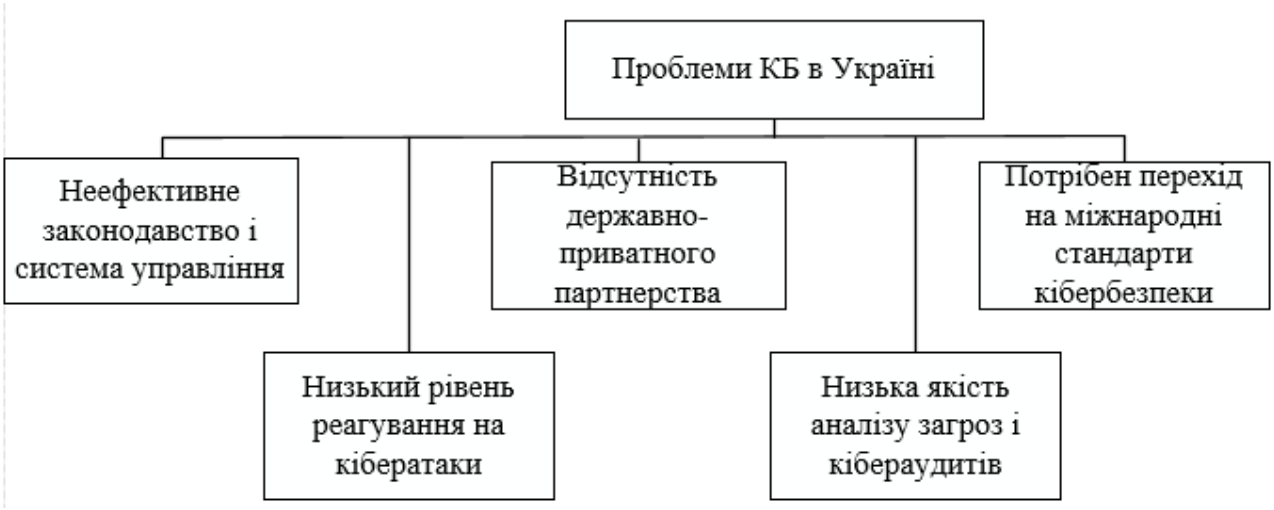

Рисунок 1.14 – Основні проблеми КБ в Україні

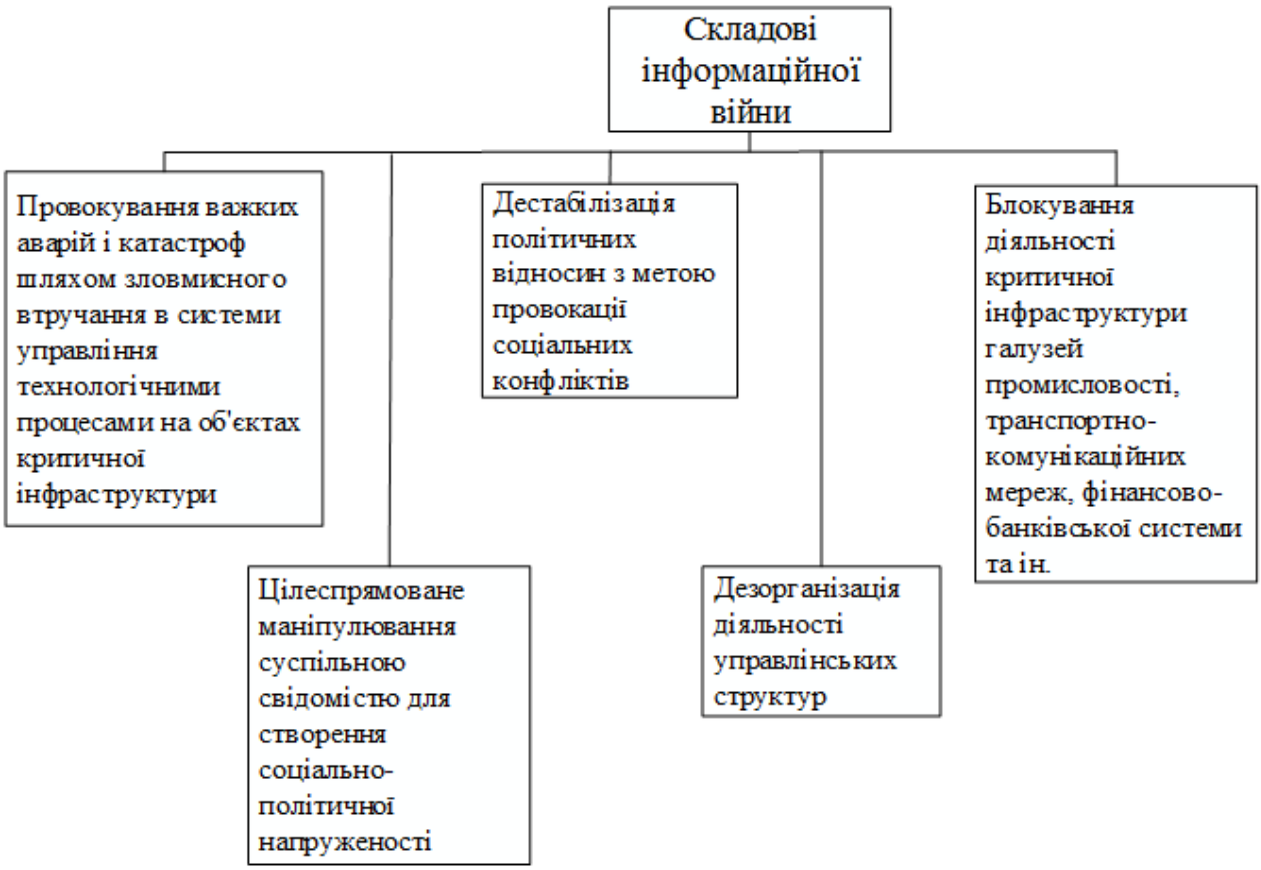

Рисунок 1.15 – Складові інформаційної війни

Рисунок 1.16– Складові НС кібербезпеки та їх завдання

Найчастіше об'єктами хакерських атак стає промисловість і урядові установи. Це свідчить про те, що злочинні формування прагнуть володіти інформацією про розвиток нових технологій, їх впровадження в промисловість, про прийняття нових законів, а також отримувати інформацію про діяльність уряду.

На основі цієї інформації ми приходимо до того, що всі випадки комп'ютерних злочинів і хуліганства повинні розслідуватися спеціалістами, для поліпшення безпеки не тільки критичних інфраструктур, а й звичайних користувачів в кіберпросторі.

1.2 Аналіз технік, методів та класифікація комп`ютерної криміналістики

Комп`ютерна криміналістика – це дисципліна, яка включає методи розслідування і аналізу для збору і збереження доказів з певного електронного або цифрового пристрою, який є підозрюваним у розслідуванні, таким чином, щоб докази підходили для подання в суді [10].

Мета цифрової криміналістики – провести структуроване розслідування при збереженні цілісності доказів і документованої ланцюжка зберігання доказів, щоб точно з'ясувати, що сталося на підозрілому пристрої і хто за це несе відповідальність (рис. 1.17).

Рисунок 1.17 – Суміжні області цифрової криміналістики

Фахівці в області комп'ютерної криміналістики незамінні при необхідності швидко виявити і проаналізувати інциденти ІБ, приклад наведений на рисунку 1.18.

Рисунок 1.18 – Завдання експертів криміналістів

Кібернетична експертиза відіграє важливу і вирішальну роль в розслідуванні кіберзлочинів. Криміналістика поєднує в собі практику виявлення, збору, збереження, аналізу та документування цифрових доказів (рис. 1.19).

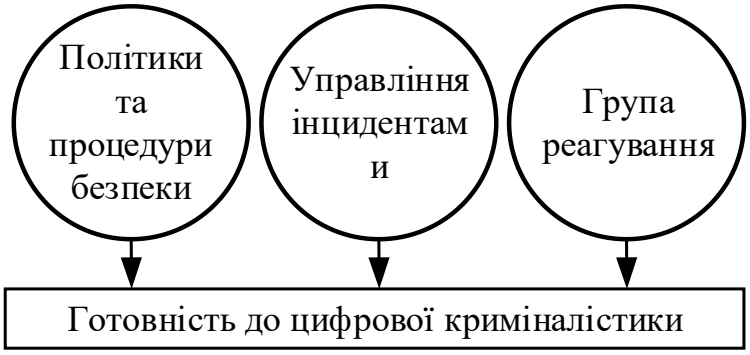

Рисунок 1.19 – Концептуальна модель цифрової криміналістики

Судові слідчі використовують різні методи і додатки для судово-медичної

Дослідники шукають приховані папки і нерасподілений дисковий простір для копій віддалених, зашифрованих або пошкоджених файлів. Будь-які докази, виявлені на зображенні підозрюваного водіння, ретельно документуються в остаточному звіті, складеному слідчим і перевіреному на оригінальному пристрої перед підготовкою до судового розгляду (рис. 1.20).

Існують різні напрямки цифрової криміналістики в залежності від типу використовуваного цифрового пристрою, зображені на рис. 1.21.

Цифрова криміналістика вирішує наступні завдання (рис. 1.22).

Але крім загальнонаукових методів, цифрова криміналістика має набір свій спеціальних методів, які показані на рис. 1.23.

Особливості тактики слідчих дії, спрямованих на збирання комп'ютерної інформації. Перед початком огляду вживаються заходи щодо запобігання пошкодження або знищення інформації (рис. 1.24).

Цифрова криміналістика, як і інші види діяльності в сфері кібербезпеки підкоряються діючими міжнародними стандартами і керівним принципам в області цифрової криміналістики, які представлена на рис. 1.25 [11].

Рисунок 1.20 – Сфери застосування цифрової криміналістики

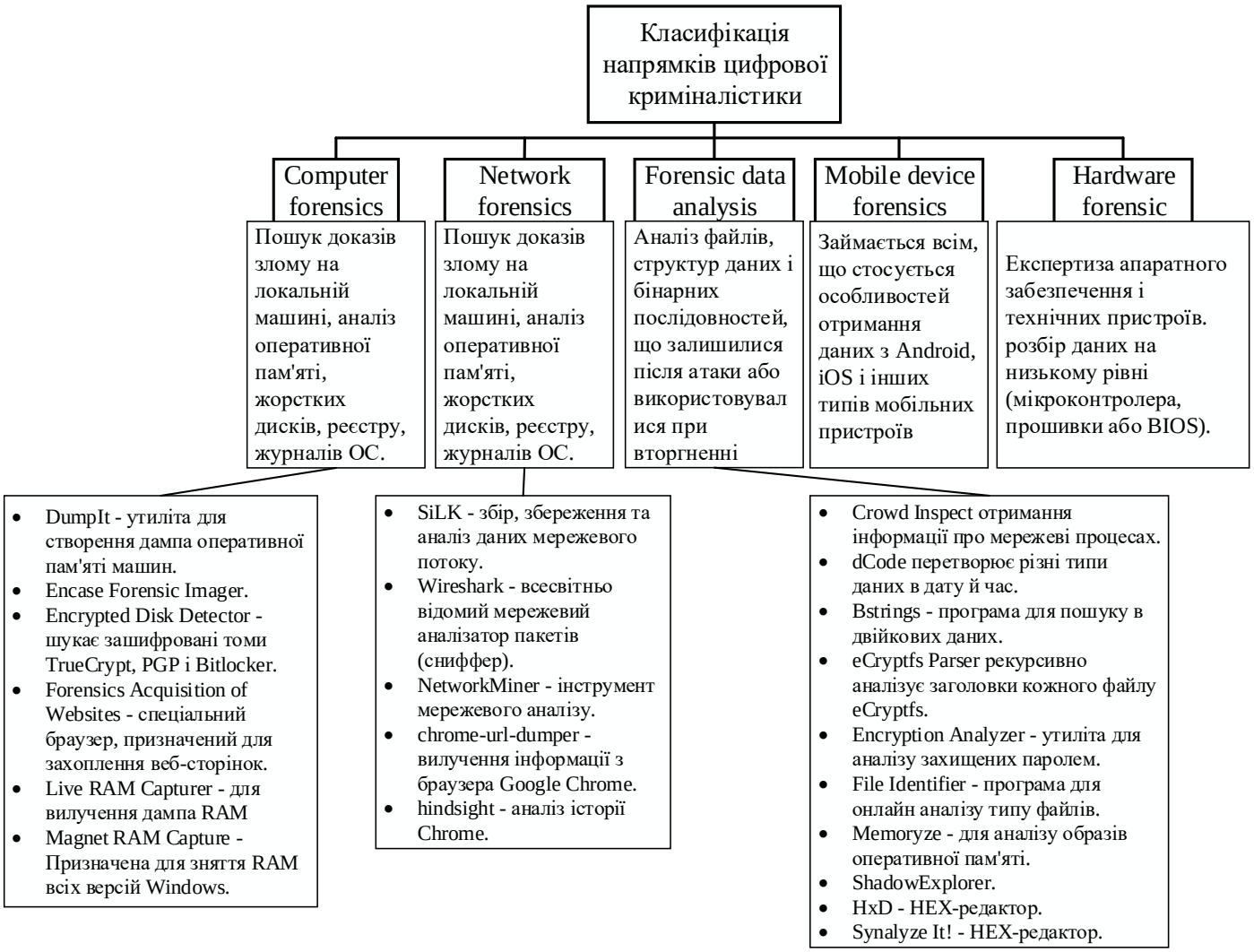

Рисунок 1.21 – Класифікація напрямків ЦК

Рисунок 1.22 – Задачі ЦК

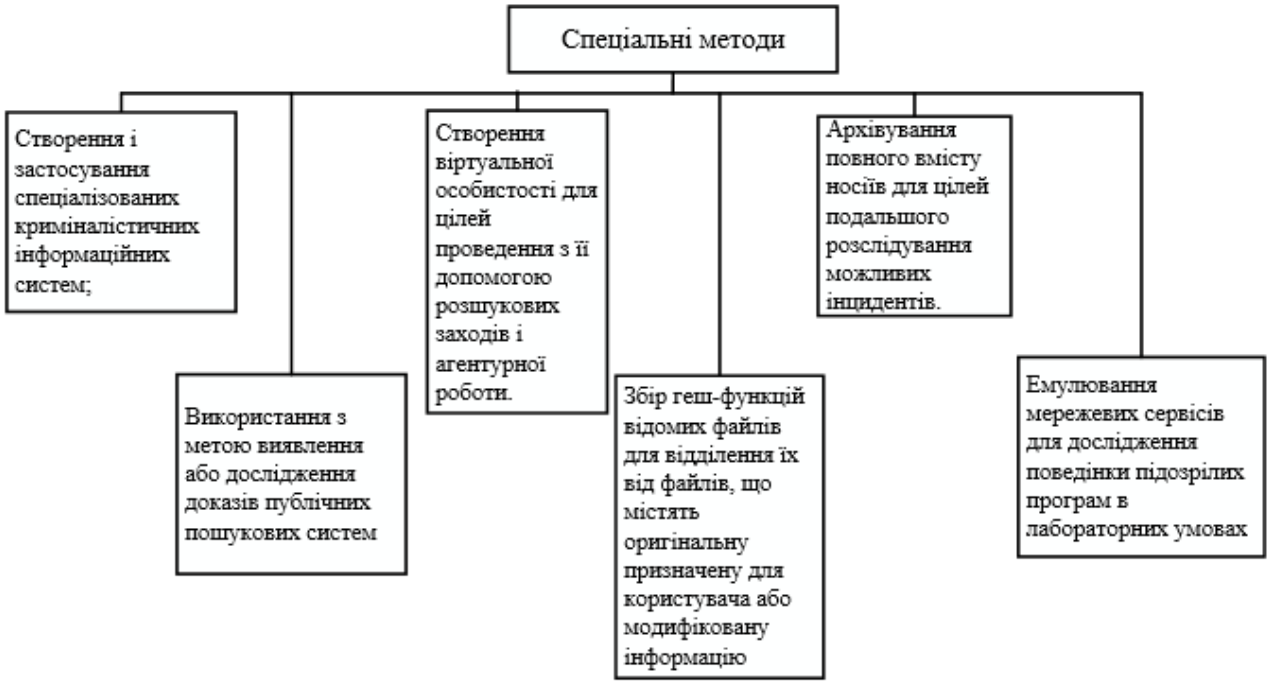

Рисунок 1.23 – Спеціальні методи ЦК

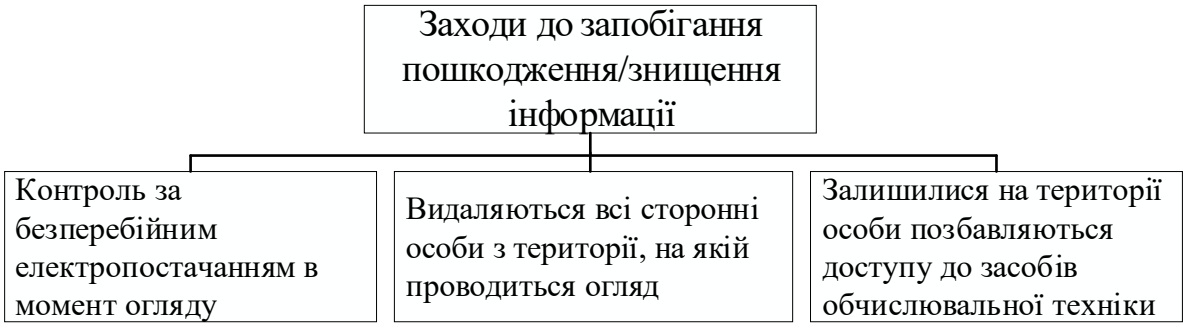

Рисунок 1.24 – Запобігання знищенню інформації

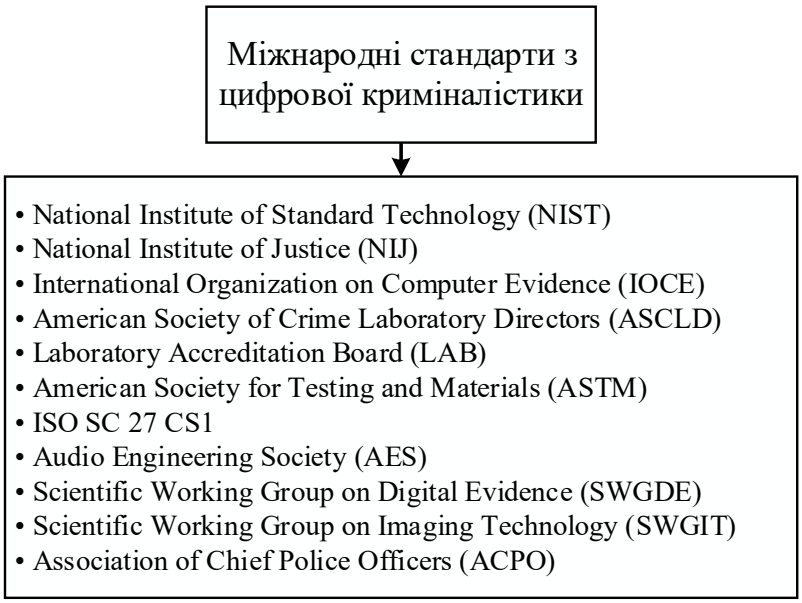

Рисунок 1.25 – Стандарти з ЦК

Ці стандарти надають керівництво по ідентифікації, збору, отримання, обробки, захисту та збереженню цифрових судових доказів, тобто «цифрових даних, які можуть мати доказову цінність» для використання в суді.

Виділяються наступні проблеми в сфері комп`ютерної криміналістики (рис. 1.26).

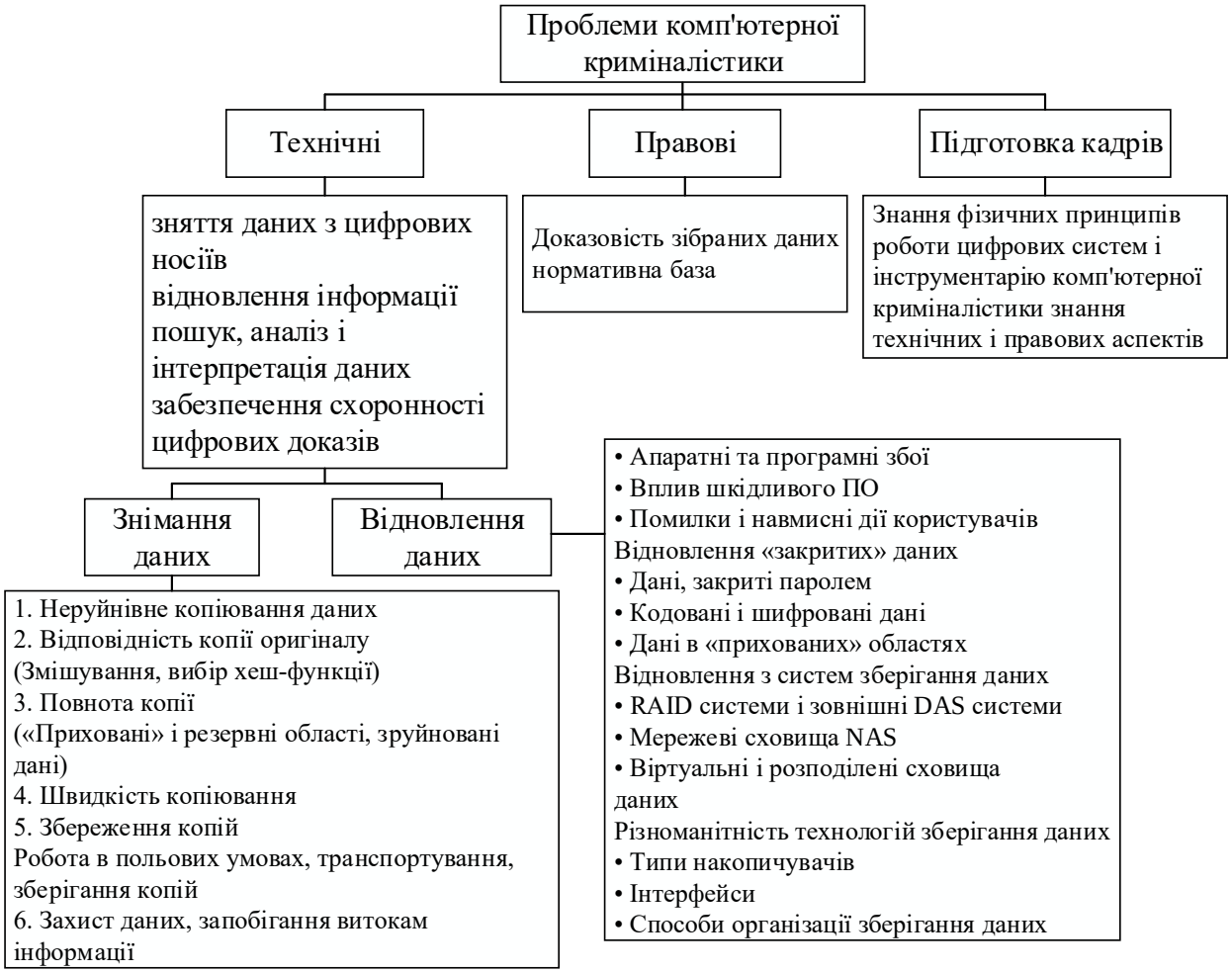

Рисунок 1.26 – Проблеми форензіки

Комп'ютерна криміналістика має наступні техніки розслідування (рис. 1.27).

OSINT як інструмент комп`ютерної криміналістики

OSINT (Open Source INTelligence) – це технологія пошуку, збору та аналізу даних, зібраних з відкритих джерел в Інтернеті, дана технологія активно використовується криміналістами для отримання даних про об'єкт дослідження. До відкритих джерелами інформації відносяться (рис. 1.28).

Міністерство оборони США визначає OSINT наступним чином: "Розвідка з відкритим вихідним кодом – це розвідка, яка виробляється на основі загальнодоступної інформації і збирається, експлуатується і поширюється своєчасно для відповідної аудиторії з метою вирішення конкретного завдання".

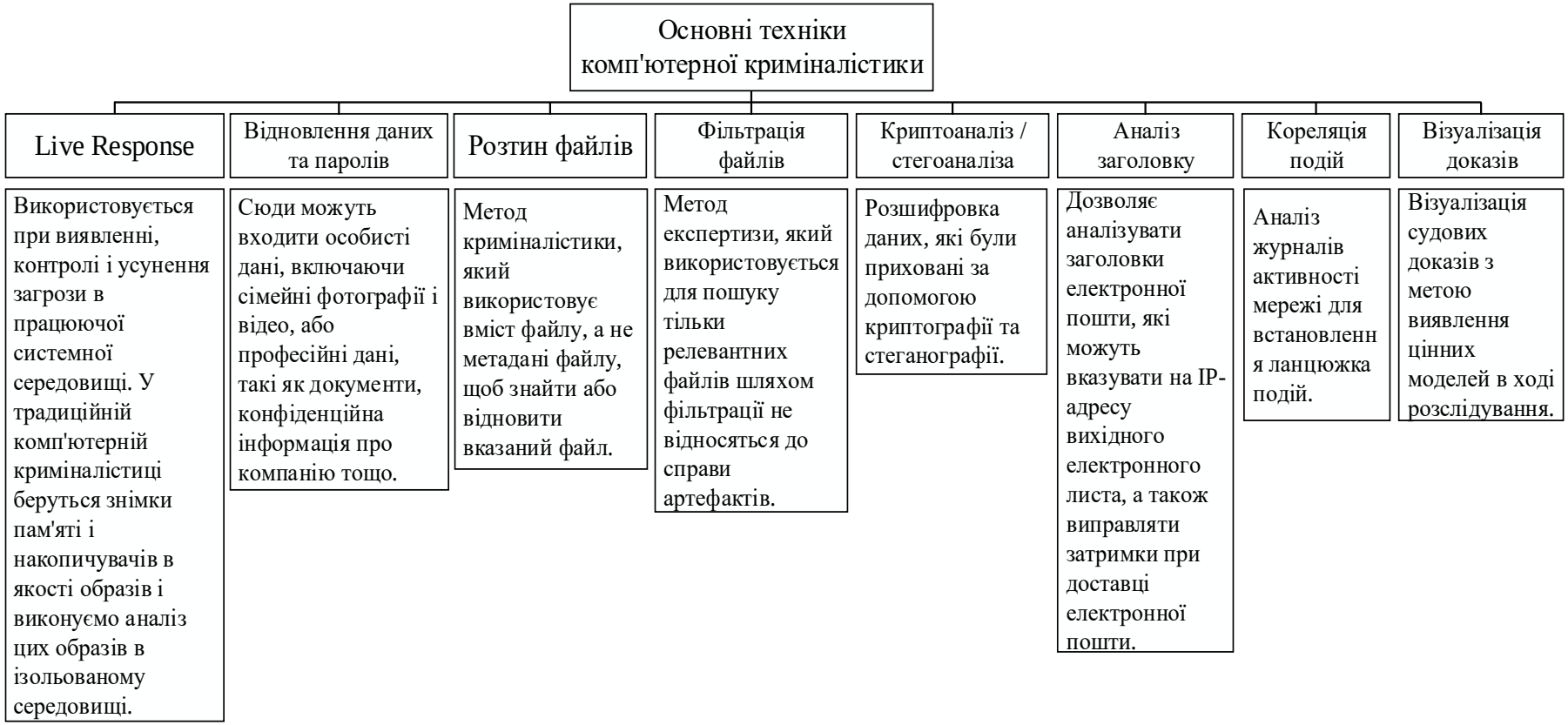

Рисунок 1.27 – Основні техніки форензіки

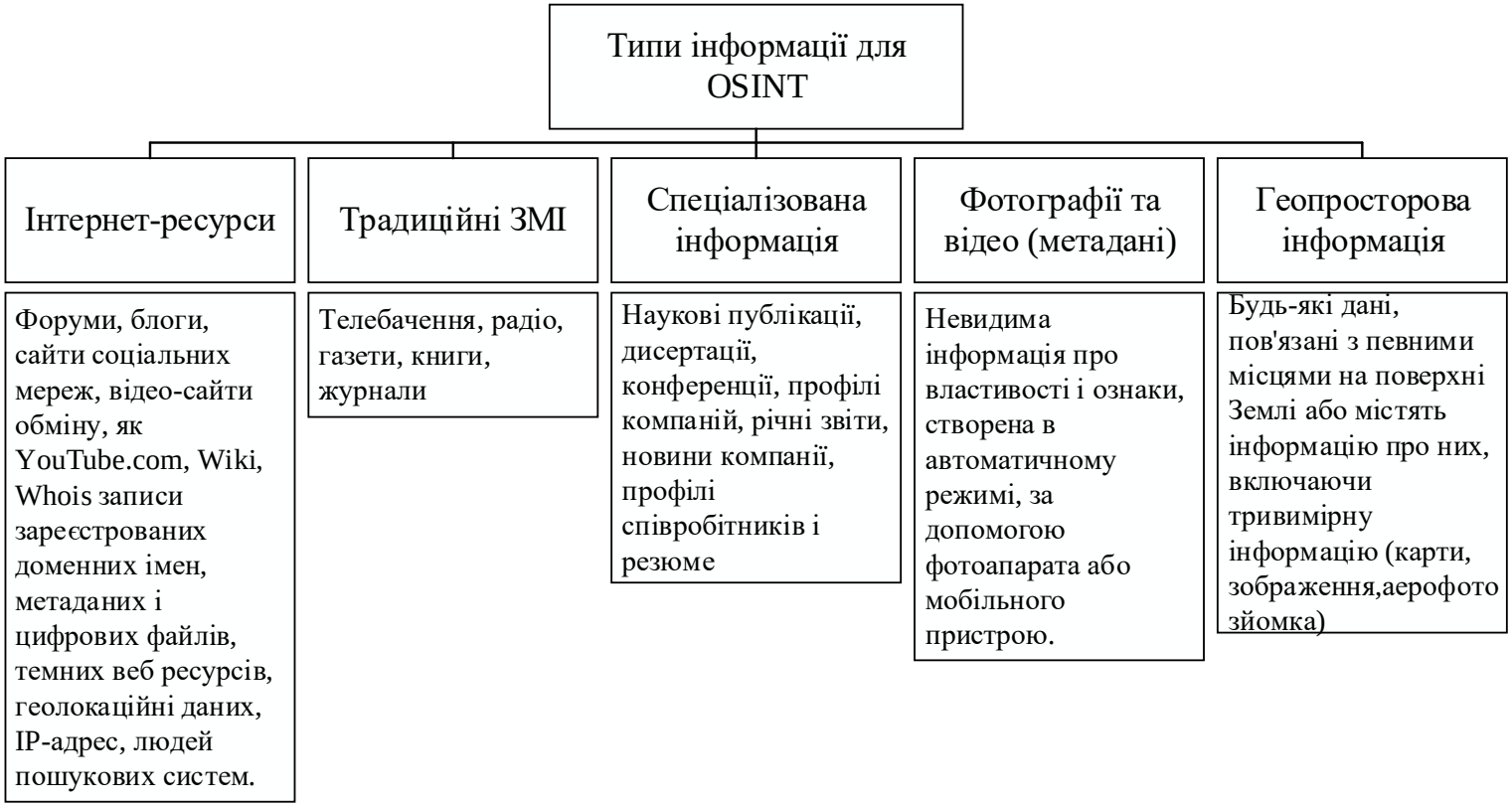

Рисунок 1.28 – Типи джерел OSINT

У сфері кібербезпеки OSINT найчастіше застосовується для збору публічних даних про компанії та користувачів (рис. 1.29).

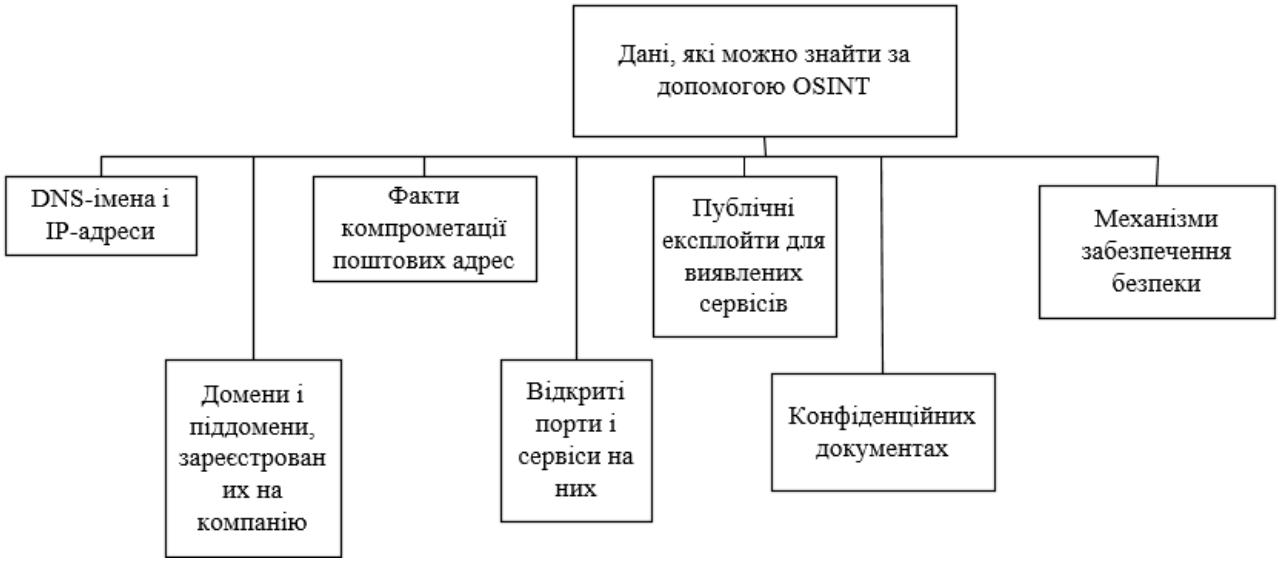

Рисунок 1.29 – Дані, що роскриваються за допомогою OSINT

Технологія дозволяє збирати максимум інформації для повноцінного аналізу. При цьому дані можуть розміщуватися в різних формах: статті, публікації обговорення на форумах і т.д.

Матеріали, складені на основі інформації, підтримують всі методи ведення розвідки шляхом накопичення розвідувальних знань, аналізу та їх поширення. Наступні фактори впливають на процес планування ведення OSINT (рис. 1.30).

У плані діяльності комп'ютерної криміналістики OSINT може застосовуватися при боротьбі з такими явищами (рис. 1.31).

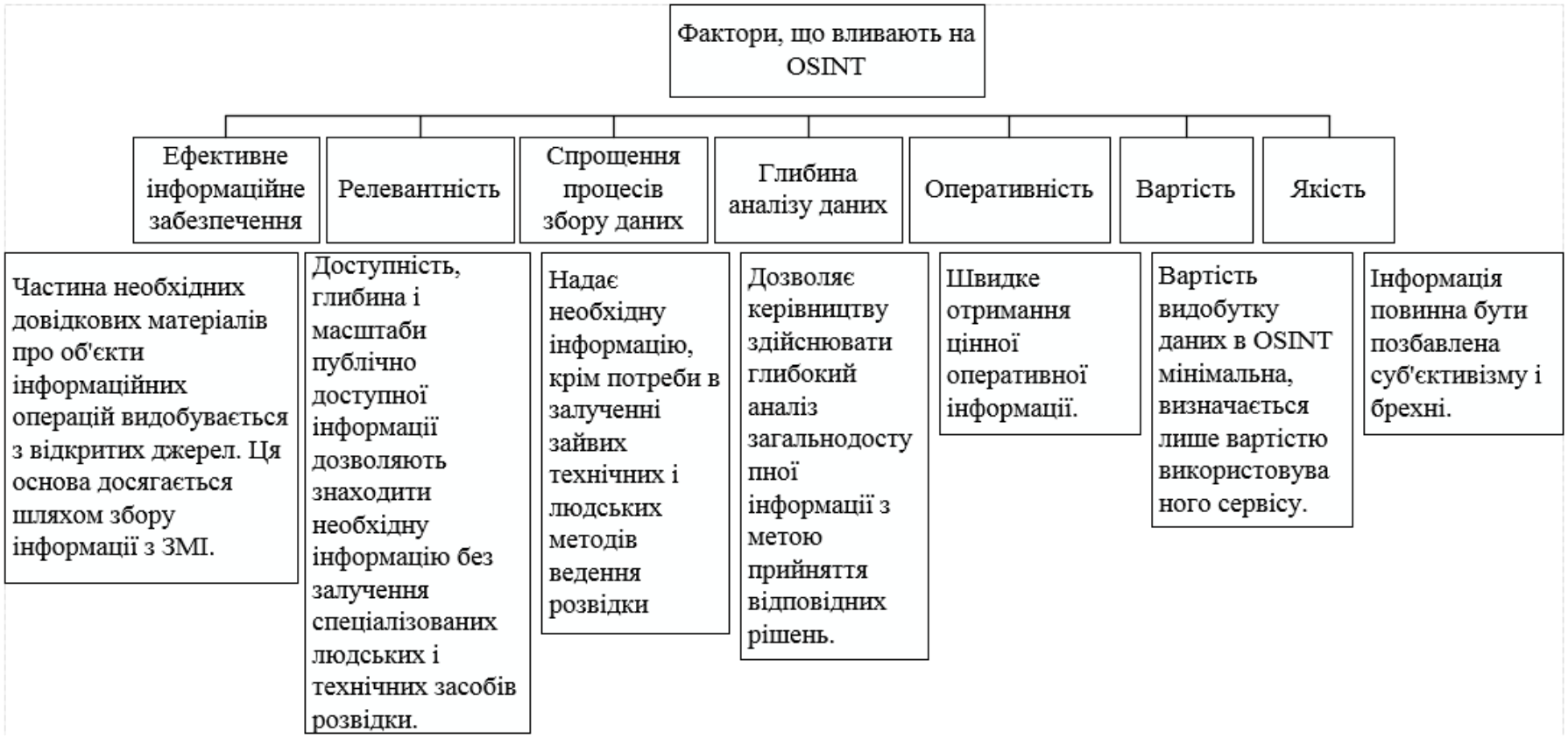

Рисунок 1.30 – Фактори процесу планування OSINT

Рисунок 1.31 – Використання OSINT для боротьби зі злочинністю

Програмні та технологічні засоби OSINT забезпечують (рис. 1.32).

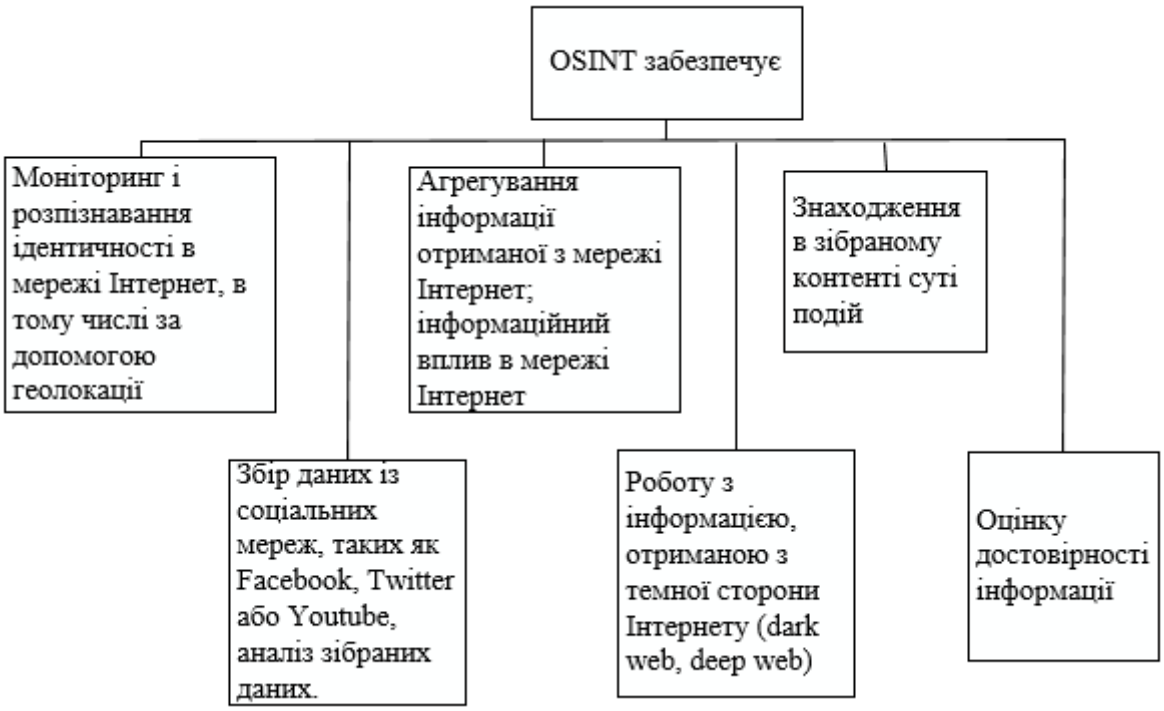

Рисунок 1.32 – Користь розвідки на основі відкритих джерел

Існує безліч варіантів застосування OSINT, з яких можна виділити наступні області (рис. 1.33).

Рисунок 1.33 – Області застосування OSINT

У OSINT основною складністю є визначення релевантних, надійних джерел з величезної кількості загальнодоступної інформації. Процес OSINT складається з чотирьох етапів: планування, підготовки, збору та виробництва кінцевого матеріалу – аналітики і чотирьох основних процесів: аналізу, накопичення розвідданих, оцінки та розподілу за напрямками [13] (рис. 1.34).

Рисунок 1.34 – Збір інформації шляхом OSINT

На рис 1.35 зображені основні інструменти та тип інформації, яку можна знайти за їх допомогою.

1.3 Огляд стадій розслідування інцидентів

Процес розслідування комп'ютерних злочинів, який проводять фахівці та експерти, прийнято ділити на наступні етапи (рис. 1.36).

На етапі оцінки відбувається підготовка до збору даних, що мають відношення до інциденту ІБ. досліджується можливість проведення розслідування, аналізуються застосовні політики і закони, визначається склад групи, яка проводитиме розслідування; вивчається топологія мережі, в якій стався інцидент, визначаються джерела значимої інформації, проводитися попередній перегляд цікавлять носіїв інформації [14].

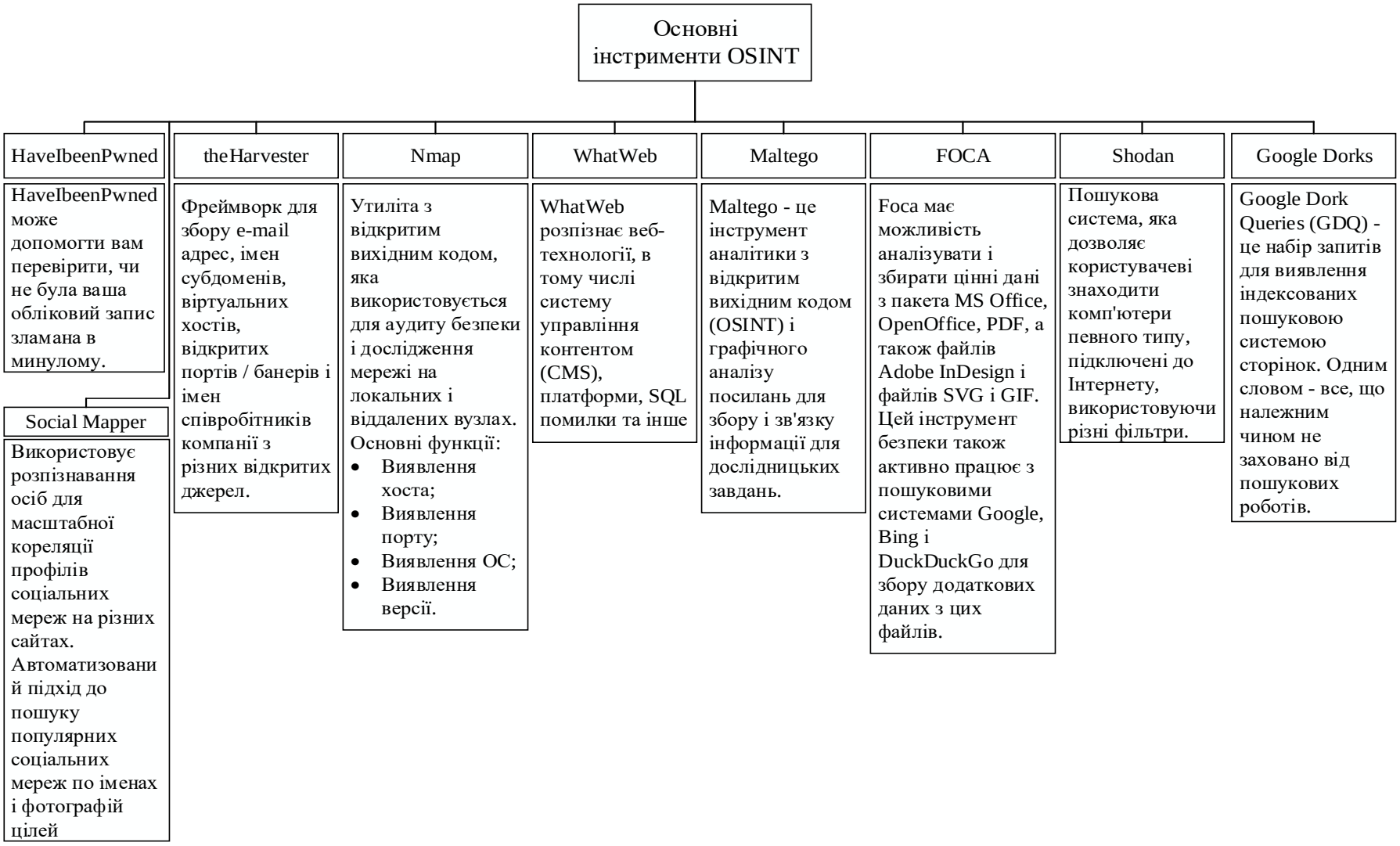

Рисунок 1.35 – Інструменти OSINT

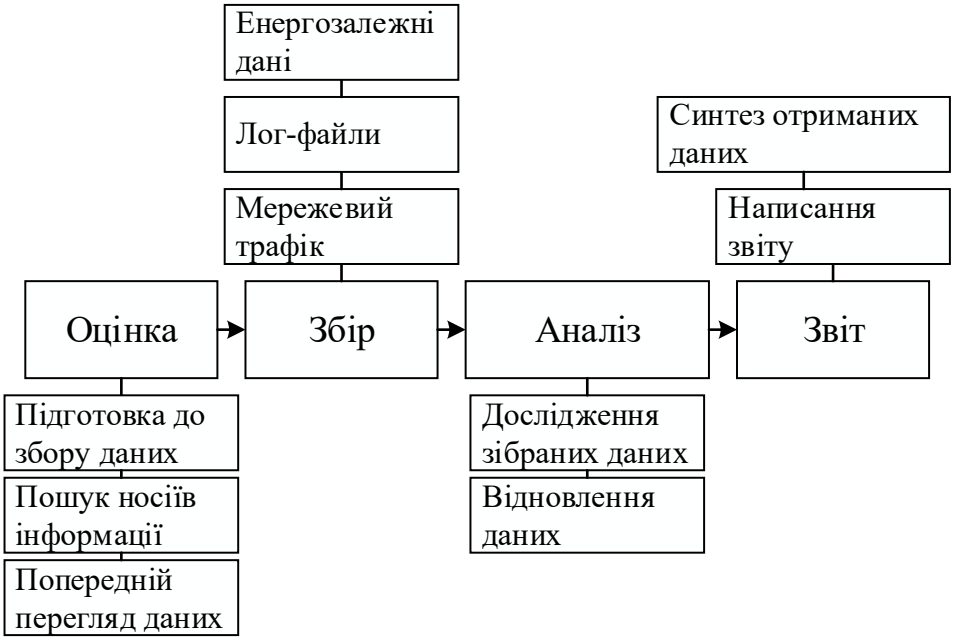

Рисунок 1.36 – Процес розслідування

На цій стадії збору даних збираються всі дані, що мають відношення до інциденту (рис. 1.37).

Рисунок 1.37 – Збір даних після інциденту

Перед тим як творця копію енергонезалежного носія інформації необхідно забезпечити цілісність його вмісту, для цього застосовуються програмні і апаратні блокатори запису (рис. 1.38).

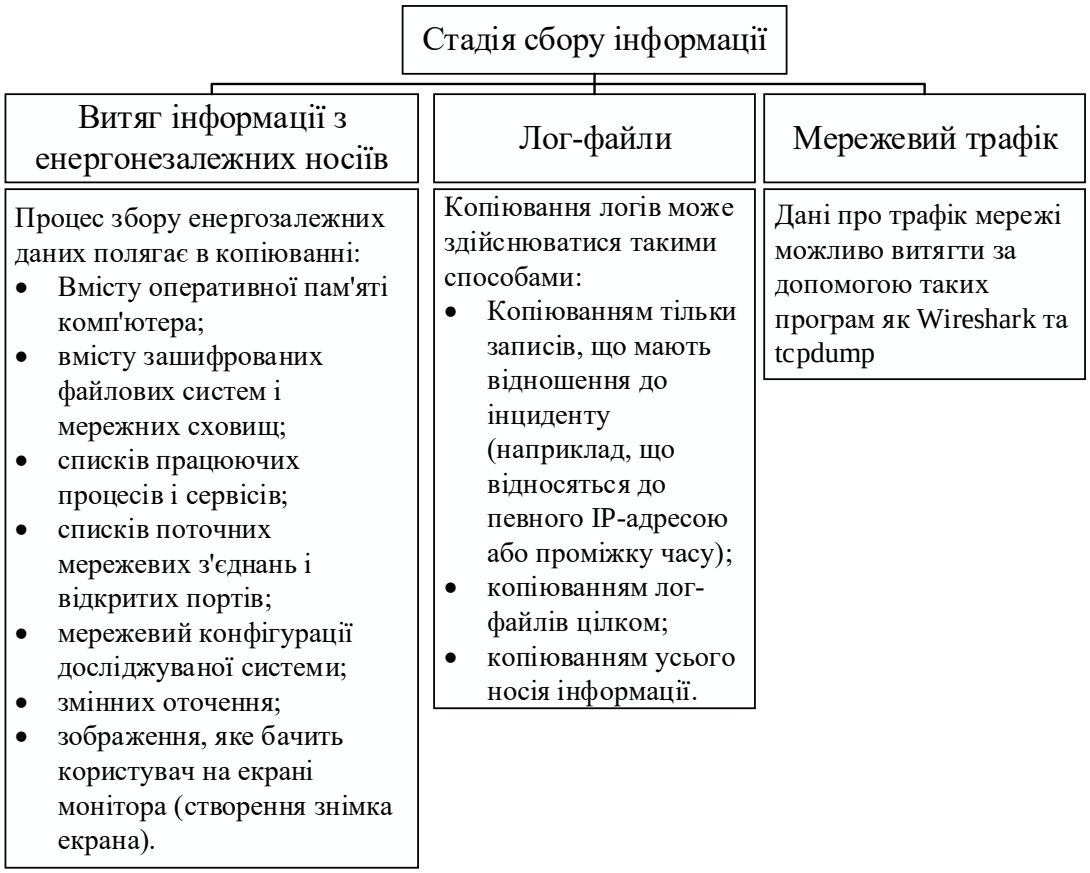

Рисунок 1.38 – Методи вилучення інформації на стадії збору

На етапі аналізу проводиться розбір всіх зібраних даних (рис. 1.39).

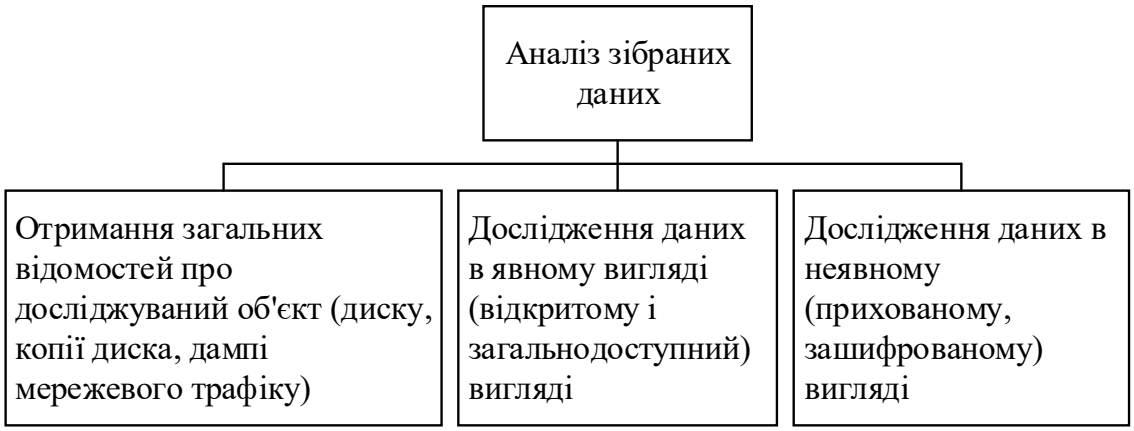

Рисунок 1.39 – Аналіз зібраних даних

Криміналістичний аналіз може виконуватися в статичному (static) і динамічному (live) режимах. Традиційний підхід забезпечує неповні доказові дані, в той час як інструменти аналізу в реальному часі можуть надати слідчим точнішу і послідовну картину поточних і раніше запущених процесів.

Перейдемо до розгляду програмних продуктів комп'ютерної криміналістиці і на основі якої методу аналізу вони реалізовані (табл. 1.1).

Таблиця 1.1 – Інструменти ЦК

Назва інструменту	Підтримувана ОС	Опис	Метод аналізу
EnCase	Windows	Використовується для збору і аналізу дампа пам'яті при цифровий криміналістичної експертизи в статичному режимі.	Статичний
PTK Forensics	LAMP	Це платформа комп'ютерної криміналістики, заснована на інструментах командного рядка.	Обидва методи
OSForensics	Windows	Призначена для пошуку та аналізу різних даних в системі.	Динамічний
WireShark	Window/Linux	Призначений для перехоплення мережевих пакетів.	Обидва методи
X-Way Forensics	Windows	Цей інструмент загального призначення використовується в шістнадцятковому редакторі Win Hex для статичного і динамічного аналізу.	Обидва методи
Tcp flow	Window/Linux	Захоплює дані, що передаються як частина TCP-з'єднань	Динамічний
Digital Forensics Framework	Window/Linux	Здатний виконувати швидкий аналіз диска і швидко мінливої пам'яті	Обидва методи
FTK (Forensic Toolkit)	Windows	Сканує жорсткий диск у пошуках різної інформації	Статичний
Registry Recon	Windows	Інструмент використовується для відновлення реєстрів Windows з будь-якого місця жорсткого диска	Статичний

До інструментів комп'ютерної криміналістики також можна віднести системи виявлення вторгнень. Стадія активного збору інформації злочинцем обов'язково позначиться на продуктивності системи (наприклад nmap може згенерувати додатковий трафік, який буде виявлений детекторами сканування портів) або викликати аномалії в системі.

Існує багато різних видів систем виявлення атак, подібні системи контролюють окремий комп'ютер, збирають і аналізують інформацію з журналів ОС і різних додатків на предмет аномального поведінки. На рис. 1.56 представлена класифікація виявлення вторгнень [16].

1.4 Висновки до розділу 1

У першому розділі було розглянуто сучасний ландшафт кібербезпеки в світі і Україні, варіантах забезпечення КБ розглянули приклади атак в 2019 і 2020-му роках, а також прийшли до висновку, що комп'ютерна криміналістика є невід'ємною частиною процесу забезпечення інформаційної безпеки.

В ході розгляду технік і методів комп'ютерної криміналістики можна прийти до висновку, що не можна розглядати дану тему не зачіпаючи теми протистояння криміналістики, що може допомогти більше зрозуміти потребу в існуванні форензіки.

2 ОГЛЯД ТА АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА ЗАСОБІВ КОНТРФОРЕНЗІКИ

2.1 Поняття контрфорензіки

Використання контрфорензікі не обмежується терористами і злочинцями. Керівники корпорацій теж застосовують їх, використовуючи ці інструменти і методи для приховування або знищення компрометуючих електронних листів, фінансових звітів і так далі. Навіть звичайні додатки, такі як веб-браузери, мають функції, які можна використовувати, щоб утруднити судово-медичну експертизу – наприклад, очистити історію Інтернету. Більшість нових браузерів мають режим «приватного перегляду», в якому не записуються такі речі, як відвідані веб-сайти і пошукові запити [17].

Антіфорензіка є складовою частиною захисту інформації. У всіх сферах, де є конфіденційна інформація, що підлягає захисту, повинні використовуватися методи для запобігання її витоку. Загальна протидія форензиці не спрямована на конкретний метод або засіб криміналістичного дослідження та реалізується засобами подвійного призначення (програмами для створення зашифрованих файлових систем і шифрування мережевого трафіку). Основне завдання даного виду протидії: захистити дані від криміналістичного дослідження шляхом їх знищення, шифрування або приховування (рис. 2.1).

Анти-криміналістика зазвичай розглядається з точки зору цифрових доказів. Чотири основні типи загроз для цифрових доказів – це збереження даних, підробка даних, приховування даних і знищення даних.

Основні цілі анти-криміналістичної експертизи (рис. 2.2).

Кіберзлочинці використовують безліч способів, щоб приховати інформацію і свої цифрові сліди. Наприклад, змінюють формат файлу.

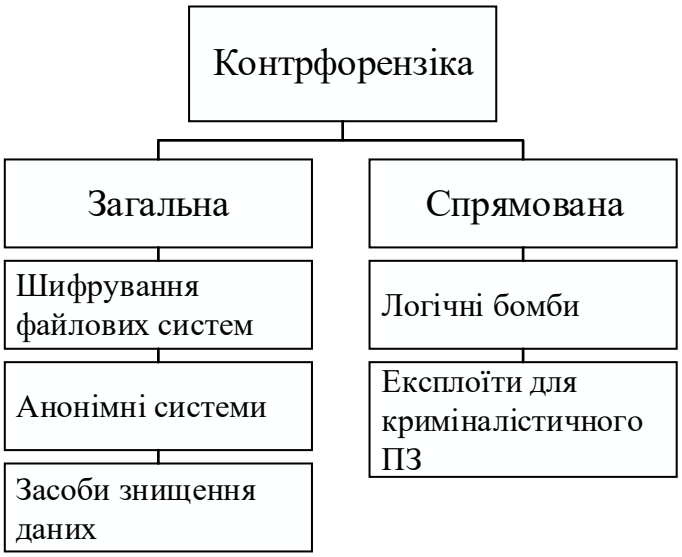

Рисунок 2.1 – Види дії контрфорензіки

Рисунок 2.2 – Цілі експертизи

Дослідник, зосереджений на певному форматі файлу, може пропустити важливі докази. Згідно з іншим методом зловмисники можуть використовувати вільний простір, тобто простір, який файлу, щоб приховати важливі розділи файлу. Поділ файлу на більш дрібні розділи і приховування інформації в резервному просторі ускладнює вилучення даних та складання даних.

В даний час комп'ютерні злочинці знайомі з методами та прийомами комп'ютерної криміналістики і намагаються використовувати методи протидії, щоб ефективно перешкоджати процесам розслідування.

2.2 Класифікація антифорензіки

В Інтернеті існує безліч способів захисту від судової експертизи, що дозволяють приховати цифрову діяльність людини. Деякі з цих методів є базовими, а деякі вимагають гарної технічної підготовки. Передові методи навмисно використовуються «чорними капелюхами», щоб перешкодити кіберрозвідку. Виділяють наступну класифікацію технік АФ (рис. 2.3).

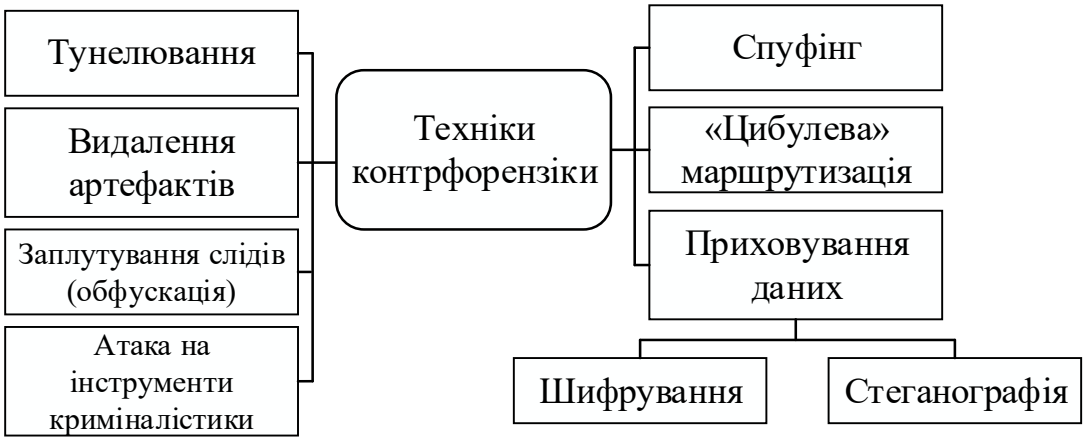

Рисунок 2.3 – Класифікація технік АФ

Розглянемо кожну з технік більш детально.

Приховування даних

Техніки приховування варіюються від простих до дуже складних. Зміна імен та розширень файлів, приховування файлів глибоко в непов'язаних каталогами, приховування файлів всередині файлів і шифрування. Використовуються для визначення наявності даних в сховищі, що робить аналіз і вивчення цифрових доказів судово-медичними експертами скрутним або неможливим. Перевага приховування даних полягає в тому, щоб підтримувати їх доступність, коли це

необхідно. Незалежно від операційної системи, використання фізичного диска для приховування даних є широко використовуваним методом, але методи, пов'язані з використовуваної ОС або файлової системою, досить поширені.

Класичні техніки включають в себе стеганографію, шифрування даних, маніпуляції з файлової системою, маніпуляції з жорстким диском і мережеве приховування даних.

Стеганографія – це спосіб приховувати приховане повідомлення в звичайному повідомленні, але не факт, що дві сторони спілкуються один з одним [18]. Готовий стего-файл складається з двох файлів. Файл, що містить секретну повідомлення, називається файлом-носієм. Файли-носії можуть бути файлами зображень, відеофайлами, аудіофайлами і документами обробки тексту. Секретне повідомлення може бути вбудовано в файли кількох типів, такі як PDF, відео, аудіо, зображення і текст. Виявити стеганографічну атаку складно, але повторювані шаблони можуть розкрити секретне повідомлення досліднику (рис. 2.4).

Рисунок 2.4 – Класифікація цифрової стеганографії за типом файлу

На відміну від стеганографії, криптографія використовується для подальшого шифрування, а не для приховування. Дані видно, але без непридатні для використання.

Основною метою шифрування є запобігання несанкціонованого доступу до конфіденційних файлів або даних. Зашифровані дані можна розшифрувати тільки за допомогою парного ключа. Це один з традиційних методів захисту даних. Злочинці використовують шифрування, щоб утруднити судове розслідування. За допомогою даного способу присутність даних не ховається від дослідників, але їх

читаність стає неможливою. Комп'ютерні злочинці зазвичай використовують два типи шифрування, що зображені на рис. 2.5.

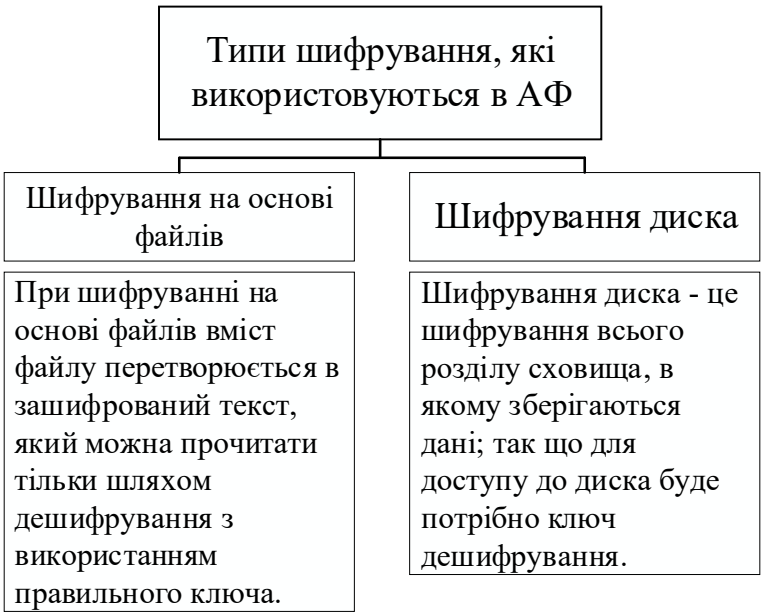

Рисунок 2.5 – Типи шифрування в АФ

При використанні фізичного диска для приховування даних ці методи стають можливими завдяки деяких опцій, реалізованим під час їх виробництва, які призначені для полегшення їх сумісності і їх поширення, в той час як інші методи приховування використовують властивість управління даними операційної системи і / або файлова система. Розглянемо методи приховування інформації за допомогою дискового простору [19] (рис. 2.6).

Для кращого розташування файлів на дисковому просторі, представлена візуалізація (рис 2.7).

Видалення артефактів

Після видалення файлу або папки з запам'ятовуючого пристрою, фактичні дані залишаються на пристрої до тих пір, поки вони не будуть перезаписані новими даними. Видалення артефактів вважається методом АФ, призначеним для повного стирання і знищення даних. Очищення артефактів може застосовуватися до файлів, всьому диску або розділу (рис. 2.8).

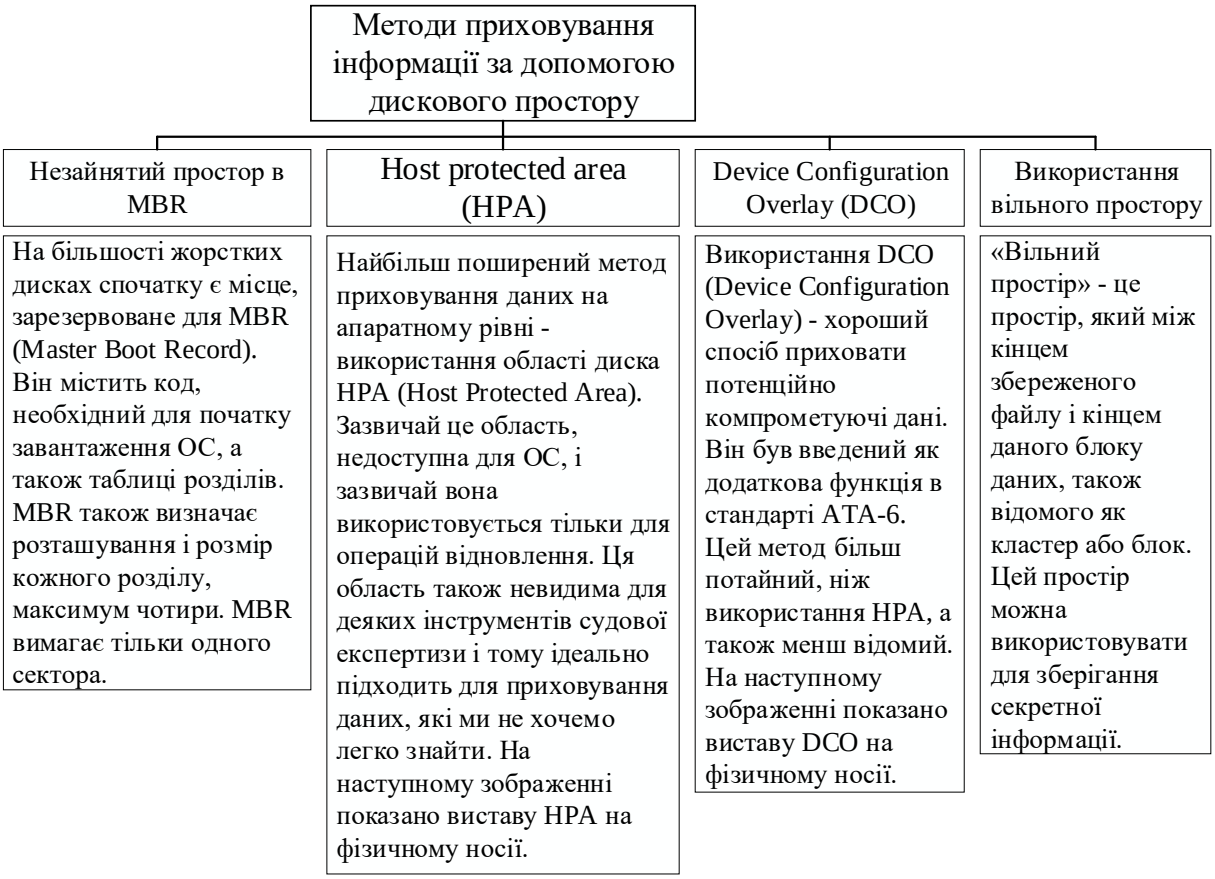

Рисунок 2.6 – Методи приховування інформації на дискі

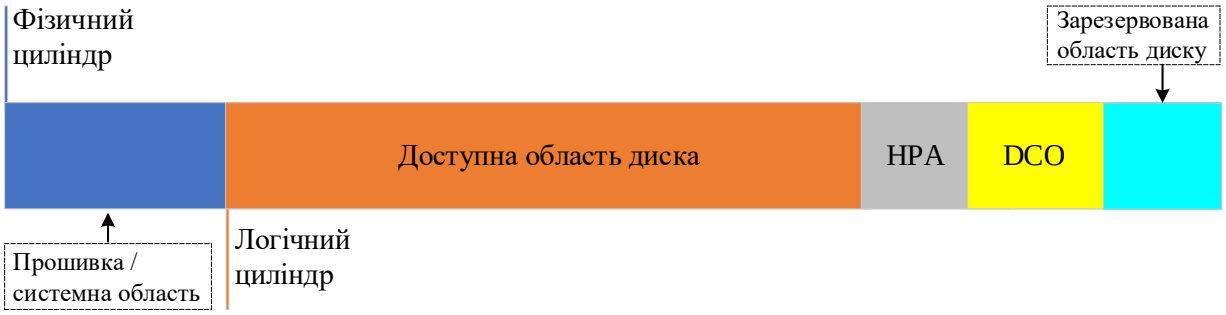

Рисунок 2.7 – Візуалізація дискового простору

Метадані відносяться до даних, які надають інформацію про інших даних. Для кожного файлу є набір пов'язаних з ним метаданих. Через свого описового характеру метадані дуже важливі для розуміння файлу. До інших прикладів метаданих файлу відносяться: його тип, розмір, автор і дата створення або зміни. Створення метаданих може бути ручним або автоматичним (рис. 2.8).

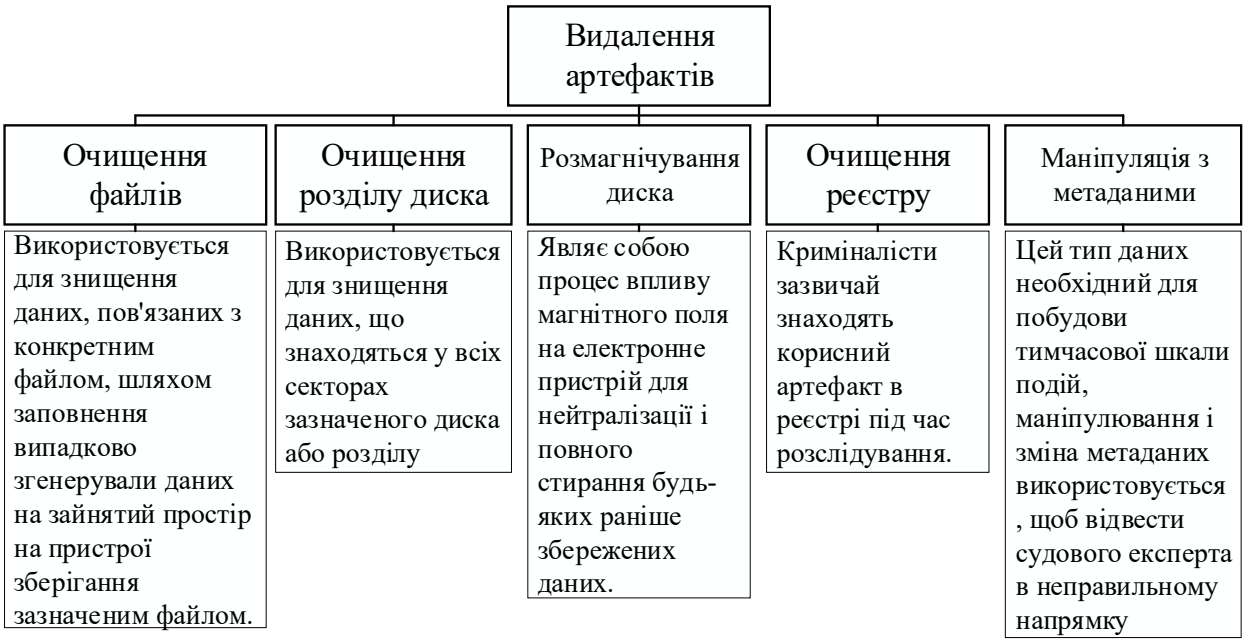

Рисунок 2.8 – Типи видалення артефактів

Ручне створення зазвичай буває більш точним, оскільки користувач може вводити будь-які дані, які він вважає важливими. Автоматизовані метадані зазвичай обмежуються кількома елементами – розмір файлу і час його модифікації, доступу і створення (MAC) (рис. 2.9).

Заплутування слідів (обфускація)

Метод, що утруднює розуміння повідомлення за допомогою використання двозначної мови, відомий як обфускація. Цей метод використовує жаргон і внутрішньо групові фрази для спілкування. Це могло бути навмисно і ненавмисно. Основна мета обфускації – зниження ризику впливу. Цього можна було досягти декількома способами (рис. 2.10).

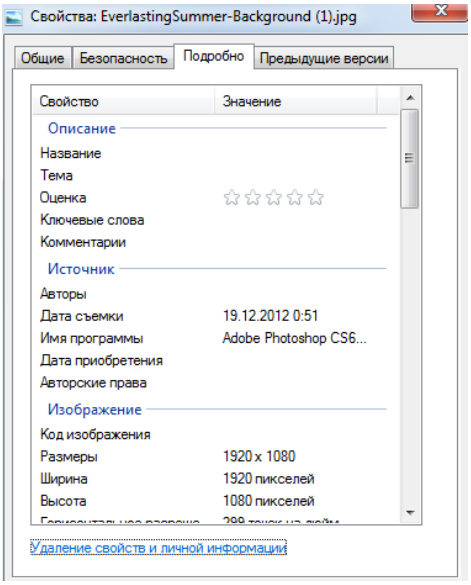

Рисунок 2.9 – Приклад перегляду метаданих за допомогою стандартних інструментів Windows

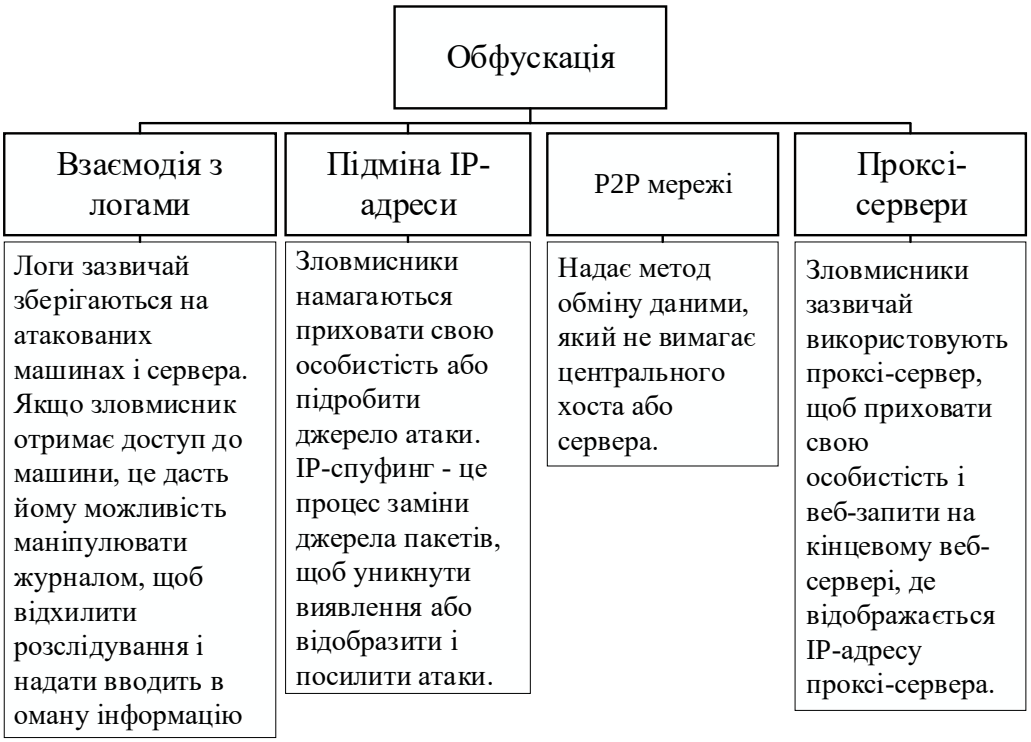

Рисунок 2.10 – Процес обфускації

«Цибулева» маршрутизація

Одним із способів, який може використовуватися в цілях протидії експертизі, а також в законних цілях для збереження конфіденційності та анонімності при роботі в Інтернеті, є TOR (Цибулевий маршрутизатор). TOR – це мережа віртуальних тунелів – відкрита та безкоштовна мережа, яка допомагає в боротьбі з так званим «аналізом трафіку».

Цибулева маршрутизація включає в себе відправку повідомлень, зашифрованими шарами. Кожне з цих повідомлень зашифровано, і до нього додається новий заголовок, цей новий заголовок має наступну адресу призначення цибулевого маршрутизатора в мережі, а також джерело наступного цибулевого маршрутизатора в мережі [20]. Шифрування повідомлень гарантує, що повідомлення буде доставлено адресату анонімно. Експерти-криміналісти в основному використовують зворотну маршрутизацію для дешифрування повідомлення, що саме по собі займає дуже багато часу. Це означає, що при обмежених ресурсах важливі докази можуть бути втрачені в разі, якщо зворотна маршрутизація неможлива (рис. 2.11).

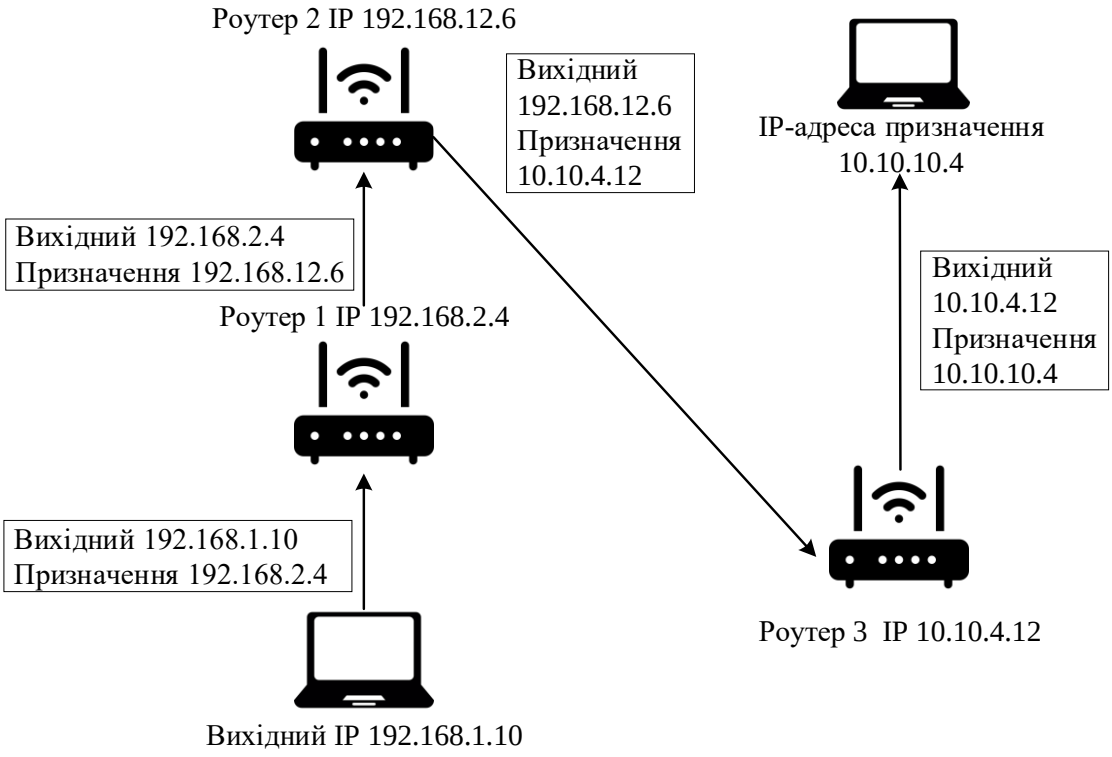

Рисунок 2.11 – Влаштування «цибулевої» маршрутизації

Спуфінг

Акт маскування зв'язку з метою отримання доступу до неавторизованих системам або даними. Спуфінга може здійснюватися через електронну пошту, телефонні дзвінки і веб-сайти. Спуфінг включає в себе маскування зв'язку з метою отримання доступу до системи без відповідних прав користувача. справжнього зловмисника під час судового розслідування.

Три найпоширеніші способи підробки (рис. 2.12).

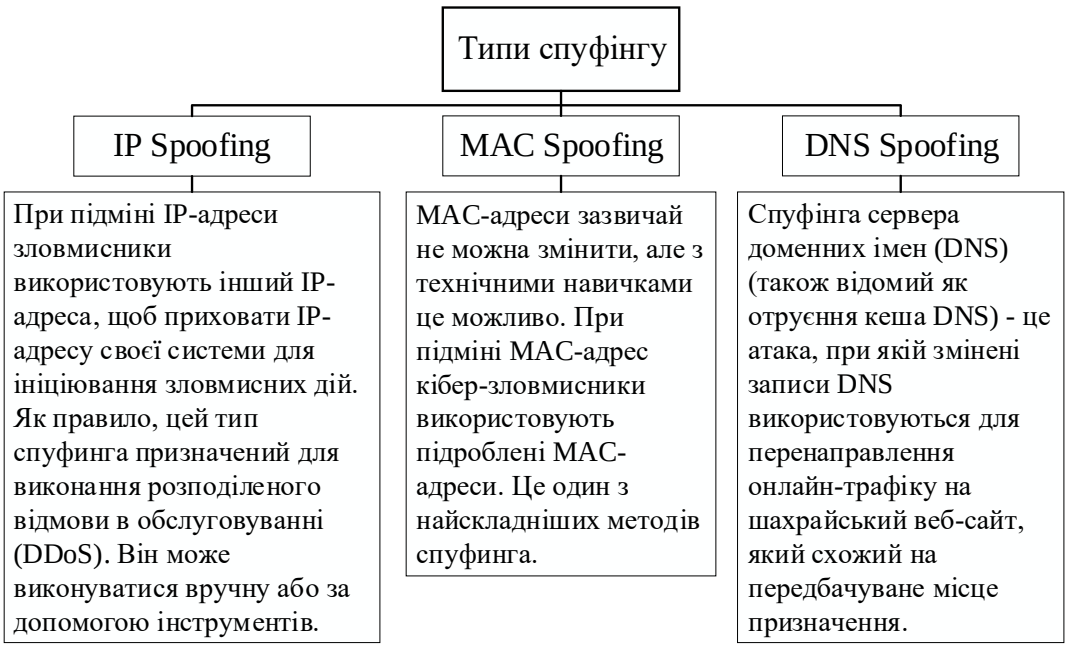

Рисунок 2.12 – Типи спуфінгу

Зловмисник відправляє пакет з IP і MAC-адресами авторизованого DHCP-клієнта на DHCP-сервер. Сервер DHCP вважає зловмисника авторизованим клієнтом DHCP і дізнається його IP і MAC-адреси. Однак авторизований DHCP-клієнт не може отримати послуги від DHCP-сервера, як показано на рис 2.13.

Способи проведення атаки з підміною DNS включають такі елементи (рис. 2.14).

Тунелювання

Цей метод використовує інкапсуляцію, що дозволяє обмінюватися приватними повідомленнями через загальнодоступну мережу. Пакети даних будуть надходити із загальнодоступних мереж, що не викликає підозр. Один з поширених способів – використовувати віртуальну приватну мережу (VPN), яка шифрує дані з міркувань безпеки (рис. 2.15).

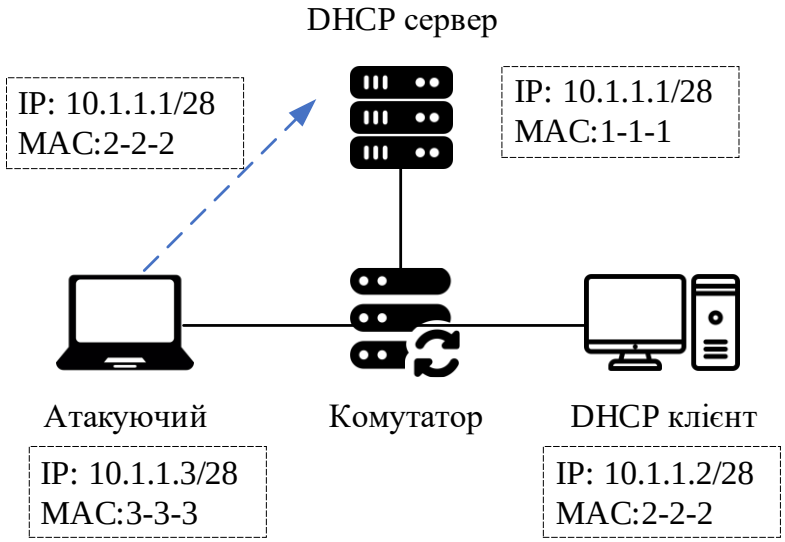

Рисунок 2.13 – Атака з підміною IP / MAC

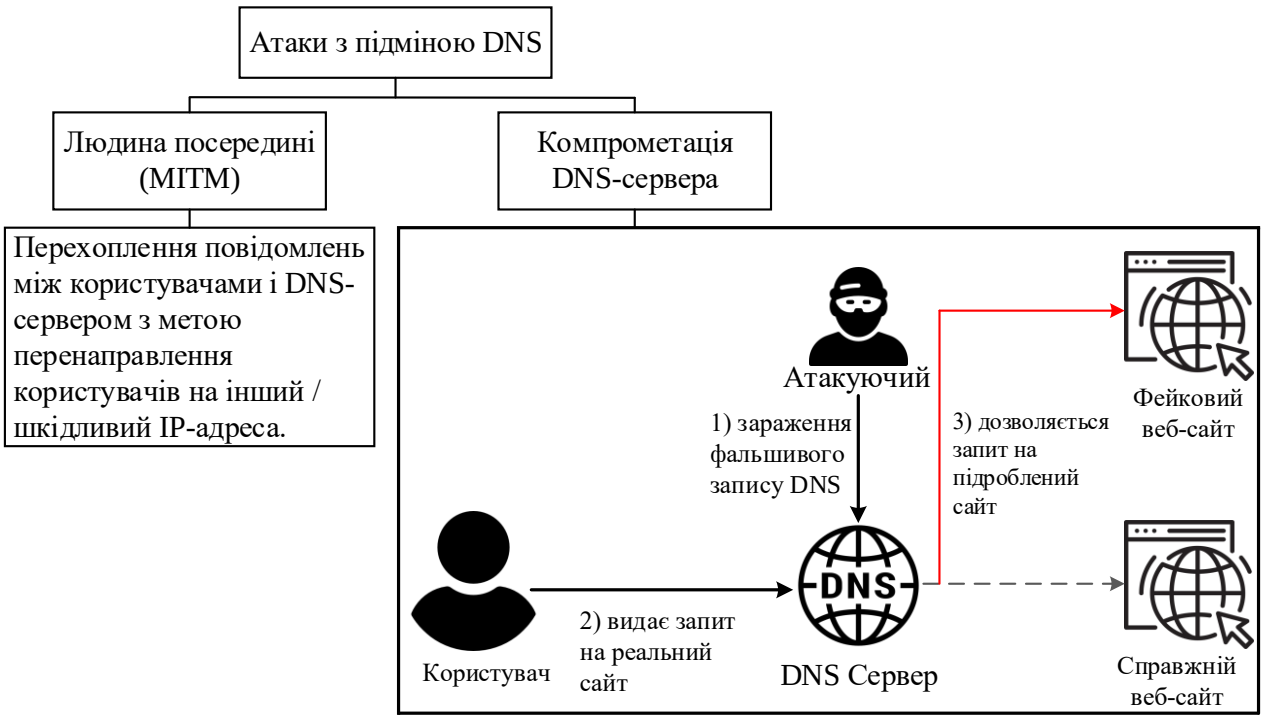

Рисунок 2.14 – Атаки з підміною DNS

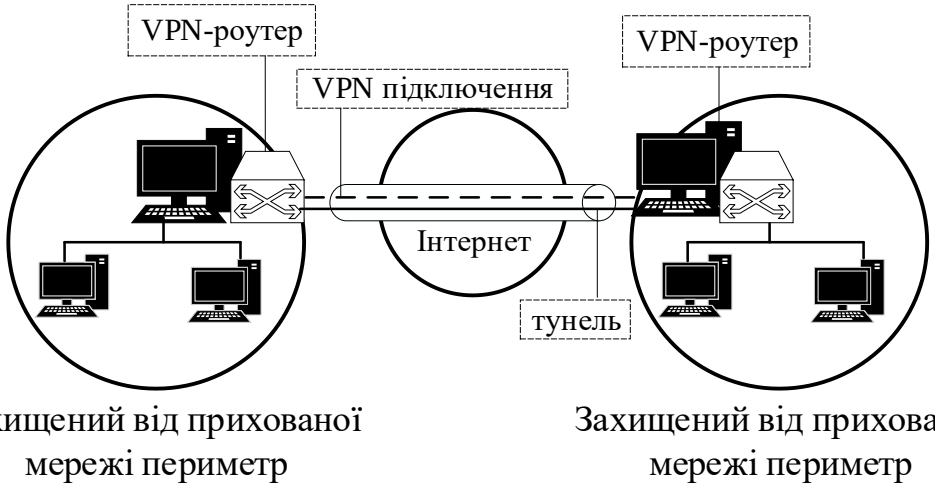

Рисунок 2.15 – Тунелювання

Атака на інструменти криміналістики

Атаки на інструменти криміналістики використовуються для того, щоб ввести в оману або відвернути експерта від отримання правильної інформації. Цей метод включає в себе атаки і засоби обману, використовувані в цифрових криміналістичних дослідженнях, щоб приховати дії, зміни деяких системних значень на комп'ютері і т.д. Його можна проводити за допомогою безлічі інструментів, деякі з яких використовуються для мінімізації займаної площі або для того, щоб зробити зворотне проектування неможливим. У деяких випадках злочинці можуть піти ще далі, намагаючись підірвати довіру до слідчих сторонам.

Один із способів – використовувати інструменти, що видаляють всі сліди активності користувача на комп'ютері, в прикладних програмах та в Інтернеті. ПЗ як засіб усунення доказів повністю видаляють всі сліди активності користувача, такі як історію переглядів, кеш-пам'ять, вільний і не розподілений дисковий простір, це запобігає виявлення цих дій. Часто на практиці використовуються інструменти для зміни системної дати і часу створення, модифікації, доступу та оновлення файлів в системі NTFS (рис. 2.16).

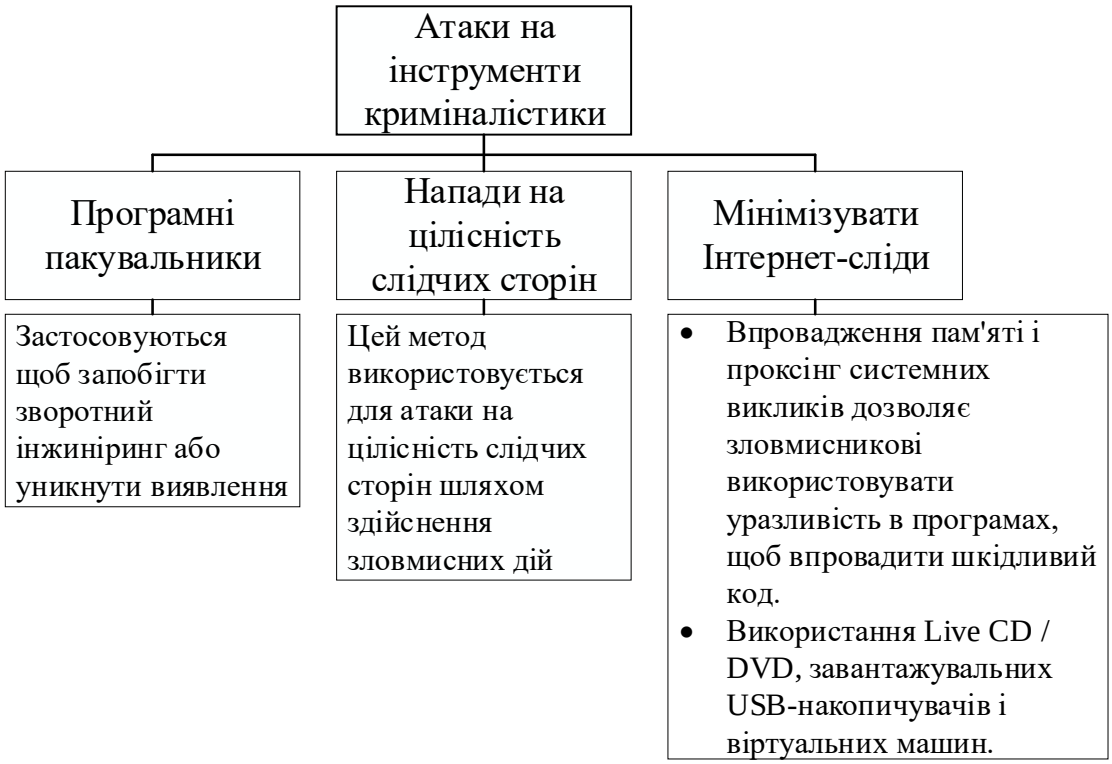

Рисунок 2.16 – Типи атак на інструменти АФ

Методи протистояння криміналістиці, що використовують помилки криміналістичних інструментів

Якщо у зловмисника є доступ до комп'ютерних інструментів судової експертизи або знання того, як цей інструмент працює, зловмисник може створити дані, які будуть виявляти помилки в цих інструментах.

У міру того як комп'ютерна криміналістика стає все більш зрозумілою, були розроблені різні інструменти і методи для приховування доказів, видалення артефактів або обмеження судово-медичної експертизи. Інструменти, включають можливість судового видалення інтернет-історій, щоб організації не могли встановити неправомірне використання, а також можливість змінювати часові мітки, щоб встановити хронологію інциденту було неможливо.

Злочинці, які вчиняють комп'ютерні злочини, використовують технологічні досягнення для розгортання витончених і індивідуальних стратегій, щоб приховати докази від судової експертизи.

Методи, які використовуються для заплутування і приховування фактів від слідчих, називаються стратегіями або методами протидії судову експертизу. Другий етап після забезпечення безпеки джерела даних – це ідентифікація і вилучення даних судової експертизи, які можуть мати відношення до розслідування. Відмінною стратегією, яка використовується на цьому етапі, є приховування даних. Ця стратегія передбачає приховування будь-яких відповідних даних судово-медичної експертизи, які можуть бути використані слідчими для розкриття злочину. Для приховування даних зазвичай використовуються три методи: шифрування, стеганографія і заплутування слідів [21] (рис. 2.17).

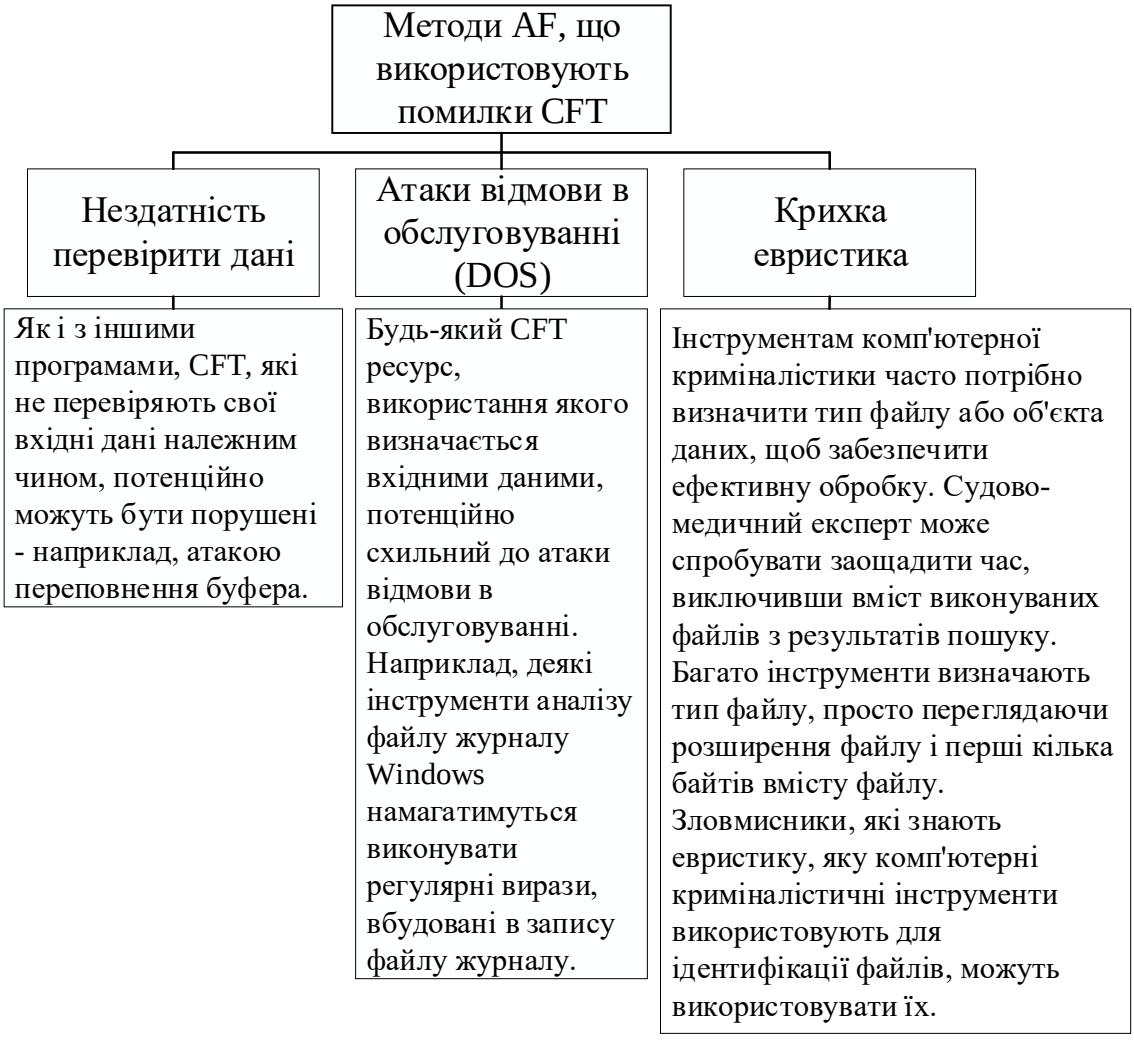

Рисунок 2.17 – Методи АФ, що використовують помилки CFT

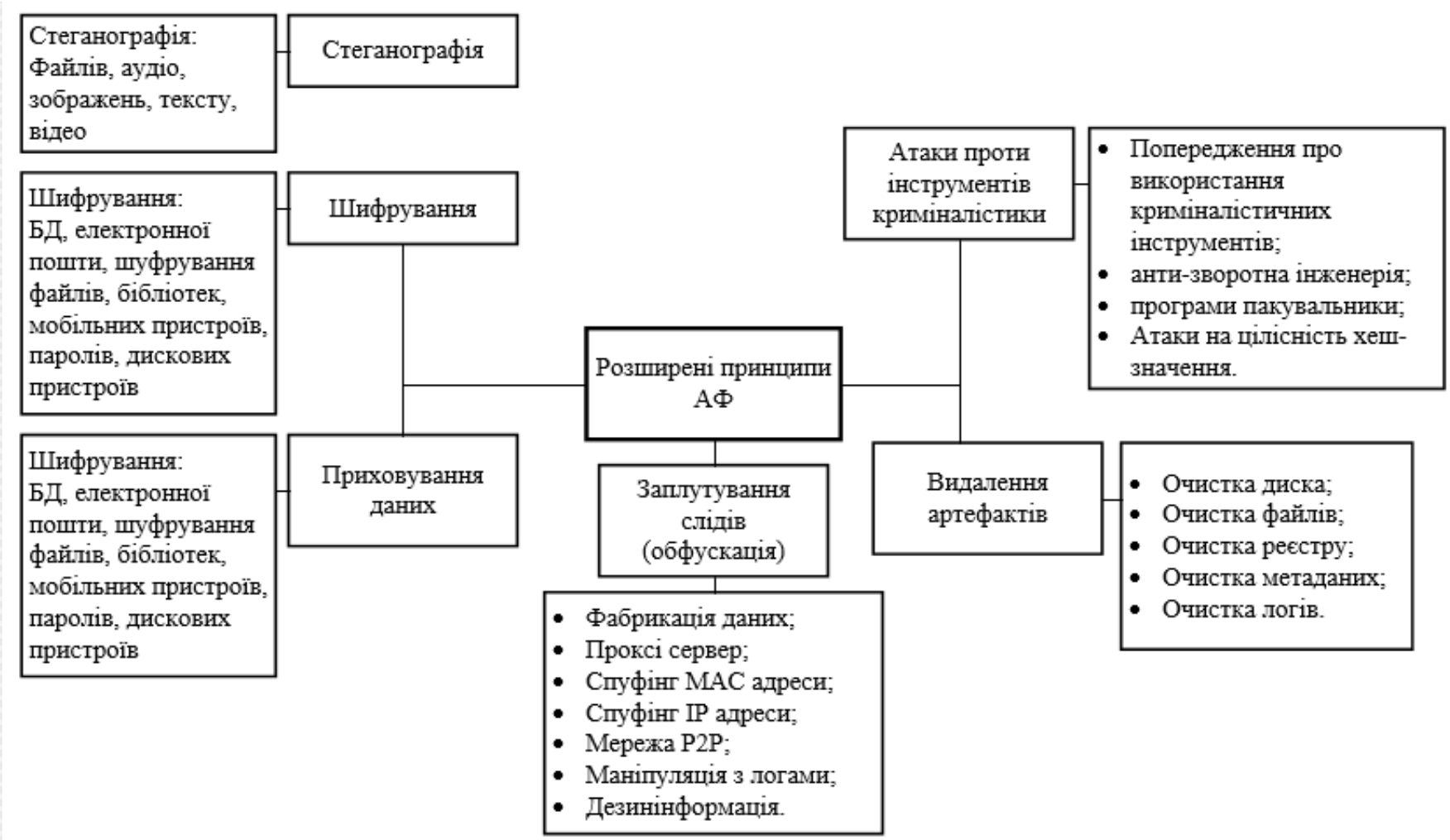

Рисунок 2.18 – Розширені принципи АФ

2.3 Огляд сучасних інструментів АФ

Інструменти шифрування даних можна розділити на: шифрування диска, шифрування файлів, шифрування даних, стеганографії, електронну пошту і мережевий транспорт. Дотримуючись класифікації, яка була вказана в минулому підрозділі, інструменти протистояння комп'ютерної криміналістики необхідно розбити на зазначені пункти.

2.3.1 Приховування даних

Методи і інструменти приховування даних використовують файлову систему, пам'ять або мережеві можливості операційної системи для приховування цифрових даних. Також до шифрування даних можна віднести системи поділу секрету, завдання якої має на увазі під собою поділ секретної інформації між учасниками так, що тільки заздалегідь задані безлічі учасників зможуть її відновити, слідчо, ймовірність компрометації цієї інформації знижується. Інструменти приховування, стеганографія і шифрування тісно пов'язані. Однак приховування даних – це більш широке поняття, а стеганографія, руткіти, шифрування – це спеціалізовані методи приховування.

1. Інструменти приховування даних файлової системи

Використання Live CD, USB завантажувачів та віртуальних машин

Live CD, завантажувальні USB-токени і віртуальні машини дають зловмисникам інструмент для запуска програм за їх вибором, одночасно стримуючи поширення критично корисної інформації в системі зловмисника (рис. 2.19).

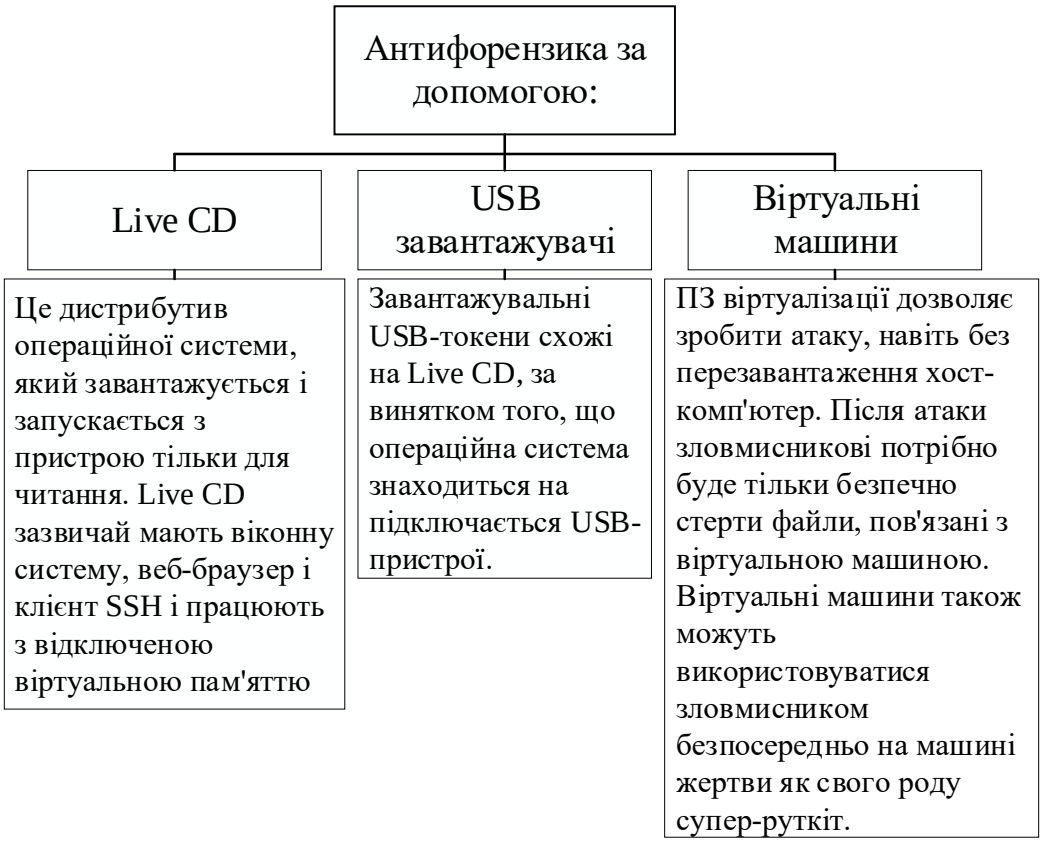

Рисунок 2.19 – Живі компакт-диски, завантажувальні USB-токени і віртуальні машини

Використання Live CD або віртуальних дає можливість отримати одноразовий образ дискового пристрою, що запам'ятовує. Хоча це не може забезпечити довгострокове рішення для приховування даних від дослідника, тим не менш, це дозволяє швидко заховати додатки і файли.

2. Інструменти приховування даних в пам'яті (Live Hiding)

Дана техніка приховування інформації схожа на методи фізичної стеганографії, коли інформація приховується в фізичні об'єкти (рис. 2.20).

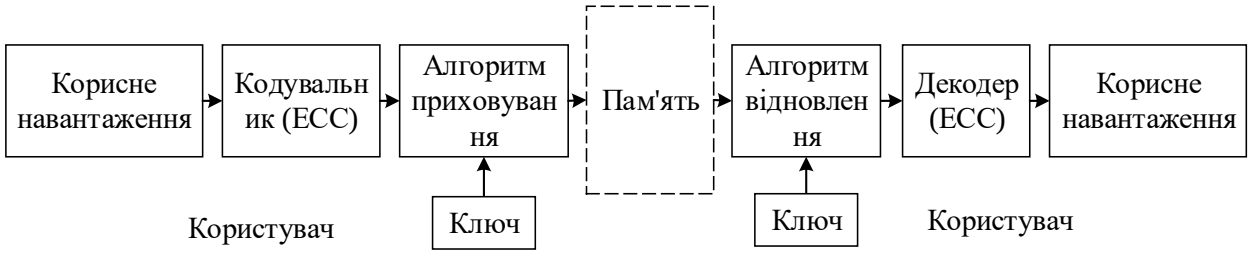

Рисунок 2.20 – Огляд операції приховування інформації.

VeraCrypt

VeraCrypt, вдосконалений інструмент шифрування TrueCrypt, працює на всіх основних комп'ютерних ОС (Windows, Linux і Mac OS) [22]. Інструмент підтримує безліч механізмів шифруван (рис. 2.21).

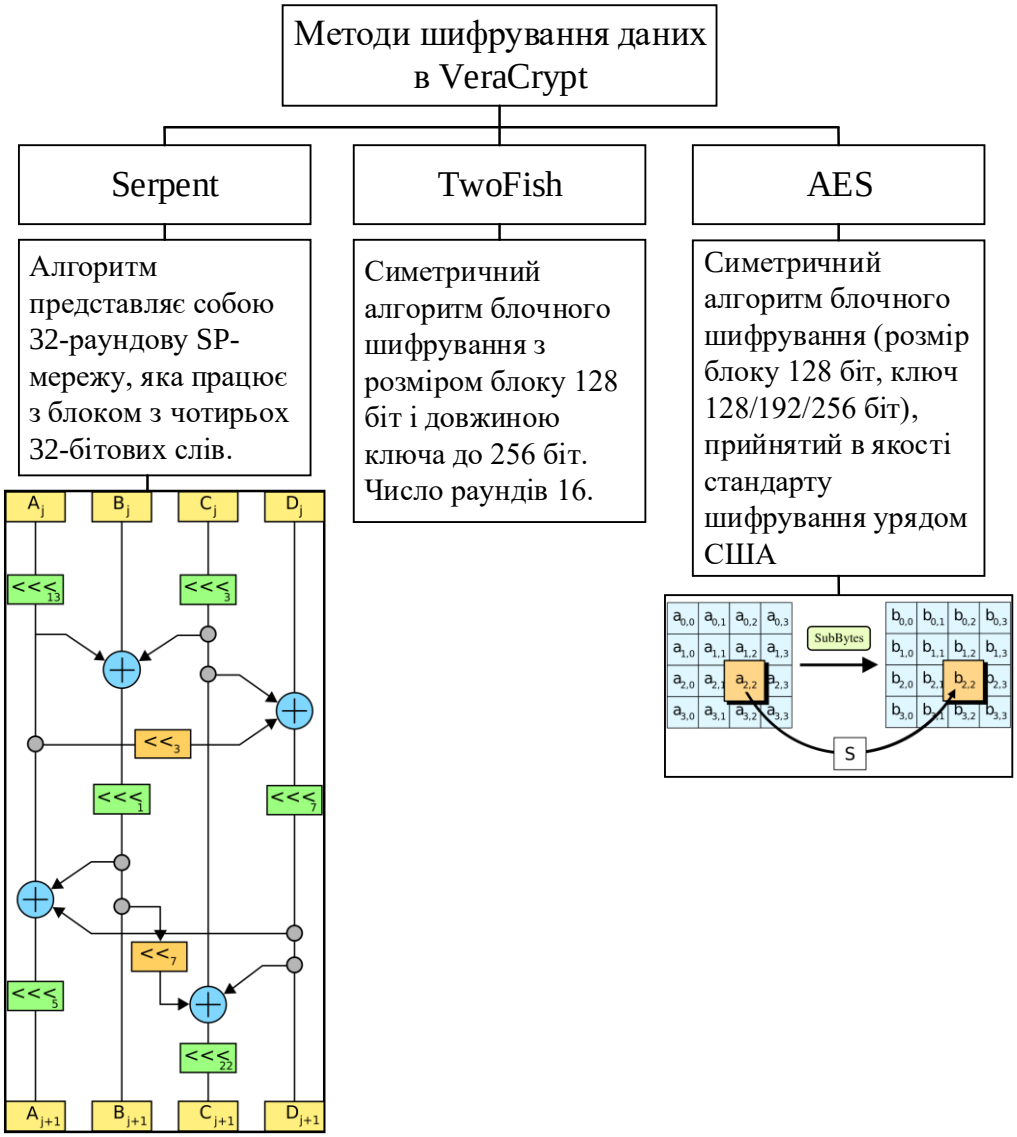

Рисунок 2.21 – Методи шифрування в VeraCrypt

VeraCrypt також забезпечує створення прихованих і зашифрованих томів всередині інших існуючих томів (рис. 2.22).

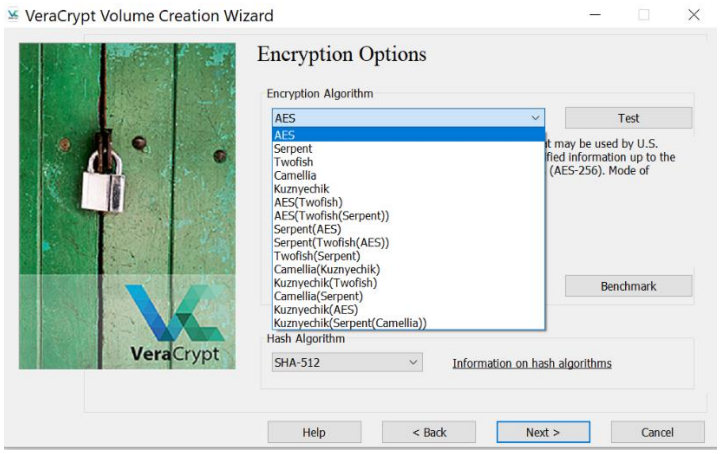

Рисунок 2.22 – Вибір методи шифрування в програмі

VeraCrypt частково є програмним забезпеченням з відкритим вихідним кодом, а його коди відкриті для огляду і вивчення. Інструмент знаходиться в постійному розвитку, при цьому кожен етап розробки перевіряється і тестується для підвищення його ефективності.

AxCrypt

AxCrypt – це інструмент для шифрування файлів призначений для Windows. Даний інструмент відрізняється простотою і зручністю у використанні. Він ефективно інтегрується з провідником Windows, тому користувач може просто натиснути файл правою кнопкою миші і вибрати зашифрувати в спадному меню (рис. 2.23).

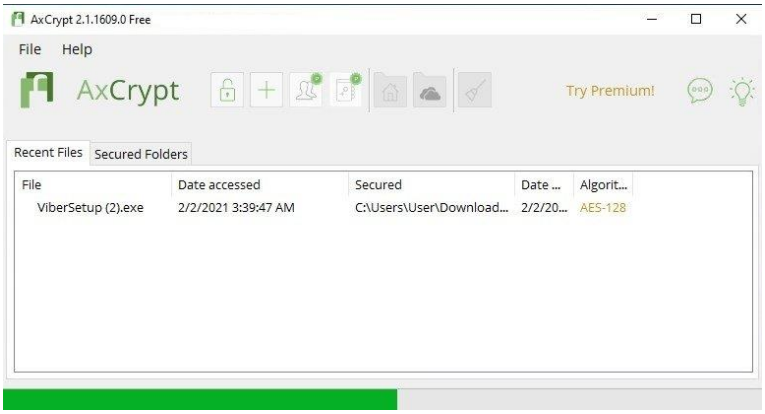

Рисунок 2.23 – Інтерфейс AxCrypt

Серед потужних функцій AxCrypt – те, що називається «синхронізоване шифрування», з цієї преміальної функцією користувач може зашифрувати файл протягом певного періоду часу, і файл буде автоматично розшифрований у встановлений час, або встановивши файл при передачі, щоб автоматично розшифрувати, як тільки він досягне передбачуваного одержувача.

Файл, зашифрований AxCrypt, можна розшифрувати, коли це необхідно або коли він використовується; а потім повторно зашифрувати себе після того, як користувач вийде з нього. AxCrypt дозволяє вибирати і спільне шифрування декількох файлів. Серед переваг цих інструментів: він підтримує як 128-бітове, так і 256-бітове шифрування AES, пропонує механізми захисту від грубої сили (рис. 2.24).

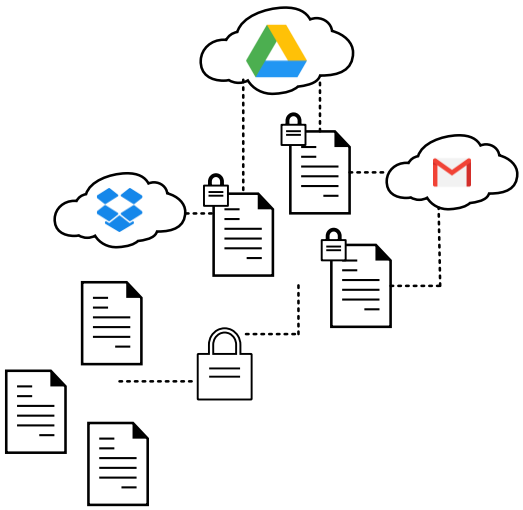

Рисунок 2.24 – AxCrypt використовує пароль для перетворення документів і плиток в надійно зашифровані файли, які можна безпечно зберігати і передавати в хмарі

BitLocker

Bitlocker – інструмент для шифрування всього диска, що входить у версії Microsoft Windows, починаючи з Windows Vista. Інструмент забезпечує захист

даних за рахунок шифрування всього обсягу сховища. За замовчуванням BitLocker використовує механізм шифрування AES. Даний інструмент шифрування, можна також використовувати для шифрування розділів або віртуальних дисків. Серед режимів аутентифікації підтримка інструменту включає: стандартний пароль та ПІН-коди, USB-ключ і Trusted Platform Module (апаратний механізм шифрування, що використовує криптографічні ключі).

Архітектура шифрування BitLocker забезпечує керовані і функціональні механізми, як в режимі ядра, так і в призначеному для користувача режимі. До основних компонентів BitLocker відносять наведені на рис. 2.25.

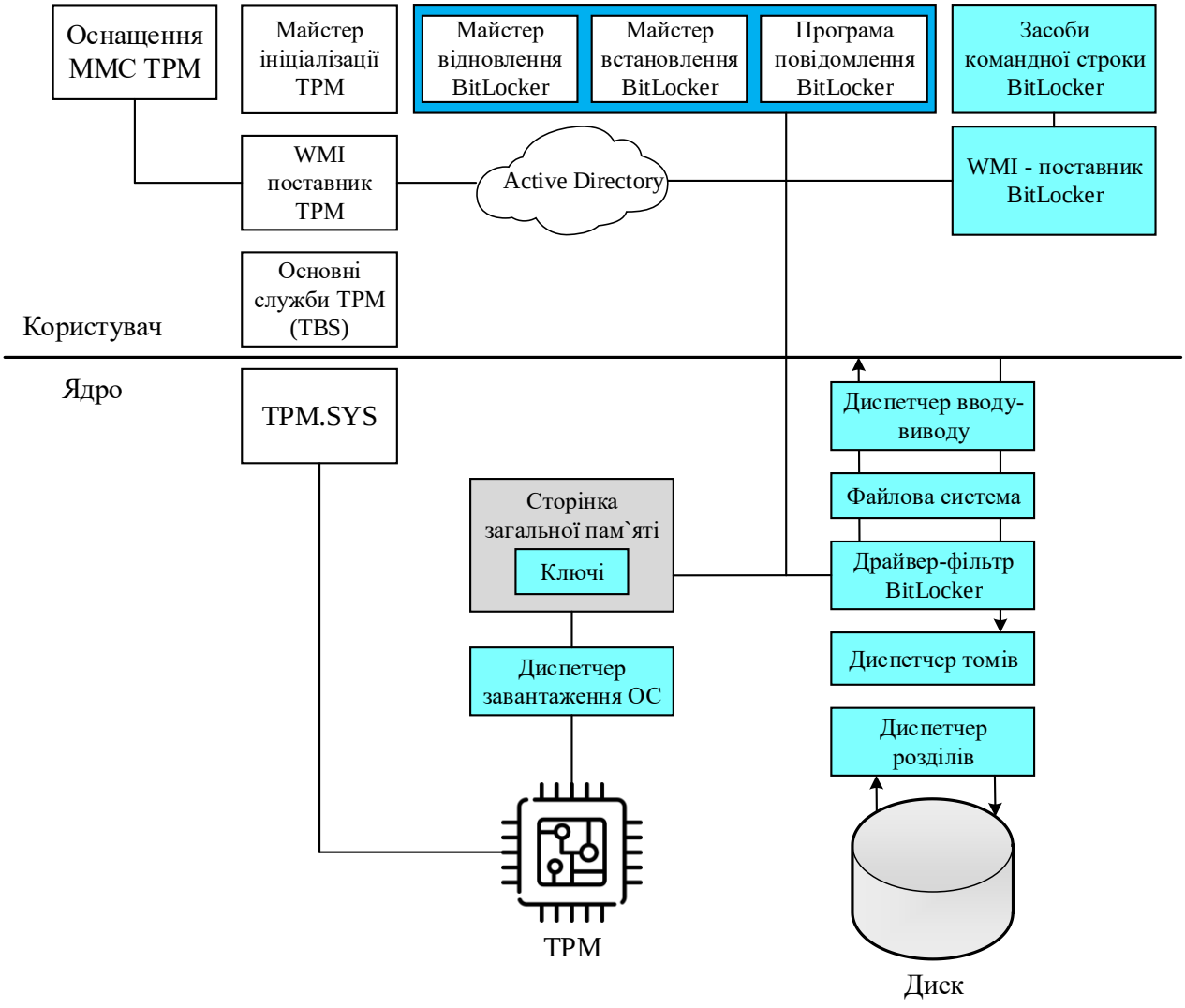

Рисунок 2.25 – Архітектура BitLocker

Gnu Privacy Guard

GNU Privacy Guard – програма для шифрування електронних листів і підписів, створена як альтернатива Pretty Good Privacy (PGP) з відкритим вихідним кодом, являє собою багатогранний інструмент шифрування, який шифрує все, від електронної пошти, загальних файлів і всього обсягу сховища. GnuPG підтримує різні механізми шифрування, в тому числі асиметричне шифрування, при якому користувачі створюють і розгортають пару ключів – приватний і відкритий. GnuPG також підтримує симетричне шифрування (такі як AES) (рис. 2.26).

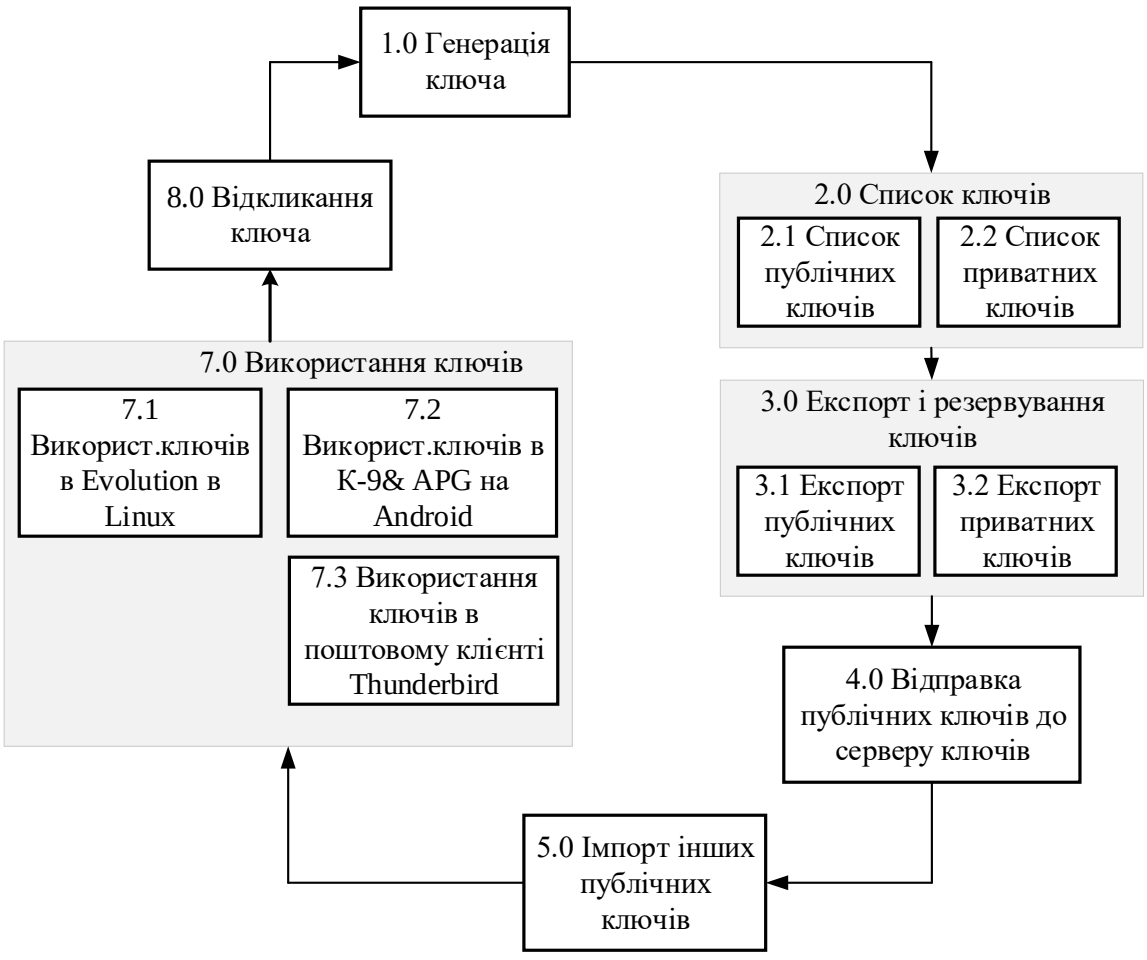

Рисунок 2.26 – Як працює GnuPG

3. Методи стеганографії (рис. 2.27).

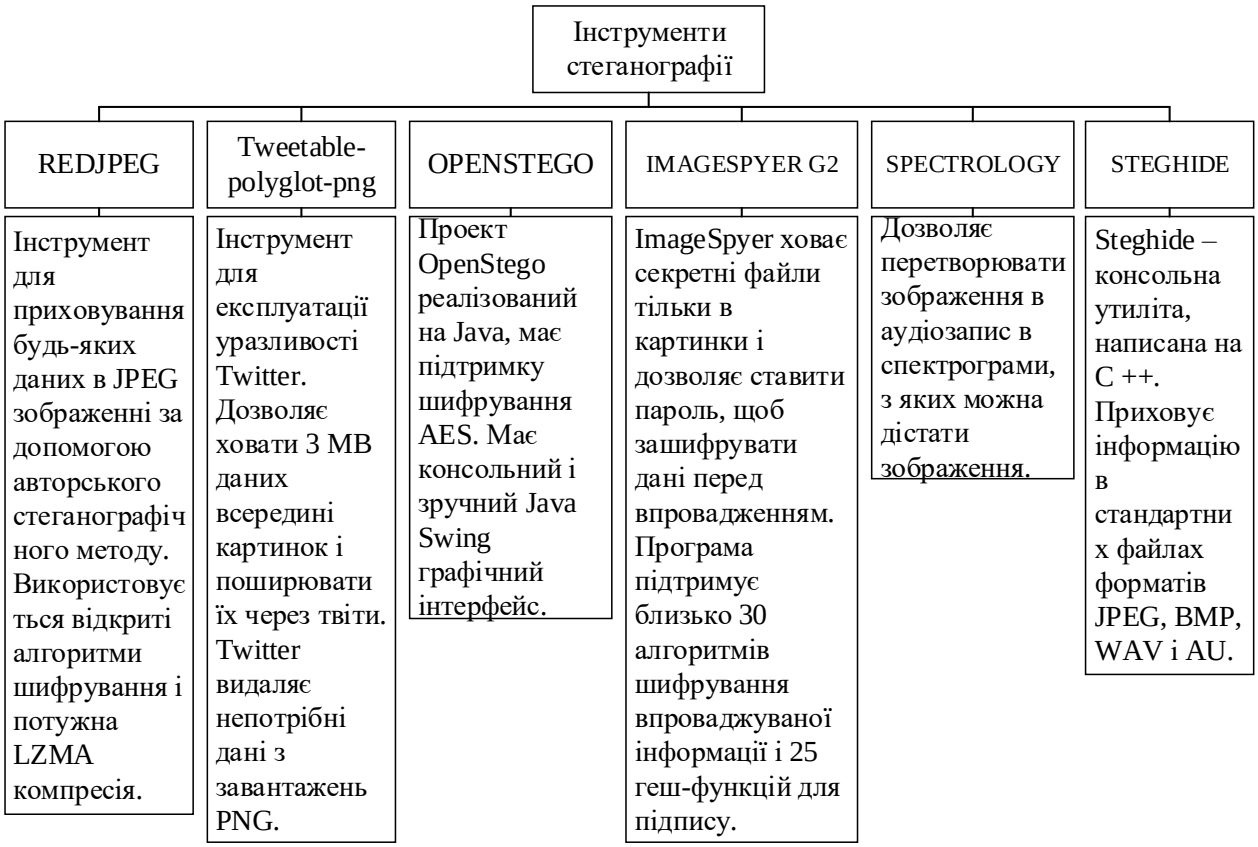

Рисунок 2.27 – Інструменти стеганографії

4. Руткіти

Руткіти – це один з методів захисту від криміналістики, який зловмисники використовують для приховування даних, шкідливих файлів і процесів. Це програмне забезпечення призначене для приховування процесів, які можуть виявити атаку з боку самої ОС. Руткіти дозволяють вірусам і шкідливим програмам «ховатися у всіх на виду», приховуючи файли таким чином, щоб антивірусне програмне забезпечення могло їх не помітити, маскуючи файли під легітимні системні файли, отсоединяя процеси і навіть ховаючись від виявлення ОС (рис. 2.28).

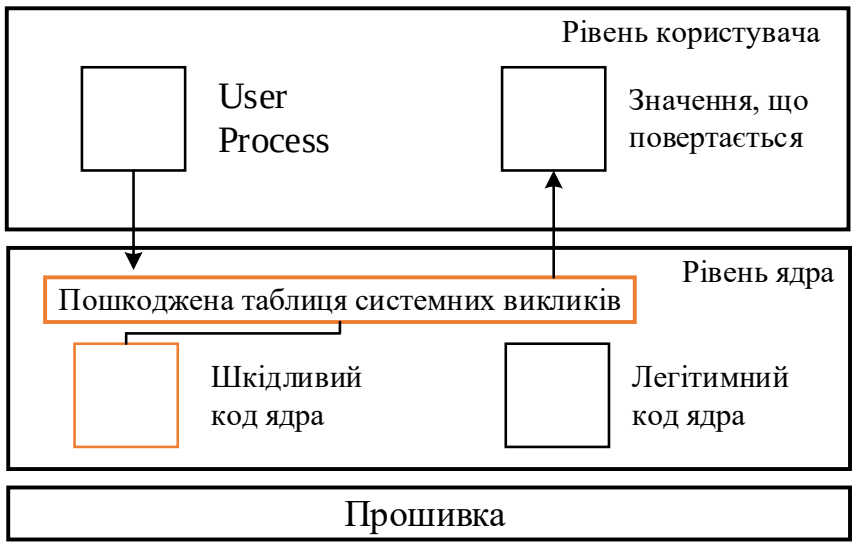

Рисунок 2.28 – Схема руткіту режиму ядра

2.3.2 Видалення артефактів

Очищення диска

Очищення диска надійно стирає дані з диска. Існує безліч загальнодоступних інструментів для очищення дисків, з яких добре відомі DBAN і WipeDisk.

Розмагнічування і руйнування диску

Використання програмних інструментів для стирання жорсткого диска має деякі переваги для підприємств, проте є значні недоліки методу програмного стирання, які додають високий ступінь ризику і невизначеності для тих, хто вважає за краще цей метод стирання томи розмагнічування. Нижче ви приведені переваги і недоліки використання програмного забезпечення для стирання жорстких дисків, і де розмагнічування даних за допомогою може бути більш підходящим.

При розмагнічування диска дані магнітно перезаписувати нулями або випадковими значеннями (рис. 2.29).

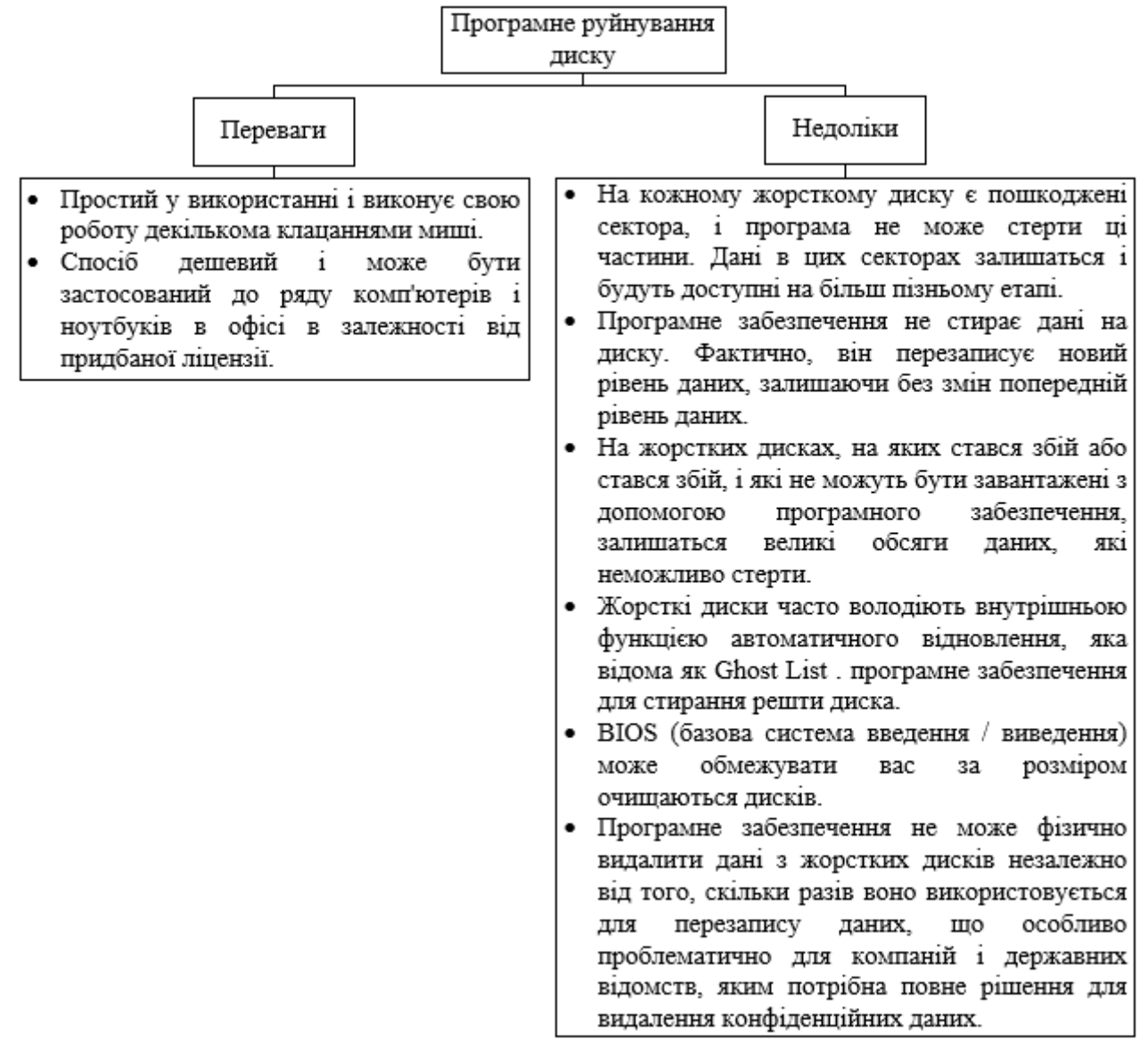

Рисунок 2.29 – Переваги та недоліки програмного руйнування дисків

2.3.3 Заплутування слідів (обфускація)

Мета цього методу – заплутати і ввести в оману судово-медичний процес, додаючи підроблені докази. Існує ряд методів, доступних для обфускації слідів, наприклад: спуфинг, очищення логів, троянські команди.

Приховування слідів охоплює різні методи і інструменти, в тому числі «очисники журналів, спуфинг, дезінформацію, між мережеве перемикання, зомбовані облікові записи, троянські команди».

Відмітка часу файлів і папок важлива для будь-якого судового розслідування. Він забезпечує час останнього доступу до створення, зміни; цей час MACE

використовується для зв'язування декількох доказів. Зміна позначки часу розриває це посилання і вводить в оману судово-медичне розслідування, додаючи фальшиву позначку часу. Timestomp дає користувачеві можливість змінювати метадані файлу, що стосуються часу дати доступу, створення і зміни [23] (рис. 2.30).

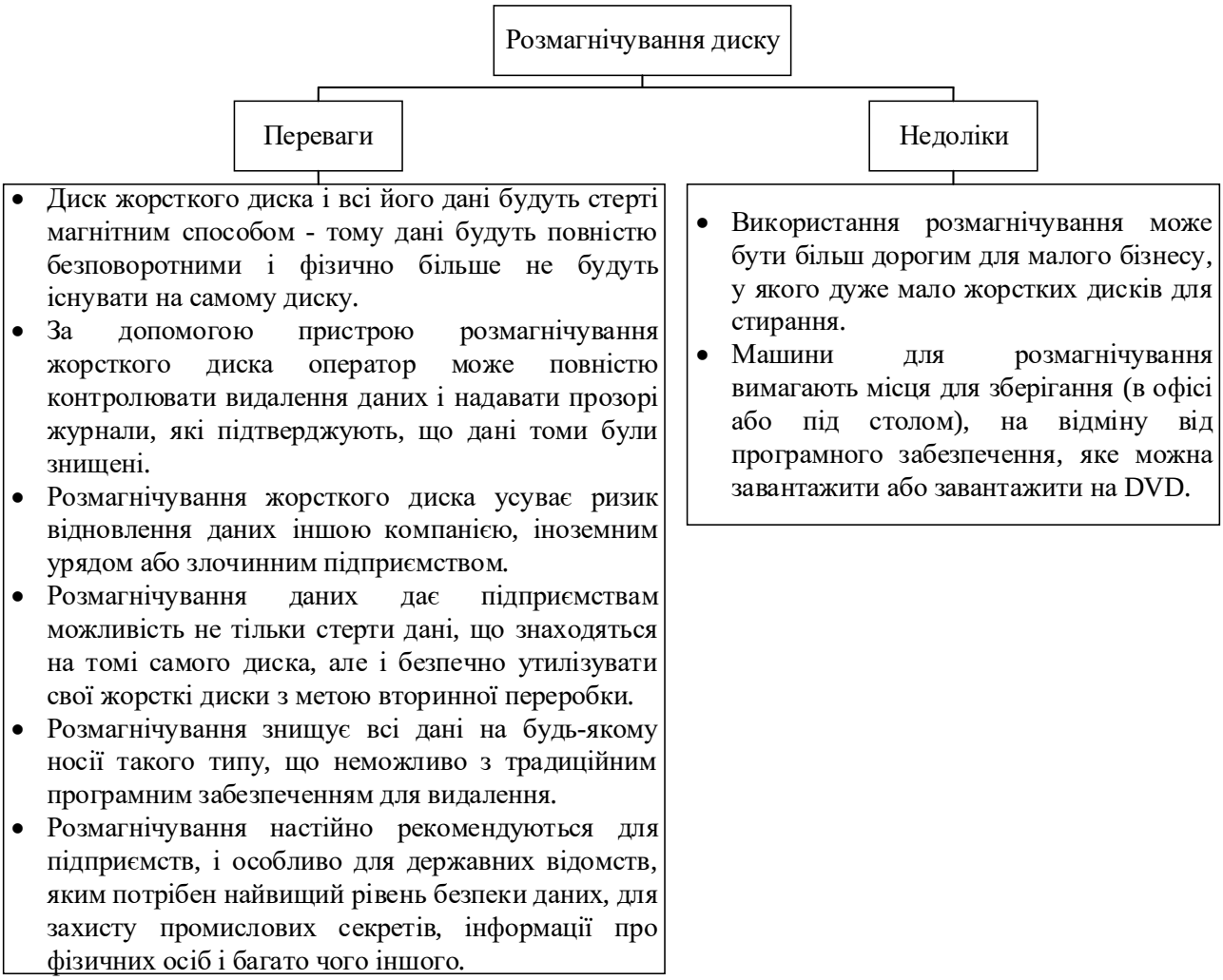

Рисунок 2.30 – Переваги та недоліки розмагнічування дисків

Використовуючи такі програми, як Timestomp, користувач може зробити будь-яку кількість файлів марними в юридичних умовах, безпосередньо поставивши під сумнів достовірність файлів (рис. 2.31).

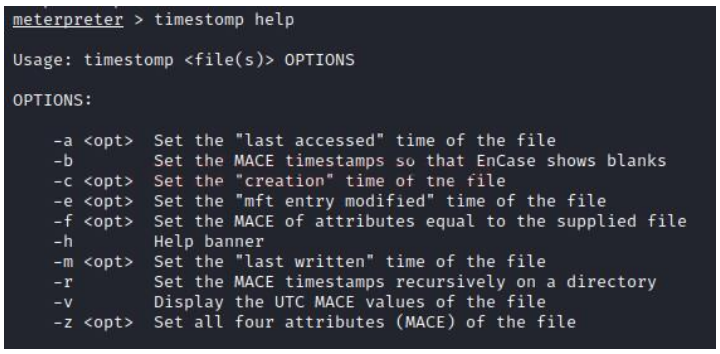

Рисунок 2.31 – Інтерфейс Metasploit Framework з підключеним Timestomp

2.3.4 Атаки проти інструментів криміналістики

Зловмисник, виявивши створення образу або аналіз логічних розділів (файлів або каталогів), може змінити цілісність докази. Відмова в обслуговуванні – ще один тип атаки на інструменти криміналістики. Виснажуючи ресурси, такі як ОЗУ і ЦП, необхідні для інструментів, зловмисник може утруднити аналіз експертів, до таких методів може бути зарахований анти-реверс-інжиніринг. Не існує добре відомого програмного забезпечення, яке працює з програмними пакувальниками, але деякі інструменти, такі як Burndump, можуть автоматично визначати, чи запущений Burneye. Підтримка систем в справному стані і в актуальному стані допомагає знизити використання переповнення буфера / купи, оскільки виправлення системи забезпечує імунітет проти відомих вразливостей, але не проти невідомих вразливостей нульового дня. Щоб уникнути використання мінімізації займаної площі, потрібні деякі заходи щодо посилення захисту: необхідно змінити BIOS, щоб зупинити завантаження з зовнішніх пристроїв, заборонити зміну порядку завантаження і захистити вхід в BIOS паролем.

Burneye являє собою інструмент шифрування виконуваних файлів і сполучного формату (ELF), який обмежує можливості зворотного проектування інструментів судової експертизи, захищаючи двійкову програму. Користувачі Burneye можуть маніпулювати виконуваним кодом, так що тільки зловмисник з паролем може запустити програму. Завантажуваний модуль ядра під назвою burndump можна використовувати для видалення Burneye з довічних файлів.

У співтоваристві кіберзлочинців також використовуються пакувальники із закритим вихідним кодом, наприклад UPX. Обидва типи пакувальників, найчастіше з закритим вихідним кодом, часто використовуються авторами шкідливих програм для обхода сигнатурних антивірусних систем і приховування аналізу шляхом шифрування корисного навантаження шкідливого ПО.

UPX – це компресор виконуваних файлів. UPX використовується для зменшення розміру переносяться виконуваних файлів приблизно на 50% -70%, також часто використовується зловмисниками для додавання шару обфускації до своїх шкідливих програм [24] (рис. 2.32).

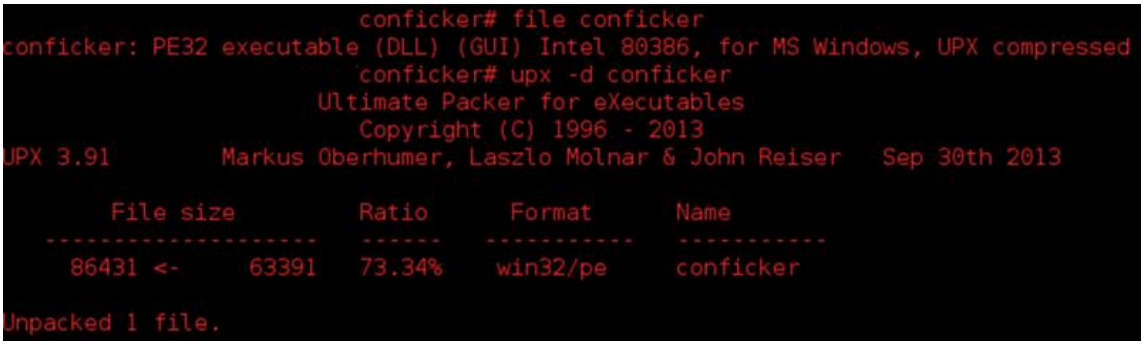

Рисунок 2.32 – Приклад шкідливого ПО, упакованого за допомогою UPX

Також поширеним способом атаки на інструменти криміналістики є Zip бомби. Zip-бомби – це звичайні zip-файли, ці файли розширюються і створюють величезний обсяг даних при розпакуванні. Коли інструмент судової експертизи намагається розпакувати zip-файли такого типу, у нього виникають проблеми, коли цей файл створює величезний обсяг даних (рис. 2.33).

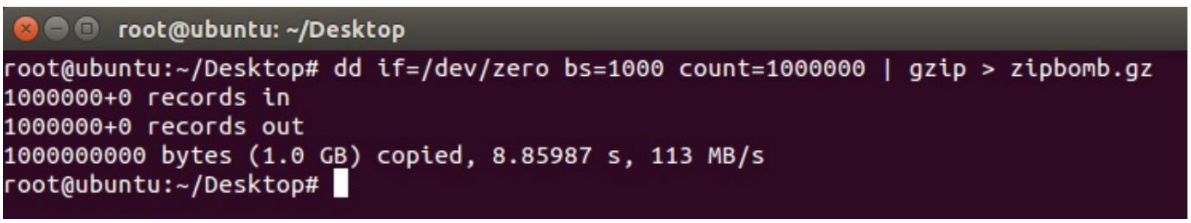

Рисунок 2.33 – Команда Linux для створення zip-бомби

Анти-криміналістичні інструменти, які виявляють комп'ютерну криміналістику

Засоби захисту від судової експертизи можуть змінити свою поведінку, якщо вони можуть виявити, що використовується комп'ютерна криміналістика. Наприклад,

пакувальник може не розшифрувати свої корисні дані, якщо він зрозуміє, що він працює на диску, образ якого був створений. Комп'ютерний хробак може відмовитися поширюватися, якщо виявить, що за мережею ведеться спостереження (рис. 2.34).

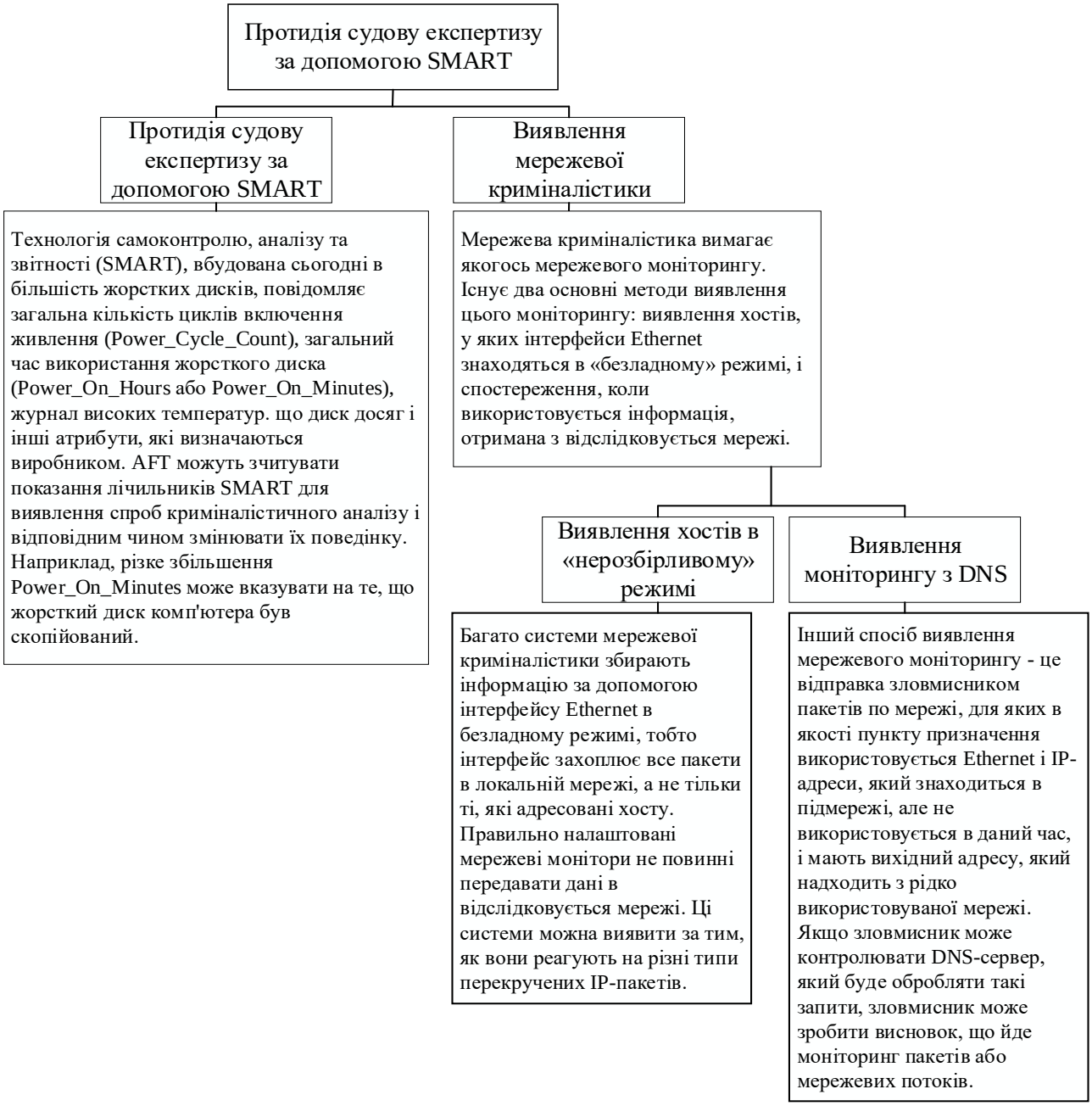

Рисунок 2.34 – Протидія судову експертизу за допомогою SMART

За підсумком огляду і аналізу механізмів дії сучасного програмного забезпечення в сфері протистояння комп'ютерної криміналістики була складена таблиця з категоріями і конкретним прикладом програми, яка працює по кожному із зазначених принципів (табл. 2.1).

Таблиця 2.1 – Техніки антифорензіки та їх програмні реалізації

Техніки	Підкатегорія	Інструменти
Приховування даних	1. Приховування даних файлової системи	Файлові потоки BMAP і NTFS, Bitlocker, Slacker, FragFS
	2. Приховування даних в пам'яті	
	3. Мережеве приховування даних	Stunnel
	4. Шифрування	VeraCrypt ,VeraCrypt Hidden OS, AxCrypt
	5. Стеганографія	steghide,cloakify,spectrology,imagespyer g2,redjpeg, openstego, silenteye, imagejs.
	6. Руткіти	
Видалення артефактів	1. Очистка диска	PCDiskEraser, DBAN, Disk Wipe, Eraser, MiniTool Partition Wizard,
	2. Розмагнічування і руйнування диску	Eraser HDD, CBL Data Shredder, MHDD, KillDisk, Hardwipe
	3. Очистка файлів	Sdelete and BitKiller
	4. Універсальна очищення даних	CCleaner
	5. Очистка метаданих	Timestomp, MetaCleaner, Metadata++, Scrambled EXIF, EXIFTool.
	6. Очищення реєстру	AuslogicsRegistryCleaner, Cleanersoft Registry Fix, CCleaner, Eusing Registry Cleaner, Free Window Registry Repair.
	7. Очищення знімного диска	Аналогічні до пункту «Очистка диска»
Заплутування слідів (обфускація)	Очисники журналів за допомогою Metasploit Фреймворк (Timestomp).	
Атаки проти інструментів криміналістики	Пакувальники (Burndump, Burneye, 7-zip, PECompact, UPX, ASPack, tElock), протидія за допомогою SMART, Zip Bombs.	
Цибулева маршрутизація	Tor браузер, Epic Browser, SRWare Iron, Comodo IceDragon, Orfox.	

2.4 Висновки до розділу 2

Таким чином у другому розділі були розглянуті сучасні методи і засоби протистояння комп'ютерної криміналістиці, наведено класифікацію та докладний опис кожного з методів АФ з візуалізацією. Після цього було проаналізовано ринок програмного забезпечення на відповідність кожному з вищеописаних методів, в деяких випадках було описано внутрішній устрій програм для кращого розуміння їх функціонування, а також закріплення розуміння методів АФ. У висновку була складена таблиця, яка допомагає швидко орієнтуватися в методах і програмах, які можуть їх реалізувати на практиці.

3. ОГЛЯД ІСНУЮЧИХ АЛГОРИТМІВ СРС, РОЗРОБКА СПОСОБУ ГЕНЕРУВАННЯ ЧАСТКОЮ СЕКРЕТНИХ ДАНИХ

3.1 Система, методи для поділу даних для зберігання в розподіленої мережі зберігання даних

Дані як від приватних осіб, так і підприємств все частіше збираються, агрегуються та аналізуються для надання нових послуг. Існує відповідне бажання забезпечити як зберігання, так і обробку таких даних безпечним і таким, що зберігає конфіденційність способом, відповідно до зростаючого суспільного занепокоєння та суворих нормативних вимог до захисту таких даних. Безпечні багатосторонні обчислення – це механізм, за допомогою якого кілька сторін можуть співпрацювати для обчислення узгодженої функції своїх вхідних даних, забезпечуючи як конфіденційність даних, так і цілісність вихідних даних. Приватні обчислення з використанням розподілених даних застосовні в багатьох сценаріях, дозволяючи кільком організаціям спільно використовувати свої приватні або бізнес-конфіденційні дані для надання послуги (наприклад, постачальникам послуг Інтернету для усунення збоїв у роботі мережі) та дозволяючи обробляти особисті дані, що зберігаються на мобільних пристроях окремих осіб. СРС може бути заснований на спільному використанні секрету або спотворених схем. При спільному використанні секрету кожен одноранговий вузол розподіляє загальні ресурси, які криптографічно сконструйовані з конфіденційних даних (тобто секретів), отже лише заздалегідь певне підмножина сторін може відновити секрети [25].

Протоколи поділу секрету покликані вирішити проблему зберігання інформації так, щоб ті групи людей, яким дозволено знати секрет, могли б його відновити, а ті групи, яким секрет знати не дозволено, відновити його не змогли навіть шляхом перебору. Більшість способів комунікації та зберігання інформації перебувають у цифровій формі. Безпека цифрових ЗМІ викликає серйозне занепокоєння і це призвело до розвитку шифрування та криптографії. Математики,

криптографи та інженери безпеки більше залучаються до процесу обміну секретами.

В теорії поділу секрету розглядається задача, яка полягає в необхідності в поділі значення секрету з деякого безлічі секретів між учасниками з деякого безлічі учасників, видавши кожному учаснику його частку секрету так, щоб заздалегідь певні, авторизовані, безлічі учасників могли, з'єднавши свої частки, обчислити справжнє значення секрету, а учасники інших, неавторизованих, множин не могли б цього зробити. Дане завдання може виникнути при поділі доступу між групою осіб, які не довіряють один одному, а також при зберіганні конфіденційної інформації, розділеної на частини.

Деякі схеми спільного використання секрету ґрунтуються на порогових значеннях, вимагаючи доступу як мінімум до t загальних папок для відновлення секрету, де t – зумовлений поріг. Спільне використання секрету Shamir - це порогова схема, яка забезпечує ідеальну секретність, тобто не відбувається жодного витоку інформації жодним підмножиною менше t часток. Проте розмір кожної частки становить щонайменше розміру секрету. Отже, використання спільного використання секрету в службах, що покладаються на великі обсяги даних, може бути обмежене.

У протоколі поділу секрету є n учасників (абонентів) P_1, P_2, ..., P_n і один виділений учасник D, званий дилером (роздає). Нехай через $P = \{P_1, P_2, ..., P_n\}$ позначено безліч всіх абонентів. Надалі будемо користуватися наступною термінологію (рис. 3.1).

Будемо вважати, що будь-який учасник P_1, P_2, ..., P_n входить хоча б в одну групу доступу, інакше присутність його присутність безглуздо. Також вважаємо, що Г замкнуто, тобто якщо $A \subset B \subset P$ і $A \subset Г$, то $B \subset Г$. Дійсно, якщо абоненти P_1, P_2, ..., P_k можуть спільно відновити секрет, то, якщо до них приєднаються додаткові учасники $P_k + P_{k+2}$, то вийшла група тим більше зможе відновити секрет.

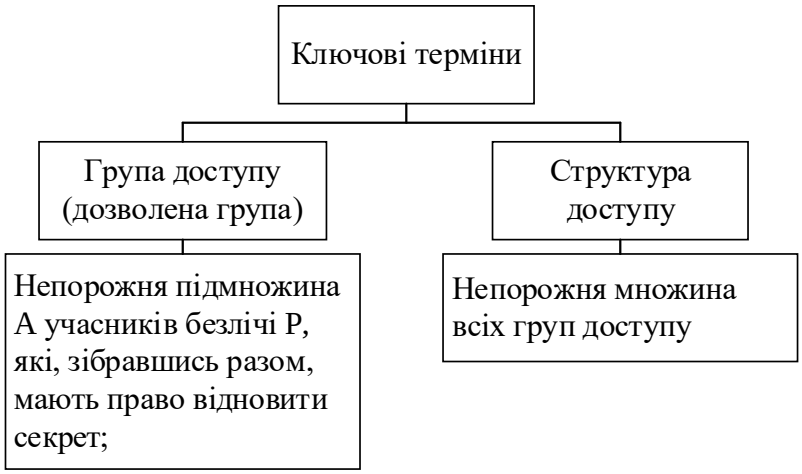

Рисунок 3.1 – Термінологія в предметній області

Протокол поділу секрету складається з двох основних фаз (рис. 3.2).

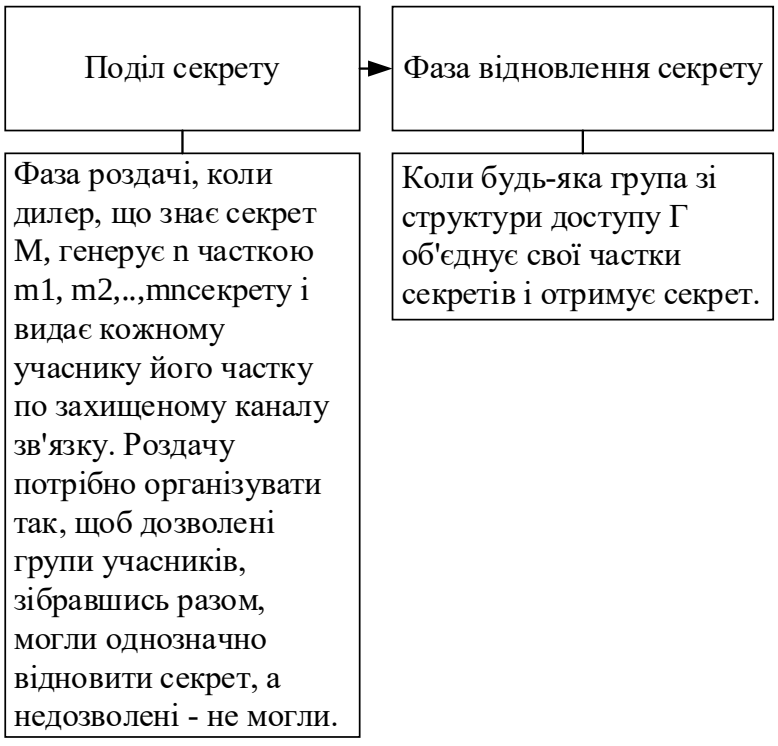

Рисунок 3.2 – Фази протоколу поділу секрету

З точки зору можливостей акцій можна виділити два класи – акції з однаковою вагою та акції з кількома вагами. В ієрархічній схемі спільного використання секретів Шаміра дилер призначає більшу кількість акцій

користувачам на вищих рівнях ієрархії, так що користувачі вищого рівня мають більшу кількість акцій, ніж користувачі нижчого рівня [26]. Тасса покращив цю концепцію, якісно виділивши ієрархічний рівень, тобто секретна частка користувачів вищого рівня містить більше інформації про вихідний секрет, ніж користувачі нижчого рівня. За здібностями поділ секретів представлено на рис. 3.3.

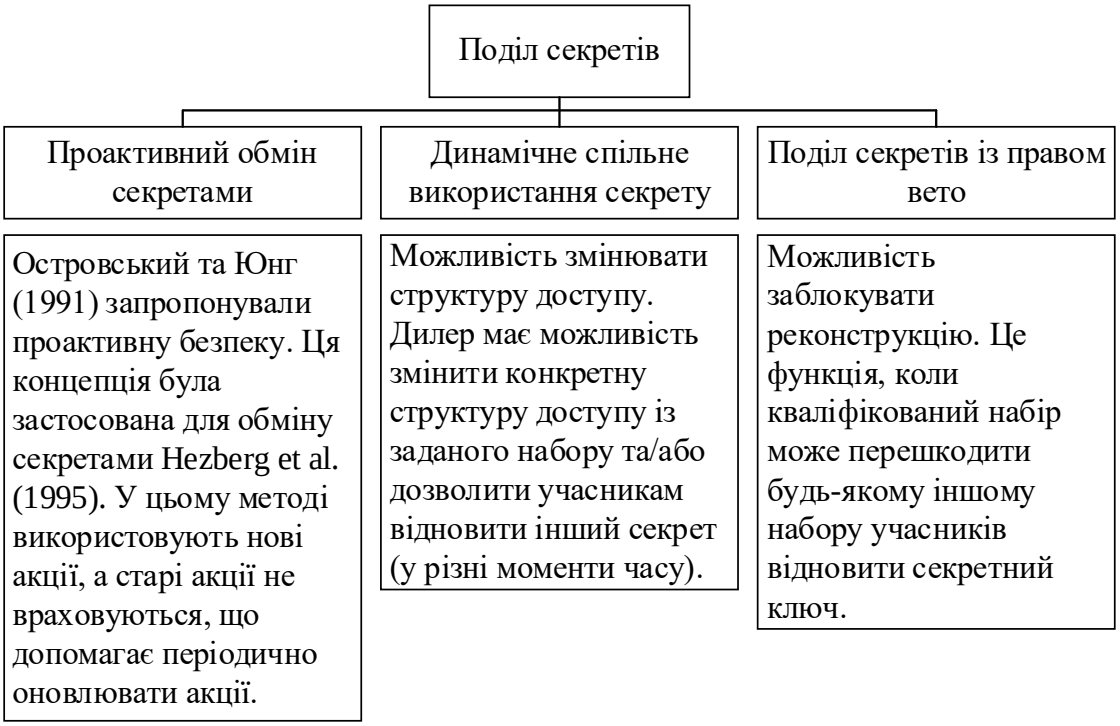

Рисунок 3.3 – Поділ секретів

3.2 Огляд порогових СРС, переваги та недоліки

Для використання порогових СРС формуються групи учасників, які використовуються для зберігання «частин» секрету. Порогові СРС дозволяють розподілити секрет між абонентами (учасниками) груп таким чином, щоб легітимні абоненти могли однозначно відновити секрет, а нелегітимність – не отримували ніякої додаткової інформації про можливий зміст секрету (рис. 3.4).

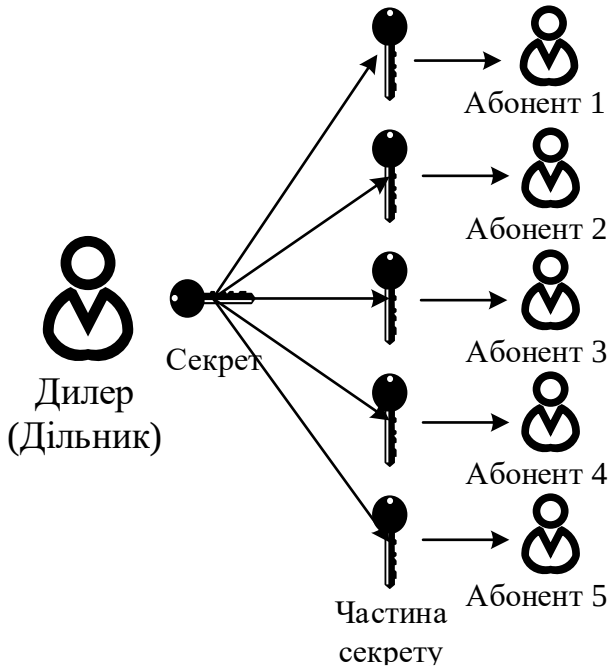

Рисунок 3.4 – Схема класичного протоколу поділу секрету

Комп'ютерна атака на порогові СРС можлива, якщо в число k учасників поділу секрету проник порушник. У порушника є маса потенційних можливостей обійти порогову схему (рис. 3.5).

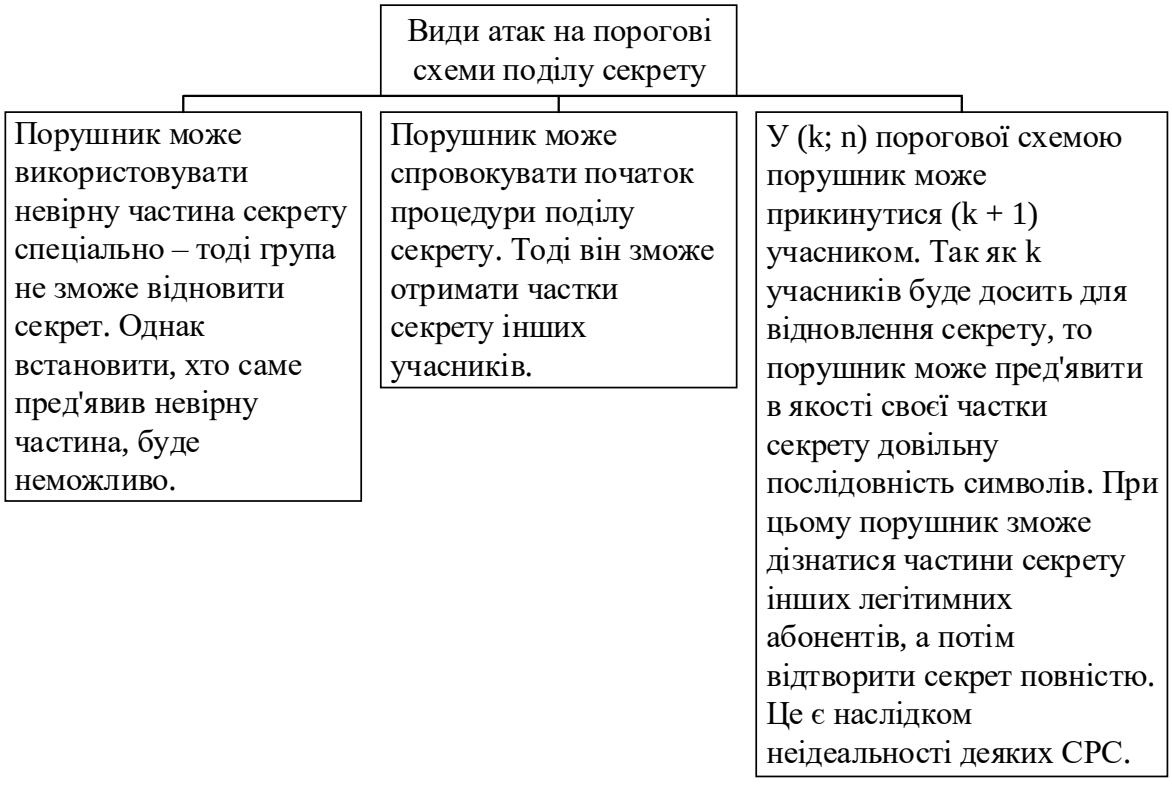

Рисунок 3.5 – Види атак на порогові СРС

Також існують загрози комп'ютерних атак на СРС по зовнішніх каналах, коли порушник намагається витягти корисну інформацію з часу виконання, кешування, з збоїв додатки і т.д. Можливість проведення таких атак зазвичай пов'язана з помилками, допущеними при розробці програмного забезпечення.

3.2.1 СРС Шаміра

У 1979 році Аді Шамір в своїй роботі запропонував досконалу (k, n)-пороговую схему, в основі якої лежить інтерполяція многочлена з коефіцієнтами із заданого поля Галуа з p елементами – GF (p). Схема Шаміра заснована на добре відомому математичному факту, який полягає в тому, що через будь-які t точок на площині можна провести безліч кривих, описуваних многочленом t-го порядку, але через будь-які t+1 різні точки можна провести тільки єдину криву, описувану многочленом t -го порядку [27] (рис. 3.6).

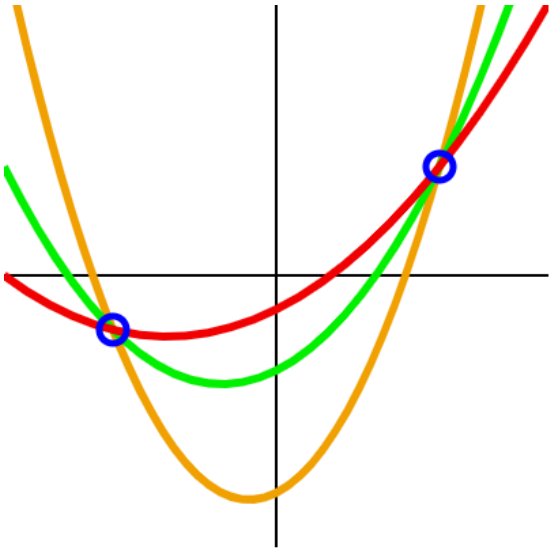

Рисунок 3.6 – Через дві. точки можна. провести необмежене число поліномів степеня 2

Щоб вибрати. з них єдиний потрібна третя точка. Так, через будь-яку точку на площині проходить безліч прямих ліній, але через дві різні точки – лише єдина. Через будь-які дві точки можна провести безліч парабол, але через будь-які три різні точки – тільки одну і т.д. Таким чином, якщо кожному з учасників криптосистеми «видати» по одній точці, то відновити криву можна буде тільки при достатній кількості учасників.

Схема поділу секрету (СРС) включає в себе дилера, формує секрет, і учасників, які отримують частку від цього секрету. Тільки об'єднавшись, учасників порогової схеми «з» можуть відновити секрет. В СРС Шаміра учасники параметризуються елементами даного кінцевого поля, що геометрично означає вісь абсцис, а так само ще одного «невласного» учасника, відповідного «нескінченно віддаленої» точці.

Поділ секрету на еліптичній кривій відбувається за наступним алгоритмом: дилер вибирає еліптичну криву з необхідною кількістю точок (не менше). Кожному з учасників СРС (в тому числі зберігачу секрету) ставиться у відповідність точка на еліптичній кривій, включаючи «нескінченно віддалену». Потім дилер вибирає многочлен ступеня на цій кривій. Коефіцієнти даного многочлена відомі тільки йому. Точка на еліптичній кривій, яка позначає учасника-хранителя секрету, відома всім. Дилер підставляє координати цієї точки в обраний ним многочлен, обчислює значення секрету. Для того, щоб кожному учаснику роздати свою частку секрету, дилер підставляє координати точки учасника в многочлен, отримуючи частку секрету для нього. В результаті учасник має точку на еліптичній кривій (login) і частку секрету (password). Декілька учасників для відновлення секрету повинні об'єднатися, щоб відновити коефіцієнти обраного дилером многочлена. Математично це зводиться до вирішення деякої системи рівнянь. Учасники, що становлять дозволену коаліцію, отримують шуканий многочлен, куди підставляють координати точки, що позначає секрет. У підсумку вони отримують секрет, який сформував дилер.

Конструкція СРС

У разі довільного поля всяку еліптичну криву можна перетворити до вигляду:

$$Y^2 + a_1 \cdot X \cdot Y + a_3 \cdot Y = X^3 + a_2 \cdot X^2 + a_4 \cdot X + a_6. \qquad (3.1)$$

Дискримінант визначається наступним чином:

$$\Delta = -b_2^2 \cdot b_8 - 8 \cdot b_4^3 - 27 \cdot b_6^2 + 9 \cdot b_2 \cdot b_4 \cdot b_6, \qquad (3.2)$$

де $b_2 = a_1^2 + 4 \cdot a_2$,

$b_4 = 2 \cdot a_4 + a_1 \cdot a_3$,

$b_6 = a_3^2 + 4 \cdot a_6$,

$b_8 = a_1^2 \cdot a_6 + 4 \cdot a_2 \cdot a_6 - a_1 \cdot a_3 \cdot a_4 + a_2 \cdot a_3^2 - a_4^2$.

Над полем характеристики, не рівної двом, еліптична крива може бути приведена до вигляду:

$$y^2 = x^3 + a \cdot x^2 + b \cdot x + c. \qquad (3.3)$$

Теорема Хассе про еліптичних кривих стверджує, що кількість точок на еліптичній кривій близько до потужності кінцевого поля:

$$(\sqrt{q} - 1)^2 \le |EC(GF(q))| \le (\sqrt{q} + 1)^2. \qquad (3.4)$$

У загальному вигляді многочлен, який вибирає дилер, має вигляд $F(P) = \alpha(x) + \beta(x) \cdot y$, где $\alpha(x)$, $\beta(x)$ – многочлени над полем $GF(q)$. Ступінь многочлену F визначається по формулі $\deg F = \max\{2 \cdot \deg\alpha, 2 \cdot \deg\beta + 3\}$. Якщо $F(P) = 0$, то точка $P = (x, y) \in EC$ називається корнем многочлена. Так, для аналога схеми Шаміра схеми «5 з N» необхідно задати многочлен ступеню п’ять. В загальному вигляді многочлен ступені рівній або меншій 5 має вигляд:

$F = \alpha(x) + \beta(x) \cdot y$, де $\alpha(x) = A \cdot x^2 + B \cdot x + C$, $\beta(x) = D \cdot x + E$. Здесь $A, B, C, D, E \in GF(q)$ и $\deg F = 5$ при $D \neq 0$.

Долі секрета для п’яти учасників дають залежність:

$$\begin{cases} (A \cdot x_1^2 + B \cdot x_1 + C) + (D \cdot x_1 + E) \cdot y_1 = s_1 \\ (A \cdot x_2^2 + B \cdot x_2 + C) + (D \cdot x_2 + E) \cdot y_2 = s_2 \\ (A \cdot x_3^2 + B \cdot x_3 + C) + (D \cdot x_3 + E) \cdot y_3 = s_3 \\ (A \cdot x_4^2 + B \cdot x_4 + C) + (D \cdot x_4 + E) \cdot y_4 = s_4 \\ (A \cdot x_5^2 + B \cdot x_5 + C) + (D \cdot x_5 + E) \cdot y_5 = s_5 \end{cases}. \quad (3.5)$$

Тут точки $P_i = (x_i, y_i)$, $(i = 1,...,n)$ відповідають учасникам, S_i, $(i = 1,...,n)$ – їх долі секрета. Для поділу секрету коаліція з $n = 5$ учасників повинна об'єднатися і вирішити систему рівнянь для п'яти невідомих A, B, C, D, E. Якщо вони однозначно знайдуть значення цих параметрів, то вони зможуть однозначно відновити секрет, значення многочлена F в будь-якій точці $P \in EC$,отже, ця коаліція є дозволеною.

Коаліція учасників буде невирішеною, якщо система лінійних рівнянь. не має однозначного вирішення, визначник d однорідної системи дорівнює нулю. Визначник d для коаліції учасників з кінцевими точками дорівнює:

$$d = \begin{vmatrix} x_1^2 & x_1 & 1 & x_1 \cdot y_1 & y_1 \\ x_2^2 & x_2 & 1 & x_2 \cdot y_2 & y_2 \\ x_3^2 & x_3 & 1 & x_3 \cdot y_3 & y_3 \\ x_4^2 & x_4 & 1 & x_4 \cdot y_4 & y_4 \\ x_5^2 & x_5 & 1 & x_5 \cdot y_5 & y_5 \end{vmatrix}. \quad (3.6)$$

Визначник для коаліції учасників з «нескінченно віддаленої» точкою P_5 має вигляд:

$$d = \begin{vmatrix} x_1^2 & x_1 & 1 & x_1 \cdot y_1 & y_1 \\ x_2^2 & x_2 & 1 & x_2 \cdot y_2 & y_2 \\ x_3^2 & x_3 & 1 & x_3 \cdot y_3 & y_3 \\ x_4^2 & x_4 & 1 & x_4 \cdot y_4 & y_4 \\ 0 & 0 & 0 & 1 & 0 \end{vmatrix} = - \begin{vmatrix} x_1^2 & x_1 & 1 & y_1 \\ x_2^2 & x_2 & 1 & y_2 \\ x_3^2 & x_3 & 1 & y_3 \\ x_4^2 & x_4 & 1 & y_4 \end{vmatrix}. \qquad (3.7)$$

Значення многочлену $F(x, y) = (A \cdot x^2 + B \cdot x + C) + (D \cdot x + E) \cdot y$ в точці $P(x, y)$ кривої ЕС можно уявити у вигляді скалярного добутку двох векторів $(A, B, C, D, E) \cdot (x^2, x, 1, x \cdot y, y)$.

Будь-який многочлен (k-1) ступеня можна однозначно відновити по будь-яким k різних точок за допомогою інтерполяції. Для цього можна використовувати, наприклад, інтерполяційну формулу Лагранжа. Таким чином будь-які k і більше учасників зможуть відновити многочлен F і обчислити значення F в точці 0, що буде значенням секрету. Очевидно, що ця схема досконала, так як будь-які k і більше учасників однозначно відновлюють секрет, а будь-які групи з менш k учасників не отримують ніякої додаткової інформації про секрет. Процес підрахування в схемі Шаміра наведено на рис. 3.7.

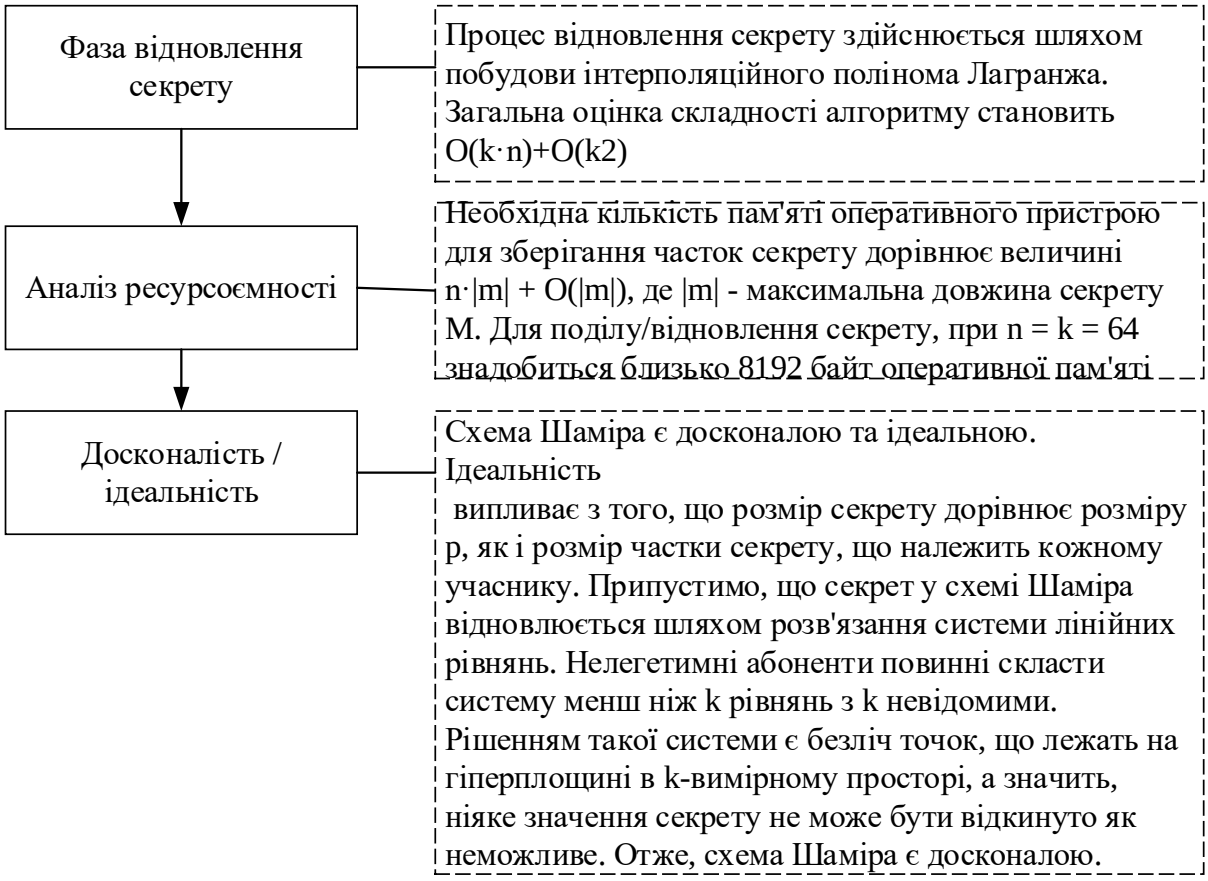

Рисунок 3.7 – Переваги СРС Шаміра

Переваги схеми Шаміра зображені на рис. 3.8.

Перейдемо до недоліків (рис. 3.9).

3.2.2 СРС Блеклі

Особливістю схеми Блеклі є використання для поділу секрету між сторонами точок багатовимірного простору. У цьому варіанті секрет задається як точка в тривимірному просторі. Кожна частка секрету задається рівнянням площини, що проходить через дану точку. Знаючи одну частку секрету можна стверджувати, що точка знаходиться на даній площині, знаючи дві частки - що точка знаходиться на прямій перетину цих площин.

Рисунок 3.8 – Переваги СРС Шаміра

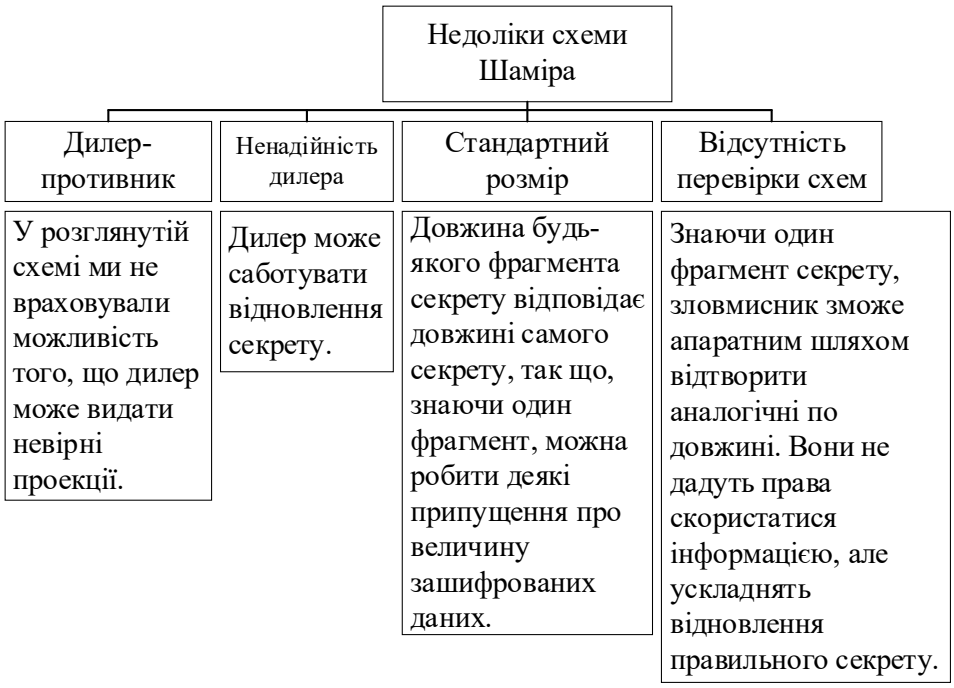

Рисунок 3.9 – Недоліки схеми Шаміра

Три площини однозначно задають точку. Дану схему можна узагальнити на t-мірний простір, де кожна частка секрету задається рівнянням t-1-мірної гіперплоскості. Схема Блеклі в трьох вимірах: кожна частка секрету – це площина, а секрет – це одна з координат точки перетину площин. Двох площин недостатньо для визначення точки перетину [28].

Схема Блеклі менш ефективна, ніж схема Шаміра: в схемі Шаміра кожна частка такого ж розміру як і секрет, а в схемі Блеклі кожна частка в t раз більше. Існують поліпшення схеми Блеклі, що дозволяють підвищити її ефективність (рис. 3.10).

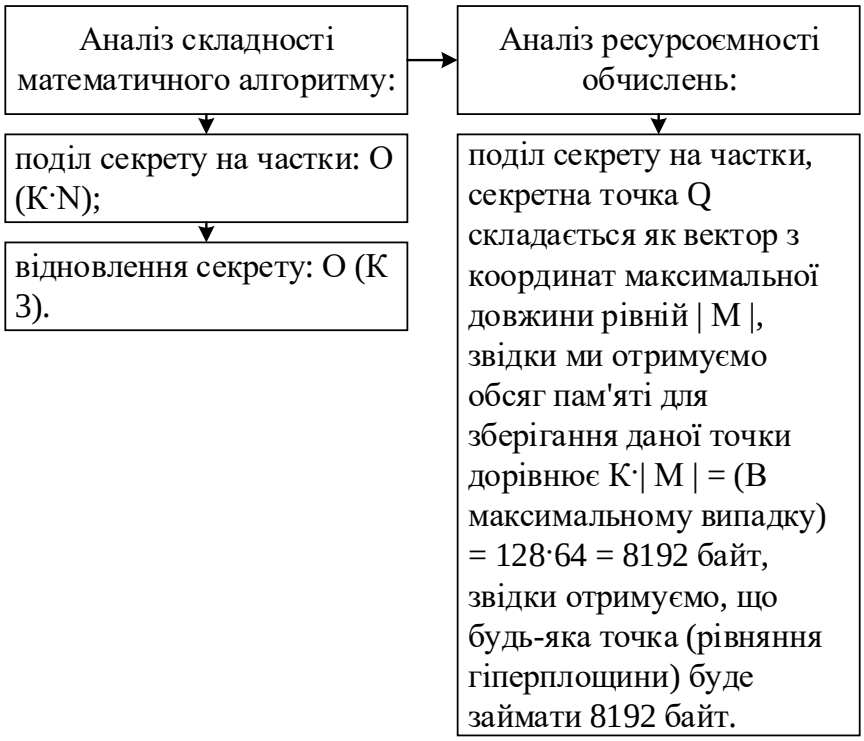

Рисунок 3.10 – Етапи аналізу в СРС Блеклі

Кроки щодо поділу секрету наведно на рис. 3.11.

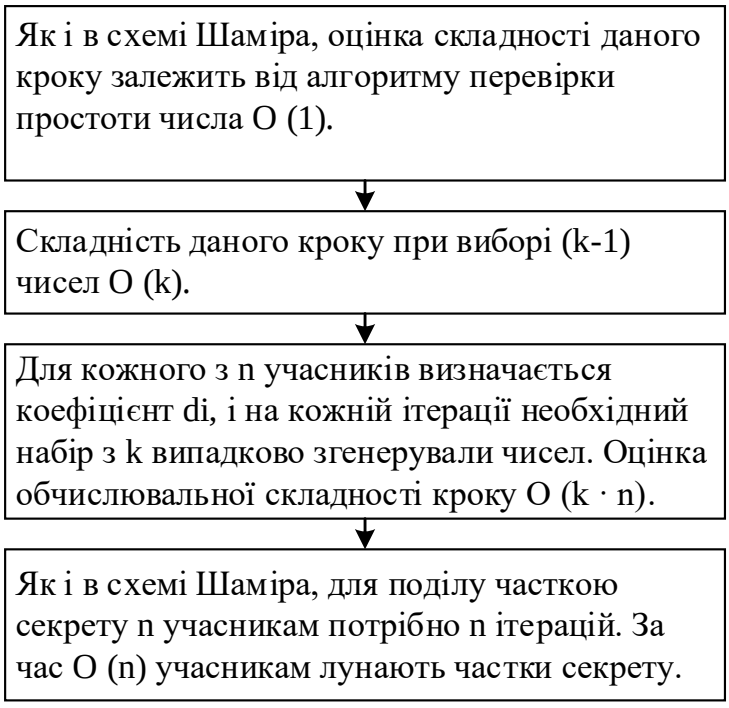

Рисунок 3.11 – Кроки по поділу секрету в СРС Блеклі

Роботу данної схеми наведно у вигляді схеми (рис. 3.12).

Фаза поділу наведена на рис. 3.13.

3.2.3 СРС Карніна-Гріні-Хелмана

Дана схема заснована на рішенні систем рівнянь алгебри. Проведемо аналіз складності обчислень [29].

Проведемо порівняння вищенаведених схем поділу секретів в табл. 3.1.

Таблиця 3.1 – Порівняння СРС

Порогова схема	Досконалість	Ідеальність	Ресурсомісткість (Кбайт)	Оцінка складності
Схема Шаміра	+	+	8	$O(n \cdot k)+O(k^2)$
Схема Блеклі	+	–	266	$O(n \cdot k)+O(k^3)$
Схема Карнина-Гріна-Хелмана	+	–	8,1	$O(n)+O(k^3)$

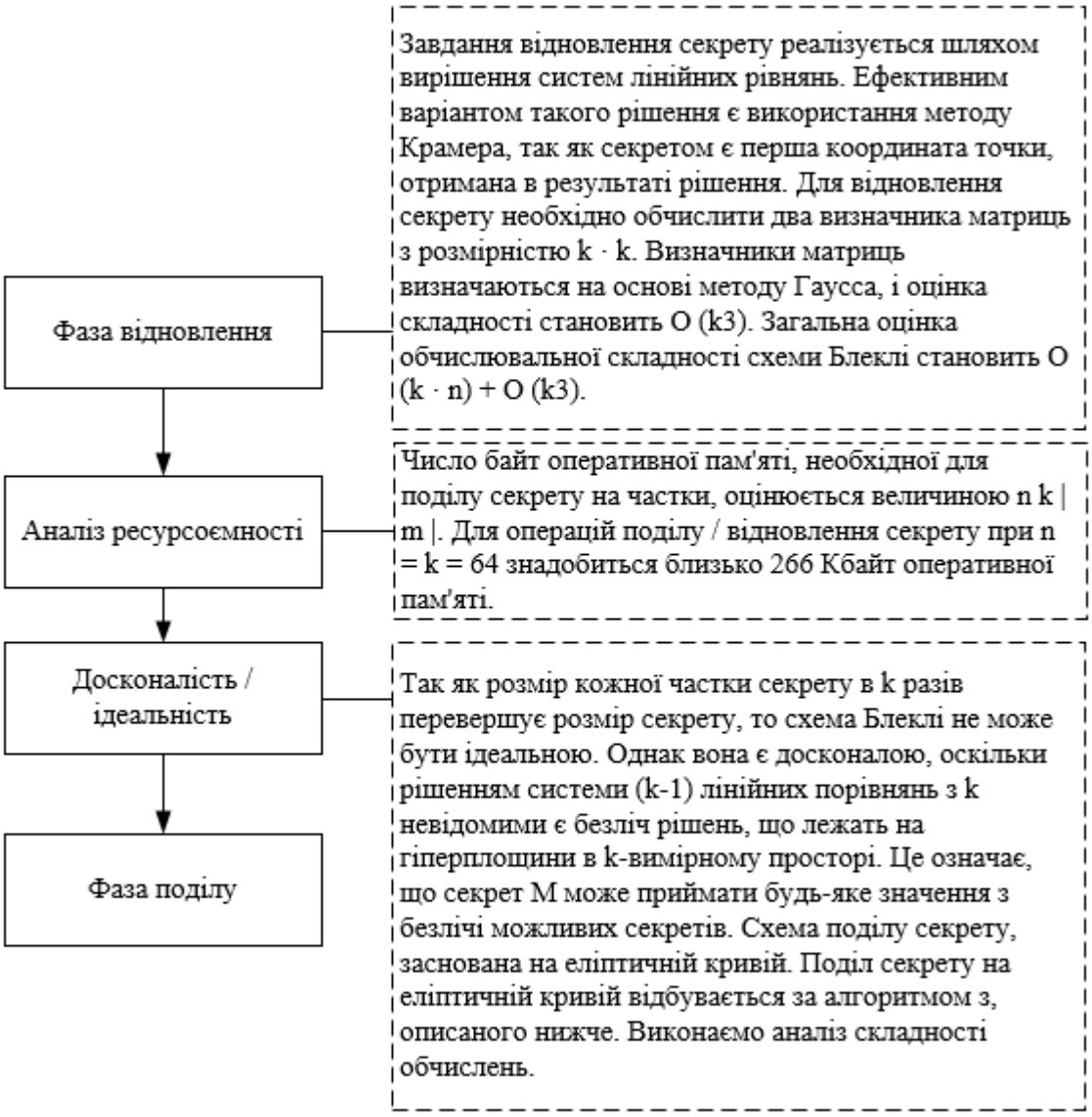

Рисунок 3.12 – Робота СРС Блеклі

Рисунок 3.13 – Фаза поділу СРС Блеклі

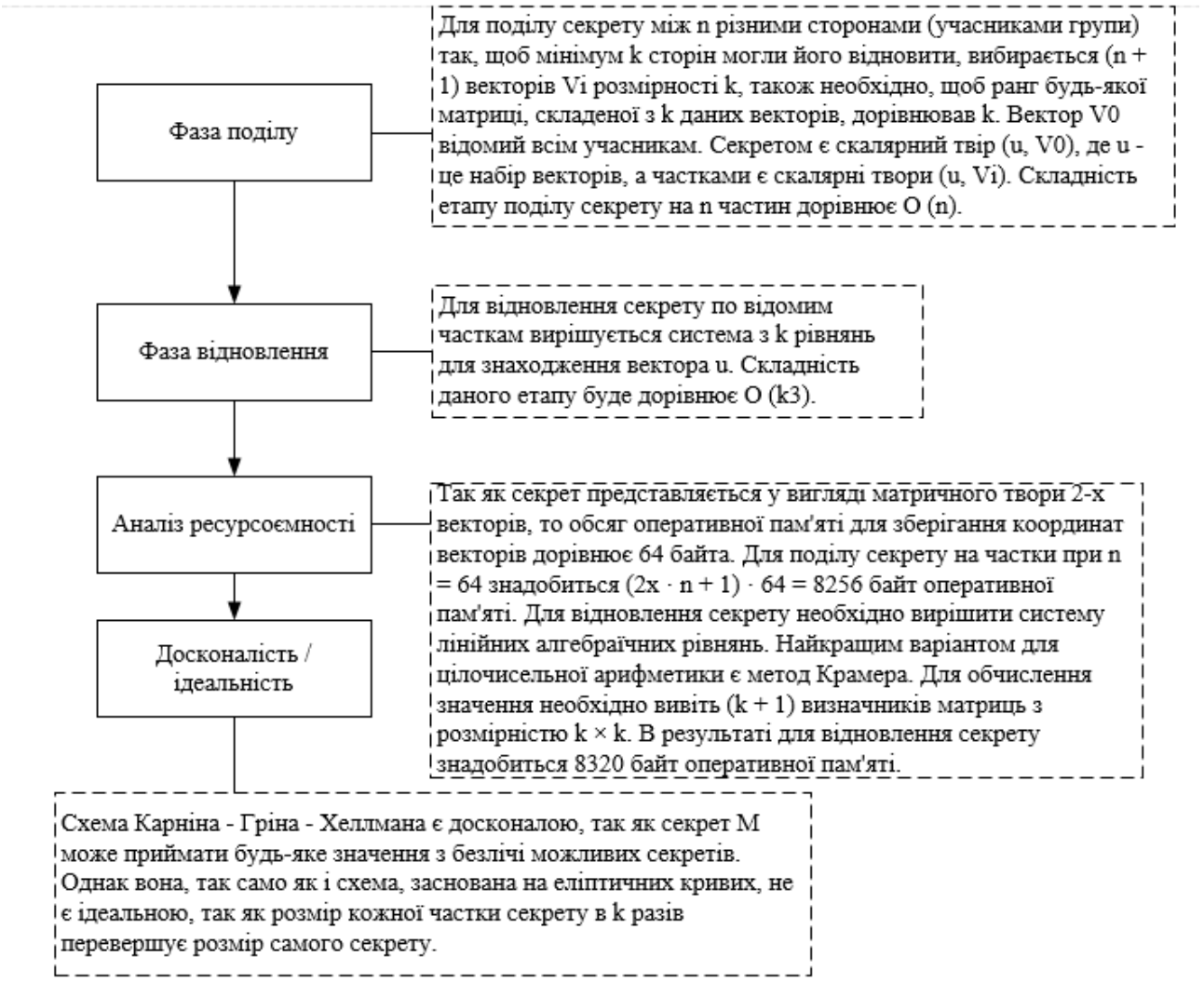

Рисунок 3.14 – Принцип роботи СРС Карніна-Гріні-Хелмана

В основі будь-якого криптографічного протоколу лежить набір певних правил, що регламентують використання криптографічного перетворення і алгоритмів в інформаційних процесах.

Можна зробити висновок, що схема Шаміра має властивості досконалості і ідеальності, вона є менш ресурсномісткої в порівнянні з іншими схемами. Результати порівняння порогових СРС свідчать про те, що за комплексом показників СРС Шаміра є найбільш ефективною в порівнянні з іншими.

3.3 Розробка способу генерації часток секретних даних

Ця робота відноситься до генерування часток секретних даних. Частки визначаються на основі секретних даних, одного або кількох елементів випадкових даних, доданих до секретних даних, та коефіцієнтів систематичного коду з поділом на максимальну відстань (MDS). Код MDS має кількість елементів вхідних даних, яка дорівнює першому пороговому значенню і також дорівнює кількості елементів секретних даних плюс кількість одного або декількох елементів випадкових даних. Метод визначення часток може використовуватися для різних наборів даних, і може бути згенеровано кілька пар часток, що дозволяє виконувати операцію між першими секретними даними та іншими секретними даними на основі розподіленої обробки кожної з множини пар.

Додавання випадкових елементів даних призводить до схеми спільного використання сходинки з другим порогом. Будь-яка кількість акцій нижче другого порога не дає жодної інформації про секрет. Регулюючи кількість випадкових елементів даних, другий поріг може бути відрегульований таким чином, що кількість часток, для яких ентропія дорівнює ентропії секретних даних, збільшується. Більший другий поріг дає додаткову цінність у багатьох додатках, оскільки забезпечує додаткову гарантію безпеки. Крім того, спосіб дозволяє кероване зменшення ентропії секретних даних, не зменшуючи ентропію будь-якого окремого елемента секретних даних, коли кількість часток менше першого порога, але більше другого порога. Оскільки частки секретних даних визначаються на основі обраної кількості випадкових даних, метод є гнучким, оскільки він може бути налаштований на різні другі порогові значення та різну кількість часток.

Інші методи забезпечують гарантію безпеки тільки для першого порога, що дозволяє відновити секретні дані, і не гарантують захист, коли кількість загальних ресурсів менша за перший поріг, але більша за другий поріг. Отже, перевагою запропонованого методу є те, що він забезпечує ширший спектр додатків і безпечніший, ніж інші методи. Інші системи можуть бути захищені від небагатьох зловмисників. Але коли існує велика кількість зловмисників, ці системи можуть

бути зламані, і зловмисники можуть дізнатися про секрети. Однак при використанні вищезгаданого методу система може протистояти великій кількості зловмисників і, як і раніше, захищати окремі елементи секретних даних.

Випадкові дані, додані до таємних даних, можуть містити випадкові дані, додані до таємних даних. Визначення часток може включати визначення кодових слів коду MDS як часток, так що кожна частка відрізняється від будь-якої частини секретних даних. Множинні набори коефіцієнтів можуть бути коефіцієнтами матриці, що породжує систематичного коду з поділом на максимальну відстань. Визначення декількох часток може включати визначення безлічі часток, так що L елементів секретних даних можуть бути визначені на основі порогового числа t безлічі часток, а визначення множин часток може включати визначення безлічі часток на основі t - L елементів випадкових даних. Визначення безлічі часток може включати визначення n часток, і щонайменше n-t+L наборів коефіцієнтів можуть містити щонайменше два коефіцієнти більше нуля. Спосіб може містити визначення, щонайменше, частини матриці, що породжує для коду з поділом на максимальну відстань з t вхідними значеннями і n+L вихідними значеннями. Спосіб може додатково включати визначення кількості елементів випадкових даних, які повинні бути додані до множини елементів секретних даних на основі t і L. Визначення кількості елементів випадкових даних може включати обчислення t–L.

Створення кількох пар може відбуватися відповідно до:

$$\begin{vmatrix} E_1^1 & E_1^2 & 0 & \cdots & 0 \\ E_1^1 + E_2^1 & E_1^2 + E_2^2 & & \ddots & \vdots \\ \vdots & & & & 0 \\ E_1^1 + E_n^1 & E_1^2 + E_n^2 & \cdots & E_n^1 & E_n^2 \end{vmatrix}, \qquad (3.8)$$

де E_i^1 – і-я перша акція,

E_i^2 – j-я друга акція.

Спосіб може додатково включати події, наведені на рис. 3.15.

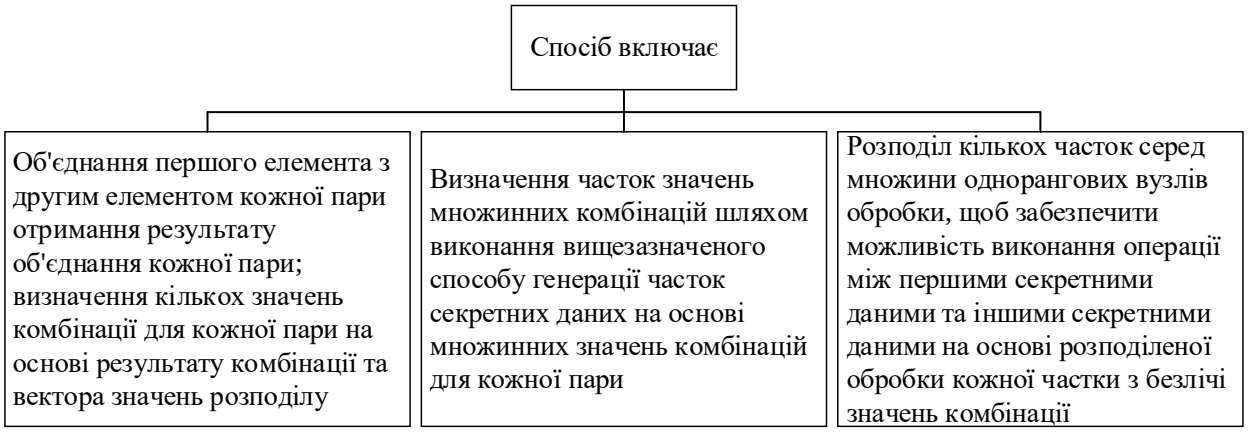

Рисунок 3.15 – Додаткові складові

Спільне використання секрету є важливим примітивом у багатьох протоколах для безпечних багатосторонніх обчислень (MPC), а схема спільного використання секрету Shamir – одна зі схем, що використовуються в MPC. У схемі поділу порогового секрету дилерський комп'ютер безпечно ділиться секретом S з групою з n учасників, таких як комп'ютери, що беруть участь, шляхом створення n загальних ресурсів E1, ..., En і роздача їх учасникам. Секрет може бути відновлений шляхом агрегування підмножини t або більше часток, де t<n – зумовлений поріг, і секрет залишається захищеним, якщо є менша кількість часток.

Нехай S – секрет, та E_1, ..., E_n – загальні. Схема поділу порогового секрету (t, n) задовольняє таку властивість: для будь-якого набору індексів i_1, ..., i_x, де x – кількість доступних загальних ресурсів:

$$H\left(S \mid E_{i_1},...,E_{i_x}\right)=\begin{cases} H(S), & \text{if } x > t \\ 0, & \text{if } t \le x \le n \end{cases}. \qquad (3.9)$$

H(S) позначає функцію ентропії Шеннона випадкової величини S зі значеннями з кінцевої непустої множини F:

$$H(S)=-\sum_{s\in F} P(S=s)\cdot \log_2\left(P(S=s)\right). \qquad (3.10)$$

P(S=s) – це ймовірність того, що S має конкретне значення sF, тому ентропія вимірює невизначеність, пов'язану з очікуваним значенням S. H(S|E) позначає умовну ентропію, вимірюючи невизначеність S, коли E відомий. Перевага лінійних схем (побудованих з лінійної комбінації елементів кінцевого поля) у тому, що лінійні властивості полегшують безпечні обчислення з урахуванням загальних ресурсів. Приклад лінійної порогової схеми є схема Шаміра, де операції здійснюються засновані на вибраному (кінцевому) полі Галуа GF наведено на рис. 3.16.

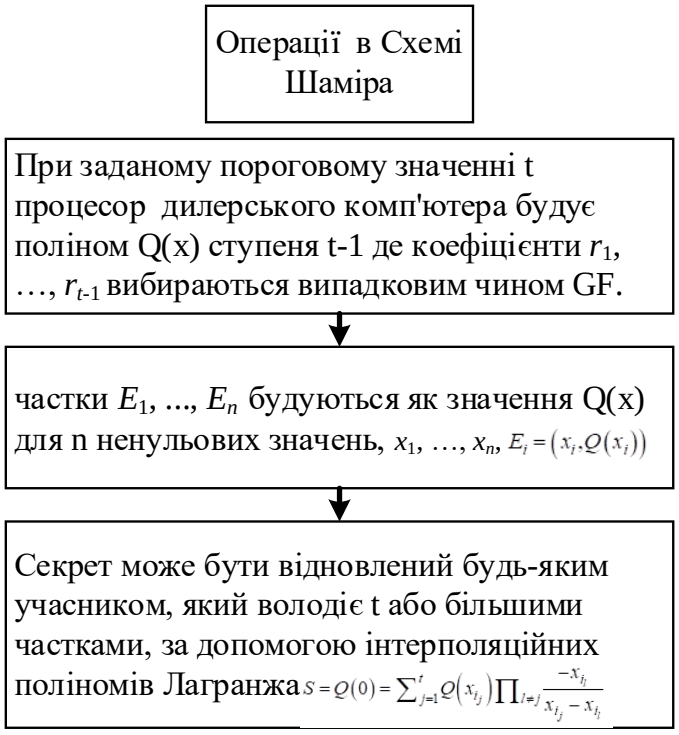

Рисунок 3.16 – Операції на прикладі схеми Шаміра

При спільному використанні секрету зазвичай розглядаються два типи атак (рис. 3.17).

Рисунок 3.17 – Атаки при спільному використанні секрету

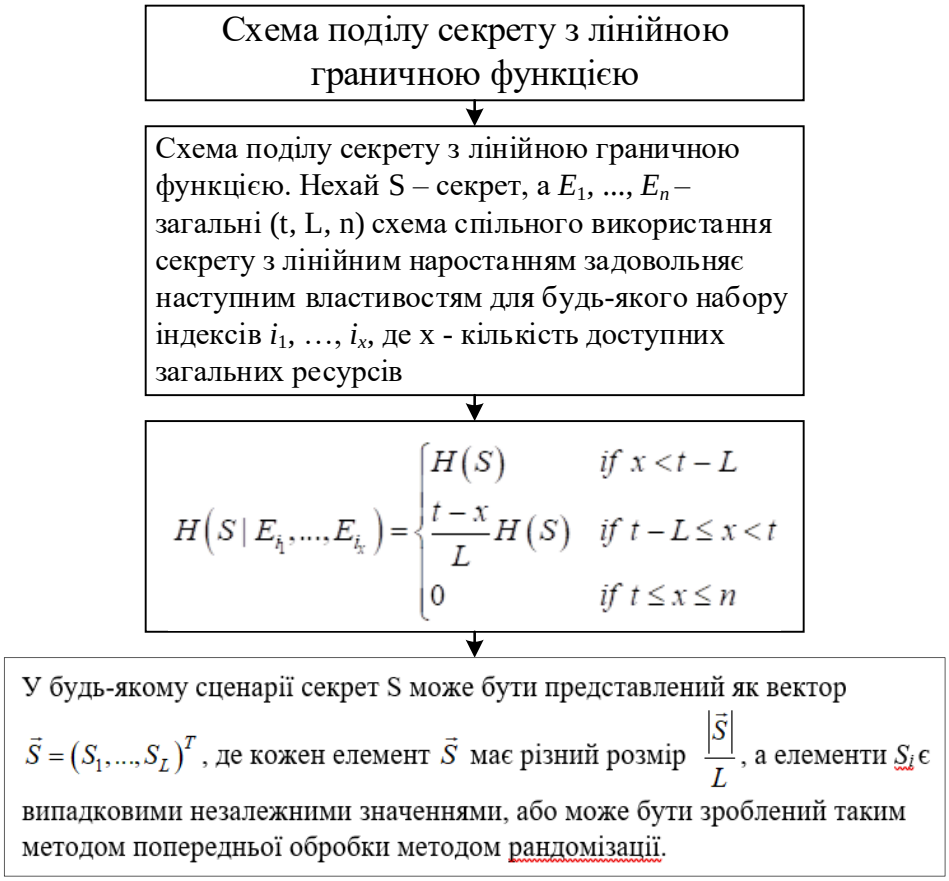

Рисунок 3.18 – Схема поділу секрету з лінійною граничною функцією

Визначення рампових схем забезпечує обмеження витоку інформації для всього секрету, а не для будь-якої підмножини секретного вектора $\vec{S}$. Фактично, дилер може спільно використовувати (безпосередньо) будь-який окремий елемент

і при цьому задовольняти умовам схеми лінійної зміни, в якій L=t. Наприклад, якщо S_1 виявлено, і припускаючи рівну ентропію для всіх елементів у $\vec{S}$, $H\left(\vec{S}\,|\,S_1\right)=\frac{t-1}{t}H\left(\vec{S}\right)$.

МРС забезпечує безпечні обчислення з урахуванням приватних вхідних даних. Враховуючи вхідні дані від m сторін (вхідних однорангових вузлів), МРС являє собою криптографічний протокол, який дозволяє n розподіленим сторонам (однорангові вузли) спільно обчислювати функції, забезпечуючи формальні гарантії конфіденційності вхідних даних і правильності результату обчислень. Сторона може мати одну або обидві ролі протоколу МРС.

Деякі методи МРС можуть використовувати спільне використання секрету, наприклад схема Шаміра. Для виконання безпечних обчислень вхідні однорангові вузли генерують загальні ресурси своїх даних і розподіляють їх між вузлами конфіденційності (зазвичай по одній частці однорангове з'єднання). Однорангові вузли конфіденційності обчислюють необхідну операцію та спільно реконструюють остаточний результат обчислення, який, нарешті, повертається одноранговим вхідним вузлам (табл. 3.2).

Таблиця 3.2 – Позначення, що використовуються для опису схем лінійної зміни та кодів

Позначення	Опис
n	Кількість долей, генерованих схем розділення секретів, еквівалентно кількості однорангових вузлів конфіденційності.
t	Поріг безпеки для схем спільного використання секрету, еквівалентний мінімальній кількості пакетів, необхідних декодування коду стирання.
L	t-L – другий поріг безпеки для схем рампи.
N	Розмір кодового слова (кількість пакетів) для коду стирання.
$G_{N\times t}$	Генераторна матриця (r, N) MDS-коду.
$\vec{S}=\left(S_1,...,S_L\right)^T$	Секрет, вектор з L елементів (пакетів)
$\vec{E}=\left(E_1,...,E_n\right)^T$	Вектор із n закодованих елементів (пакетів) або вектор із n часток, згенерований схемою спільного використання секретів.

$\vec{V} = (S_1,...,S_L, r_1,..., r_{t-L})$	Векторний секрет, заповнений випадковими елементами (використовується в процесі генерації часток)
$M_{\{i1,...,ij\}}$	Подматриця будь-якої матриці M, побудованої з строк $\{i_1,\ldots,i_j\}$
I_t	Матриця ідентичності розміру t
$0_{i,j}$	Нульова матриця розміру i×j

Алгоритм: генерація спільного доступу з систематичного коду MDS наведено на рис. 3.19.

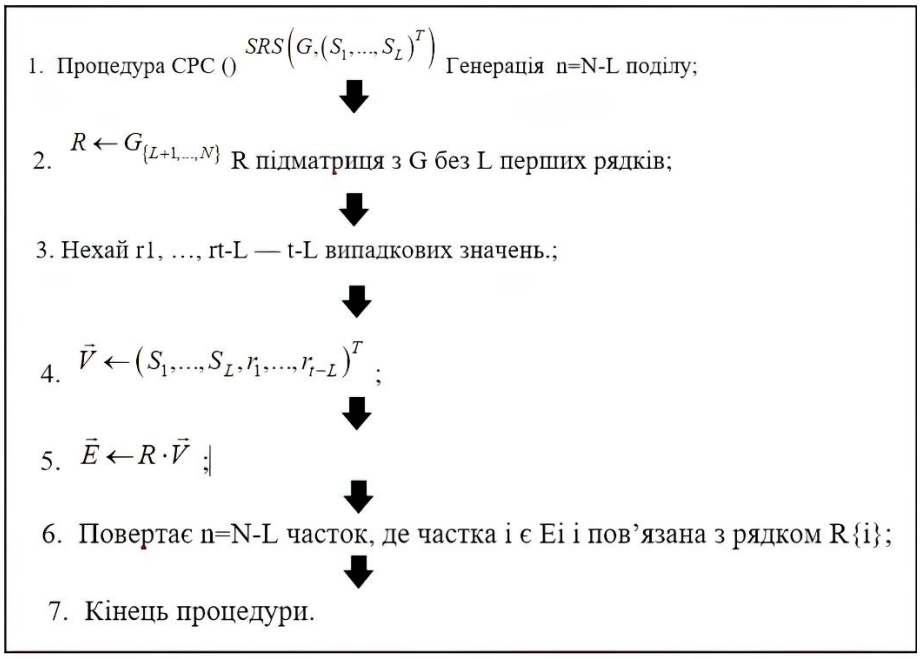

Рисунок 3.19 – Процес генерації спільного доступу

З цією метою підматрица $R_{(N\_L)>t}$ отримується шляхом взяття останніх N-L строк матриць G. Потім секретний вектор $\vec{S}$ розширюється до вектора $\vec{V}$ довжини t шляхом додавання до нього t-L випадкових значень. Зрештою, результатом $R \cdot \vec{V}$ є вектор, що становить частки N-L, де кожна частка пов'язана з відповідним рядком R, який її згенерував ($E_i = R_{\{i\}} \cdot \vec{V}$). Передбачається, що матриця R та призначення рядків учасникам та їх часткам є загальнодоступними.

Будь-яка підмножина $\vec{E}' = \left\{E_{i_1},...,E_{i_t}\right\}$ t часток, пов'язане з підмножиною рядків R, достатньо для відновлення вектора $\vec{V}$ строки $R_{\{i_1\}},...,R_{\{i_t\}}$ утворюють квадратну матрицю R', яка гарантовано неособлива, оскільки є підматрицею G а

генераторна матриця MDS-коду. Отже, існує лише одне рішення $R' \cdot \vec{X} = \vec{E}'$ і оскільки $\vec{V}$ це правильне рішення, обов'язково $\vec{X} = \vec{V}$ та перші L елементів цього вектора є відновленими загальними секретами.

Додавання t-L випадкових значень вектора V відповідає нижній межі випадковості, яка використовується для отримання схеми лінійної зміни (рис. 3.20).

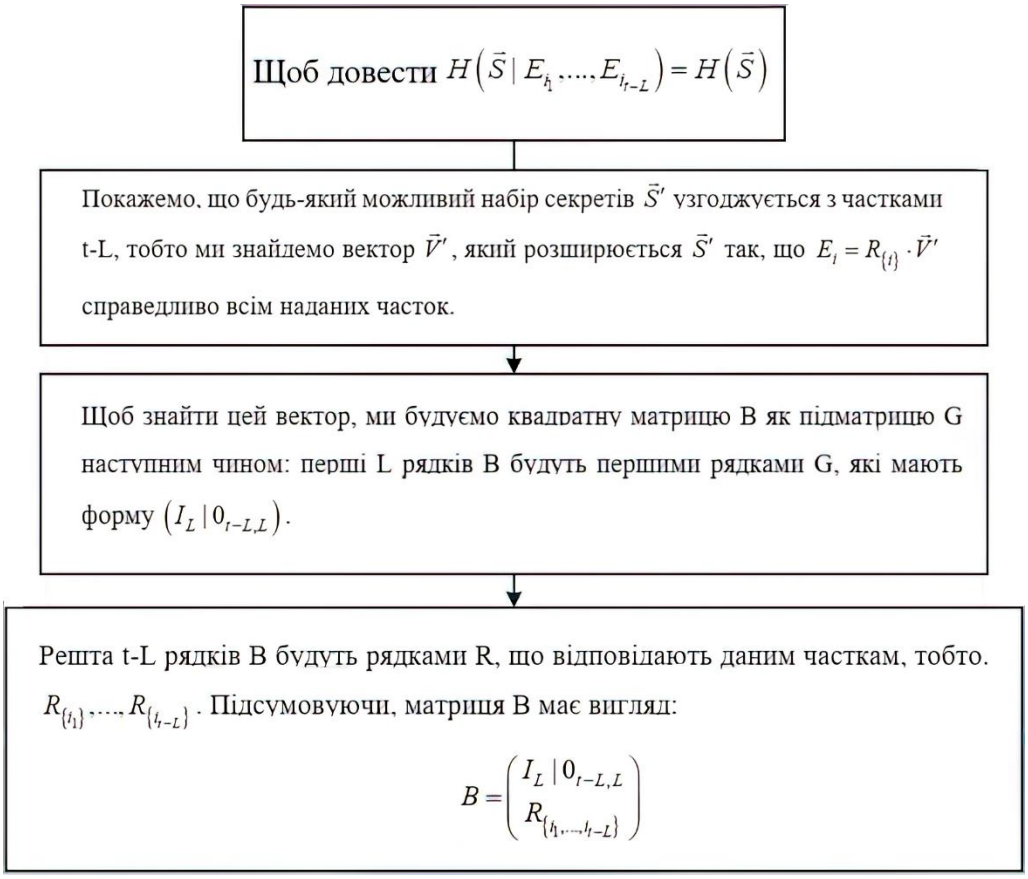

Рисунок 3.20 – Процес доведення

Пропонується додатковий метод побудови сильної схеми наростання, починаючи з розподілу секрету Шаміра. Як ми покажемо в наступному розділі, ця схема забезпечує 25 додаткових обчислювальних можливостей відповідно до схеми Шаміра (тобто не обмежується операціями GF (2q) Поля Галуа, які найчастіше використовуються для кодів Ріда-Соломона).

Багаточлен ступеня t-1 може бути однозначно визначений своїми/коефіцієнтами, але він також може бути однозначно визначений t його точок. У схемі Шаміра використовується лише один секрет, тому фіксується лише

постійний коефіцієнт, який також є точкою полінома на абсцисі 0. Потім випадково вибираються інші коефіцієнти.

Нехай $\vec{S} = (S_1,...,S_L)^T$ буде секретним вектором для спільного використання, та нехай r_1, …, r_{t-L} будуть t-L випадковими значеннями. Багаточлен Q ступеня t-1 однозначно визначається t точками $(x_0, Q(x_0) = S_1),...,(x_{L-1}, Q(x_{L-1}) = S_L),(x_L, Q(x_L) = r_1),...,(x_{t-1}, Q(x_{t-1}) = r_{t-L})$, де $x_0,\ldots,x_{t-1}$ різні. З цих точок значення x-х. поліном Q можна інтерполювати для будь-якого $x: Q(x) = \sum_{i=0}^{t-1} Q(x_i) \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}$. Потім, як і у схемі Шаміра, частки виводяться з полінома шляхом обчислення нових точок.

Властивість, що полягає в тому, що схема є суворою схемою наростання, випливає з теореми 2: лінійна схема, що визначається точками $(x_0, Q(x_0) = S_1),...,(x_{L-1}, Q(x_{L-1}) = S_L),(x_L, Q(x_L)),...,(x_{n+L-1}, Q(x_{n+L-1}))$, є (t, N) систематичним MDS-кодом з N = n + L, оскільки поліном можна інтерполювати з будь-яких t точок, а вихідні інформаційні пакети – це перші точки $Q(x_0)$, …, $Q(x_{t-1})$. Отже, проколювання (тобто видалення) L елементів, що з секретами, створює сильну схему лінійного зміни (рис. 3.21).

Клас Randomization гарантує, що (кілька) секретів взаємно незалежні – це необхідна умова для ентропійної гарантії безпеки рампових схем. Це робиться шляхом додавання (локально згенерованої) випадкової послідовності секретів на стороні вхідного однорангового вузла і шляхом видалення комбінації випадкових даних після того, як результат повертається (одержувачам) вхідним одноранговим вузлам [30].

3.4 Висновки до розділу 3

У третьому розділі дипломної роботи було представлено покращену модель СРС засновану на схемі Шаміра. Спосіб виконання операції між першими секретними даними та іншими секретними даними, що містить: виконання способу

для визначення перших часток перших секретних даних виконання способу для визначення других часток других секретних даних, генерація декількох пар, кожна з декількох пар містить перший елемент на основі перших часток і другий елемент на основі других часток, щоб забезпечити можливість

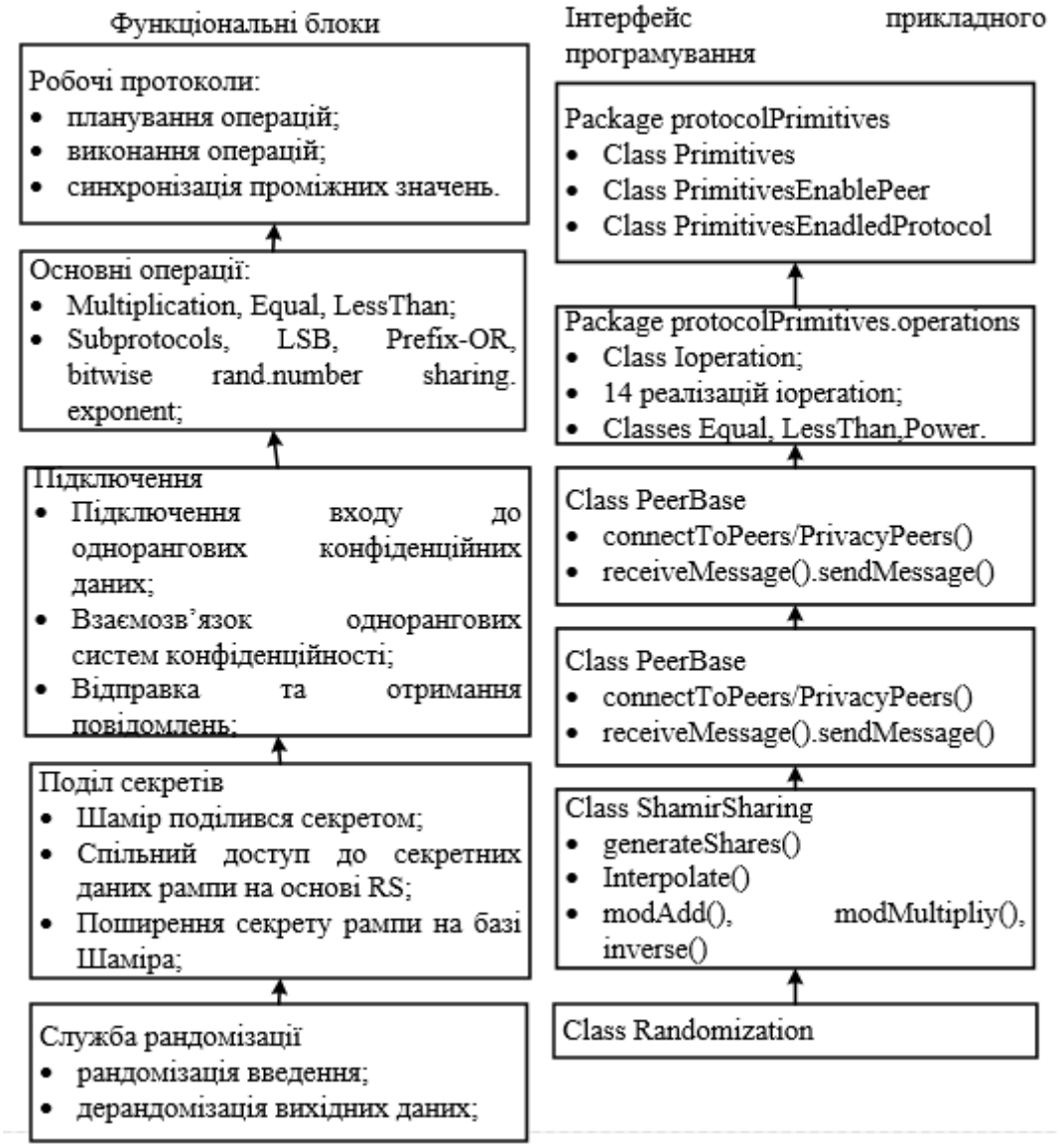

Рисунок 3.21 – Функціональні будівельні блоки та відповідні елементи модифікованої бібліотеки API

виконання операції між першими секретними даними з іншими секретними даними на основі розподіленої обробки кожної з множини пари.

Обчислення на основі лінійних схем можуть застосовуватися до попарних операцій з елементами вектора. Існує низка сценаріїв, що включають агрегацію даних різнорідних (множинних) елементів, які виграють від покращень, що вносяться цими схемами, і, можливо, допустять зниження рівня безпеки. Практична значимість запропонованого методу полягає в поліпшенні існуючого методу поділу секретів для кращого приховування даних, що передаються.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Ергономічні проблеми безпеки життєдіяльності

Під ергономікою розуміють галузь знань, яка комплексно вивчає трудову діяльність людини у системах ЛМС з метою забезпечення її ефективності, безпеки та комфорту.

Мета ергономіки — підвищення ефективності системи ЛМС, забезпечення безпеки праці.

Завдання ергономіки:

- розробка основ проектування діяльності людини-оператора з врахуванням специфіки експлуатації технічних систем та факторів навколишнього середовища;
- вивчення закономірностей взаємодії людини з технічними системами та навколишнім середовищем;
- формування принципів побудови системи Л МС та алгоритмів дії у них людини-оператора;
- розробка перспективних форм праці людини і пов'язаних з нею технічних систем, факторів навколишнього середовища;
- розробка методів дослідження, проектування та експлуатації системи Л МС, які забезпечують безпеку людини, ефективність праці.

Предметом ергономіки є трудова діяльність людини у процесі взаємодії з технічними системами та в умовах особливого впливу на неї факторів навколишнього природного середовища.

У системі ЛМС завжди є 3 елементи: предмет праці, засоби праці та суб'єкт праці. Найменшою цільною одиницею, де наявні вказані елементи, є місце праці.

Місце праці — це зона, де є необхідні технічні засоби, де відбувається трудова діяльність людини. Місце праці обладнане засобами відображення інформації, органами керування та допоміжним обладнанням.

Організацією місця праці називається проведення системи заходів шодо його обладнання засобами та предметами праці і їх розташуванням у визначеному порядку з метою досягнення:

- оптимізації умов трудової діяльності;
- безпеки праці;
- максимальної ефективності;
- комфортності роботи людини.

До робочого місця ставляться такі вимоги:

- достатній робочий простір, який дає змогу працюючій людині здійснювати необхідні рухи та переміщення;
- достатні фізичні, зорові та слухові зв'язки між людиною та обладнанням, а також між людьми під час виконання спільного трудового завдання;
- необхідний рівень освітлення;
- наявність необхідних засобів захисту;
- оптимальне розташування робочих місць, а також безпечні та достатні проходи для працюючих людей.

Органи керування повинні забезпечити перехід дій від людини до машини. Вони мають бути надійними у роботі та зручними в користуванні, не допускати аварій, травм при перевантаженнях та помилкових діях людини. При організації робочого місця враховують основні антропометричні дані людини. Найважливішою характеристикою робо чого місця є зона досягнення моторного поля.

Моторне поле — це простір робочого місця, в якому розміщені органи керування та інші технічні засоби, в якому людина здійснює рухові дії для виконання робочого завдання.

Розрізняють зони легкого та оптимального досягнення.

Легке досягнення — при русі руку плечовому суглобі з опорою Оптимальне досягнення — рух у ліктьових суглобах з опорою.

При організації місця праці потрібно враховувати:

- ступінь рухливості оператора (сидячи, стоячи);
- конфігурацію і спосіб розміщення каналів індикаторів та органів

керування;

- потребу в огляді робочого простору;
- необхідність використання робочої поверхні для писання та інших робіт, розміщення телефонів, розташування інструкцій тощо.

Велике значення має правильний вибір робочого сидіння Конструкція робочого сидіння повинна забезпечити підтримку основної робочої пози, не утруднювати робочих рухів, зміну положення, забезпечити умови для відпочинку.

Продуктивність праці, працездатність людини в багатьох випадках визначаються правильним встановленням режиму праці та відпочинку, що означає зміну періодів праці та відпочинку протягом доби, тижня та довшого терміну.

Реалізація основних ергономічних вимог до режимів праці та відпочинку дає змогу забезпечити необхідний рівень працездатності, зменшити втому, зберегти здоров'я людей.

Для операторів, які працюють з екранами дисплеїв та інших індикаторів, можуть бути рекомендовані такі режими праці та відпочинку.

Тривалість безперервної праці не повинна перевищувати 4—6 год. В іншому випадку працездатність через втому зору раптово знижується. Під час праці, яка не допускає відхилення уваги, її тривалість слід скорочувати. Наприклад, оператор, який стежить за екраном індикатора, найуважніше і найточніше працює протягом перших 30 хв чергування. За цей час він допускає мінімальну кількість помилок (пропусків та хибних тривог). Надалі, внаслідок втоми зорового аналізатора, кількість помилок зростає май же в два рази та залишається незмінною до кінця другої години. Тому для підтримки високої ефективності праці може бути рекомендований 30-хвилинний період чергування з наступною 30-хвилинною перервою.

Для обслуговуючого персоналу, при роботі якого допускаються нерегламентовані перерви і не потрібне постійне перебування на місці праці, тривалість безперервної праці може перевищувати 6 год.

Тривалість відпочинку повинна бути у 2 рази (а при інтенсивному навантаженні — у 3 рази) більшою, ніж тривалість безперервної роботи.

Максимальний інтервал між періодами праці не повинен перевищувати 48 год, тому що більша тривалість відпочинку призводить до значного збільшення часу спрацьованості (у 4—10 разів).

Організація відпочинку має дві мети:

- зняти втому, яка виникла внаслідок попередньої праці;
- забезпечити швидке включення у роботу відпочиваючої зміни (збереження трудової готовності).

При організації праці протягом тижня, місяця потрібно враховувати ту обставину, що з часом організм людини пристосовується до нічної праці і часто злам складеного стереотипу негативно впливає на його працездатність. Разом з тим тривала праця в нічну зміну порушує соціальні та інші зв'язки, що викликає негативну психологічну реакцію. Тому доцільніше чергувати роботу у денну та нічну зміни.

4.2 Перша допомога людині, яка уражена електричним струмом

Широке застосування електроенергії вимагає правильного поводження з нею, оскільки порушення правил електробезпеки може призвести до важкої і навіть смертельної травми. Установлено, що при напрузі 42 В електричний струм, який проходить через тіло людини, є безпечним. Напруга вище 50 В викликає тепловий і електролітичний ефект.

Найчастіше ураження виникає внаслідок невиконання техніки безпеки при роботі з електричними приладами як у побуті, так і на виробництві.

Звільнення потерпілого від дії електричного струму відбувається наступним чином. У першу чергу необхідно знеструмити обладнання або провід, які стали причиною ураження людини струмом. Підходять для цього всі способи: вимкнути рубильник, вивернути або вимкнути пробки на електричному щитку, припинити подачу живлення роз’єднанням найближчого штепсельного роз’єму.

У разі неможливості припинення подачі електричного струму штатними засобами, необхідно перерубати окремо кабелі живлення, використовуючи будь-які ріжучі предмети з ізольованими рукоятками.

Якщо ж і це зробити немає можливості, потерпілого необхідно відтягнути від електричної установки або скинути з нього провід за допомогою будь-якого струмонепровідного предмету. При цьому важливо захистити себе від впливу електричного струму, надівши на руки гумові рукавички або обмотавши їх сухою тканиною. На ноги бажано одягнути гумове взуття, у разі його відсутності підкласти під ноги гумовий килимок, суху дошку або згорнуту сухий одяг. Відтягувати потерпілого слід за краї одягу, уникаючи контакту з відкритими ділянками його тіла.

Перша допомога проявляється в тому, що відразу ж, протягом 10-20 секунд, необхідно визначити ступінь ураження людини електричним струмом. Поклавши потерпілого на спину і розстебнувши одяг, що утруднює дихання, потрібно перевірити наявність у нього пульсу на шиї в районі сонної артерії або на променевій артерії в області зап'ястя, переконатися у присутності дихання з підйому і опускання грудної клітини, перевірити кровообіг мозку по наявності рефлекторної реакції звуження зіниці ока при попаданні на нього яскравого світла.

Якщо потерпілий перебуває у свідомості, однак тривалий час піддавався впливу електричного струму або ж отямився після непритомності, йому потрібно забезпечити спокій з подальшим спостереженням за ним на протязі 3-4 годин, але все ж таки краще викликати бригаду швидкої медичної допомоги. Можна дати йому теплий чай, 20 крапель валеріанової настоянки і тепло вкрити ковдрою.

У разі погіршення стану потерпілого, при появі серцевої недостатності, частому переривчастому диханні, збліденні шкірних покривів, необхідно без зволікання приступати до виконання штучного дихання і масажу серця.
Заборонено припиняти виконання реанімаційних заходів до прибуття лікаря, їх необхідно продовжувати і в тому випадку, коли у постраждалого геть відсутні всі ознаки життя.

Незалежно від ступеню ураження струмом, потерпілий ще деякий час має бути під наглядом медичного персоналу. Не варто відправляти таку особу додому або відразу допускати її до роботи. Адже дія електричного струму на організм може проявитися через кілька годин і привести до тяжких наслідків.

ВИСНОВКИ

У роботі вирішена актуальна науково-прикладна задача покращення моделі СРС на основі схеми Шаміра, який дозволяє покращити безпеку інформаційних систем та зменшити вирогідність компрометації одного або кількох зберігачів:

1. Проведений аналіз. ландшафту загроз інформаційних. системи показав, що в умовах стрімкого росту обчислювальних можливостей техніки та проблем, які виникли під час пандемії COVID-19, атаки набули масового характеру, тому слід розглядати їх в комплексі.

2. Щоб гарантувати протидію атакам використовуються програмні застосунки, що допомагають виявляти їх дію та правильно їх класифікувати. Серед яких окремо можливо виділити інструменти комп'ютерної криміналістики для розслідування та формування доказової бази. Був зроблений висновок, що не можна розглядати дану тему не зачіпаючи теми антифорензіки.

3. Розглянуті сучасні методи і засоби протистояння ЦК, наведено класифікацію та докладний опис кожного з методів АФ з візуалізацією. Проаналізовано ринок програмного забезпечення на відповідність кожному з методів АФ.

4. Розроблено покращену модель СРС засновану на схемі Шаміра, де частки визначаються на основі секретних даних, одного або кількох елементів випадкових даних, доданих до секретних даних, та коефіцієнтів систематичного коду з поділом на максимальну відстань (MDS). Метод визначення часток може використовуватися для різних наборів даних, і може бути згенеровано кілька пар часток, що дозволяє виконувати операцію між першими секретними даними та іншими секретними даними на основі розподіленої обробки кожної з множини пар.

За результатами дипломної роботи було опубліковано тези доповіді на міжнародних науково-практичних конференціях [31, 32, 33].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Євсєєв С., Хохлачова Ю., Король О. Оцінка забезпечення безперервності бізнес-процесів в організаціях банківського сектора на основі синергетичного підходу, ч. 2 // Сучасна спеціальна техніка. Науково-практичний журнал, 2017. № 2. С. 10–17.

2. Євсєєв С. П. Аналіз захисту в національній системі масових електронних платежів // Інформаційна безпека, 2014. № 3. С. 15.

3. Kopeytsev V., Park S. Lazarus targets defense industry with ThreatNeedle. 2021. URL: https://securelist.com/lazarus-threatneedle/100803/ (дата звернення: 07.08.2021).

4. Cyber attack trends: 2020 mid-year report. 2020. URL: https://research.checkpoint.com/2020/cyberattack-trends-2020-mid-year-report/ (дата звернення: 08.08.2021).

5. Hi-Tech Crime Trends 2020/2021. 2020. URL: https://www.group-ib.ru/resources/threat-research/2020-report.html (дата звернення: 08.08.2021).

6. Gray J. Practical Social Engineering: A Primer for the Ethical Hacker, 2021.

7. Про основні засади забезпечення кібербезпеки України // Верховна Рада України. 2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 12.08.2021).

8. Cybersecurity strategy of Ukraine // Центр стратегічних комунікацій StratCom Ukraine. 2020. URL: https://stratcomua.org/ua (дата звернення: 12.08.2021).

9. Проект Закону України від 14.04.2016 № 2126а // Верховна Рада України. 2016. URL: https://ips.ligazakon.net/document/JH1N268B (дата звернення: 15.08.2021).

10. Oettinger W. Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence 1st Edition, Birmingham: Pact, 2020.

11. ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/standard/44381.html (дата звернення: 21.08.2021).

12. Bielska A. Open source intelligence tools and resources handbook 2020. 2020. URL: https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf (дата звернення: 23.08.2021).

13. Everything about Open Source Intelligence and OSINT Investigations // Maltego Team. 2021. URL: https://www.maltego.com/blog/what-is-open-source-intelligence-and-how-to-conduct-osint-investigations/ (дата звернення: 23.08.2021).

14. Cyber Security Intelligence and Analytics / Xu Z., Choo K.-K. R., Dehghantanha A., Parizi R., 2020. 1478 с.

15. Sasa M., Alvin H., Ernedin Z. Combining static and live digital forensic analysis in virtual environment // XXII International Symposium on Information, Communication and Automation Technologies. URL: https://ieeexplore.ieee.org/document/5348415/authors#authors (дата звернення: 23.08.2021).

16. Intrusion Detection System. 2020. URL: https://www.barracuda.com/glossary/intrusion-detection-system (дата звернення: 27.08.2021).

17. Bhat W. Forensic analysis of anti-forensic file-wiping tools on Windows // Journal of Forensic Sciences. 2021. URL: https://www.researchgate.net/publication/355156039_Forensic_analysis_of_anti-forensic_file-wiping_tools_on_Windows (дата звернення: 27.08.2021).

18. Грибунін В. Г. Цифрова стеганографія. Мінськ: Академія, 2018.

19. Data hiding in the NTFS file system. 2016. URL: https://doi.org/10.1016/j.diin.2016.10.005 (дата звернення: 27.08.2021).

20. Onion Routing // GeeksforGeeks. 2018. URL: https://www.geeksforgeeks.org/onion-routing/ (дата звернення: 27.08.2021).

21. Gary C. Kessler. Anti-Forensics and the Digital Investigator // Champlain College. 2007. URL: https://www.garykessler.net/library/2007_ADFC_anti-forensics.pdf (дата звернення: 29.08.2021).

22. VeraCrypt – практичні посібники з використання програми, інструкції VeraCrypt, зашифрувати диск VeraCrypt, зашифрувати системний диск у Windows та Linux URL: https://veracrypt.ru/ (дата звернення: 29.08.2021).

23. Timestomp [Електронний ресурс] – URL: https://forensicswiki.xyz/wiki/index.php?title=Timestomp. 2018 (дата звернення: 29.08.2021).

24. The Ultimate Packer for eXecutables. 2019 URL: https://github.com/upx/upx (дата звернення: 29.08.2021).

25. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. Мінськ: Тріумф,2018.

26. Шнайер Б. Алгоритмы разделения секрета // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. 2018. С. 588–591.

27. Схема разделения секрета Шамира. 2018. RL: https://habr.com/ru/post/431392/ (дата звернення: 29.08.2021).

28. Zafarzhon N. Analysis of cryptographic secret sharing schemes for backing up key information // Astrakhan State University. 2019. URL: https://www.researchgate.net/publication/340135824_ANALYSIS_OF_CRYPTOGRAPHIC_SECRET_SHARING_SCHEMES_FOR_BACKING_UP_KEY_INFORMATION (дата звернення: 30.08.2021).

29. Karnin E.D., Greene J. Hellman M.E. On secret sharing systems // IEEE Transactions on, 2003. С. 35–41.

30. Smith G., Boreli R. Generating shares of secret data. New South Wales: Université de Toulouse, 2016.

31. Макаренко А. О. Використання системи для розподіленого зберігання інформації в анти-форензиці // Всеукраїнська науково-технічна конференція застосування програмного забезпечення в інфокомунікаційних технологіях, 2021. С. 76–77.

32. Макаренко А. О. Використання системи для розподіленого зберігання інформації в анти-форензиці // XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів «Стан, досягнення та перспективи інформаційних систем і технологій», 2021. С. 42–44.

33. Макаренко А. О. Використання системи для розподіленого зберігання інформації в анти-форензиці // XI Міжнародна науково-технічна конференція студентства та молоді «Світ інформації та телекомунікацій», 2021. С. 291–292.