Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«МОДЕЛЬ КРИМІНАЛІСТИЧНОГО РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ»

Виконав: студент 2-го курсу, групи 1БС-22м
спеціальності 125 – Кібербезпека
(шифр і назва напряму підготовки, спеціальності)

_____Леонід МАЙДАНЕВИЧ
(ім'я та прізвище)

Керівник к. т. н., доц. каф. ЗІ
_____Олеся ВОЙТОВИЧ
(ім'я та прізвище)

Опонент: к. т. н., доц. каф. ПЗ
_____Олександр ХОШАБА
(ім'я та прізвище)

«__11__» ____12____ 2023 р.

Допущено до захисту
Завідувач кафедри ЗІ
д. т. н., проф.
_____Володимир ЛУЖЕЦЬКИЙ
«__12__» ____12____ 2023 р.

Вінниця ВНТУ – 2023 року

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти другий (магістреський)
Спеціальність 125 Кібербезпека
ОПП Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ

Завідувач кафедри ЗІ, д. т. н., проф.

_____Володимир ЛУЖЕЦЬКИЙ

19 09 2023 року

ЗАВДАННЯ
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Майданевичу Леоніду Олександровичу

1. Тема роботи: «Модель криміналістичного розслідування кіберзлочинів» керівник роботи: Войтович Олеся Петрівна, к. т. н., доц. каф. ЗІ, затверджена наказом ректора ВНТУ від 18.09.2023 року № 247.

2. Строк подання студентом роботи 10 грудня 2023 року.

3. Вихідні дані до роботи:

- звіти про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2022-2023рр. (Державна служба спеціального зв'язку та захисту інформації України);
- перелік категорій кіберінцидентів (схвалений Національним координаційним центром кібербезпеки при РНБО України, протокол №18 від 28.10.2021 №16/320/21);
- кіберзлочини передбачені Кримінальним кодексом України;
- теоретико-методологічні принципи дослідження кіберзлочинів.

4. Зміст розрахунково-пояснювальної: Вступ. 1. Аналіз джерел за темою дослідження. 2. Розробка моделі розслідування кіберзлочинів. 3.Використання спеціальних знань при розслідуванні кіберзлочинів. 4. Економічна частина. Висновки. Перелік використаних джерел. Додатки.

5. Перелік ілюстративного матеріалу: Перелік категорій кіберінцидентів (плакат, А4). Теоретико-множинні моделі категорій кіберінцидендів (плакат, А4). Характеристика підготовчих дій на початковому етапі розслідування кіберзлочинів (плакат, А4). Модель розслідування кіберзлочинів (плакат, А4). Схема моделі роботи з електронними доказами при розслідуванні кіберзлочинів (плакат, А4). Схема покрокової моделі розслідування кіберзлочинів (плакат, А4). Сутнісні ознаки комп'ютерно-технічної та телекомунікаційної експертизи (плакат, А4). Причини які впливають на проведення експертизи при розслідуванні кіберзлочинів (плакат, А4). Критерії оцінки та використання

результатів судових експертиз при розслідуванні кіберзлочинів (плакат, А4). Спрощена схема аналізу контрольних точок (на базі рекурсивних платформ) (плакат, А4). Критерії оцінки та використання результатів судових експертиз спеціально уповноваженими суб'єктами при розслідуванні кіберзлочинів (плакат, А4). Приклад криміналістичного дослідження кіберзлочину передбаченого ч.1 ст. 361-1 КК України (плакат, А4).

6. Консультанти розділів роботи

Розділ	Ім'я та прізвище, посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Олеся ВОЙТОВИЧ, к. т. н., доц. каф. ЗІ	19.09	25.09
2	Олеся ВОЙТОВИЧ, к. т. н., доц. каф. ЗІ	19.09	19.10
3	Олеся ВОЙТОВИЧ, к. т. н., доц. каф. ЗІ	19.09	30.10
4	Ольга РАТУШНЯК, к. е. н., доц. каф. ЕПВМ	19.09	27.11

7. Дата видачі завдання 1 вересня 2023 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	01.09.2023 – 10.09.2023	
2	Аналіз літературних джерел за напрямком магістерської кваліфікаційної роботи	10.09.2023 – 15.09.2023	
3	Науково-технічне обгрунтування	16.09.2023 – 22.09.2023	
4	Розробка технічного завдання	23.09.2023 – 29.09.2023	
5	Розробка рішень	30.09.2023 – 12.10.2023	
6	Практична реалізація, моделювання, експериментування, результати	14.10.2023 – 10.11.2023	
7	Розробка розділу економічного обгрунтування доцільності розробки	11.11.23 – 17.11.2023	
8	Аналіз виконання ТЗ, висновки	18.11.2023 – 24.11.2023	
9	Оформлення пояснювальної записки	25.11.2023 – 30.11.2023	
10	Попередній захист та доопрацювання МКР	28.11.2023 – 01.12.2023	
11	Перевірка магістерської роботи на наявність плагіату	02.12.2023 – 10.12.2023	
12	Представлення МКР до захисту	11.12.2023 – 14.12.2023	
13	Захист МКР	14.12.2023 – 21.12.2023	

Студент _____ Леонід МАЙДАНЕВИЧ

Керівник роботи _____ Олеся ВОЙТОВИЧ

АНОТАЦІЯ

УДК 004.056

Майданевич Л. Модель криміналістичного розслідування кібірзлочинів. Магістерська кваліфікаційна робота зі спеціальності 125 Кібербезпека, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2023. 89 с.

Укр. мовою. Бібліогр.: 43 назв; рис.: 8; табл.: 41; формул: 29.

Магістерська кваліфікаційна робота присвячена розробці моделі криміналістичного розслідування кіберзлочинів. Здійснено аналіз відомих рішень при розслідуванні кіберзлочинів. Розроблено теоретико-множинні моделі кіберінцидентів та теоретико-множинні моделі ознак кіберзлочинів передбачених статтями 190, 200, 361 – 363^1 Кримінального кодексу України. Розроблено модель криміналістичного розслідування кіберзлочинів із застосуванням міждисциплінарного та трансдисциплінарного підходу, які враховують відмінності між нормативними та технічними визначеннями та вимогами. Результатом є покращення існуючих криміналістичних моделей розслідування кіберзлочинів та надання рекомендацій щодо підвищення ефективності цього процесу.

В економічному розділі оцінено витрати на розробку.

Ключові слова: кібербезпека, кіберінциденти, кіберзлочини, теоретико-множинні моделі кіберінцидентів, теоретико-множинні моделі ознак кіберзлочинів, модель криміналістичного розслідування кіберзлочинів.

ABSTRACT

Maidanevych L. Model of forensic investigation of cybercrimes. Master's thesis in the specialty 125 – cybersecurity. Vinnytsia: VNTU, 2023. 89 p.

In Ukrainian language. Bibliographer: 43 titles; fig.: 8; table. 41; formulas: 29.

The master's thesis is devoted to the development of a model for the forensic investigation of cybercrimes. An analysis of known solutions in investigation of cybercrimes was carried out. Theoretical-multiple models of cyber incidents and theoretical-multiple models of signs of cybercrimes provided for in Articles 190, 200, 361 – 363^1 of the Ukraine's Criminal Code have been developed. A model for forensic investigation of cybercrime has been developed using an interdisciplinary and transdisciplinary approach, taking into account the differences between regulatory and technical definitions and requirements. The result is to improve existing forensic models for investigating cybercrimes and provide recommendations to improve the efficiency of this process.

In the Economic part estimates development costs.

Keywords: cyber security, cyber incidents, cyber-crimes, theoretical-multiple models of cyber incidents, theoretical-multiple models of cybercrime features, model of forensic investigation of cybercrimes.

ЗМІСТ

ВСТУП

Актуальність теми. Сучасний розвиток інформаційного суспільства в країні та світі обумовлює нові виклики, які в концепції кібербезпеки ще не мають дієвих методів їх вирішення. Насамперед, це стосується кіберзлочинності. Власне, кіберзлочинність – є нагальною перешкодою в еволюційному розвитку інформаційних технологій через недобросовісне та/або злочинне користування можливостями кіберпростору.

Згідно офіційних звітів Держспецзв'язку протягом ІІІ кварталу 2023 року продовжується реальна загроза від кіберінцидентів (кібератак), націлених на українські організації різних форм власності та галузей економіки.

Основою теоретико-методологічних принципів дослідження стали праці науковців – Р. Благута, О. Волков, О. Войтович, А. Дудатьєв, Р. Киричок, Д. Кларк, Л. Куперштейн, М. Можаєв, В. Лужецький, К. Рушер, І. Субач, Б. Теплицький, В. Хаханов та ін.

Метою дослідження є покращення існуючих криміналістичних моделей розслідування кіберзлочинів та надання рекомендацій щодо підвищення ефективності цього процесу.

Для досягнення поставленої мети в магістерській роботі були сформульовані такі ***завдання***:

- проаналізувати відкриті джерела інформації;
- проаналізувати відомі рішення при розслідуванні кіберзлочинів;
- дослідити організаційно-технічну модель кіберзахисту та розробити теоретико-множинні моделі кіберінцидентів;
- розробити теоретико-множинні моделі кіберзлочиннів;
- розробити модель криміналістичного розслідування кіберзлочинів;
- дослідити види та можливості судових експертиз під час розслідування кіберзлочинів;

- визначити критерії оцінок та використання результатів судових експертиз під час розслідування кіберзлочинів та провести експериментальне дослідження кіберзлочинів;
- провести обґрунтування економічної доцільності розробки.

Об'єктом дослідження є процес розслідування кіберзлочинів.

Предметом дослідження є модель криміналістичного розслідування кіберзлочинів.

Методи дослідження. При вирішенні завдань магістерської роботи використовувалися, зокрема: *системний аналіз* (при дослідженні інформації, рішень, відмінностей, критеріїв), *структурно-функціональний аналіз* (при розкритті ієрархічності та функціональних проявів моделей, схем), *теоретико-множинний підхід* (при розробці моделей), *міждисциплінарний* та *трансдисциплінарний підходи* (як певні алгоритми дослідження), *прагматичний підхід* (при забезпеченні розслідування).

Наукова новизна магістерської роботи полягає в тому, що: розроблено модель криміналістичного розслідування кіберзлочинів, яка враховує відмінності між нормативними та технічними визначеннями та вимогами; підготовлено методичні рекомендації які дозволяють покращити використання спеціальних знань при розслідуванні кіберзлочинів.

Практична цінність даної магістерської роботи полягає в тому, що розроблена модель допомагає удосконалити методику розслідування кіберзлочинів.

Публікації результатів магістерської кваліфікаційної роботи. Результати магістерської роботи доповідалися на таких конференціях:

1. Майданевич Л. Діалектичний аналіз кіберзлочинів // Інформаційні технології та комп'ютерна інженерія. Молодь в науці: дослідження, проблеми, перспективи (МН-2024).

2. Майданевич Л. Кіберпростір: основні аспекти // Інформаційні технології та комп'ютерна інженерія. 2023.черв.18.

1 АНАЛІЗ ДЖЕРЕЛ ЗА ТЕМОЮ ДОСЛІДЖЕННЯ

1.1 Аналіз відкритих джерел інформації

Згідно звітів Держспецзв'язку [1; 2; 3] останній постійно фіксує значну кількість кіберінцидентів та кібератак на державні інформаційні ресурси та об’єкти критичної інформаційної інфраструктури. Власне, від початку активної фази війни тренд на зростання кількості кібератак зберігається.

Так, протягом ІІІ кварталу 2023 року за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було:

- опрацьовано 4 мільярди подій, отриманих за допомогою засобів моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки;
- детектовано 1.5 мільйона підозрілих подій інформаційної безпеки (при первинному аналізі);
- опрацьовано 12 тисяч критичних подій інформаційної безпеки (потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу);
- зафіксовано та оброблено безпосередньо аналітиками безпеки 355 кіберінцидентів.

При цьому (порівняно з ІІ кварталом 2023 року) кількість зареєстрованих кіберінцидентів зросла на 46%. Також до Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки протягом звітного періоду було підключено 14 нових об’єктів кіберзахисту, що належать до урядового (12), енергетичного (1) та військового (1) секторів.

Порівняно з ІІ кварталом 2023 року збільшилась кількість об’єктів кіберзахисту відповідно до підсистем: збір мережевої телеметрії – на 3; захист кінцевих точок – на 18; сканування вразливостей – на 8. Серед автономних систем (AS), інфраструктура яких найчастіше ідентифікувалась як джерело

активного сканування під час звітного періоду, можна виокремити «AMAZON-02», «OVN SAS», «AMAZON-AES», «GOOGLE», «Cloudflarenet» [3].

Основною метою хакерів є кібершпіонаж, порушення доступності державних інформаційних сервісів та навіть знищення інформаційних систем за допомогою програм-вайперів. Також, Держспецзв'язку зафіксувало істотне зростання активності хакерських груп щодо розповсюдження шкідливого програмного забезпечення, серед якого є як програми, що викрадають дані, так і ті, які спрямовані на знищення даних.

Порівняно зі статистичними даними за II квартал 2022 року, кількість подій ІБ з високим рівнем критичності зросла у 3,8 разів. Відповідно, кількість зареєстрованих кіберінцидентів з високим рівнем критичності зросла на 128%.

Порівняно з I та II кварталами, у III кварталі 2022 року кількість критичних подій ІБ, джерелом яких є IP-адреси росії, зросла у 35 разів. Також, порівняно з II кварталом 2022 року, майже вдвічі зросла кількість детектованих подій ІБ, пов'язаних із активним скануванням, джерелом яких є IP-адреси росії.

Саме з цих IP здійснювали кібератаки на українські інформаційні ресурси, розповсюджували фейкову інформацію, що стосується дискредитації державних органів під час російсько-української війни.

Наразі найбільша кількість критичних подій ІБ пов'язана з IP-адресами зі США. Проте автоматично визначена геолокація IP-адрес джерел необов'язково означає атрибуцію кібератак до ідентифікованого місцерозташування. Втім, за атрибуцією абсолютна більшість кіберінцидентів пов'язана з хакерськими угрупуваннями, що фінансуються урядом рф. Зокрема, це UAC-0010 (Gamaredon) та інші.

BARAT, Emotet, Cobalt Strike та Meris представляють найчастіше експлуатовану C2 інфраструктуру, детектовану як джерело спроб мережевих вторгнень або порушень політик безпеки організацій, виявлених у вхідному мережевому трафіку Підсистемою збору телеметрії Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки.

Серед сімейств ШПЗ, детектованих у подіях ІБ категорії «02 Шкідливий програмний код» протягом 2023 року, переважають Snake Keylogger, Agent Tesla, LokiBot, PurpleFox та Formbook (рис.1.1).

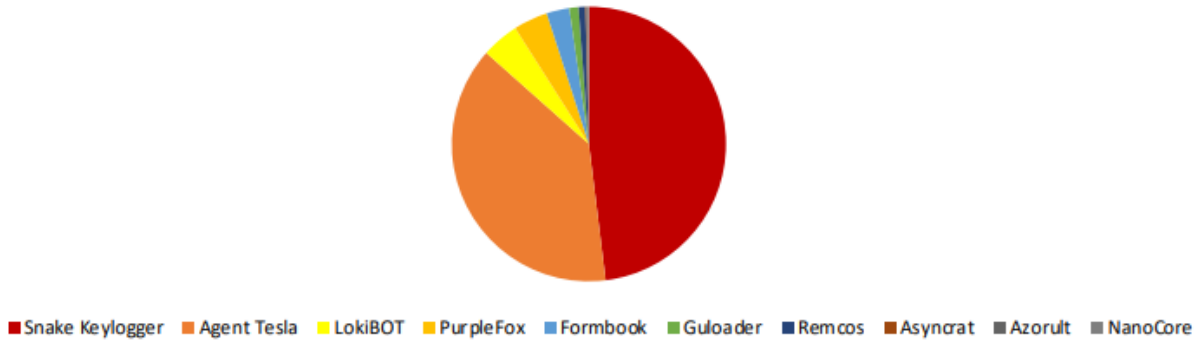


Рисунок 1.1 – Сімейства ШПЗ, виявлених у подіях ІБ категорії «02 Шкідливий програмний код» протягом 2023 року [3]

З початку 2023 року помітно (з різницею у 1.5-2.9 разів для різних секторів) знизилась кількість атак, організованих проросійськими угрупованнями хактивістів, націлених на комерційний, фінансовий сектор, уряд та місцеві органи влади, сектор безпеки та оборони (порівняно з IV кварталом 2022 року). При цьому інтенсивність атак на сектор енергетики та ЗМІ залишається на тому ж рівні.

XakNet, NoName057(16), RussianHackersTeam, RaHDit та Free Civillian є найактивнішими проросійськими угрупованнями хактивістів, кількість атак, організованих якими протягом І кварталу 2023 року, складає 90% від загальної кількості зафіксованих атак, організованих аналогічними угрупованнями протягом звітного періоду (рис. 1.2).

Згідно популярного Кібертрекеру російсько-української війни, підтримуваного користувачем @Cyberknow20, месенджер Telegram активно використовується проросійськими хактивістами як провідна платформа для організації зловмисної активності. Інтерес до платформи, як до «екосистеми кіберзлочинності», підтверджується нещодавнім релізом статті Telegram - How a

messenger turned into a cybercrime ecosystem by 2023 від компанії KELA, що займається кіберрозвідкою [2; 3].

На думку О. Самойленко, криміналістичне дослідження кіберзлочинів обумовлене природою кіберпростору, і це впливає на пізнання обстановки його вчинення [4].

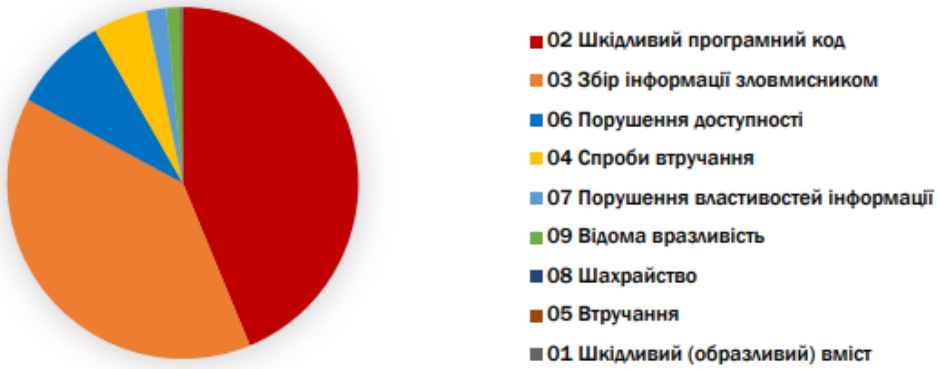


Рисунок 1.2 – Категорії подій ІБ [2]

Кіберпростір – це сукупність взаємодіючих по метриці інформаційних процесів та явищ, які використовуються в якості носія комп'ютерних систем та мереж. Метрика – це спосіб вимірювання відстані в просторі між компонентами процесів та явищ. Відстань в кіберпросторі – це кодова відстань по Гемінгу між парою векторів, які визначають компоненти процесу або явища. Відстань, похідна (бульова), ступінь зміни, відмінності чи близькості є ізоморфними поняттями, які пов'язані із визначенням відношення двох компонентів процесу або явища. Поняття близькості (відстані) компонентів в кіберпросторі є міра їх відмінностей. Похідна – міра бінарного відношення динамічних або статичних компонентів в процесах або явищах. Процедури порівняння, вимірювання, оцінки, розпізнання, тестування, діагностування, ідентифікації мають місце за наявності хоча б одного відношення [5].

Початковий Інтернет був розроблений у довірливому робочому середовищі університетів та дослідницьких лабораторій. Однак це припущення

вже давно втратило чинність з комерціалізацією Інтернету. Безпека стала однією з найважливіших сфер інтернет-досліджень. Оскільки все більше і більше підприємств працюють в Інтернеті, а безліч додатків знаходять нові способи використання Інтернету, безпека, безсумнівно, буде головною проблемою для наступного покоління. В Інтернеті наступного покоління безпека буде частиною архітектури, а не надбудовою над початковою архітектурою, як у нинішньому Інтернеті. Багаторічний досвід досліджень у сфері безпеки дозволив встановити той факт, що безпека не є окремою функцією якогось конкретного рівня стеку протоколів, а є спільною відповідальністю кожної основної комунікаційної функції, яка бере участь у загальному процесі комунікації [6].

Найперше, сучасні інформаційні технології дозволяють: 1) підключення електронних пристроїв до інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; 2) постійно перебувати із ними на мережевому зв’язку та здійснювати обмін інформації: в режимі «онлайн»; в автоматичному режимі; 3) використовувати різні форми та способи збереження інформації: на «фізичних» пристроях (як ноутбуки, смартфони тощо); в «хмарах» (віртуальних сховищах, як: Google Drive від Google**,** OneDrive від Microsoft, MEGA, Dropbox, Samsung Cloud, iCloud від Apple, Xiaomi Cloud тощо).

Цікавим для нашого дослідження буде використання моделі запропонованої Девідом Кларком (David Clark) [7], в якій він обґрунтовує чотири рівні кіберпростору (табл. 1.1).

Вважаємо, що разом із моделлю запропонованою Девідом Кларком (David Clark) доцільно враховувати й запропоновані Карлом Рушером (*Karl Rauscher*) [8] елементи інфраструктури кіберпростору (табл. 1.2). Такий евристичний підхід забезпечить сутнісне пізнання особливостей кіберпростору як об’єкта криміналістичного дослідження.

Таблиця 1.1 – Рівні кіберпростору за Девідом Кларком (David Clark) [7]

Рівні кіберпростору	Примітки
фізичний рівень	фізичну основу кіберпростору становлять фізичні пристрої, з яких він побудований; враховано, що Інтернет в основному складається з пристроїв семи видів: повторювачів, мостів, маршрутизаторів, комутаторів, шлюзів, хостів і вузлів
логічний рівень	природа кіберпростору – його сильні сторони чи вразливості – більше залежать від рішень, прийнятих на логічному рівні ніж на фізичному; логічний рівень у цілому більше обумовлений кодом, який включає програмне забезпечення та протоколи, які в ньому мають застосунок; природа кіберпростору – це безперервна і швидка еволюція нових можливостей і послуг, заснована на створенні та комбінуванні нових логічних конструктів, кожен з яких стоїть на фізичному фундаменті; таким чином, на логічному рівні кіберпростір – це низка платформ, на кожній з яких створюються нові можливості, які, в свою чергу, стають платформою для наступної інновації; рекурсивні процедури
інформаційний рівень	все більше інформації створюється динамічно на вимогу, розмиваючи межі між зберіганням та обчисленням; інформація наразі стає все більше особистим досвідом, а не спільним; питання власності, автентичності та надійності є критично важливими, оскільки все більше інформації переміщується в онлайн; це рівень контенту – на якому інформація створюється, використовується, зберігається та обробляється у кіберпросторі
соціальний рівень	всі користувачі визначають та формують характер кіберпростору тим, як вони його використовують; наприклад, проект «Ноутбук за 100 доларів» (OLPC) – має на меті забезпечити потреби дітей (у країнах що розвиваються) недорогими ноутбуками та зосереджений на мирному часі, на соціальних та економічних мотиваціях, але цей проект може мати наслідки і для державного протистояння; також соціальний прошарок включає урядові організації, юридичні особи публічного та приватного права, громадянське суспільство та суб’єкти технічного співтовариства

Таблиця 1.2 – Характеристика інфраструктури кіберпростору за Карлом Рушером (*Karl Rauscher*) [8]

Елементи інфраструктури	Примітки
середовище	будівлі, місця розташування веж стільникового зв'язку, орбіти супутників, морське дно, де пролягають кабелі зв'язку тощо
енергія	електрика, батареї, генератори тощо
апаратне забезпечення	напівпровідникові мікросхеми, магнітні картки і друковані плати, системи дротового і оптоволоконного передавання даних тощо
програмне забезпечення	вихідні коди, скомпільовані програми, системи контролю та управління версіями, бази даних тощо
мережі	вузли, з'єднання, топологія мережі тощо
передачі	інформація, передана за допомогою мереж, статистика і схеми передачі трафіку, перехоплення даних, псування даних тощо
персонал	інженери, розробники, оператори, обслуговуючий персонал тощо
політика	угоди, стандарти, інструкції та нормативні документи

Унікальність глобальної мережі Інтернет, зазначає А.Журба, полягає в тому, що «вона не перебуває у віддані конкретної фізичної особи, приватної компанії, державної або громадської організації і навіть окремої держави. Тут відсутні які-небудь форми контролю, що відкриває не обмеженні можливості для доступу до будь якої інформації, все ширше використовувані в злочинній діяльності, яка набуває транснаціонального, організованого і групового характеру» [9].

На думку Б.Теплицького, в ході боротьби із кіберзлочинністю можна з'ясувати такі негативні фактори: 1) у сфері інформаційної безпеки України

неналагоджена система організаційно-технічного забезпечення об’єктів кібербезпеки; 2) неналежне фінансування розвитку об’єктів кіберзахисту; 3) неналежна підготовка спеціально уповноважених суб’єктів, внаслідок чого кіберзлочини в більшій частині є латентними [10].

Тобто, проблемним аспектом є розвиток «цифрової криміналістики» (digital forensics). Спеціальні знання, навички та вміння (в цій сфері), а також належний матеріально-технічний рівень – це те, що гарантовано забезпечить ефективне криміналістичне розслідування кіберзлочинів (насамперед, в ході проведення комп’ютерно-технічної експертизи). Також, в цьому процесі варто враховувати й функціональну відмінність спеціалістів та експертів, під час розслідування кіберзлочинів.

Отже, кіберзлочинність є новою формою протиправної поведінки, яка потребує специфічної державної політики у протидії цим кримінальним правопорушенням.

1.2 Аналіз відомих рішень при розслідуванні кіберзлочинів

Архітектура і принципи обробки інформації, незважаючи на розвиток технологій, залишаються тими самими. Постійному зростанню піддаються швидкість, обсяги і якість обробки інформації. Особи, що скоюють кіберзлочини, можуть створити, удосконалити, змінити способи вчинення такого виду злочинів, проте загальна схема вчинення залишиться тією самою. Тому необхідно використовувати визначальні елементи поняття кіберзлочину, не динамічні, а відносно постійні [11]. Це обумовлено також тим, що перебуваючи на межі між правом і технічною сферою, злочини цієї категорії часто є недоступними для розуміння особам, що провадять розслідування у кримінальній справі і не володіють спеціальними знаннями [9].

Наприклад, при досудовому розслідуванні кіберзлочинів пов’язаних зі створенням, розповсюдженням чи збутом шкідливих програмних засобів,

криміналістичне версіювання є комбінацією декількох видів цього інституту, оскільки синергетично поєднуються як версії щодо формату, способів і методів створення самого шкідливого програмного (технічного) засобу, так і класичні формати версіювання, що розуміють під собою ті обставини, події та факти, які спонукали особу до вчинення кримінального правопорушення, обстановку, у якому воно вчинялось, а також інші «позакібернетичні елементи».

Це доводить, що кіберзлочини мають здебільшого латентний характер та є складними для виявлення та розкриття. Як практичну допомогу (на початковому етапі розслідування) О. Мотлях [12] пропонує враховувати типові слідчі ситуації, що можуть скластися (табл. 1.3).

Таблиця 1.3 – Типові слідчі ситуації при розслідуванні кіберзлочинів [12]

Ситуаційні дані	Особливі примітки
виявлено факт несанкціонованого втручання в інформацію, що циркулює у банківській чи кредитно-фінансовій сфері	але відсутні дані про спосіб вчинення злочину та причетних до нього осіб
виявлено факт внесення будь-якого плану змін у комп'ютерну інформацію	при цьому спосіб доступу до баз даних відсутній або ж має опосередкований характер, суб'єкт злочину невідомий
виявлено факт внесення змін у комп'ютерну інформацію	зафіксовано спосіб доступу до баз даних, окремих програм, відома імовірна особа злочинця
виявлено факт внесення в програмне забезпечення чи окремі файли шкідливих, небезпечних вірусних програм	спосіб зараження та особа злочинця невідомі
виявлено факт знищення інформації у комп'ютерній системі	дані про спосіб вчинення та причетних до злочину осіб невідомі
виявлено факт викрадення (заволодіння) комп'ютерною інформацією	при цьому дані про спосіб доступу до інформацію та про суб'єкта злочину невідомі
виявлено факт модифікації баз даних чи маніпуляції інформацією в окремих програмних файлах	дані про спосіб та про імовірного суб'єкта відомі

Водночас, наведені вище слідчі ситуації (див. табл. 1.3) мають характер вихідних міркувань. Наприклад, якщо ми звернемо увагу лише на кіберзлочин передбачений ст. 361-1 КК України, тоді можна на базі вихідних слідчих ситуацій сформулювати слідчі версії (в межах ознак вказаного злочину).

Таблиця 1.4 – Типові слідчі версії при розслідуванні злочинів, пов'язаних зі створенням, використанням, розповсюдженням або збутом шкідливих програмних засобів [11]

Слідча версія	Особливі примітки
виявлено факт ШПЗ	відомі дані про: шкідливе втручання комп'ютерних програм у роботу операційної системи комп'ютера /комп'ютерів або окремих комп'ютерних програм; сліди такого втручання; підозрюваних, які дають правдиві свідчення
	відомі дані про: шкідливе втручання комп'ютерних програм у роботу операційної системи комп'ютера /комп'ютерів або окремих комп'ютерних програм; сліди такого втручання; підозрюваних, які заперечують свою вину та можливість доказу їх вини ускладнена (за умов неможливості перевірити їх свідчення)
	установлено факт шкідливого програмного впливу на операційні системи комп'ютера/комп'ютерів або окремих комп'ютерних програм; є сліди вчинення злочину; установлено осіб, які можуть бути зацікавлені у здійсненні шкідливого комп'ютерного впливу та відповідальні за комп'ютерну безпеку, але обставини вчинення злочину не встановлено
	установлено факт шкідливого програмного впливу на операційні системи комп'ютера/комп'ютерів або окремих комп'ютерних програм; сліди відсутні; не встановлено осіб, підозрюваних в учиненні такого злочину

Таким чином, обумовлені слідчі ситуації при розслідуванні кіберзлочинів забезпечують способи та методи першочергових слідчих дій. На думку М. Скригонюка: 1) слідча ситуація (при розслідуванні кіберзлочинів) буде поєднанням певних обставин, події, фактів тощо; 2) слідча версія (при розслідуванні кіберзлочинів) має бути конкретною, логічною, а також, кожна версія повинна мати контраверсію. Важливим також є, щоб як слідча ситуація так і слідча версія передбачали можливість їх перевірки [13].

Як вірно зазначає О. Волков, «слідчі версії – це можливі пояснення розслідуваної події та її обставин, які використовують із метою встановлення істини в провадженні. Саме криміналістичне версіювання вможливлює як планування досудового розслідування, так і формування основних методик його здійснення за окремими видами кримінальних правопорушень. Лише чітке, об'єктивно оцінене й змістовно сформульоване уявлення про вчинення кримінального правопорушення – дотримання певного стандарту розуміння протиправної поведінки та вжиття відповідних заходів реагування, використання форм дослідження цих фактів можуть призвести до ефективного вирішення всіх завдань досудового розслідування» [11].

Отже, для ефективного вирішення завдань розслідування кіберзлочинів необхідно враховувати природу електронних (цифрових) доказів, які мають такі специфічні ознаки: 1) вони існують у кіберпросторі; 2) оригінал доказу може бути в різних місцях одночасно; 3) їх збереження, збирання, дослідження можливе лише за допомогою ЕОТ [14].

В теперішній практиці розслідування кіберзлочинів гідної уваги заслуговує програмне забезпечення CAINE [15]. Найперше, постає запитання: чи весь електронно-цифровий ресурс можна відстежити в мережі за допомогою OS CAINE?

CAINE (Computer Aided Investigative Environment – дослідження комп'ютеризованого середовища) забезпечує сувору безпеку та інтегровані інструменти криміналістичних розслідувань. CAINE побудовано на повному

дослідницькому середовищі, яке організоване для інтеграції існуючих програмних засобів як програмних модулів і забезпечення зручного графічного інтерфейсу користувача.

Щодо мети впровадження CAINE та його основні цілі (які CAINE прагне гарантувати) відомо про таке:

- його операційне середовище розроблено таким чином, щоб забезпечити всі необхідні криміналістичні інструменти для виконання процесів цифрового криміналістичного розслідування, таких як збереження, збір, дослідження та аналіз;
- він забезпечує зручний графічний інтерфейс користувача з дружніми криміналістичними інструментами;
- він може завантажуватися зі знімних носіїв, таких як флеш-накопичувачі або оптичний диск, і працювати в пам’яті;
- його можна легко встановити на фізичну або віртуальну систему;
- у режимі LIVE CAINE може працювати з об’єктами сховища даних без завантаження операційної системи.

Розглянемо певні системні вимоги для опанування роботи з CAINE. Оскільки CAINE базується на 64-розрядній версії Ubuntu 16.04 і використовує ядро Linux 4.4.0-97, і якщо ви хочете запустити CAINE як живий диск, системні вимоги CAINE подібні до вимог Ubuntu 16.04. Двоядерний процесор 2 ГГц або краще 2 Гб системної пам'яті. Він може працювати у фізичній системі або віртуальному середовищі, наприклад VMWare Workstation.

Щодо платформ, то CAINE Linux має кілька програмних додатків, бібліотек і сценаріїв, які можна використовувати в командному рядку або графічному середовищі для виконання криміналістичних дій. Також він може виконувати аналіз даних створених у Microsoft Windows, Linux і деяких системах Unix. А щодо особливостей CAINE Linux версії 9.0 – за замовчуванням усі блокові пристрої встановлюються в режимі лише для читання.

CAINE Linux використовує лише робоче середовище MATE, яке є розгалуженням робочого середовища GNOME 2. MATE зберігає простий і практичний інтерфейс користувача до оновлення GNOME 3, тому це хороший вибір для швидкого та надійного робочого столу.

Поєднання CAINE і MATE забезпечує плавний інтерфейс і простий робочий стіл. Налаштування панелі – за замовчуванням зливається безпосередньо з фоном робочого столу. Піктограми програм можна легко закріпити на інформаційній панелі або робочому столі для швидкого запуску. Ви можете додати аплет Virtual Workplace Switcher до док-станції для легкого доступу за допомогою вказівки та перемикання (табл.1.5).

Таблиця 1.5 – Характеристика інструментів які входять до CAINE Linux

Інструменти	Особливі примітки
Розтин *(це графічний інтерфейс користувача для Detective Kit)*	це цифровий криміналістичний інструмент із відкритим кодом, який підтримує: - криміналістичний аналіз файлів - хеш-фільтрація - аналітика електронної пошти та веб-артефакти - пошук за ключовими словами
Sleuth Kit	це інструмент командного рядка з відкритим кодом, який підтримує криміналістичну перевірку файлових систем і дискових томів
Wireshark:	це інструмент цифрової експертизи, який підтримує аналіз захоплених пакетів даних (*.pcap) не в реальному часі та інтерактивний збір мережевого трафіку
PhotoRec:	цей інструмент підтримує відновлення втрачених файлів із жорсткого диска, оптичного носія та цифрової камери
Fsstat:	цей інструмент відображає статистичну інформацію файлової системи про зображення або об’єкт зберігання
RegRipper:	це інструмент із відкритим кодом, написаний на Perl і витягує/розбирає інформацію, як-от ключі, значення, дані тощо (база даних реєстру для аналізу даних)
Tinfoleak:	це інструмент із відкритим вихідним кодом для збору детальної інформації з Twitter

Основні криміналістичні засоби. CAINE Linux надає різноманітні програмні інструменти, які можна використовувати для пам'яті, бази даних, мереж і криміналістики. Аналіз файлової системи зображень файлових систем, таких як FAT/ExFAT, NTFS, Ext2, Ext3, HFS і ISO 9660, можливий як у режимі командного рядка, так і в режимі графічного інтерфейсу.

CAINE Linux підтримує образи дисків у необробленому форматі (dd), а також у файловому форматі експертного/розширеного формату. Образи дисків можна отримати за допомогою вбудованих інструментів CAINE або сторонніх інструментів, таких як EnCase або Forensic Toolkit.

Також українські вчені Р.Благута, А.Мовчан, Б.Теплицький [10; 16] розглядали й інші засоби (рішення) для дослідження комп'ютерної техніки та програмних продуктів при розслідуванні кіберзлочинів. Тут нижче ми проведемо аналіз певних програмних та апаратних засобів для дослідження комп'ютерної техніки та програмних продуктів (табл. 1.6 – 1.11).

Таблиця 1.6 – Результати аналізу апаратних засобів мобільної криміналістики [16]

Найменування засобу	Аналіз засобу	Особливі примітки
Cellebrite UFED Touch 2	Концептуально розділений на дві частини: - фірмовий планшет *CellebriteUFEDTouch 2* (або *UFED 4PC*– програмний аналог *Cellebrite UFEDTouch 2*, що встановлюється на комп'ютер або ноутбук фахівця; використовуються тільки для отримання даних); - *UFED Physical Analyzer* – програмна частина, призначена для аналізу даних, витягнутих із мобільних пристроїв	- концепція використання обладнання передбачає, що за допомогою Cellebrite UFED Touch 2 фахівець отримує дані в польових умовах, а потім у лабораторії здійснює їх аналіз за допомогою UFED Physical Analyzer; - відповідно, лабораторний варіант становить два самостійні програмні продукти UFED 4PC і - UFED Physical Analyzer, які встановлені на комп'ютері дослідника; - цей комплекс забезпечує отримання даних із максимально можливої кількості мобільних пристроїв

Продовження табл. 1.6

MSAB XR / MSAB XRY Field	- аналог продуктів Cellebrite, що розробляється шведською компанією MicroSystemation; - на відміну від парадигми Cellebrite, компанія MicroSystemation передбачає, що в більшості випадків їхні продукти використовуватимуться на стаціонарних комп'ютерах або ноутбуках; - до продукту додається фірмовий USB-хаб, який називають на сленгу «шайба», та комплект перехідників і дата-кабелів для підключення різних мобільних пристроїв	- також розроблені версії (апаратні продукти, призначені для отримання даних із мобільних пристроїв) реалізовані у вигляді планшета і кіоску; - *MSAB XRY* добре зарекомендував себе за отримання даних із застарілих мобільних пристроїв - завдяки закритій конфігурації та автоматичному веденню журналу аудиту MSAB Kiosk допомагає відповідати вимогам ISO 17025 та 27037:2012
набір адаптерів польської компанії Rusolut	засоби для проведення chip-off (метод отримання даних безпосередньо з чипів пам'яті мобільних пристроїв)	- за допомогою цього обладнання можна отримувати дані з пошкоджених мобільних пристроїв і пристроїв, заблокованих PIN-кодом або графічним паролем; - компанія Rusolut пропонує кілька наборів адаптерів для отримання даних із певних моделей мобільних пристроїв; - наприклад, комплект адаптерів для отримання даних із чипів пам'яті, які переважно використовуються в «китайських телефонах»

Таблиця 1.7 – Результати аналізу програмних засобів мобільної криміналістики [16]

Програмний засіб	Аналіз засобу	Особливі примітки
Мобільний криміналіст	- одна з найкращих програм для аналізу даних, отриманих із мобільних пристроїв; - інтегровані переглядачі баз даних *SQLite* і *plist-файлів* дозволяють більш досконально досліджувати певні SQLite-бази даних і plist-файли вручну;	- особливістю програми є жорстка прив'язка шляхів, за якими розташовані файли – бази даних додатків; - тобто, якщо структура бази даних будь-якої програми залишилася незмінною, але змінився шлях, яким база даних знаходиться в мобільному пристрої, «Мобільний

Продовження табл. 1.7

		криміналіст» просто пропустить таку базу даних під час аналізу; - тому дослідження подібних баз даних доведеться проводити в ручному режимі, використовуючи файловий браузер «Мобільного криміналіста» і допоміжні утиліти
*Magnet AXIOM (*програма канадської компанії) Magnet Forensics *Belkasoft Evidence Center* (розробка компанії Belkasoft)	- у переліку програм для мобільної криміналістики саме такі програми посідають гідні місця - ці програми за функціональними можливостями щодо отримання даних із мобільних пристроїв дещо поступаються програмним і апаратним засобам, описаним вище; - але вони добре здійснюють їх аналіз і можуть використовуватися для контролю повноти вилучення різних типів даних	- обидві програми активно розвиваються і стрімко нарощують свій функціонал у дослідженні мобільних пристроїв

Таблиця 1.8 – Результати аналізу апаратних блокіраторів запису [16]

Найменування засобу	Аналіз засобу	Особливі примітки
Tableau T35U	- апаратний блокіратор компанії Tableau дозволяє безпечно підключати досліджувані жорсткі диски до комп'ютера дослідника по шині USB3	- цей блокіратор має роз'єми, які дозволяють підключати до нього жорсткі диски за інтерфейсами IDE і SATA (а за наявності перехідників – і жорсткі диски з іншими типами інтерфейсів); - особливістю цього блокіратора є можливість емуляції операцій «читання-запис»; - це буває корисним у дослідженні накопичувачів, заражених шкідливим програмним забезпеченням
Wiebitech Forensic UltraDock v5	- апаратний блокіратор компанії CRU має функціонал, аналогічний блокіратору Tableau T35U	- додатково цей блок можна з'єднати з комп'ютером дослідника по більшій кількості інтерфейсів; - якщо до цього блокіратора буде підключено жорсткий диск, доступ до даних на якому

Продовження табл. 1.8

		обмежений АТА-паролем, на дисплеї блокіратора з'явиться відповідне повідомлення; - крім того, у підключенні жорсткого диска, що має технологічну зону DCO (Device Configuration Overlay), ця зона автоматично буде розблокована для того, аби фахівець міг скопіювати дані, що знаходяться в ній

Таблиця 1.9 – Результати аналізу програмних засобів комп'ютерної експертизи [10]

Програмний засіб	Аналіз засобу	Особливі примітки
Encase Forensics	- ефективний при «нестандартних» випадках: коли необхідно досліджувати комп'ютери під управлінням ОС MacOS або сервера під керуванням ОС Linux, витягувати дані з файлів рідкісних форматів	- в Encase Forensics макромова Ensripts містить величезну бібліотеку готових скриптів, реалізованих виробником і ентузіастами, за допомогою яких можна здійснити аналіз великої кількості різних операційних і файлових систем
Access Data FTK	- намагається підтримувати функціональність продукту на необхідному рівні, але час обробки накопичувачів значно перевищує розумну кількість часу, яку може дозволити собі витратити середньостатистичний фахівець на подібне дослідження	До особливостей *Access Data FTK* слід віднести: - пошук за ключовими словами реалізований на дуже високому рівні; - аналітика різних кейсів, що дозволяє виявляти взаємозв'язки в пристроях, вилучених у різних справах; - можливість налаштування інтерфейсу програми під себе; - підтримка файлів рідкісних форматів (приміром, баз даних Lotus Notes); - Encase Forensics і AccessData FTK можуть обробляти величезні масиви вихідних даних, що вимірюються сотнями терабайт
Magnet AXIOM	- є безперечним лідером програмних засобів для комп'ютерної криміналістики; - ця програма покриває функціоналом цілі сегменти: дослідження мобільних пристроїв, витяг	- програма має зручний і функціональний інтерфейс, у якому все під рукою, і може застосовуватися для розслідування інцидентів інформаційної безпеки, пов'язаних із зараженням комп'ютерів або мобільних пристроїв шкідливим програмним забезпеченням або з витоками даних

Продовження табл. 1.9

	із хмарних сховищ, вивчення механізмів підуправлінням операційної системи MacOS тощо.	
Belkasoft Evidence Center	- дозволяє витягувати і аналізувати дані з мобільних пристроїв, хмарних сховищ і жорстких дисків; - при аналізі жорстких дисків здійснюється вилучення даних із веб-браузерів, чатів, інформації про хмарні сервіси, детектування зашифрованих файлів і розділів, витяг файлів за заданим розширенням, даних про геолокацію, електронної пошти, даних із платіжних систем і соціальних мереж, мініатюр, системних файлів, системних журналів тощо; - має гнучкий функціонал щодо вилучення віддалених даних	Переваги програми Belkasoft Evidence Center такі: - широкий спектр даних із різних носіїв інформації; - вмонтований переглядач баз даних SQLite; - збір даних із віддалених комп'ютерів і серверів; - інтегрований функціонал щодо перевірки виявлених файлів на Virustotal. Недоліками програми є незручний інтерфейс і неочевидність виконання окремих дій в програмі. Для ефективного використання програми необхідно пройти відповідне навчання
X-Ways Forensics	- особливістю цієї швейцарської програми є велика швидкість обробки даних (порівняно з іншими програмами цієї категорії) та оптимальний функціонал, що задовольняє основні потреби фахівця з комп'ютерної криміналістики; - програма має вмонтований механізм, що дозволяє мінімізувати хибнопозитивні результати (тобто дослідник, здійснюючи відновлення файлів із жорсткого диска обсягом 100 Гб, бачить не 1	За допомогою програми X-Ways Forensics можливо: - знаходити й аналізувати дані електронної пошти; - аналізувати історію веб-браузерів, журнали ОС Windows та інші системні артефакти; - відфільтрувати результати, залишити тільки цінні й актуальні відомості; - побудувати тимчасову шкалу і переглянути активності в період, що цікавить; - реконструювати RAID; - монтувати віртуальні диски; - здійснювати перевірку на наявність шкідливого програмного забезпечення;

Продовження табл. 1.9

	Тб відновлених файлів (велика частина з яких є хибнопозитивними результатами, як це зазвичай відбувається у використанні програм відновлення), а саме ті файли, які реально були відновлені)	- ця програма дуже добре зарекомендувала себе у ручному аналізі жорстких дисків, витягнутих із відеореєстраторів; - задопомогою функціоналу X-Tension є можливість підключення в програмі модулів сторонніх розробників. До недоліків X-Ways Forensics слід віднести: - аскетичний інтерфейс; - відсутність повноцінного вбудованого переглядача баз даних SQLite; - необхідність глибокого вивчення програми; - виконання деяких дій, необхідних для отримання потрібного фахівцю результату, не завжди очевидно

Таблиця 1.10 – Результати аналізу апаратних засобів відновлення даних [10]

Апаратний засіб	Аналіз засобу	Особливі примітки
ACELab	- апаратні засоби для аналізу, діагностики та відновлення жорстких дисків (комплекси PC-3000 Express, PC-3000 Portable, PC-3000 UDMA, PC-3000 SAS); - SSD накопичувачів (комплекс PC-3000 SSD); - флеш-накопичувачів (комплекс PC-3000 Flash); - RAID (комплекси PC-3000 Express RAID, PC-3000 UDMA RAID, PC-3000 SAS RAID)	Домінування ACELab на ринку апаратних рішень із відновлення даних обумовлено високою якістю перелічених продуктів і ціновою політикою ACELab, яка не дозволяє конкурентам увійти на цей ринок.

Таблиця 1.11 – Результати аналізу програмного забезпечення [16]

Програмне забезпечення	Аналіз забезпечення	Особливі примітки
Autopsy	- зручний інструмент для аналізу комп'ютерів під управлінням операційної системи Windows і мобільних пристроїв під управлінням операційної системи Android, що має графічний інтерфейс	Може бути використаний у розслідуванні комп'ютерних інцидентів
Photorec	–одна з ліпших безкоштовних програм для відновлення даних	
Eric Zimmerman Tools –	- комплект безкоштовних утиліт, кожна з яких дає змогу досліджувати якийсь окремий артефакт Windows; - як засвідчила практика, використання Eric Zimmerman Tools підвищує ефективність роботи фахівця за реагування на інцидент у «польових умовах»	Нині ці утиліти доступні у вигляді пакету програм *Kroll Artifact Parser and Extractor (KAPE)*

1.3 Постановка завдання

Проведений аналіз джерел за темою доводить, що кількість кіберінцидентів (кібератак) на державні інформаційні ресурси та об'єкти критичної інформаційної інфраструктури зростає. Насамперед, встановлено істотне зростання щодо розповсюдження шкідливого програмного забезпечення. В 2023 році (серед виявлених ШПЗ) переважають: Snake Keylogger, Agent Tesla, LokiBot, PurpleFox та Formbook. Відтак, в кіберпросторі існують специфічні умови для вчинення кіберзлочинів різних видів, які потребують прогресу в їх дослідженні та розробки нових методів розслідування.

Проаналізовані апаратні та програмні засоби для дослідження комп'ютерної техніки та програмних продуктів мають різні спеціальні конфігурації, функції тощо. Водночас, ці засоби мають свої обмеження, які впливають на їх ефективність у виявленні, наприклад, формату, способів та

методів створення шкідливого програмного засобу. Це доводить, чому кіберзлочини мають здебільшого латентний характер та є складними для розслідування. Статистика вказує, що рівень латентності кіберзлочинів становить 90-95 відсотків.

Типові слідчі ситуації та слідчі версії вказують лише напрямок в розслідуванні, а визначення унікальності кіберзлочину та його ефективне розслідування – обумовлено компетенцією спеціально призначених суб'єктів. Проведений аналіз джерел доводить, що нині в Україні спеціально призначені суб'єкти (слідчі, детективи, прокурори, судді та адвокати) не володіють достатніми знаннями в сфері комп'ютерних наук, і це призводить до неефективного попередження, виявлення та розслідування кіберзлочинів.

В другому розділі магістерської роботи варто здійснити такі наукові розвідки: дослідити організаційно-технічну модель кіберзахисту; розробити теоретико-множинні моделі кіберінцидентів та найпоширеніших кіберзлочинів, з'ясувати їх сутність та взаємообумовленість; розробити модель криміналістичного розслідування кіберзлочинів.

В третьому розділі магістерської роботи варто здійснити такі наукові розвідки: дослідити види та можливості судових експертиз під час розслідування кіберзлочинів; визначити критерії оцінок та використання результатів судових експертиз під час розслідування кіберзлочинів; провести експериментальне дослідження кіберзлочинів та надати рекомендації щодо підвищення ефективності цього процесу.

В четвертому розділі варто здійснити такі наукові розвідки: розробити науково-обґрунтовані рекомендації в економічній сфері щодо криміналістичного забезпечення розслідування кіберзлочинів.

2 РОЗРОБКА МОДЕЛІ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

2.1 Розробка теоретико-множинної моделі категорій кіберінцидентів

В 2021 році Кабінет Міністрів України затвердив Положення про організаційно-технічну модель кіберзахисту [17]. Це Положення було прийнято на виконання статті 8 Закону України «Про основні засади забезпечення кібербезпеки України».

Згідно цього Положення під «організаційно-технічною моделлю кіберзахтисту» (ОТМ) розуміється: 1) розвиток можливостей щодо оперативного реагування на кіберінциденти (кібератаки); 2) порядок запобігання негативним наслідкам від кіберінцидентів (кібератак) для інфраструктури.

Структура ОТМ [18; 19] обумовлена на трьох рівнях: 1) адміністративно-управлінський рівень; 2) технологічний рівень; 3) інфраструктурний рівень (рис. 2.1). Така модель покращує ефективність роботи основних суб'єктів національної системи кібербезпеки, підвищує їх відповідальність та надає можливість формування кадрового ресурсу.

На думку І. Субача, основою побудови ефективної системи кіберзахисту інформаційно-комунікаційних систем (ІКС) має бути застосування проактивної SIEM-системи. Такий підхід забезпечує управління інформаційною безпекою та управління кіберінцидентами (кібератаками) в реальному часі [20]. Тобто, програмний продукт SIEM (*Security information and event management*) здатний в реальному часі виконувати великий спектр задач, зокрема: отримувати інформацію від мережевих пристроїв; здійснювати генерацію звітів про отриманні данні задля сумісності із іншими базами даних (табл.2.1) [21].

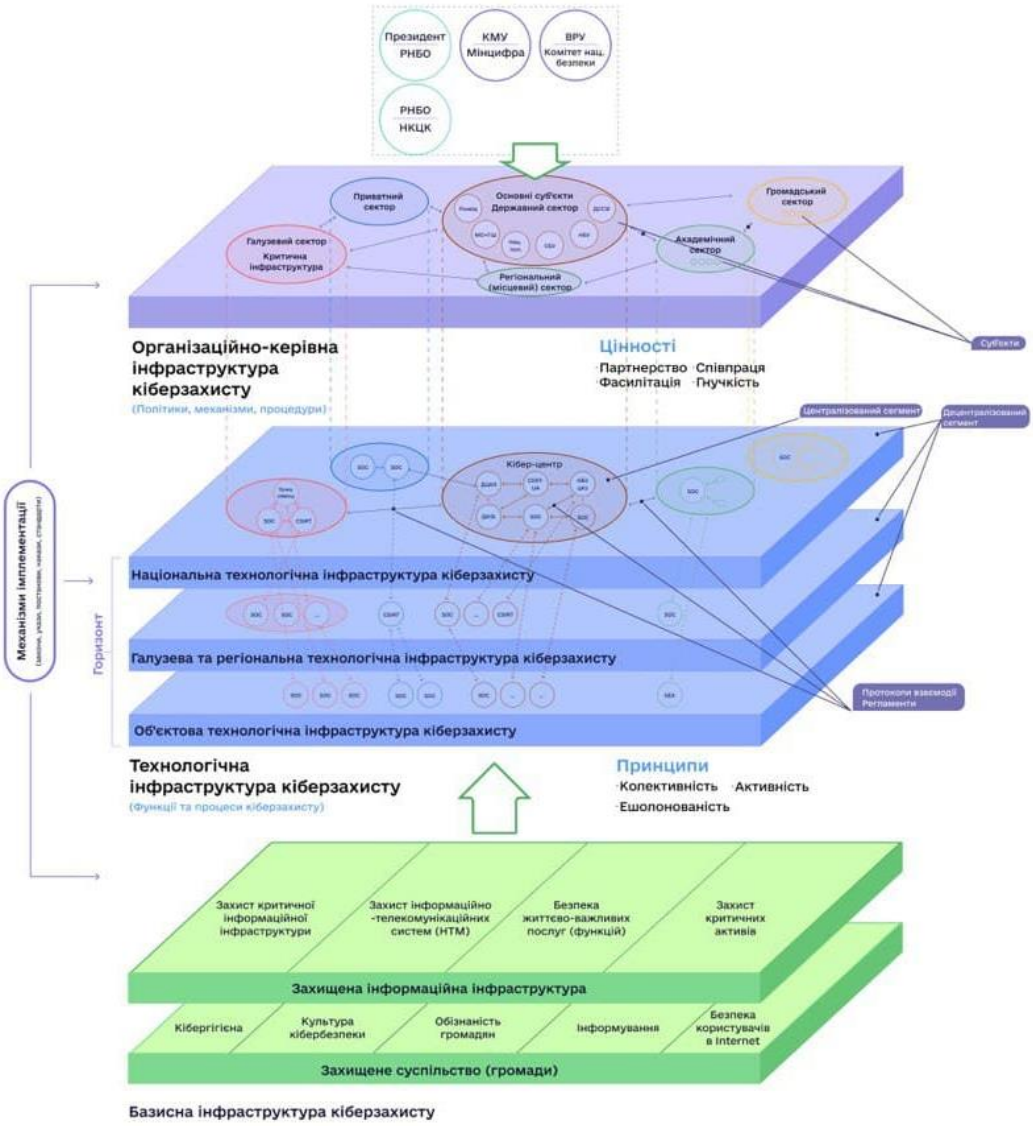


Рисунок 2.1 – Архітектура організаційно-технічної моделі кіберзахисту [19]

Кіберпростір (як об’єкт криміналістичного дослідження) не варто ототожнювати з «віртуальним простором». Етимологічно «віртуальний» (від лат. *virtus – потенційни, можливий*) – вигаданий, уявний, реально не існуючий. Відтак, віртуальний простір більш ширше поняття, а кіберпростір – є однією із його ознак. Кіберзлочини вчиняються у кіберпросторі, і вони є реальними, а не уявними. Сліди кіберзлочинів в кіберпросторі за допомогою ЕОТ стають відомими та досліджуваними.

Таблиця 2.1 – Характеристика SIEM-системи [21]

Структура системи	Задачі системи	Механізми системи
Управління інформаційною безпекою Управління подіями безпеки	збір, обробка та аналіз подій безпеки, що поступають до неї з множини різнорідних розподілених джерел	нормалізація, фільтрація, класифікація, агрегація, кореляція, пріоритезація та аналіз подій і кіберінцидентів та їх наслідків, а також генерація різноманітних звітів, повідомлень і візуального представлення даних для оперативного та обґрунтованого прийняття рішень

Задля з'ясування особливостей дослідження кіберпростору, як об'єкта криміналістичного дослідження, найперше, необхідно дослідити відмінності кіберзлочину від інших кіберінцедентів (кібератак):

- *відмінність в суб'єктному складі*: кіберзлочини – розслідують слідчі та інші особи згідно кримінально-процесуального законодавства; кіберінциденти – ідентифікацію, виявлення, захист, відновлення тощо здійснюють команди реагування на комп'ютерні надзвичайні події (п. 6 Положення про організаційно-технічну модель кіберзахисту) [18];
- *не кожен кіберінцидент містить ознаки кримінального правопорушення*. Для цього М.Кулешов [22] пропонує кіберінциденти поділяти (в залежності їх природи): 1) прості кіберінциденти (наприклад, в силу природних, технологічних факторів тощо); 2) ускладнені (наприклад, обставини, події обумовленні умисними чи необережними діями/бездіяльністю певних осіб, але за відсутності ознак кібератаки); 3) кібератака (дії, які передбачені п. 4 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України»);

- *правові підстави для розслідування*. Так, за відсутності звернення потерпілого у формі приватного обвинувачення (ст. 477 КПК України) відсутні правові підстави для розслідування виявлених кіберінцидентів в яких є склади злочину, наприклад, передбачені частиною першої статті 361 та частиною першою статті 362 КК України. Водночас, тут необхідно зауважити, що законодавець не синхронізував внесенні зміни до частини першої статті 361 КК України із частиною першою статті 477 КПК України (в якій нині йде відсилання на частину першу статті 361 КК України в редакції до 24.03.2022 року) [23];
- *характер об'єкта правопорушення* (визначає підслідність кіберзлочину).

Таблиця 2.2 – Перелік категорій кіберінцидентів [24]

Код хх	Категорія інциденту	Код хх	Тип інциденту	Тип інциденту англійською	Опис типу інциденту
01.	Шкідливий (образливий) вміст (Abusive content)	01	Спам	Spam	Надсилання небажаних повідомлень або великої кількості повідомлень (флуд)
02.	Шкідливий програмний код (Malicious Code)	01	Зараження шкідливим програмним забезпеченням (далі – ШПЗ)	Malware infection	У системі виявлено ШПЗ.
		02	Розповсюдження ШПЗ	Malware distribution	Розповсюдження ШПЗ, наприклад шляхом розсилки повідомлень електронної пошти, що містять вкладення з ШПЗ або посилання на його завантаження
		03	Командно-контрольний центр (C2)	Command & Control (C2)	Система, яка використовується як точка керування та управління ботнетом та/або служить точкою для збору інформації, викраденої ботнетами
		04	Шкідливе підключення	Malicious connection	Спроби з'єднання від/до IP/URL - адреси, пов'язаної з відомим ШПЗ, наприклад C2C або ресурсом розповсюдження компонентів, пов'язаних із активністю певної бот-мережі
03.	Збір інформації зловмисником (Information Gathering)	01	Сканування	Scanning	Збір інформації про системи або мережі
		02	Сніфінг	Sniffing	Несанкціоноване перехоплення (логічне або фізичне) та аналіз мережевого трафіку. Несанкціонований моніторинг та зчитування мережевого трафіку

Продовження табл. 2.2

		03	Фішинг	Phishing	Спроба збору інформації про користувача чи систему за допомогою методів соціальної інженерії (масова розсилка електронною поштою спрямована на збір даних, може містити посилання на фішингові сайти)
04.	Спроби втручання (Intrusion Attempts)	01	Спроба експлуатації вразливості	Vulnerability exploitation attempt	Спроба вторгнення з використанням вразливості у системі, компоненті чи мережі
		02	Спроби авторизації/входу в систему	Login attempts	Спроба входу до служб або механізмів автентифікації / доступу. Невдала спроба підбору автентифікаційних даних чи використання раніше скомпрометованих вже не актуальних даних
05.	Втручання (Intrusion)	01	Компрометація облікового запису	Account compromise	Фактичне вторгнення в систему, компонент або мережу шляхом компрометації облікового запису користувача або адміністратора
		02	Компрометація системи	System compromise	Фактичне вторгнення в систему чи її компоненту, сервісу, застосунку через використання вразливості в компоненті або мережі. Несанкціонований доступ до системи або компоненту в обхід системи контролю доступу
06.	Порушення доступності (Availability)	01	Атака на відмову в обслуговуванні	DoS/DDoS	Вплив на нормальне функціонування системи чи сервісу що досягається направленням з одного чи багатьох джерел до цільового ресурсу запитів для перенасичення пропускної здатності чи системних ресурсів
		02	Саботаж / шкідливі дії	Sabotage	Дії (навмисні або ненавмисні), спрямовані на пошкодження системи, переривання процесів, зміну або видалення інформації тощо
		03	Збій	Outage, no malice	Збій в роботі системи чи її компоненту без зловмисного втручання
07.	Порушення властивостей інформації (Information Content Security)	01	Несанкціонований доступ до інформації	Unauthorised access to information	Несанкціонований доступ до інформації. Несанкціонований обмін конкретним набором інформації
		02	Несанкціонована модифікація	Unauthorised modification of info	Несанкціонована зміна або видалення певного набору інформації.
08.	Шахрайство (Fraud)	01	Шахрайський сайт	Fraudulent site	Створення фішингових сайтів для збору автентифікаційних чи інших даних користувачів. Використання ресурсів установи для цілей, відмінних від передбачуваних
09.	Відома вразливість (Vulnerable)	01	Вразливість	Vulnerability	Наявність в системі чи її компонентах відомих вразливостей, відкритих для експлуатації
		02	Некоректна конфігурація	Misconfiguration	Недоліки в налаштуваннях, що можуть бути використані зловмисником (налаштування за замовчуванням тощо)
10.	Інше (Other)	01	Невизначений інцидент	Undetermined incident	Недостатньо даних для обробки інциденту

Наведений перелік категорій кіберінцидентів (див. табл. 2.2) буде мати такі теоретико-множинні моделі категорій кіберінцидендів:

$$КТІ = \{ КТІ.01; КТІ.02; КТІ.03; КТІ.04; КТІ.05; КТІ.06; КТІ.07; КТІ.08;; КТІ.09; КТІ.10\}, \quad (2.1)$$

$$КТІ.01 = \{ КТІ.01.01\}, \quad (2.2)$$

$$КТІ.02 = \{ КТІ.02.01; КТІ.02.02; КТІ.02.03; КТІ.02.04\}, \quad (2.3)$$

$$КТІ.03 = \{ КТІ.03.01; КТІ.03.02; КТІ.03.03\}, \quad (2.4)$$

$$КТІ.04 = \{ КТІ.04.01; КТІ.04.02\}, \quad (2.5)$$

$$КТІ.05 = \{ КТІ.05.01; КТІ.05.02\}, \quad (2.6)$$

$$КТІ.06 = \{ КТІ.06.01; КТІ.06.02; КТІ.06.03\}, \quad (2.7)$$

$$КТІ.07 = \{ КТІ.07.01; КТІ.07.02\}, \quad (2.8)$$

$$КТІ.08 = \{ КТІ.08.01\}, \quad (2.9)$$

$$КТІ.09 = \{ КТІ.09.01; КТІ.09.02\}, \quad (2.10)$$

$$КТІ.10 = \{ КТІ.10.01\}, \quad (2.11)$$

Також вважаємо, що необхідно перевіряти найпоширеніші передумови (обставини) за яких розповсюджуються (здійснюються, реалізуються) найбільш відомі кіберінцеденти (кібератаки), наприклад: чи використовувалися

комп’ютерні віруси щодо конкретної системи; чи були спроби дізнатися конфіденційну інформацію за допомогою фішингових листів; чи в інший спосіб була спроба компрометації даних (з метою проникнення в систему) [25].

2.2 Розробка теоретико-множинної моделі найпоширеніших кіберзлочинів

В Конвенції Ради Європи про кіберзлочинність від 23.11.2001 року обумовлено такі групи кіберзлочинів: 1) правопорушення проти конфіденційності, цілісності та доступності комп’ютерних даних і систем (незаконний доступ (ст. 2), нелегальне перехоплення (ст. 3), втручання у дані (ст. 4) втручання у систему (ст. 5), зловживання пристроями (ст. 6)); 2) правопорушення пов’язані з комп’ютерами (підробка та шахрайство, пов’язані з комп’ютерами (статті 7, 8)); 3) правопорушення, пов’язані зі змістом (правопорушення, пов'язані з дитячою порнографією (ст. 9) тощо); 4) правопорушення, пов'язані з порушенням авторських та суміжних прав (ст. 10) [26].

Згідно пункту 8 частини першої статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» «кіберзлочин (комп’ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України» [17].

Коло обставин, що підлягають доказуванню за комп’ютерними злочинами, залежить від виду вчиненого кіберзлочину. Суттєвою особливістю предмета доказування є відмінність складових його елементів не лише в межах категорії злочинів, але й за кожною конкретною кримінальною справою. Загальне коло обставин, що належать до предмета доказування, міститься в законі. Встановити в законодавчому порядку точний і вичерпний перелік обставин, які підлягають

доказуванню, абсолютно неможливо. Він обумовлений багатьма особливостями в межах кожного конкретного діяння [27]. Нині в Кримінальному кодексі України [28] передбачено ряд злочинів, які вчиняються в кіберпросторі (відомості про найпоширеніші із них наведено в таблицях 2.3 – 2.10).

Таблиця 2.3 – Характеристика кіберзлочину передбаченого статтею 190 Кримінального кодексу України

стаття КК України	Ознаки складу злочину							
	Діяння	Предмет	Потер-пілий	Наслідки	Місце, час, спосіб, засоби, знаряддя, обставини, ситуація	Суб'єкт	Форма вини	Мета, мотив, емоційний стан
1	2	3	4	5	6	7	8	9
ч.1 ст.190	Заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою (шахрайство)	чуже майно чи документи, що підтверджують право на майно	-	-	спосіб – обман чи зловживання довірою	-	прямий умисел	-
ч.2 ст.190	те саме	те саме	людина	значна шкода потерпілому	спосіб – обман чи зловживання довірою; обставини – повторно; за попередньою змовою групою осіб	-	прямий умисел до діяння, умисел або необережн. до наслідків	-
ч.3 ст.190	те саме	те саме – у великих розмірах	-	-	спосіб – обман чи зловживання довірою; ***незаконні операції з використанням електронно обчислювальної техніки; засоби -елктр. обчислювальна техніка***	-	прямий умисел	-
ч.4 ст.190	те саме	те саме – в особливо великих розмірах	-	-	спосіб – обман чи зловживання довірою; організованою групою	-	те саме	-

За таких обставин теоретико-множинна модель ознак кіберзлочину передбаченого ч.3 ст. 190 КК України буде мати такий вигляд:

$$O.190 = \{ Д.190;\ Пр.190;\ П.190;\ С.190;\ Ф.190;\ КТІ \}, \qquad (2.12)$$

де $O.190$ – ознаки складу кіберзлочину

Д.190	– діяння злочину	заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою (шахрайство)
Пр.190	– предмет злочину	чуже майно чи документи, що підтверджують право на майно
П.190	– потерпілий	особа
С.190	– спосіб вчинення	спосіб – обман чи зловживання довірою; незаконні операції з використанням електронно обчислювальної техніки; засоби – ЕОТ
Ф.190	– форма вини	прямий умисел
КТІ	– категорія та тип інциденту обумовлені згідно Переліку (див. табл.2.2)	

Таблиця 2.4 – Характеристика кіберзлочину передбаченого статтею 200 Кримінального кодексу України

стаття КК України	Ознаки складу злочину							
	Діяння	Предмет	Потерпілий	Наслідки	Місце, час, спосіб, засоби, знаряддя, обставини, ситуація	Суб'єкт	Форма вини	Мета, мотив, емоційний стан
1	2	3	4	5	6	7	8	9
ч.1 ст.200	підробка придбання зберігання перевезення пересилання використання збут	документи на переказ грошових коштів; платіжні картки чи інші засоби доступу до банківських рахунків; підроблені документи на переказ грошових коштів чи платіжні картки	-	-	засоби- підроблені документи на переказ грошових коштів чи платіжні картки	-	прямий умисел	мета - збут
ч.2 ст.200	те саме	те саме	-	-	обставини – повторно; засоби- підроблені документи на переказ грошових коштів чи платіжні картки (при використанні) спосіб – за попередньою змовою групою осіб	-	те саме	те саме

За таких обставин теоретико-множинна модель ознак кіберзлочину передбаченого статтею 200 КК України буде мати такий вигляд:

$$O.200 = \{ Д.200; Пр.200; С.200; Ф.200; М.200; КТІ\} , \quad (2.13)$$

де *О.200* – ознаки складу кіберзлочину

Д.200	– діяння злочину	підробка, придбання, зберігання перевезення, пересилання, випуск, використання, збут
Пр.200	– предмет злочину	документи на переказ грошових коштів; платіжні картки чи інші засоби доступу до банківських рахунків; підроблені документи на переказ грошових коштів чи платіжні картки;
С.200	– спосіб вчинення злочину	засоби- підроблені документи на переказ грошових коштів чи платіжні картки; повторно; за попередньою змовою
Ф.200	– форма вини	прямий умисел
М.200	– мета	неправомірний випуск або використання електронних грошей

КТІ – категорія та тип інциденту обумовлені згідно Переліку (див. табл.2.2)

Окремої уваги заслуговують кіберзлочини передбачені в Розділі XVI Кримінального кодексу України [28].

Таблиця 2.5 – Характеристика кіберзлочину передбаченого статтею 361 Кримінального кодексу України

стаття КК України	Ознаки складу злочину							
	Діяння	Предмет	Потерпілий	Наслідки	Місце, час, спосіб, засоби, знаряддя, обставини, ситуація	Суб'єкт	Форма вини	Мета, мотив, емоційний стан
1	2	3	4	5	6	7	8	9
ч.1 ст.361	втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж	інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі	-	-	спосіб – несакціоно-ваний ;	-	прямий умисел до діяння, умисел або необережн. до наслідків	-
ч.2 ст.361	те саме	те саме	-	-	спосіб – несакціоно-ваний ; обставини – вчинений повторно; або у спосіб - за	-	те саме	-

Продовження табл. 2.5

					попередньою змовою групою осіб			
ч.3 ст.361	те саме	те саме	-	призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації	те саме	-	те саме	-
ч.4 ст.361	те саме	те саме	-	заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків	те саме	-	те саме	-
ч.5 ст.361	те саме	те саме	-	-	вчинені під час дії воєнного стану	-	те саме	-

За таких обставин теоретико-множинна модель ознак кіберзлочину передбаченого статтею 361 КК України буде мати такий вигляд:

$$O.361 = \{ Д.361;\ Пр.361;\ С.361;\ Ф.361;\ КТІ \}, \qquad (2.14)$$

де *О.361* – ознаки складу кіберзлочину

Д.361 – діяння злочину — втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж

Пр.361 – предмет злочину — інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі

С.361 – спосіб вчинення — спосіб – несанкціонований; обставини – вчинений повторно; за попередньою змовою; під час дії воєнного стану

Ф.361 – форма вини — прямий умисел до діяння, умисел або необережний до наслідків

КТІ – категорія та тип інциденту обумовлені згідно Переліку (див. табл.2.2)

Таблиця 2.6 – Характеристика кіберзлочину передбаченого статтею 361-1 Кримінального кодексу України

стаття КК України	Ознаки складу злочину							
	Діяння	Предмет	Потер-пілий	Наслідки	Місце, час, спосіб, засоби, знаряддя, обставини, ситуація	Суб'єкт	Форма вини	Мета, мотив, емоційний стан
1	2	3	4	5	6	7	8	9
ч.1 ст.361-1	Створення, використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу	інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі	-	-	спосіб – несанкціоноване втручання, засоби- створені шкідливі програмні чи технічні засоби	-	прямий умисел до діяння, умисел або необережн. до наслідків	мета – протиправне використання, розповсюдження або збут
ч.2 ст.361-1	те саме	те саме	-	заподіяли значну шкоду	спосіб – несанкціоноване втручання, засоби- створені шкідливі програмні чи технічні засоби вчинені повторно або за попередньою змовою групою осіб	-	те саме	те саме

За таких обставин теоретико-множинна модель ознак кіберзлочину передбаченого статтею 361-1 КК України буде мати такий вигляд:

$$O.361.1 = \{ Д.361.1;\ Пр.361.1;\ Н.361.1;\ С.361.1;\ З.361.1;\ Ф.361.1;\ М.361.1;\ КТІ \}, \quad (2.15)$$

де *О.361.1* – ознаки складу кіберзлочину

Д.361.1 – діяння злочину створення, використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу

Пр.361.1	– предмет злочину	інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі
Н.361.1	– наслідки	заподіяли значну шкоду
С.361.1	– спосіб вчинення	несанкціоноване втручання; повторно; за попередньою змовою
З.361.1	– засіб вчинення	створені шкідливі програмні чи технічні засоби
Ф.361.1	– форма вини	прямий умисел до діяння, умисел або необережний до наслідків
М.361.1	– мета	протиправне використання, розповсюдження або збут
КТІ	– категорія та тип інциденту обумовлені згідно Переліку (див. табл.2.2)	

Таблиця 2.7 – Характеристика кіберзлочину передбаченого статтею 361-2 Кримінального кодексу України

стаття КК України	Ознаки складу злочину							
	Діяння	Предмет	Потер-пілий	Наслідки	Місце, час, спосіб, засоби, знаряддя, обставини, ситуація	Суб'єкт	Форма вини	Мета, мотив, емоційний стан
1	2	3	4	5	6	7	8	9
ч.1 ст.361-2	збут або розповсюдження інформації з обмеженим доступом	електронно-обчислювальні машини (комп'ютера), автоматизовані системи, комп'ютерні мережі або носії такої інформації	-	-	спосіб – несанкціонований	-	прямий умисел до діяння, умисел або необережн. до наслідків	мета – розповсюдження або збут
ч.2 ст.361-2	те саме	те саме	-	заподіяли значну шкоду	спосіб –вчинені повторно або за попередньою змовою групою осіб	-	те саме	те саме

За таких обставин теоретико-множинна модель ознак кіберзлочину передбаченого статтею 361-2 КК України буде мати такий вигляд:

$$O.361.2 = \{ Д.361.2;\ Пр.361.2;\ Н.361.2;\ С.361.2;\ Ф.361.2;\ М.361.2;\ КТІ \}, \quad (2.16)$$

де *О.361.2* – ознаки складу кіберзлочину

Д.361.2 – діяння злочину збут або розповсюдження інформації з обмеженим доступом

Пр.361.2 – предмет злочину електронно-обчислювальні машини (комп'ютера), автоматизовані системи, комп'ютерні мережі або носії такої інформації

Н.361.2 – наслідки заподіяли значну шкоду

С.361.2 – спосіб вчинення несанкціонований, вчинені повторно або за попередньою змовою групою осіб

Ф.361.2 – форма вини прямий умисел до діяння, умисел або необережний до наслідків

М.361.2 – мета розповсюдження або збут

КТІ – категорія та тип інциденту обумовлені згідно Переліку (див. табл.2.2)

Таблиця 2.8 – Характеристика кіберзлочину передбаченого статтею 362 Кримінального кодексу України

стаття КК України	Ознаки складу злочину							
	Діяння	Предмет	Потер-пілий	Наслідки	Місце, час, спосіб, засоби, знаряддя, обставини, ситуація	Суб'єкт	Форма вини	Мета, мотив, емоційний стан
1	2	3	4	5	6	7	8	9
ч.1 ст.362	зміна, знищення або блокування інформації	електронно-обчислювальні машини (комп'ютера), автоматизовані системи, комп'ютерні мережі або носії такої інформації	особа	зміна, знищення або блокування інформації	спосіб – несанкціонований	особа має право доступу	прямий умисел до діяння, умисел або необережн. до наслідків	мета – зміна, знищення або блокування інформації
ч.2 ст.362	перехоплення або копіювання інформації, яка оброблюється	те саме	-	виток інформації	те саме	те саме	те саме	мета - перехоплення або копіювання інформації
ч.3 ст.362	зміна, знищення або блокування інформації перехоплення або копіювання інформації, яка оброблюється	те саме	-	заподіяли значну шкоду	спосіб –вчинені повторно або за попередньою змовою групою осіб	те саме	те саме	мета - зміна, знищення або блокування інформації перехоплення або копіювання інформації

За таких обставин теоретико-множинна модель ознак кіберзлочину передбаченого статтею 362 КК України буде мати такий вигляд:

$$О.362 = \{ Д.362; Пр.362; Ос.362; Н.36 ; С.362; Ф.362; М.362; КТІ \} , \quad (2.17)$$

де *О.362* – ознаки складу кіберзлочину

Д.362 – діяння злочину зміна, знищення або блокування інформації перехоплення або копіювання інформації, яка оброблюється

Пр.362 – предмет злочину електронно-обчислювальні машини (комп'ютера), автоматизовані системи, комп'ютерні мережі або носії такої інформації

Ос.362 – особа

Н.362 – наслідки зміна, знищення або блокування інформації; виток інформації; заподіяли значну шкоду

С.362 – спосіб вчинення злочину несанкціонований, вчинені повторно або за попередньою змовою групою осіб

Ф.362 – форма вини прямий умисел до діяння, умисел або необережний до наслідків

М.362 – мета зміна, знищення або блокування інформації перехоплення або копіювання інформації

КТІ – категорія та тип інциденту обумовлені згідно Переліку (див. табл.2.2)

Таблиця 2.9 – Характеристика кіберзлочину передбаченого статтею 363 Кримінального кодексу України

стаття КК України	Ознаки складу злочину							
	Діяння	Предмет	Потер-пілий	Наслідки	Місце, час, спосіб, засоби, знаряддя, обставини, ситуація	Суб'єкт	Форма вини	Мета, мотив, емоційний стан
1	2	3	4	5	6	7	8	9
ч.1 ст.363	порушення правил експлуатації	правила експлуатації, порядок або правила захисту інформації	-	заподіяли значну шкоду	-	особа яка відповідає за експлуатацію	умисел або необережність до діяння, необережн. до наслідків	мета – зміна, знищення або блокування інформації

За таких обставин теоретико-множинна модель ознак кіберзлочину передбаченого статтею 363 КК України буде мати такий вигляд:

$$О.363 = \{ Д.363; Пр.363; Н.363; Суб.363; Ф.363; М.363; КТІ \} , \quad (2.18)$$

де *О.363* – ознаки складу кіберзлочину

Д.363 – діяння злочину порушення правил експлуатації

Пр.363 – предмет злочину правила експлуатації, порядок або правила захисту інформації

Н.363 – наслідки вчинення злочину заподіяли значну шкоду

Суб.363 – суб'єкт особа яка відповідає за експлуатацію

Ф.363 – форма вини умисел або необережність до діяння, необережн. до наслідків

М.363 – мета зміна, знищення або блокування інформації

КТІ – категорія та тип інциденту обумовлені згідно Переліку (див. табл.2.2)

Таблиця 2.10 – Характеристика кіберзлочину передбаченого статтею 363-1 Кримінального кодексу України

стаття КК України	Ознаки складу злочину							
	Діяння	Предмет	Потер-пілий	Наслідки	Місце, час, спосіб, засоби, знаряддя, обставини, ситуація	Суб'єкт	Форма вини	Мета, мотив, емоційний стан
1	2	3	4	5	6	7	8	9
ч.1 ст.363-1	масове розповсюдження повідомлень електрозв'язку	електронно-обчислювальні машини (комп'ютера), автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку	особа	порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку	-	-	прямий умисел до діяння, умисел або необережн. до наслідків	мета – зміна, знищення або блокування інформації
ч.2 ст.363-1	те саме	те саме	те саме	заподіяли значну шкоду	спосіб – вчинені повторно або за попередньою змовою групою осіб		прямий умисел до діяння, умисел або необережн. до наслідків	мета – зміна, знищення або блокування інформації

За таких обставин теоретико-множинна модель ознак кіберзлочину передбаченого статтею 363-1 КК України буде мати такий вигляд:

$$О.363.1 = \{ Д.363.1; Пр.363.1; П.363.1; Н.363.1; С.363.1; Ф.363.1; М.363.1; КТІ \}, \quad (2.19)$$

де *О.363.1* – ознаки складу кіберзлочину

Д.363.1	– діяння злочину	масове розповсюдження повідомлень електрозв'язку
Пр.363.1	– предмет злочину	обчислювальні машини (комп'ютера), автоматизовані системи, комп'ютерні мережі чи мережі електрозв’язку
П.363.1	– потерпілий	особа
Н.363.1	– наслідки	порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; заподіяли значну шкоду
С.363.1	– спосіб вчинення	вчинені повторно або за попередньою змовою групою осіб
Ф.363.1	– форма вини	прямий умисел або необережність до діяння, необережн. до наслідків
М.363.1	– мета	зміна, знищення або блокування інформації
КТІ	– категорія та тип інциденту обумовлені згідно Переліку (див. табл.2.2)	

Загальна теоретико-множинна модель ознак кіберзлочину передбаченого в КК України буде мати такий вигляд:

$$О = \{ Д; Пр; П; Н; С; З; Суб.; Ф; М; КТІ \}, \quad (2.20)$$

де *О* – ознаки складу кіберзлочину

Д – діяння злочину

Пр – предмет злочину

Н – наслідки вчинення злочину

Суб. – суб’єкт

Ф – форма вини

М – мета

КТІ – категорія та тип інциденту

2.3 Розробка моделі розслідування кіберзлочинів

Розслідування кіберзлочину (як дослідження проблеми) завжди розпочинається із збирання вихідних даних за певними методами (табл. 2.11).

Таблиця 2.11 – Характеристика підготовчих дій на початковому етапі розслідування кіберзлочинів

Вихідні дані	Аналіз процесу	Особливі примітки
історія виникнення проблеми	що, де, коли відомо про проблему	
засоби електронних комунікацій	про які відомо елементи технічної інфраструктури, що забезпечують віртуальне існування проблеми в кіберпросторі (обладнання, пристрої, засоби, вузли, маршрутизатори, мережне обладнання, IMEI/IMSI тощо)	
ситуаційні дані	про які відомо електронні/ віртуальні сліди проблеми (інформація яка має сенс при розслідуванні, наприклад: чи є данні з телефонної книги; про SMS/MMS; чи є дані про надісланні повідомлення; чи є дані з електронної пошти; чи відомо історію відвідування ресурсів в кіберпросторі; чи є дані про геолокацію; чи є видалена інформація тощо)	так, під час огляду гаджета, ноутбука може виникнути необхідність фіксації та збирання інформації про кіберзлочин з дотриманням вимог копіювання та збереження в ході процесуальної дії; збирання інформації може відбуватися, як із дисків, браузерів, чатів, хмар, платіжних систем, журналів тощо.
реєстратор-реєстрант (IP/доменні імена/сайти/сторінки)	способи встановлення власників (офіційних користувачів) IP/доменних імен що в сфері/змісті проблеми	
провайдер	хто провайдер (и) та які послуги провайдера забезпечували (ють) формування/існування проблеми в кіберпросторі	Вид хостингу: віртуальний хостинг; віртуальний сервер; виділений сервер; хмарний хостинг тощо
технічна інфраструктура	яка комунікаційна система обумовлювала (є) проблему	
архітектура протоколів *(попередні висновки)*	які стандарти було порушено при використанні протоколів в сфері/змісті проблеми	топологія мереж та потік даних

Продовження табл. 2.11

програмне забезпечення використані утиліти *(на етапі збору вихідних даних)*	важливо, застосовувати правильні засоби, методи, методологію при копіюванні, дослідженні ЕОМ, накопичувачів, трафіку тощо.	

Отже, важливим на цьому етапі підготовчих дій – це брати до уваги, яка системоутворююча сукупність засобів телекомунікації обумовлює проблему та які об'єкти задіянні в інформаційній взаємодії. Тут під об'єктами можуть бути як «термінальні пристрої користувачів так і кінцеві системи мережі (окремі мережі тощо). А інтерфейсною точкою в телекомунікаційній мережі буде роз'єм (до якого під'єднаний пристрій користувача) або кінцеве мережеве обладнання, яке забезпечує з'єднання мереж (міжмережевий інтерфейс)» (рис. 2.3) [29].

Також враховується, кіберзлочинець свої дії вчиняє через певну «інтерфейсну точку», що забезпечує надалі використання електронно комунікаційної системи як «з'єднувального компонента» в загальній інформаційно-комунікаційній системі. Достовірність встановлення цих точок підвищує ефективність розслідування кіберзлочинів

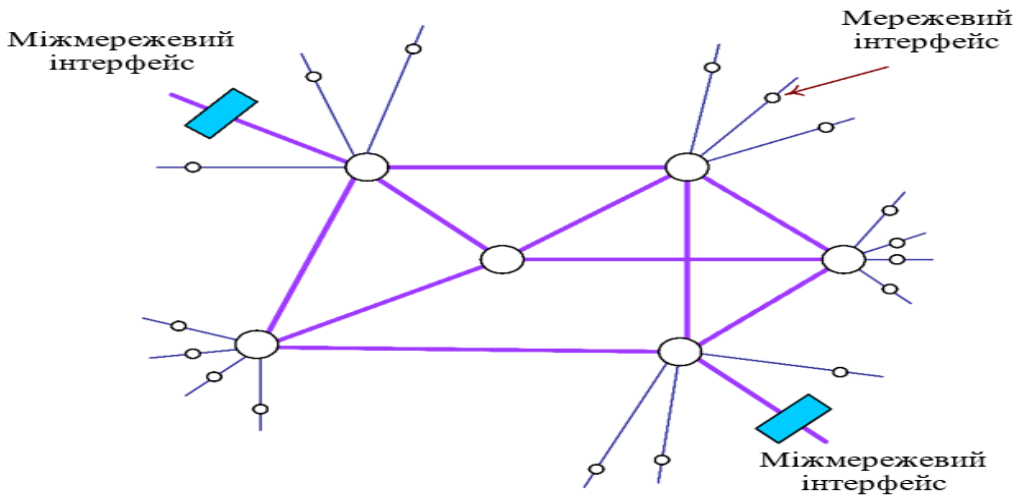


Рисунок 2.2 – Телекомунікаційна мережа [29]

Ми вважаємо, що покращення процесу комунікації між суб'єктами уповноваженими розслідувати кіберзлочини та спеціалістами (експертами) в

сфері комп'ютерної техніки та програмних продуктів є можливим, шляхом впровадження (для такої спеціальної комунікації) вихідного понятійно-категоріального апарату (табл. 2.12). Власне, перелік понять, які можуть обумовлювати тотожне міркування юристів та спеціалістів в сфері інформаційних технологій запозичений із доробку І. Канта [30].

Таблиця 2.12 – Перелік первісних чистих понять синтезу [30]

КІЛЬКОСТІ	ЯКОСТІ	ВІДНОШЕННЯ	МОДАЛЬНОСТІ
- одиничність - множинність - тотальність	- реальність - заперечення - обмеження	- належності й самостійності - причинності й залежності (*причина і діяння*) - спілкування (*взаємодія між діяльним і пасивним*)	- можливість-неможливість - існування-небуття - необхідність-випадковість

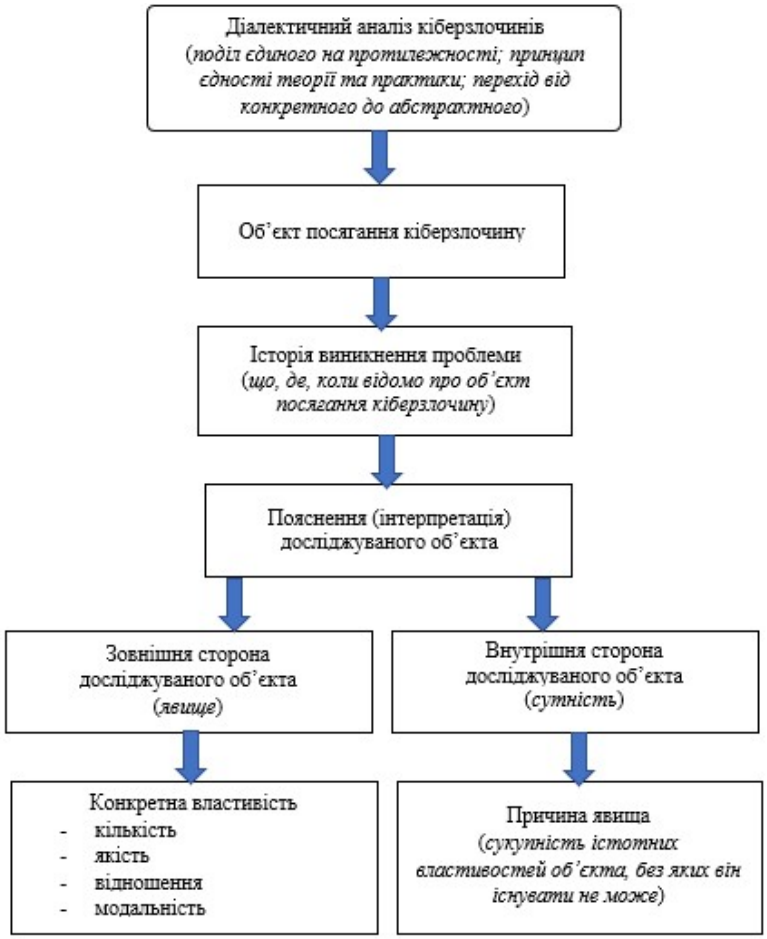


Рисунок 2.3 – Схема діалектичного аналізу кіберзлочинів

Таблиця 2.13 – Модель розслідування кіберзлочинів

Етапи	Сутність процесу	Особливі примітки
Виявлення проблеми	- з'ясування історії виникнення проблеми, ідентифікації/здобуття, фіксація, збирання, та збереження електронних доказів (згідно ознак ситуації); -вирішення питання про залучення консультанта (спеціаліста, експерта в сфері комп'ютерних наук) до моменту внесення відомостей в ЄРДР	Найперше керуються: - рекомендаціями щодо поводження з електронними (цифровими) доказами, які викладені в ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів»; - Переліком категорій кіберінцидентів (*який схвалений НКЦК при РНБО України 28.10.2021; в редакції на час звернення*)
Стадія досудового розслідування	ця стадія має специфічні функції, критерії, задачі: – нормативно визначена процесуальна діяльність; – процесуальну діяльність здійснюють виключно спеціально уповноважені суб'єкти; – коло засобів доказування обмежене; – розслідування має ретроспективний характер; – при розслідуванні, як правило, є протидія у встановленні обставин кіберзлочину.	Найперше керуються: КПК України
Стадія судового провадження	Особливе завдання, яким є вирішення кримінального провадження по суті, тобто питання про винуватість обвинуваченого і про ступінь його відповідальності у випадку визнання винним (з'ясовуючи ці питання, суд здійснює правосуддя, а тому і завдання судового розгляду співпадають, звичайно, із завданнями	Найперше керуються: КПК України

Продовження табл. 2.13

	кримінального судочинства загалом); - коло суб'єктів провадження, до якого окрім суду і вказаних у п.26 ст.3 КПК України учасників судового провадження долучаються свідки, експерти, спеціалісти тощо; - процесуальною формою здійснення судового розгляду є судове засідання, в межах якого, насамперед, допускається вчинення процесуальних дій (особливо тих, що спрямовані на дослідження доказів); - прийняття судового рішення, яке є завершальним не лише для даної стадії, але й для провадження загалом (вироку, ухвали про закриття тощо)	
Узагальнення досвіду (практичного матеріалу)	- проводять врахування досвіду правозастосування (на основі юридичних фактів та конкретних правових норм) та нової інформації про кіберінциденти від суб'єктів забезпечення кібербезпеки; - готують методичні рекомендації для підвищення ефективності розслідування кіберзлочинів	Найперше керуються: відомчими інструкціями

На етапі «виявлення проблеми» та «стадії досудового розслідування» важливим є дотримання базових вимог ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» [31; 32] (див. Додаток Б. Методичні рекомендації юристам (схеми, алгоритми)).

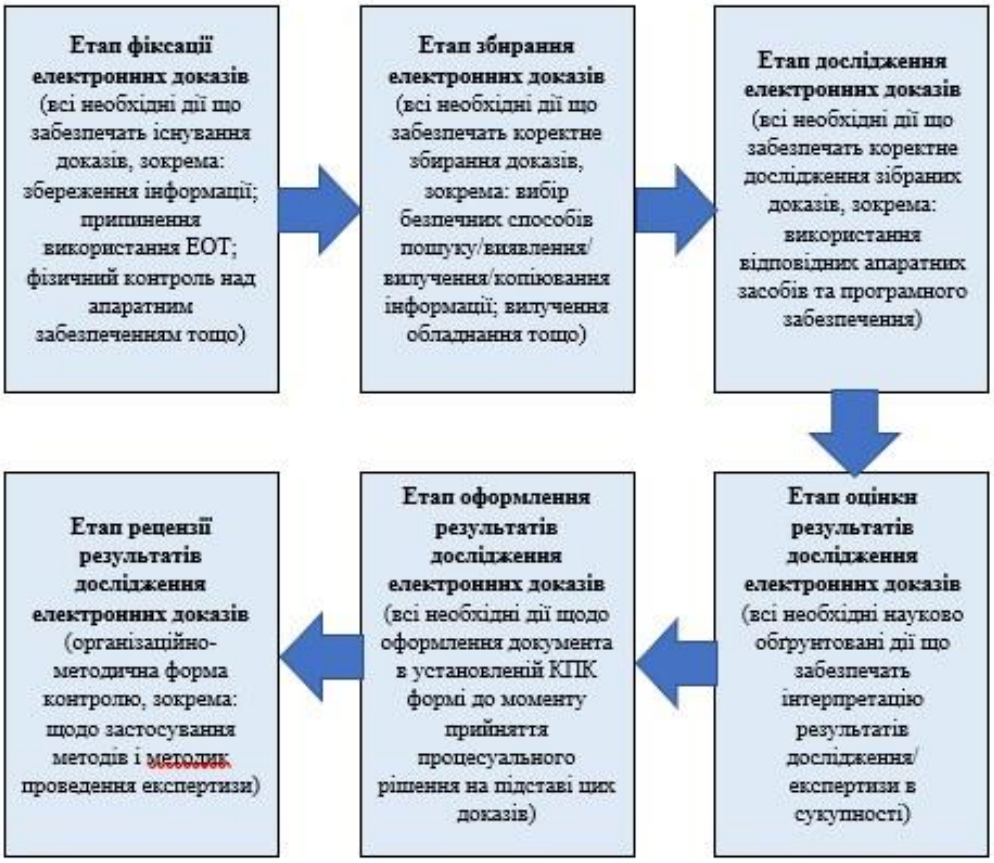


Рисунок 2.4 – Схема моделі роботи з електронними доказами при розслідуванні кіберзлочинів

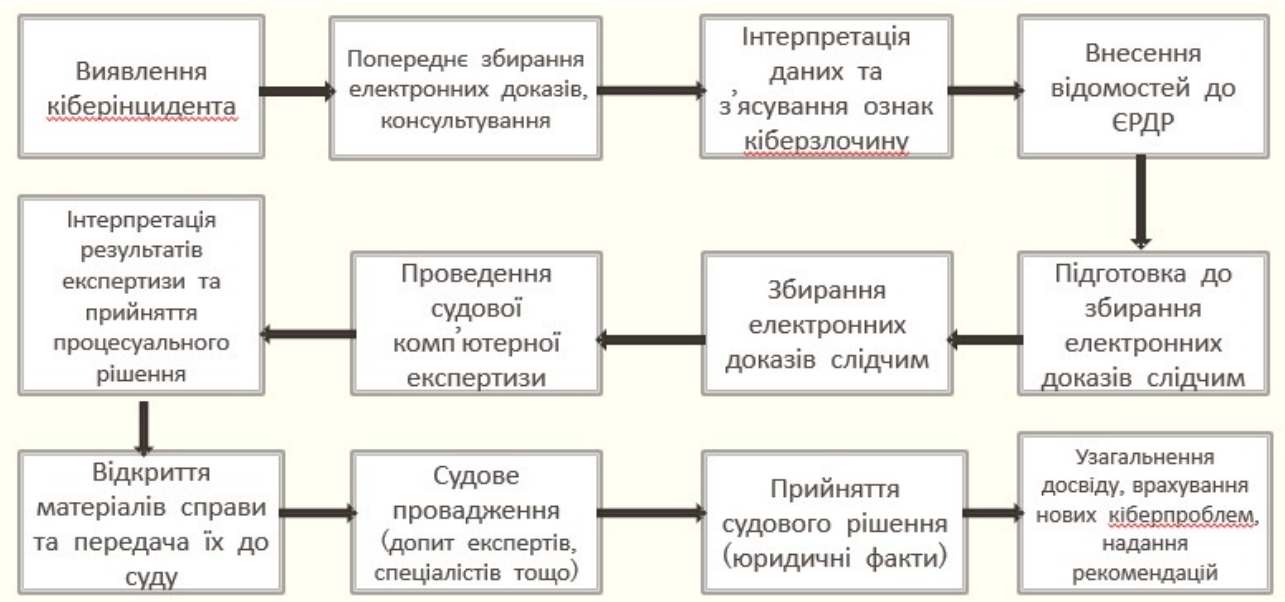


Рисунок 2.5 – Схема покрокової моделі розслідування кіберзлочинів

Висновки до 2 розділу

З’ясовано, що впровадження організаційно-технічної моделі кіберзахисту визначає відповідальність за виконання конкретних завдань кожного суб’єкта кібербезпеки. Також, при ефективному використанні цієї моделі є можливість сформувати якісну систему ресурсного забезпечення (в тому числі кадрового ресурсу).

Досліджено відмінності кіберзлочину від інших кіберінцедентів (кібератак), насамперед: не кожен кіберінцидент містить ознаки кримінального правопорушення; відмінність в суб’єктному складі при виявленні та розслідуванні (дослідженні) кіберінцидентів та кіберзлочинів; існують спеціальні процедури при розслідуванні кіберзлочинів, які обумовлені характером вчиненого правопорушення.

Розроблено теоретико-множинні моделі кіберінцидентів та теоретико-множинні моделі ознак кіберзлочинів передбачених статтями 190, 200, 361 – 363[1] Кримінального кодексу України.

Надана характеристика підготовчих дій щодо збирання технічних даних на початковому етапі розслідування кіберзлочинів. Розроблена модель розслідування кіберзлочинів, яка складається із чотирьох етапів: етап виявлення проблеми; стадія досудового розслідування; стадія судового провадження; етап узагальнення досвіду (практичного матеріалу) задля підготовки методичних рекомендацій для підвищення ефективності розслідування кіберзлочинів. Надалі, ця модель представлена в структурних елементах: схема моделі роботи з електронними доказами; схема покрокової моделі розслідування кіберзлочинів.

3 ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

3.1 Види та можливості судових експертиз під час розслідування кіберзлочинів

Проведення судової експертизи при розслідуванні кіберзлочинів у вітчизняному законодавстві регламентується: Законом України «Про судову експертизу» від 25.02.1994 № 4038-XII [33]; Кримінальним процесуальним кодексом України (ст.ст. 69, 70, 101, 102, 232, 242-245, 518) [23]; Інструкцією про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень від 08.10.98 №53/5[34]; Інструкцією про особливості здійснення судово-експертної діяльності атестованими судовими експертами, що не працюють у державних спеціалізованих експертних установах від 12.12.2011 № 3505/5 [35]; Положенням про Експертну службу МВС України, затвердженим наказом МВС України від 03.11.2015 № 1343 [36].

В ході розслідування кіберзлочинів постає нагальна необхідність у використанні спеціальних знань в сфері комп'ютерних наук. Для цього підшуковуються відповідні засоби, методи збирання та дослідження електронних слідів ЕОМ в інформаційних системах, кіберпросторі тощо [37].

Як зазначає О. Волков, «при розслідуванні кримінальних правопорушень використання спеціальних знань здебільшого здійснюється у разі: 1) проведення процесуальних чи інших дій із залученням спеціаліста в ІТ сфері; 2) проведення судових експертиз; 3) проведення перевірок, обстежень, консультацій; 4) допиту спеціалістів та експертів (як свідків), якщо вони брали участь у проведенні перевірок, досліджень або експертиз» [11].

Отже, комп'ютерно-технічна експертиза є однією з найбільш розповсюджених під час здійснення досудового розслідування кримінальних

правопорушень відповідної категорії. Її проведення дозволяє визначити статус об'єкта посягання (конкретний комп'ютерний пристрій), детально дослідити цей об'єкт не лише з технічного погляду, а й крізь призму його функцій і призначення, що дозволить отримати доступ до інформації, яку він зберігає або якою оперує.

В пунктах 13 та 14 Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень (затверджених наказом Міністерства юстиції України від 08.10.1998 № 53/5) [34] визначено такі види експертиз: (п.13) Експертиза комп'ютерної техніки і програмних продуктів; (п.14) Експертиза телекомунікаційних систем та засобів.

Таблиця 3.1 – Експертиза комп'ютерної техніки і програмних продуктів (основні акценти) [34]

Основні завдання експертизи	Орієнтовний перелік вирішуваних питань	Особливі примітки
- установлення робочого стану комп'ютерно-технічних засобів; - установлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення; - виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях; -установлення відповідності програмних продуктів певним версіям чи	- чи міститься на даному носії інформація стосовно (зазначити, яка інформація цікавить) і у якому вигляді? - чи містить носій досліджуваного комп'ютера інформацію про певні (зазначити, які саме)дії користувача? - чи піддавався досліджуваний накопичувач певним процедурам з метою знищення інформації? - чи могла бути створена зазначена інформація на цьому комп'ютері чи вона перенесена з іншого носія? - яким чином інформація (зазначити, яка саме) перенесена до досліджуваного комп'ютера (носія)? - яка технологія та хронологія створення електронного документа (зазначити	- для дослідження інформації, що міститься на комп'ютерних носіях, експерту надається сам комп'ютерний блок (комплекс комп'ютерних засобів, до складу якого входить досліджуваний носій); - для збереження наданих на дослідження носіїв інформації в робочому стані вони надаються в окремих пакуваннях (системні блоки персональних комп'ютерів надаються в пакуваннях, що унеможливлюють доступ до носіїв інформації безпосередньо чи підключення системного блоку до мережі живлення); - для встановлення відповідності програмних продуктів певним параметрам експерту надається носій з копією досліджуваного програмного продукту або програмного коду;

Продовження табл. 3.1

вимогам на його розробку	електронний документ та певний зміст)? - які атрибути (час друку, редагування, створення, видалення тощо) файлів, що містять інформацію ... (зазначити зміст)? - чи містить накопичувач інформації досліджуваного комп'ютера певне (зазначити, яке саме – встановлене, не встановлене) програмне забезпечення? - які функціональні несправності мають дане комп'ютерне обладнання або його окремі складові та пристрої і як ці несправності впливають на роботу обладнання в цілому? - чи можливо виконання певних дій за допомогою даного програмного продукту? - чи можливе вирішення певного завдання за допомогою даного програмного продукту? - чи реалізовані у даному програмному продукті (програмному коді) функції, передбачені технічним завданням на його розробку?	- для дослідження робочого стану комп'ютерно-технічних засобів експерту надаються ці комп'ютерно-технічні засоби, а також технічна документація до них; - з метою визначення, які саме об'єкти слід надати експерту в кожному конкретному випадку, а також як їх відбирати для дослідження, доцільно отримати консультацію експерта (спеціаліста) в галузі комп'ютерної техніки

Таблиця 3.2 – Експертиза телекомунікаційних систем та засобів (основні акценти) [34]

Основні завдання експертизи	Орієнтовний перелік вирішуваних питань	Особливі примітки
- визначення характеристик та параметрів телекомунікаційних систем та засобів; - встановлення фактів та способів передачі (отримання) інформації в телекомунікаційних системах;	- які тип, марка, модель телекомунікаційного засобу (системи)? - чи в робочому стані знаходиться телекомунікаційний засіб (об'єкт)?	- об'єктами експертизи телекомунікаційних систем та засобів є телекомунікаційні системи, засоби, мережі і їх складові частини та інформація, що ними передається,

Продовження табл. 3.2

- встановлення фактів та способів доступу до систем, ресурсів та інформації у сфері телекомунікацій; - визначення якості надання телекомунікаційних послуг на рівні їх споживання; - встановлення конфігурації та робочого стану телекомунікаційних систем та засобів; - встановлення типу, марки, моделі та інших класифікаційних категорій телекомунікаційних систем та засобів; - дослідження алгоритмів обробки інформації та її захисту в сфері телекомунікації	- які характеристики підключень до мережі має телекомунікаційний засіб? - чи змінювалися користувачем телекомунікаційні мережі налаштування окремих пристроїв, у який час, які їх значення? - який загальний характер підключень до телекомунікаційної мережі виконував об'єкт (телекомунікаційна система, засіб)? - за допомогою яких програмних засобів здійснювалось підключення до телекомунікаційної мережі? - яка топологія апаратних засобів, об'єднаних у телекомунікаційну систему? - чи відповідає функціонування телекомунікаційного засобу (системи) технічній документації? - які технічні характеристики (параметри) має телекомунікаційний засіб (система)? - чи мав місце факт доступу до телекомунікаційної системи та в який спосіб? - чи мало місце використання ресурсів та інформації в телекомунікаційній системі та в який спосіб? - чи мав місце факт передачі (отримання) інформації в телекомунікаційній системі та в який спосіб? - чи є ознаки втручання в роботу телекомунікаційної системи? - чи могли апаратні засоби об'єднуватись у телекомунікаційну мережу та за якими ознаками? - які шляхи маршрутизації даних у телекомунікаційній системі?	приймається та обробляється

Продовження табл. 3.2

	- чи можливо використання телекомунікаційного засобу (обладнання) для вказаних цілей?	

Об’єкт та предмет (експертне завдання) судових експертиз під час розкриття та розслідування кіберзлочинів залежить від способу та механізму скоєння та приховування злочину.

Таблиця 3.3 – Сутнісні ознаки комп’ютерно-технічної та телекомунікаційної експертизи

Експертиза комп’ютерної техніки і програмних продуктів Експертиза телекомунікаційних систем та засобів	1) використання спеціальних знань; 2) проведення дослідження з метою встановлення обставин, які мають значення для провадження; 3) наявність спеціального суб’єкта експертизи; 4) визначену процесуальну форму; 5) оформлення результатів у процесуальному документі – висновку експерта

3.2 Оцінка та використання результатів судових експертиз під час розслідування кіберзлочинів

Призначення судової експертизи на стадії досудового розслідування сприяє об’єктивності, повноті та всебічності пізнання події та обставин злочину (внаслідок застосування спеціальних знань та отримання певних результатів).

Таблиця 3.4 – Причини які впливають на проведення експертизи при розслідуванні кіберзлочинів

Об’єктивні причини	особливості слідів ЕОТ, комп’ютерних мереж і мереж електрозв’язку, які обумовлюють складність процесу розслідування

Продовження табл. 3.4

Суб'єктивні причини	відсутні належні знання, навички та вміння в сфері комп'ютерних наук щодо усвідомлення сутності кіберпростору та його особливостей, що стає причиною нецілеспрямованого та неефективного розслідування кіберзлочинів спеціально уповноваженими суб'єктами (найперше, слідчими, прокурорами, суддями)

Таблиця 3.5 – Критерії оцінки та використання результатів судових експертиз при розслідуванні кіберзлочинів

Вид експертизи	Критерії
Експертиза комп'ютерної техніки і програмних продуктів Експертиза телекомунікаційних систем та засобів	- володільцем інформації повинні бути визначені умови та правила отримання і обробки інформації; - власник (розпорядник) ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи оператор (провайдер) мереж електрозв'язку повинні розробити та впровадити заходи захисту інформації в системі; - власник (розпорядник) комп'ютерів, систем та оператор (провайдер) мереж повинні розробити правила роботи системи; - між власником (оператором, провайдером) системи та володільцем інформації повинен бути укладений договір щодо захисту інформації в системі; - злочинець виконав хоча б одну із операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання інформації

Кіберпростір дуже *пластичний,* і його можна описати як *рекурсивний*: платформи на платформах на платформах. Платформи можуть відрізнятися в деталях, але їх об'єднує те, що вони є фундаментом для наступної платформи над ними [7]. Також вірно зазначає Д.Кларк, що аналіз контрольних точок – це набір інструментів, які допомагають строго продумати дизайн системи з певної точки зору та визначити, які актори отримують владу завдяки контролю над ключовими компонентами системи: 1) можна діяти кількома способами, які доповнюють один одного; 2) можна скласти каталог усіх частин системи і занотувати схему контролю, яка до них застосовується; 3) можна простежити кроки звичайних дій (наприклад, у випадку Інтернету – пошук веб-сторінки) і на кожному кроці запитувати, чи не зустрічався вам важливий пункт контролю (цей

метод може допомогти виявити точки в системі, які могли бути пропущені в початковому каталозі); 4) можна подивитися на кожного з учасників екосистеми і запитати, які форми контролю вони здійснюють (це дає змогу поглянути на той самий набір питань під третім кутом) .

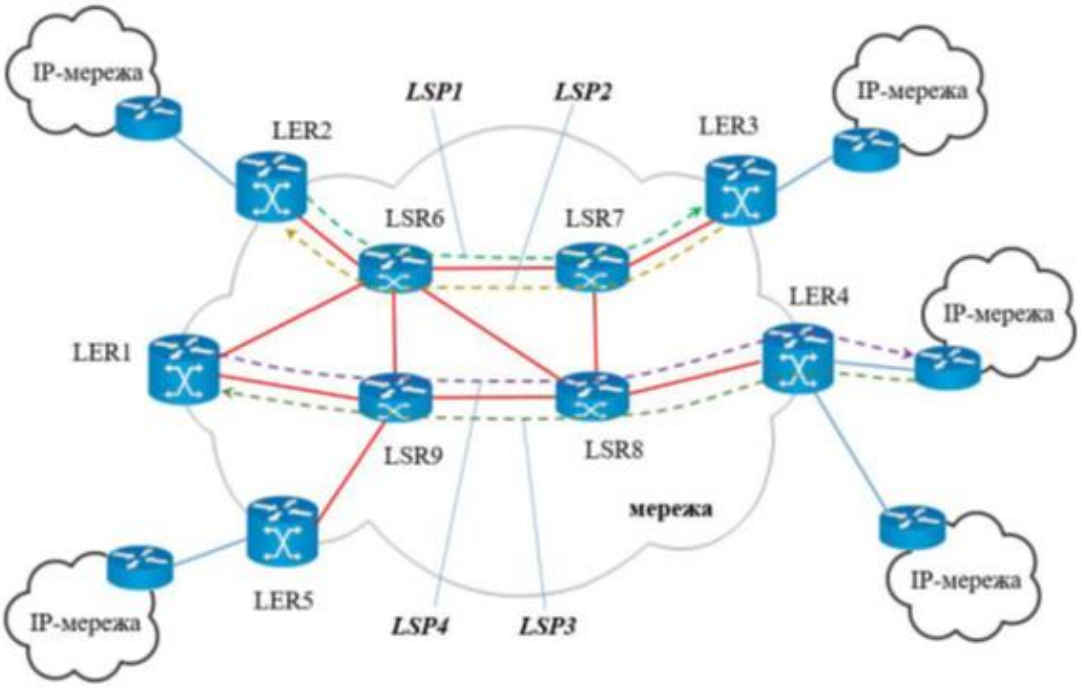


Рисунок 3.1 – Спрощена схема аналізу контрольних точок
(на базі рекурсивних платформ)

Відповідно до ст. 94 КПК України, «слідчий, прокурор, слідчий суддя, суд за своїм внутрішнім переконанням, яке ґрунтується на всебічному, повному і неупередженому дослідженні всіх обставин кримінального провадження, керуючись законом, оцінюють кожний доказ з точки зору належності, допустимості, достовірності» [23]. Для виконання цієї норми закону – експерт у своїх висновках зобов’язаний всебічно вивчити надані на експертизу докази, доцільно застосовувати спеціальні знання, засоби та методологію, а також, обґрунтувати отриманні результати (у разі необхідності, роз’яснити природу отриманих результатів). Тобто, експерт використовує спеціальні знання при проведенні судової експертизи задля отримання результатів та їх оцінки [10].

Взявши до уваги матеріали слідчої та судової практики, Верховний Суд України у Постанові № 8 від 30.05.1997 року «Про судову експертизу в кримінальних і цивільних справах» звертає увагу на те, що при перевірці та оцінці експертного висновку суд повинен з'ясувати: 1) чи було додержано вимоги законодавства при призначенні та проведенні експертизи; 2) чи не було обставин, які виключали участь експерта у справі; 3) компетентність експерта, і чи не вийшов він за межі своїх повноважень; 4) достатність наданих експертові об'єктів дослідження; 5) повноту відповідей на порушені питання та їх відповідність іншим фактичним даним; 6) узгодженість між дослідницькою частиною та підсумковим висновком експертизи; 7) обґрунтованість експертного висновку та його узгодженість з іншими матеріалами справи [38].

Таблиця 3.6 – Критерії оцінки та використання результатів судових експертиз спеціально уповноваженими суб'єктами при розслідуванні кіберзлочинів

Спеціально уповноважені суб'єкти	Аспекти оцінки
Слідчі, детективи, прокурори, судді, адвокати	- перевірка достатності наданих для експертизи об'єктів (оскільки недостатня їх кількість, особливо у випадку вирішення ідентифікаційного питання, може стати причиною помилкового висновку чи відмови від його дачі); - якість об'єктів, що визначається відповідністю зразків для експертного дослідження досліджуваним об'єктам, належними способами вилучення, упакування, збереження, транспортування об'єктів експертизи, правильності вихідних даних для експертного дослідження; - перевірка доцільності, правомірності застосованих експертом методики, методів дослідження та оцінку їх наукової обґрунтованості (з цією метою визначається: чи відповідає використана експертом методика поставленим перед ним питанням, чи придатна вона для виявлення необхідних властивостей наданих об'єктів, чи знаходить ця методика застосування в експертній практиці); - перевірка повноти проведених досліджень, встановлення всіх ознак об'єктів судової експертизи (для чого визначається: чи всі

Продовження табл. 3.6

	процедури і види досліджень стосовно об’єкта виконані згідно з обраною методикою); - перевірка правильності опису та інтерпретації встановлених ознак об’єктів (в даному випадку визначається: чи кожна виявлена в перебігу експертного дослідження ознака детально описана та оцінена експертом, як з точки зору відображення властивостей об’єкта, так і з точки зору його значущості для вирішення поставленого питання); - перевірка наукової обґрунтованості проміжних і підсумкових висновків, що є логічним завершенням оцінки (для цього встановлюється: чи зроблені проміжні висновки за результатами проведених досліджень, чи достатньо виявлених ознак для цих висновків, чи є остаточні висновки наслідком сукупної оцінки проміжних); - визначення фахової компетентності експерта на підставі всебічного аналізу висновку

3.3 Експериментальне дослідження кіберзлочинів як основа розробки методики

Ефективність розслідування кіберзлочинів напряму залежить від методів отримання та аналізу електронних (цифрових) доказів. Також, нині існує проблема координації обміну інформацією між суб’єктами уповноваженими розслідувати кіберзлочини (наприклад, слідчим) та спеціалістами (експертами) в сфері комп’ютерної техніки та програмних продуктів. Це обумовлено використанням різних підходів до інтерпретації обставин (процесів) в кіберпросторі та в його інфраструктурі, в силу використання відмінного понятійно-категоріального апарату (які формують канву дослідження). Тобто, в ході розслідування кіберзлочинів (або проведення експертизи) між експертом та слідчим відбувається взаємодія, яка обумовлена обміном інформацією про отриманні результати та щодо уточнення завдань перед експертом.

Враховуючи сучасні тенденції розвитку ІТ-сфери, наступним кроком буде «конвергенція, яка забезпечить перехід до мереж наступного покоління (NGN – Next Generation Network), які мають на меті якісно змінити всі сфери життя й

діяльності людини» [29]. Насамперед, ці зміни передбачають впровадження на всіх рівнях розвитку кіберпростору нових продукційних правил (англ. *Production rules*): створення логічних моделей, що візуалізують знання про існуючі процеси. Отже, враховуючи тенденції та семантичне навантаження вказаних тут вище понять (категорій) (див. табл. 2.12), та беручи до уваги актуальність їх використання, ми можемо застосувати діалектичний аналіз кіберзлочинів (див. рис.2.3) для узгодження світоглядних професійних позицій суб'єктів уповноважених розслідувати кіберзлочини та спеціалістів (експертів) в сфері комп'ютерної техніки та програмних продуктів що забезпечить підвищення ефективності розслідування кіберзлочинів.

Із ухвали Ленінського районного суду м. Запоріжжя від 22.03.2023 року у справі № 334/4848/22 досудовим розслідуванням (*за ознаками кримінального правопорушення передбаченого ч. 3 ст. 190 КК України, в редакції Закону до 13.07.2023; після цієї дати цей кіберзлочин передбачений ч.4 ст. 190 ККУ*) встановлено, що 06 серпня 2022 року ОСОБА_4 маючи умисел, направлений на заволодіння чужим майном, шляхом обману, за допомогою незаконних операцій з використанням електронно-обчислювальної техніки, з метою особистого збагачення за рахунок інших осіб, діючи умисно, усвідомлюючи протиправність своїх дій та свідомо бажаючи настання наслідків свого діяння, з корисливих мотивів, за допомогою додатку «Viber», представившись волонтером на ім`я ОСОБА_5 , умисно надав недостовірні відомості потерпілій ОСОБА_6 , про те, він є волонтером та має змогу надати останній послугу, що полягала у передачі грошових коштів родичам на тимчасово-окуповану територію Запорізької області. Після чого, 06.08.2022 р. о 11 годині 11 хвилин, ОСОБА_4 , в ході подальшого листування з ОСОБА_6 , під приводом передачі грошових коштів, отримав грошові кошти у сумі 4000 гривень 00 копійок з розрахункового рахунку банківської картки емітованої АТ «Державний ощадний банк України» на ім`я потерпілої ОСОБА_6 НОМЕР_1 на банківську картку АТ «АКБ«КОНКОРД» № НОМЕР_2 на ім`я ОСОБА_7 , яка не будучи обізнаною про злочинний намір

останнього, надала йому реквізити своєї онлайн-картки та дані для входу до інтернет-банкінгу. Так, продовжуючи реалізацію свого протиправного умислу, ОСОБА_4 , за допомогою інтернет-банкінгу здійснив вхід до мобільного додатку «NeoBank», № НОМЕР_2 на ім`я ОСОБА_7 та здійснив переказ грошових коштів на банківську карту АТ«ТАСКОМБАНК» № НОМЕР_3 емітовану на ім`я ОСОБА_4 , після чого, 06.08.2022 р. о 14 годині 08 хвилин, ОСОБА_4, знаходячись за адресою: АДРЕСА_1 , використовуючи банкомат CAZA7830 перевів у готівку отримані шляхом обману грошові кошти, належні потерпілій ОСОБА_6 , якими в подальшому розпорядився на власний розсуд, спричинив потерпілій ОСОБА_8 матеріальний збиток на суму 6 200 гривень 00 копійок.

Таблиця 3.7 – Порядок криміналістичного дослідження кіберзлочину передбаченого ч.3 ст. 190 Кримінального кодексу України

Категорія та тип інциденту	Кіберзлочин	Докази, які необхідно здобути (згідно ознак за формулою 2.12)	Інструменти	Примітки до використання інструменту
категорія інциденту – 10. Інше (Other); тип інциденту – 01.Невизначений інцидент (Undetermined incident)	ч. 3 ст. 190 КК України	які операційні системи iOS чи Android використовували (злочинець, потерпіла) щоб користуватися додатком Viber, та характеристики ЕОТ	*Програмний засіб: Belkasoft Evidence Center*	- дозволяє витягувати і аналізувати дані з мобільних пристроїв, хмарних сховищ і жорстких дисків; - при аналізі жорстких дисків здійснюється вилучення даних із веб-браузерів, чатів, інформації про хмарні сервіси, детектування зашифрованих файлів і розділів, витяг файлів за заданим розширенням, даних про геолокацію, електронної пошти, даних із платіжних систем і соціальних мереж, мініатюр, системних файлів, системних журналів тощо; - має гнучкий функціонал щодо вилучення віддалених даних
		характеристика IP-телефонії (злочинця, потерпілої тощо)		
		характеристика інтернет-банкінгу із якого злочинець здійснив вхід до мобільного додатку «NeoBank»		
		характеристика банкомату CAZA7830		

Із Вироку Великописарівського районного суду Сумської області від 21.11.2023 року у справі № 575/1041/23 щодо засудженої ОСОБА_4 у вчиненні

кримінальних правопорушень передбачених ч. 1 ст. 200, ч. 1 ст. 209 КК України стає відомо, що Рішенням Ради національної безпеки і оборони України (далі РНБО України) «Про застосування та скасування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» від 2 травня 2018 року, введених в дію Указом Президента України від 14травня 2018 року № 126/2018 та «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» від 14 травня 2021 року, введених в дію Указом Президента України від 21 травня 2021 N 203/2021, застосовано ряд обмежувальних заходів відносно ТОВ «ВМ Трансфер ЛТД» (WebMoney Ltd), Литовська Республіка, м. Вільнюс, вул. В.Кудіркос, 18А-1, ЛТ-03105, яке є власником та адміністратором платіжної системи «WebMoney Transfer», що виразилось у повному припиненні та забороні її діяльності на території України. Відповідно введених в дію санкцій відносно «WebMoney» Національним банком України скасовано реєстрацію внутрішньодержавної системи рахунків, відкликано (анульовано) ліцензії на переказ коштів у національній валюті без відкриття рахунків, скасовано реєстрацію учасника платіжних систем, скасовано реєстрацію оператора послуг платіжної інфраструктури. Незважаючи на перелічені закони та нормативні акти, нехтуючи їх положеннями ОСОБА_4, усвідомлюючи незаконність своїх дій, 20 березня 2023 року знаходячись в с. Ямне Охтирського (Великописарівського) району Сумської області, в денний період часу, приблизно з 16 год. 44 хв. до 17 год. 49 хв., діючи з корисливих мотивів та з метою особистого збагачення і отримання незаконних (неконтрольованих Державою) доходів, не маючи ліцензії (дозволу) Національного банку України, надав послуги з обміну (вводу, виводу) заборонених електронних грошей шляхом використання забороненої платіжної системи «WebMoney Transfer». ОСОБА_4 з метою отримання незаконного доходу за надання послуг обміну (вводу, виводу) заборонених електронних грошей, діючи без ліцензії (дозволу) Національного банку України на обмін та переказ коштів у національній валюті, без відкриття рахунків та не будучи

комерційним агентом з рахунків у сфері використання електронних грошей, використовуючи оголошення на веб-ресурсі «OLX» «ІНФОРМАЦІЯ_2» на якій розміщено оголошення «Вывод ввод "WebMoney" (Вебмани), оплата услуг в интернет», безпосередньо надав послуги з обміну, вводу, виводу електронних коштів через заборонену платіжну систему «WebMoney Transfer» 20 березня 2023 року здійснив обмін (ввід, вивід) 10000 грн. у WMZ (різновид заборонених електронних грошей), а саме о 17 год. 19 хв. отримав вказані кошти на власну банківську картку № НОМЕР_1 від ОСОБА_6 з банківської картки № НОМЕР_2. Після чого о 17 год. 49 хв. ОСОБА_4 з електронного гаманця забороненої платіжної системи «WebMoney Transfer» № НОМЕР_3 здійснив переказ заборонених електронних грошей в розмірі 250 (двісті п'ятдесят) одиниць в номіналі «WMZ» на електронний гаманець ОСОБА_6 N НОМЕР_4. Так, ОСОБА_4 усвідомлюючи протиправність своїх дій, використав заборонену платіжну систему «WebMoney Transfer» та здійснив обмін (ввід, вивід) заборонених електронних грошей «WMZ». Таким чином ОСОБА_4 діючи умисно, неправомірно використав електронні гроші, тобто вчинив кримінальне правопорушення, передбачене ч. 1 ст. 200 КК України.

Таблиця 3.8 – Порядок криміналістичного дослідження кіберзлочину передбаченого ч.1 ст. 200 Кримінального кодексу України

Категорія та тип інциденту	Кіберзлочин	Докази, які необхідно здобути (згідно ознак за формулою 2.13)	Інструменти	Примітки до використання інструменту
категорія інциденту – 07. Порушення властивостей інформації (Information Content Security; тип інциденту – 01. Несанкціонований доступ до інформації (Unauthorised	ч. 1 ст. 200 КК України	характеристики ЕОТ які забезпечили злочинцю роботу із платіжною системою «WebMoney Transfer»	*Програмний засіб: Belkasoft Evidence Center*	- дозволяє витягувати і аналізувати дані з мобільних пристроїв, хмарних сховищ і жорстких дисків; - при аналізі жорстких дисків здійснюється вилучення даних із веб-браузерів, чатів, інформації про хмарні сервіси, детектування зашифрованих файлів і розділів, витяг файлів за заданим розширенням,
		характеристика IP-телефонії (злочинця)		
		характеристика ЕОТ, який забезпечив роботу на веб-ресурсі «OLX» та дані такої роботи		
		характеристики банківських карток із якої		

Продовження табл. 3.8

access to information)		перерахувалися гривні і на яку зарахувалися (картка злочинця), дані проведених операцій		даних про геолокацію, електронної пошти, даних із платіжних систем і соціальних мереж, мініатюр, системних файлів, системних журналів тощо; - має гнучкий функціонал щодо вилучення віддалених даних
		характеристика електронних гаманців платіжної системи «WebMoney Transfer», та дані проведених операцій		

Із Вироку Рівненського міського суду від 08.02.2023 у справі № 569/12262/22 щодо засудженої ОСОБА_3 у вчиненні кримінальних правопорушень, передбачених ч. 1 ст. 361 (*в редакції Закону від 01.07.2020 до 02.04.2022*), ч. 3 ст. 354, ч. 2 ст. 361 (*в редакції Закону від 01.07.2020 до 02.04.2022*), ч. 4 ст. 354 КК України: ОСОБА_3, працюючи на посаді сестри медичної (дільничної) патронажної Комунального некомерційного підприємства «Центр первинної медико-санітарної допомоги «Північний» Рівненської міської ради (код ЄДРПОУ 33982708), маючи у користуванні ідентифікатор доступу (логін та пароль) входження до інформаційно-телекомунікаційної системи «Хелсі» сімейного лікаря Центр ПМСД «Північний» ОСОБА_5, в період з 16.08.2021 по 17.03.2022, перебуваючи за своїм робочим місцем, що розташоване в приміщенні лікарні за адресою м. Рівне, вул. Академіка Грушевського, буд. 11, усвідомлюючи суспільно-небезпечний характер свого діяння, передбачаючи його суспільно-небезпечні наслідки та бажаючи їх настання, діючи умисно, з корисливого мотиву, з метою особистого збагачення, за рахунок отримання неправомірної вигоди, достовірно знаючи, що ОСОБА_6, ОСОБА_7 та ОСОБА_8, не проходили вакцинацію від гострої респіраторної хворобиCOVID-19, вносила особисто від імені користувача ОСОБА_5 до автоматизованої системи «Хелсі» завідомо для себе недостовірну інформацію про проходження всіма вказаними особами вакцинації від гострої респіраторної хвороби COVID-19, тим самим не санкціоновано втрутилась у роботу автоматизованої системи «Хелсі», що призвело до підробки інформації, яка міститься у вказаній системі

щодо медичних даних пацієнтів та проходження всіма вказаними особами вакцинації.

Таблиця 3.9 – Порядок криміналістичного дослідження кіберзлочину передбаченого ч.1 та ч. 2 ст. 361 Кримінального кодексу України

Категорія та тип інциденту	Кіберзлочин	Докази, які необхідно здобути (згідно ознак за формулою 2.14)	Інструменти	Примітки до використання інструменту
категорія інциденту – 07. Порушення властивостей інформації (Information Content Security); тип інциденту – 01. Несанкціонований доступ до інформації (Unauthorised access to information) та 02. Несанкціонована модифікація інформації (Unauthorised modification of info)	ч.1 та ч.2 ст. 361 КК України	характеристики ЕОТ які забезпечили злочинцю роботу в ІТС Хелсі, та дані про роботу в ІТС Хелсі	*Програмний засіб: Belkasoft Evidence Center*	- дозволяє витягувати і аналізувати дані з мобільних пристроїв, хмарних сховищ і жорстких дисків; - при аналізі жорстких дисків здійснюється вилучення даних із веб-браузерів, чатів, інформації про хмарні сервіси, детектування зашифрованих файлів і розділів, витяг файлів за заданим розширенням, даних про геолокацію, електронної пошти, даних із платіжних систем і соціальних мереж, мініатюр, системних файлів, системних журналів тощо; - має гнучкий функціонал щодо вилучення віддалених даних
		характеристика IP-телефонії (злочинця та осіб в інтересах яких відбулася підробка інформації)		
		характеристика мобільних пристроїв та дані про комунікації злочинця та осіб в інтересах яких відбулася підробка інформації		
		характеристики банківських карток із якої перерахувалися кошти і на яку зарахувалися (картка злочинця), дані проведених операцій		

Із Вироку Приморського районного суду міста Одеси від 09.06.2022 року у справі № 522/8425/21 щодо засудженої ОСОБА_3 у вчиненні кримінального правопорушення передбаченого ч. 1 ст. 361-1 КК України, стає відомо: 15 грудня 2020 року ОСОБА_3 перебуваючи за місцем свого проживання за адресою: АДРЕСА_1, за допомогою свого персонального комп’ютера «SpiderMan», являючись користувачем веб-ресурсів тіньової тематики ІНФОРМАЦІЯ_2, ІНФОРМАЦІЯ_3, ІНФОРМАЦІЯ_4, ІНФОРМАЦІЯ_5, використовуючи нік-нейм «ОСОБА_6», розмістив на вказаних сайтах оголошення про продаж

шкідливого програмного забезпечення «opencart (admpanel) brut.db+brut joomla, wp, drupal, Magento» призначеного для виконання несанкціонованих втручань до облікових записів різних поштових та інформаційних ресурсів, у яких, відповідно до ст. 31 Конституції України,ч. 2 ст. 21 ЗУ «Про інформацію» містилась інформація з обмеженим доступом, шляхом проведення атаки типу «brut-force». Окрім того, продаж шкідливого програмного забезпечення «opencart (adm panel) brut.db+brutjoomla, wp, drupal, Magento», призначеного для виконання несанкціонованих втручань до облікових записів різних поштових та інформаційних ресурсів, виконувався ОСОБА_3 в месенджері «Telegram» з використанням нік-нейму «ОСОБА_7» з прив'язаним номером мобільного телефону «НОМЕР_1». Шкідливе програмне забезпечення ОСОБА_3 розробляв власноруч з метою його подальшого збуту на веб-ресурсах тіньової тематики з метою отримання грошової винагороди у вигляді переказів грошових коштів в електронній валюті «Bitcoin». В подальшому за допомогою програмного забезпечення Private Keeper, ОСОБА_3 здійснював налаштування шкідливого програмного забезпечення «opencart (adm panel) brut.db+brut joomla, wp, drupal, Magento» та забезпечував його роботоспроможність. Також вказане програмне забезпечення було налаштовано таким чином, що повністю адмініструвалось ОСОБА_3 шляхом надання новим користувачам авторизаційного логіну. Реалізовуючи свій намір, діючи умисно, з корисливих мотивів, з метою збуту шкідливого програмного засобу «opencart (adm panel) brut.db+brut joomla, wp, drupal, Magento», використовуючи всесвітню комп'ютерну мережу Інтернет, та в месенджері «Telegram» 15 грудня 2020 року надав невідомій особі, яка в месенджері «Telegram» використовує нік-нейм «ОСОБА_8» шкідливе програмне забезпечення «opencart (adm panel) brut.db+brutjoomla, wp, drupal, Magento» на базі оболонки «ОСОБА_9» за що отримав грошові кошти на свій електронний гаманець системи електронних платежів «Bitcoin» «15P5mQNrN4heSJ5iqc4p5FFnb6MXTiHyu4». Збут в мережі Інтернет шкідливого програмного забезпечення «opencart (adm panel) brut.db+brut joomla, wp, drupal, Magento» ОСОБА_3

здійснював з власного персонального комп'ютера марки «SpiderMan» до моменту проведення співробітниками поліції санкціонованого обшуку за адресою: АДРЕСА_1, а саме до 12.01.2021 р. Таким чином ОСОБА_3 своїми умисними діями вчинив кримінальне правопорушення, передбачене ч. 1 ст. 361-1 КК України, за кваліфікуючими ознаками створення з метою використання та збуту, а також збут шкідливих програмних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів) та автоматизованих систем.

Таблиця 3.10 – Порядок криміналістичного дослідження кіберзлочину передбаченого ч.1 ст. 361-1 Кримінального кодексу України

Категорія та тип інциденту	Кіберзлочин	Докази, які необхідно здобути (згідно ознак за формулою 2.15)	Інструменти	Примітки до використання інструменту
категорія інциденту – 02. Шкідливий програмний код (Malicious Code); тип інциденту – 02. Розповсюдження ШПЗ (Malware distribution)	ч. 1 ст. 361-1 КК України	характеристики ЕОТ (зокрема персонального комп’ютера «SpiderMan» та інші засоби електронної комунікації), які забезпечили злочинцю роботу на веб-ресурсів тіньової тематики	апаратний блокіратор *Tableau T35U*	дозволяє безпечно підключати досліджувані жорсткі диски до комп’ютера дослідника по шині USB3 (це буває корисним у дослідженні накопичувачів, заражених шкідливим програмним забезпеченням)
		характеристика ШПЗ «brut-force» (характеристика методу пошуку паролів)	Програмний засіб *Belkasoft Evidence Center*	Переваги програми Belkasoft Evidence Center такі: - широкий спектр даних із різних носіїв інформації; - вмонтований переглядач баз даних SQLite; - збір даних із віддалених комп’ютерів і серверів; - інтегрований функціонал щодо перевірки виявлених файлів на Virustotal.
		характеристика IP-телефонії (злочинця),		
		характеристика ЕОТ, який забезпечив роботу в месенджері «Telegram», дані такої роботи		
		характеристика банківських карток (картки злочинця), дані проведених операцій		
		характеристика електронного гаманця електронних платежів Bitcoin, та дані проведених операцій		

Із Вироку Деснянського районного суду міста Києва від 22.11.2023 року у справі № 754/13848/23 щодо засудженого ОСОБА_3 у вчиненні кримінального правопорушення передбаченого ч. 2 ст. 361-2 КК України, стає відомо: ОСОБА_3, маючи умисел на несанкціоноване розповсюдження інформації з обмеженим доступом, яка зберігається в автоматизованій системі, створеній та захищеній відповідно до чинного законодавства, вчинене за попередньою змовою групою осіб, вчинив кримінальне правопорушення за наступних обставин. Так, ОСОБА_3, будучи учасником групи месенджеру «Telegram», під назвою «ІНФОРМАЦІЯ_2», посилання ІНФОРМАЦІЯ_3 використовує акаунт з обліковим записом «ІНФОРМАЦІЯ_4», ID: НОМЕР_1 (ІНФОРМАЦІЯ_4 мобільного месенджеру «Telegram», порушуючи встановлений законодавством України порядок регулювання суспільних відносин у сфері обігу інформації з обмеженим доступом, діючи з прямим умислом, переслідуючи корисливий мотив та спеціальну мету – розголошення відомостей з обмеженим доступом, усвідомлюючи протиправність своїх дій, бажаючи одержати особисту матеріальну вигоду шляхом незаконного розголошення за грошову винагороду інформацію, доступ до якої обмежено, діючи за попередньою змовою групою осіб, розповсюдив інформацію з автоматизованої інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України», яка відноситься до інформації з обмеженим доступом. 29.07.2023 у період часу з 12:00 год. по 15:30 год., ОСОБА_6, використовуючи мобільний месенджер «Telegram» з абонентським номером НОМЕР_2, увійшов до групи під назвою «ІНФОРМАЦІЯ_2», де виявив повідомлення від користувача з ніком «ОСОБА_7» від 28.07.2023 з наступним текстом: «Пробив Украйна, Анкета физ лица - 20$.За 15 минут. Пробив другой информации. Гарант.+». В подальшому, 29.07.2023 о 15:02 год. ОСОБА_6, перебуваючи під контролем працівників правоохоронного органу за адресою: АДРЕСА_2, здійснив замовлення у ОСОБА_3 – користувача мобільного месенджеру «Телеграм» з ніком «ОСОБА_7», інформацію з інформаційно-телекомунікаційної системи «ІПНП»,

стосовно ОСОБА_8, ІНФОРМАЦІЯ_5, після чого, користувачем мобільного месенджеру «Телеграм» з ніком «ОСОБА_9», який являється «гарантом» групи мобільного месенджеру «Телеграм» під назвою «ІНФОРМАЦІЯ_2», було створено мобільний чат під назвою «ІНФОРМАЦІЯ_6», в якому обговорені умови угоди, а саме вартість послуги у сумі 120 (одиниць) «usdt» (назва крипто валюти, що рівноцінно 1 одиниці «usdt» до 1 долара США) та 20 (одиниць) usdt, користувачеві мобільного месенджеру «Телеграм» ніком «ОСОБА_9», за послуги «гаранта», який надав для сплати інтернет гаманець «TCxfXEusobtT2n6juch 5kdnbkeQVk1Xeqz». Після чого, 29.07.2023 о 17:21 год. перебуваючи за адресою: вул. Залізничне шосе, 9 в м. Києві, ОСОБА_6,здійснив зарахування 140 (одиниць) «usdt» на інтернет гаманець TCxfXEusobtT2n6juch5kdnbkeQVk1Xeqz.

Таблиця 3.11 – Порядок криміналістичного дослідження кіберзлочину передбаченого ч.2 ст. 361-2 Кримінального кодексу України

Категорія та тип інциденту	Кіберзлочин	Докази, які необхідно здобути (згідно ознак за формулою 2.16)	Інструменти	Примітки до використання інструменту
категорія інциденту – 07. Порушення властивостей інформації (Information Content Security); тип інциденту – 01. Несанкціонований доступ до інформації (Unauthorised access to information)	ч. 2 ст. 361-2 КК України	характеристики ЕОТ (зокрема комп'ютера та інші засоби електронної комунікації), які забезпечили злочинцю роботу в захищеній ІТС, дані такого несанкціонованого втручання	Програмний засіб *Belkasoft Evidence Center*	Переваги програми Belkasoft Evidence Center такі: - широкий спектр даних із різних носіїв інформації; - вмонтований переглядач баз даних SQLite; - збір даних із віддалених комп'ютерів і серверів; - інтегрований функціонал щодо перевірки виявлених файлів на Virustotal.
		характеристика IP-телефонії (злочинної групи)		
		характеристика ЕОТ, який забезпечив роботу в месенджері «Telegram», дані такої роботи (кожного із злочинної групи осіб)		
		характеристика банківських карток (кожного із злочинної групи осіб), дані проведених операцій		
		характеристика електронного гаманця електронних платежів usdt, та дані проведених операцій		

Із Вироку Турійського районного суду Волинської області від 22.11.2023 року у справі № 169/877/23 щодо засудженої ОСОБА_3 у вчиненні кримінальних правопорушень передбачених ч. 3 ст. 362, ч.1 ч.2 ст.332 КК України, стає відомо: ОСОБА_3 будучи фізичною особою підприємцем, яка має ліцензію на міжнародні перевезення вантажів вантажними автомобілями (крім перевезення небезпечних вантажів та небезпечних відходів), та, маючи персональний доступ до електронного кабінету перевізника Єдиного комплексу інформаційних систем (системи «Шлях»), адміністратором якої є Державна служба України з безпеки на транспорті, вчинила несанкціоновану зміну інформації, яка оброблюється у вказаній системі за наступних обставин. Так, 10.07.2022, точного часу в ході досудового розслідування не встановлено, ОСОБА_3, перебуваючи по місцю свого проживання за адресою: АДРЕСА_1, діючи умисно, за попередньою з мовою з особою, відносно якого матеріали досудового розслідування виділено в окреме провадження, у порушення вимог ст. 9 Закону України «Про ліцензування видів господарської діяльності» № 222-VIII від 02.03.2015, п. п. 9, 10, 16, 20, 27, 33 Ліцензійних умов провадження господарської діяльності з перевезення пасажирів, небезпечних вантажів та небезпечних відходів автомобільним транспортом, міжнародних перевезень пасажирів та вантажів автомобільним транспортом, затверджених постановою Кабінету Міністрів України від 02.12.2015 № 1001,усвідомлюючи суспільно небезпечний характер своїх дій, керуючись метою незаконного переправлення ОСОБА_6 через державний кордон України, достовірно знаючи, що останній не перебуває з нею у трудових відносинах як водій, використовуючи належний їй ноутбук марки «ASUS» серійний номер F4N0CV45624416D та кваліфікований сертифікат особистого ключа, внесла отримані від останнього його особисті дані до Єдиного комплексу інформаційних систем (системи «Шлях») як водія належного їй транспортного засобу «RENAULT MASTER», реєстраційний номер НОМЕР_1, для перетину державного кордону України через пункт пропуску «Угринів», чим доповнила дійсну інформацію неправдивими даними та, як наслідок вчинила,

несанкціоновану зміну інформації, яка оброблюється в автоматизованих системах. (**Судом встановлено що такі дії ОСОБА_3 вчинила повторно за попередньою змовою, а тому дії ОСОБА_3 правильно кваліфіковані: за ч. 3 ст. 362 КК України, тобто несанкціоновані зміни інформації, яка оброблюється в автоматизованих системах, вчиненої особою, яка має право доступу до неї, за попередньою змовою групою осіб*).

Таблиця 3.12 – Порядок криміналістичного дослідження кіберзлочину передбаченого ч.3 ст. 362 Кримінального кодексу України

Категорія та тип інциденту	Кіберзлочин	Докази, які необхідно здобути (згідно ознак за формулою 2.17)	Інструменти	Примітки до використання інструменту
категорія інциденту – 07. Порушення властивостей інформації (Information Content Security); тип інциденту – 02. Несанкціонована модифікація (Unauthorised modification of info)	ч. 3 ст. 362 КК України	характеристики ЕОТ (зокрема ноутбук та інші засоби електронної комунікації), які забезпечили злочинцю роботу в захищеній ІТС Шлях, дані такого несанкціонованого втручання	Програмний засіб *Belkasoft Evidence Center*	Переваги програми Belkasoft Evidence Center такі: - широкий спектр даних із різних носіїв інформації; - вмонтований переглядач баз даних SQLite; - збір даних із віддалених комп'ютерів і серверів; - інтегрований функціонал щодо перевірки виявлених файлів на Virustotal.
		характеристика IP-телефонії (злочинної групи)		
		характеристика банківських карток (кожного із злочинної групи осіб), дані проведених операцій		

Із ухвали Київського апеляційного суду від 30.10.2023 року у справі №761/32185/23 стає відомо: як вбачається з наданих апеляційному суду матеріалів, що Головним підрозділом детективів Бюро економічної безпеки України здійснюється досудове розслідування у кримінальному провадженні №42023000000000193, що внесене до Єдиного реєстру досудових розслідувань 09 лютого 2023 року, за ознаками вчинення кримінальних правопорушень, передбачених ч. 5 ст. 191, ст. 363 КК України. Підставою внесення відомостей до Єдиного реєстру досудових розслідувань стали матеріали та відомості

працівників ВПК в Київській області Департаменту кіберполіції (міжрегіональний територіальний орган)Національної поліції України. Відповідно до вказаних матеріалів встановлено, що невстановлені службові особи за попередньою змовою між собою в 2022 році заволоділи бюджетними коштами шляхом зловживання службовим становищем, в особливо великих розмірах, при виконанні умов договорів щодо закупівлі серверів (комплекси для зберігання даних систем технологічного відеоспостереження для філій та апарату управління ПрАТ «Укргідроенерго» та програмної продукції для забезпечення кібербезпеки ПрАТ «Укргідроенерго» та в порушення порядку правил захисту інформації, яка в них оброблюється, при експлуатації серверів (комплексів для зберігання даних систем технологічного відеоспостереження для філій та апарату управління ПрАТ «Укргідроенерго»), а також програмної продукції для забезпечення кібербезпеки, заподіяли значну шкоду ПрАТ «Укргідроенерго» вчинені особою, яка відповідає за їх експлуатацію.

Таблиця 3.13 – Порядок криміналістичного дослідження кіберзлочину передбаченого ст. 363 Кримінального кодексу України

Категорія та тип інциденту	Кіберзлочин	Докази, які необхідно здобути (згідно ознак за формулою 2.18)	Інструменти	Примітки до використання інструменту
категорія інциденту – 06. Порушення доступності (Availability); тип інциденту – 02. Саботаж / шкідливі дії (Sabotage)	ст. 363 КК України	характеристики ЕОТ (зокрема сервери та інші засоби електронної комунікації), при експлуатації яких відбулося порушення правил експлуатації, порядок або правила захисту інформації	Програмний засіб *Мобільний криміналіст*	- інтегровані переглядачі баз даних *SQLite* і *plist-файлів* дозволяють більш досконально досліджувати певні SQLite-бази даних і plist-файли вручну; - особливістю програми є жорстка прив'язка шляхів, за якими розташовані файли – бази даних додатків
		характеристика IP-телефонії (злочинної групи)		
		характеристика банківських карток (кожного із злочинної групи осіб), дані проведених операцій		

Висновки до 3 розділу

З’ясовано, що процес розслідування кіберзлочинів обумовлений, в першу чергу, необхідністю використання спеціальних знань, засобів, методів збирання та дослідження електронних (цифрових) слідів, що утворюються безпосередньо в ЕОМ та їх системах, на носіях інформації, в кіберпросторі. При розслідуванні кіберзлочинів спеціальні знання використовуються шляхом: 1) комунікації із спеціалістами, експертами; 2) проведення судових експертиз; 3) проведення тематичних консультацій; 4) допиту спеціалістів (експертів) як свідків (у випадках передбачених законом).

Досліджено, що в пунктах 13 та 14 Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень (затверджених наказом Міністерства юстиції України від 08.10.1998 № 53/5) визначено такі два види експертиз. Надано сутнісні ознаки комп’ютерно-технічної та телекомунікаційної експертизи.

Доведено, що причинами які впливають на проведення експертизи при розслідуванні кіберзлочинів є: об’єктивні причини (особливості слідів електронно-обчислювальних машин, комп’ютерних мереж і мереж електрозв’язку, які обумовлюють складність процесу розслідування); суб’єктивні причини (у відповідних суб’єктів відсутні належні знання, навички та вміння в сфері комп’ютерних наук щодо усвідомлення сутності кіберпростору та його особливостей). Надано критерії оцінки та використання результатів судових експертиз при розслідуванні кіберзлочинів спеціально уповноваженими суб’єктами.

Проведено експериментальне дослідження найпоширеніших кіберзлочинів із застосуванням міждисциплінарного та трансдисциплінарного підходу (задля покращення процесу комунікації між суб’єктами уповноваженими розслідувати кіберзлочини та спеціалістами (експертами) в сфері комп’ютерної техніки та програмних продуктів).

4 ЕКОНОМІЧНА ЧАСТИНА

4.1. Проведення наукового аудиту науково-дослідної роботи

Науковий ефект НДР метою якої є розробка науково-обґрунтованих рекомендацій щодо криміналістичного забезпечення розслідування кіберзлочинів можна охарактеризувати двома показниками: ступенем наукової новизни та рівнем теоретичного опрацювання.

Значення показників ступеня новизни науково-дослідної роботи в балах конкретно для нашого випадку наведено в табл. 4.1.

Таблиця 4.1 – Показники ступеня новизни науково-дослідної роботи [39]

Ступінь новизни	Характеристика ступеня новизни	Значення показника ступеня новизни, бали
Принципово нова	Робота якісно нова за постановкою задачі і ґрунтується на застосуванні оригінальних методів дослідження. Результати дослідження відкривають новий напрям в цій галузі науки і техніки. Отримано принципово нові факти, закономірності; розроблено нову теорію. Створено принципово новий пристрій, спосіб, метод	60…100
Нова	Отримано нову інформацію, яка суттєво зменшує невизначеність наявних значень (по-новому або вперше пояснено відомі факти, закономірності, впроваджено нові поняття, розкрито структуру змісту). Проведено суттєве вдосконалення, доповнення і уточнення раніше досягнутих результатів	40…60
Відносно нова	Робота має елементи новизни в постановці задачі і методах дослідження. Результати дослідження систематизують і узагальнюють наявну інформацію, визначають шляхи подальших досліджень; вперше знайдено зв’язок (або знайдено новий зв’язок) між явищами. В принципі, відомі положення поширено на велику кількість об’єктів, в результаті чого знайдено ефективне рішення. Розроблено більш прості способи для досягнення відомих результатів. Проведено часткову раціональну модифікацію (з ознаками новизни)	10…40
Традиційна	Робота виконана за традиційною методикою. Результати дослідження мають інформаційний характер. Підтверджено або поставлено під сумнів відомі факти та твердження, які потребують перевірки. Знайдено новий варіант рішення, який не дає суттєвих переваг порівняно з існуючим	2…10
Не нова	Отримано результат, який раніше зафіксований в інформаційному полі та не був відомий авторам	1…2

За даними таблиці 4.1 ступінь новизни науково-дослідної роботи складає $k_{нов}$ = 50 балів.

Значення показників рівня теоретичного опрацювання науково-дослідної роботи в балах конкретно для нашого випадку наведено в табл. 4.2.

Таблиця 4.2 – Показники рівня теоретичного опрацювання науково-дослідної роботи [39]

Характеристика рівня теоретичного опрацювання	Значення показника рівня теоретичного опрацювання, бали
Відкриття закону, розробка теорії	80…100
Глибоке опрацювання проблеми: багатоаспектний аналіз зв'язків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу	60…80
Розробка способу (алгоритму, програми), пристрою, отримання нової речовини	20…60
Елементарний аналіз зв'язків між фактами та наявною гіпотезою, класифікація, практичні рекомендації для окремого випадку тощо	6…20
Опис окремих елементарних фактів, викладення досвіду, результатів спостережень, вимірювань тощо	1…5

За даними таблиці 4.2. ступінь новизни науково-дослідної роботи складає $k_{теор}$ = 70 балів.

Показник, який характеризує науковий ефект, визначається за виразом:

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор}, \qquad (4.1)$$

де $k_{нов}$, $k_{теор}$ – показники ступенів новизни та рівня теоретичного опрацювання науково-дослідної роботи, бали;

0,6 та 0,4 – питома вага (значимість) показників ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи.

$$E_{нау} = 0,6 \cdot 50 + 0,4 \cdot 70 = 58$$

Отримані значення порівнюємо з граничними, які наведені в таблиці 4.3.

Таблиця 4.3 – Граничні значення показника наукового ефекту

Досягнутий рівень показника	Кількість балів
Високий	70…100
Середній	50…69
Достатній	15…49
Низький (помилкові дослідження)	1…14

Встановивши рівень наукового ефекту проведеної науково-дослідної роботи, який є середнім, можна сказати, що розробка та її впровадження є актуальним в теперішній час.

4.2 Прогнозування витрат на виконання науково-дослідної роботи

Витрати, пов’язані з проведенням науково-дослідної роботи групуються за такими статтями: витрати на оплату праці, витрати на матеріали, паливо та енергія для науково-виробничих цілей, амортизація, накладні витрати тощо.

1. Основна заробітна плата кожного із дослідників $З_О$, якщо вони працюють в наукових установах бюджетної сфери визначається за формулою:

$$З_0 = \frac{М}{Т_р} * t \text{ (грн)} \quad (4.2)$$

де M – місячний посадовий оклад конкретного розробника (інженера, дослідника, науковця тощо), грн.;

T_P – число робочих днів в місяці; приблизно $T_P \approx 21...23$ дні;

t – число робочих днів роботи дослідника.

Для розробки науково-обгрунтованих рекомендацій щодо криміналістичного забезпечення розслідування кіберзлочинів було залучено наукового керівника роботи. Витрати на заробітну плату керівника складають:

$$З_О = \frac{20000}{21} * 5 = 4761,9$$

2. Нарахування на заробітну плату $Н_{ЗП}$ дослідників та робітників, які брали участь у виконанні даного етапу роботи, розраховуються за формулою (4.3):

$$Н_{ЗП} = (З_о + З_р + З_д) * \frac{\beta}{100} \text{ (грн)} \quad (4.3)$$

де $З_о$ – основна заробітна плата розробників, грн.;

$З_д$ – додаткова заробітна плата всіх розробників та робітників, грн.;

$З_р$ – основну заробітну плату робітників, грн.;

β – ставка єдиного внеску на загальнообов'язкове державне соціальне страхування, % .

Дана діяльність відноситься до бюджетної сфери, тому ставка єдиного внеску на загальнообов'язкове державне соціальне страхування буде складати 22%, тоді**:**

$$Н_{ЗП} = (4761,9) * \frac{22}{100} = 1047,62 \text{(грн)}$$

3. Сировина та матеріали.

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби й предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за прямим призначенням згідно з нормами їх витрачання, а також витрачені придбані напівфабрикати, що підлягають монтажу або виготовленню й додатковій обробці в цій організації, чи дослідні зразки, що виготовляються виробниками за документацією наукової організації.

Витрати на матеріали (М) у вартісному вираженні розраховуються окремо для кожного виду матеріалів за формулою:

$$М = \sum_{i=1}^{n} H_j \cdot Ц_j \cdot К_j - \sum_{i=1}^{n} В_j \cdot Ц_{вj}, \quad (4.4)$$

де Нj – норма витрат матеріалу j-го найменування, кг;

n – кількість видів матеріалів;

Цj – вартість матеріалу j-го найменування, грн/кг;

Кj – коефіцієнт транспортних витрат, (Кj = 1,1 … 1,15);

Вj – маса відходів j-го найменування, кг;

Цвj – вартість відходів j-го найменування, грн/кг.

Проведені розрахунки зведені в таблицю 4.4.

Таблиця 4.4 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна, грн	Норма витрат, шт	Вартість витраченого матеріалу, грн
Папір	180	1	180
Ручка	20	1	20
Картридж	450	1	450
Всього			650

4. Амортизація обладнання, комп’ютерів та приміщень, які використовувались під час виконання даного етапу роботи

Дані відрахування розраховують по кожному виду обладнання, приміщенням тощо.

$$A = \frac{Ц \cdot T}{Tкор \cdot 12} \quad [грн], \quad (4.5)$$

де Ц – балансова вартість даного виду обладнання (приміщень), грн.;

$Т_{кор}$ – час користування;

Т – термін використанн яобладнання (приміщень), цілі місяці.

Згідно пункта 137.3.3 Податкового кодекса амортизація нараховується на основні засоби вартістю понад 2500 грн. В нашому випадку для написання

магістерської роботи використовувався персональний комп'ютер вартістю 20000 грн.

$$\text{А} = \frac{20000 \cdot 1}{2 \cdot 12} = 833{,}33$$

5. До статті «Паливо та енергія для науково-виробничих цілей» відносяться витрати на всі види палива й енергії, що безпосередньо використовуються з технологічною метою на проведення досліджень.

$$\text{В}_\text{е} = \sum_{\text{і}=1}^{n} \frac{W_{yt} \cdot t_i \cdot \text{Ц}_\text{е} \cdot \text{К}_{\text{впі}}}{\eta_\text{і}} \qquad (4.6)$$

де W_{yt} – встановлена потужність обладнання на певному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$\text{Ц}_\text{е}$ – вартість 1 кВт-години електроенергії, грн;

$\text{К}_{\text{впі}}$ – коефіцієнт, що враховує використання потужності, $\text{К}_{\text{впі}} < 1$;

$\eta_\text{і}$ – коефіцієнт корисної дії обладнання, $\eta_\text{і} < 1$.

Для написання магістерської роботи використовується персональний комп'ютер для якого розрахуємо витрати на електроенергію.

$$\text{В}_\text{е} = \frac{0{,}25 \cdot 170 \cdot 7{,}5 \cdot 0{,}5}{0{,}8} = 199{,}21$$

6. Накладні (загальновиробничі) витрати Внзв охоплюють: витрати на управління організацією, оплата службових відряджень, витрати на утримання, ремонт та експлуатацію основних засобів, витрати на опалення, освітлення, водопостачання, охорону праці тощо. Накладні (загальновиробничі) витрати Внзв можна прийняти як (100…150)% від суми основної заробітної плати розробників та робітників, які виконували дану МКНР, тобто:

$$\text{В}_{\text{нзв}} = \left(\text{З}_\text{о} + \text{З}_\text{р}\right) \cdot \frac{\text{Н}_{\text{нзв}}}{100\%}, \qquad (4.7)$$

де $\text{Н}_{\text{нзв}}$ – норма нарахування за статтею «Інші витрати».

$$В_{нзв} = (4761{,}9) \cdot \frac{200}{100\%} = 9523{,}8 \text{ грн}$$

Сума всіх попередніх статей витрат дає витрати, які безпосередньо стосуються даного розділу МКНР

В =4761,9+1047,62+650+833,33+199,21+9523,8=17015,86 грн

Прогнозування загальних втрат ЗВ на виконання та впровадження результатів виконаної МКНР здійснюється за формулою:

$$ЗВ = \frac{В}{\eta}, \qquad (4.8)$$

де η – коефіцієнт, який характеризує стадію виконання даної НДР.

Оскільки, робота знаходиться на стадії науково-дослідних робіт, то коефіцієнт β = 0,1.

Звідси:

$$ЗВ = \frac{17015{,}86}{0{,}1} = 170158{,}6 \text{ грн.}$$

4.3 Оцінювання важливості та наукової значимості науково-дослідної роботи фундаментального чи пошукового характеру

Оцінювання та доведення ефективності виконання науково-дослідної роботи фундаментального чи пошукового характеру є достатньо складним процесом і часто базується на експертних оцінках, тому має вірогідний характер.

В результаті науково-дослідної роботи можна отримати висновки яких доходить експерт у процесі проведення експертизи, які повинні ґрунтуватися на всебічному вивченні наданих слідчим об’єктів із залученням спеціальних знань та необхідного комплексу засобів, методів та методик дослідження.

Для обґрунтування доцільності виконання науково-дослідної роботи використовується спеціальний комплексний показник, що враховує важливість,

результативність роботи, можливість впровадження її результатів у виробництво, величину витрат на роботу.

Комплексний показник K_P рівня науково-дослідної роботи може бути розрахований за формулою:

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t}, \qquad (4.9)$$

де I – коефіцієнт важливості роботи, $I = 2...5$;

n – коефіцієнт використання результатів роботи; $n = 0$, коли результати роботи не будуть використовуватись; $n = 1$, коли результати роботи будуть використовуватись частково; $n = 2$, коли результати роботи будуть використовуватись в дослідно-конструкторських розробках; $n = 3$, коли результати можуть використовуватись навіть без проведення дослідно-конструкторських розробок;

T_C – коефіцієнт складності роботи, $T_C = 1...3$;

R – коефіцієнт результативності роботи; якщо результати роботи плануються вище відомих, то $R = 4$; якщо результати роботи відповідають відомому рівню, то $R = 3$; якщо нижче відомих результатів, то $R = 1$;

B – вартість науково-дослідної роботи, тис. грн;

t – час проведення дослідження, років.

Визначення показників *I, n, T_C, R, B, t* здійснюється експертним шляхом або на основі нормативів.

$$K_P = \frac{2^3 \cdot 2 \cdot 3}{170{,}16 \cdot 0{,}17} = 1{,}66$$

Якщо $K_P > 1$, то науково-дослідну роботу можна вважати ефективною з високим науковим, технічним і економічним рівнем.

Висновки до 4 розділу

Розробка науково-обґрунтованих рекомендацій щодо криміналістичного забезпечення розслідування кіберзлочинів є актуальною в теперішній час, про що свідчить середнє значення показника, який характеризує науковий ефект.

Розраховано витрати на науково-дослідну роботу, які склали 170,16 тис. грн. Комплексний показник рівня науково-дослідної роботи склав 1,66, що свідчить що науково-дослідна робота вважається ефективною з високим науковим, технічним і економічним рівнем.

ВИСНОВКИ

У висновках магістерської роботи представлено підсумки, що узагальнено відображають мету, завдання й наукову новизну дослідження.

1. Проведений аналіз джерел за темою доводить, що кількість кіберінцидентів (кібератак) на державні інформаційні ресурси та об’єкти критичної інформаційної інфраструктури зростає. Насамперед, встановлено істотне зростання щодо розповсюдження шкідливого програмного забезпечення. В 2023 році (серед виявлених ШПЗ) переважають: Snake Keylogger, Agent Tesla, LokiBot, PurpleFox та Formbook. Відтак, в кіберпросторі існують специфічні умови для вчинення кіберзлочинів різних видів, які потребують прогресу в їх дослідженні та розробки нових методів розслідування.

2. Проаналізовані апаратні та програмні засоби для дослідження комп’ютерної техніки та програмних продуктів мають різні спеціальні конфігурації, функції тощо. Водночас, ці засоби мають свої обмеження, які впливають на їх ефективність у виявленні, наприклад, формату, способів та методів створення шкідливого програмного засобу. Це доводить, чому кіберзлочини мають здебільшого латентний характер та є складними для розслідування. Статистика вказує, що рівень латентності кіберзлочинів становить 90-95 відсотків.

3. Типові слідчі ситуації та слідчі версії вказують лише напрямок в розслідуванні, а визначення унікальності кіберзлочину та його ефективне розслідування – обумовлено компетенцією спеціально призначених суб’єктів. Проведений аналіз джерел доводить, що нині в Україні спеціально призначені суб’єкти (слідчі, детективи, прокурори, судді та адвокати) не володіють достатніми знаннями в сфері комп’ютерних наук, і це призводить до неефективного попередження, виявлення та розслідування кіберзлочинів.

4. З’ясовано, що впровадження організаційно-технічної моделі кіберзахисту визначає відповідальність за виконання конкретних завдань

кожного суб'єкта кібербезпеки. Також, при ефективному використанні цієї моделі є можливість сформувати якісну систему ресурсного забезпечення (в тому числі кадрового ресурсу).

5. Досліджено відмінності кіберзлочину від інших кіберінцедентів (кібератак), насамперед: не кожен кіберінцидент містить ознаки кримінального правопорушення; відмінність в суб'єктному складі при виявленні та розслідуванні (дослідженні) кіберінцидентів та кіберзлочинів; існують спеціальні процедури при розслідуванні кіберзлочинів, які обумовлені характером вчиненого правопорушення.

6. Розроблено теоретико-множинні моделі кіберінцидентів та теоретико-множинні моделі ознак кіберзлочинів передбачених статтями 190, 200, 361 – 363[1] Кримінального кодексу України.

7. Надана характеристика підготовчих дій щодо збирання технічних даних на початковому етапі розслідування кіберзлочинів. Розроблена модель розслідування кіберзлочинів (яка складається із чотирьох етапів). Надалі, ця модель представлена в структурних елементах: схема моделі роботи з електронними доказами; схема покрокової моделі розслідування кіберзлочинів.

8. З'ясовано, що процес розслідування кіберзлочинів обумовлений, в першу чергу, необхідністю використання спеціальних знань, засобів, методів збирання та дослідження електронних (цифрових) слідів, що утворюються безпосередньо в ЕОМ та їх системах, на носіях інформації, в кіберпросторі. При розслідуванні кіберзлочинів спеціальні знання використовуються шляхом: 1) комунікації із спеціалістами, експертами; 2) проведення судових експертиз; 3) проведення тематичних консультацій; 4) допиту спеціалістів (експертів) як свідків (у випадках передбачених законом).

9. Досліджено, що в пунктах 13 та 14 Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень (затверджених наказом Міністерства юстиції України від

08.10.1998 № 53/5) визначено два види експертиз. Надано сутнісні ознаки комп'ютерно-технічної та телекомунікаційної експертизи.

10. Доведено, що причинами які впливають на проведення експертизи при розслідуванні кіберзлочинів є: об'єктивні причини (особливості слідів електронно-обчислювальних машин, комп'ютерних мереж і мереж електрозв'язку, які обумовлюють складність процесу розслідування); суб'єктивні причини (у відповідних суб'єктів відсутні належні знання, навички та вміння в сфері комп'ютерних наук щодо усвідомлення сутності кіберпростору та його особливостей). Надано критерії оцінки та використання результатів судових експертиз при розслідуванні кіберзлочинів спеціально уповноваженими суб'єктами.

11. Проведено експериментальне дослідження найпоширеніших кіберзлочинів із застосуванням міждисциплінарного та трансдисциплінарного підходу (задля покращення процесу комунікації між суб'єктами уповноваженими розслідувати кіберзлочини та спеціалістами (експертами) в сфері комп'ютерної техніки та програмних продуктів).

12. Розробка науково-обґрунтованих рекомендацій щодо криміналістичного забезпечення розслідування кіберзлочинів є актуальною в теперішній час, про що свідчить середнє значення показника, який характеризує науковий ефект. Розраховано витрати на науково-дослідну роботу, які склали 170,16 тис. грн. Комплексний показник рівня науково-дослідної роботи склав 1,66, що свідчить що науково-дослідна робота вважається ефективною з високим науковим, технічним і економічним рівнем.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2022: Державна служба спеціального зв'язку та захисту інформації України. Київ. 2022. URL: https://nsarchive.gwu.edu/sites/default/files/documents/rr9q9n-glu5j/2023-01-00-SSCIP-Vulnerability-Detection-System-and-Response-to-Cyber-Incidents-and-Cyber-Attacks-%20via-website.pdf (дата звернення: 08.10.2023)

2. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2023 (Q1): Державна служба спеціального зв'язку та захисту інформації України. Київ. 2023. URL: https://scpc.gov.ua/api/files/a7de388d-14d3-4248-b8be-ada8b5cb0710 (дата звернення: 08.10.2023)

3. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2023 (Q3): Державна служба спеціального зв'язку та захисту інформації України. Київ. 2023. URL: https://scpc.gov.ua/api/files/22c75b41-d1d8-4da6-bd46-fa5489af9c6e (дата звернення: 20.11.2023)

4. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія. Одеса : ТЕС, 2020. 372 с.

5. Хаханов В.И., Чумаченко С.В., Литвинова Е.И., Мищенко А.С., Адамов А.С. Инфраструктура анализа и информационной безопасности киберпространства // Радиоэлектроника и информатика : науч.-техн. журн. 2011. Вып.2. С. 40–60. URL: http://openarchive.nure.ua/handle/document/2210 (дата звернення: 08.10.2023)

6. Pan Jianli , Jain Raj. Architectures for the Future Networks and the Next Generation // Article *in* Computer Communications. №34 (1). January 2011. P.2–42. URL: https://www.researchgate.net/publication/222668747 (дата звернення: 08.09.2023)

7. Clark, David. Characterizing cyberspace: past, present and future // MIT,CSAIL. Version1.2. of March12 2010. URL:https://ecir.mit.edu/sites/default/files/documents/%5BClark%5D%20Characterizing%20Cyberspace-%20Past%2C%20Present%20and%20Future.pdf (дата звернення: 01.10.2023)

8. Karl F. Rauscher, Richard E. Krock, James P. Runyon.Eight ingredients of communications infrastructure : A systematic and comprehensive framework for enhancing network reliability and security// Bell Labs Technical Journal. Vol.11, Issue: 3, Fall 2006. P.73–81. URL: https://ieeexplore.ieee.org/document/6768554 (дата звернення: 08.09.2023)

9. Журба А. І. Особливості предмета доказування у справах про комп'ютерні злочини : дис. ... канд. юрид. наук : 12.00.09. Харків, 2008. 230с.

10. Теплицький Б. Б. Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : дис. ... канд. юрид. наук : 12.00.09. Київ, 2021. 21 с.

11. Волков О. О. Початковий етап розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів : дис. ... канд. юрид. наук : 12.00.09. Дніпро, 2023. 198 с.

12. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : дис... канд. юрид. наук : 12.00.09. Київ, 2005. 221 с.

13. Скригонюк М. І. Криміналістика : підручник. Київ : Атіка, 2005. 496 с.

14. Метелев О.П. Збирання цифрової інформації як окремий спосіб отримання доказів під час кримінального провадження // Правове забезпечення оперативно-службової діяльності: актуальні проблеми та шляхи їх вирішення : матеріали постійно діючого наук.-практ. семінару (м. Харків, 23 трав. 2019 р.) / редкол.: С. О. Гриненко (голов. ред.) та ін. Харків : Право, 2019. Вип. 10. С. 177 – 181.

15. C.A.IN.E. (Computer Aided Investigative Environment). URL : https://www.caine-live.net/ (дата звернення: 08.09.2023)

16. Благута Р. І., Мовчан А. В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 256 с.

17. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 року № 2163-VIII . Відомості ВРУ від 10.11.2017. 2017 р. № 45, стор. 42, стаття 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 08.10.2023)

18. Про затвердження Положення про організаційно-технічну модель кіберзахисту : Постанова Кабінету Міністрів України; Положення від 29.12.2021 № 1426. від 29.12.2021. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF (дата звернення: 08.09.2023)

19. Науково-практичний коментар до Положення про організаційно-технічну модель кіберзахисту (затвердженого постановою Кабінету Міністрів України від 29 грудня 2021 р. № 1426) / Щиголь Ю., Потій О, Семенченко А., Дубов Д., Бакалинський О. та Мялковський Д. URL: https://cip.gov.ua/ua/news/naukovo-praktichnii-komentar-do-polozhennya-pro-organizaciino-tekhnichnu-model-kiberzakhistu-zatverdzhenogo-postanovoyu-kabinetu-ministriv-ukrayini-vid-29-grudnya-2021-r-1426 (дата звернення: 08.09.2023)

20. Субач І.Ю, Кубрак В.О. Модель ідентифікації кіберінцидентів SIEM-системою захисту інформаційно-комунікаційних систе // Кібербезпека: освітня, наука, техніка. №4 (20). 2023. С. 81 – 91.

21. SIEM (Security information and event management). URL: https://uk.wikipedia.org/wiki/SIEM (дата звернення: 08.09.2023)

22. Кулешов М.В. Сутність та зміст розслідування кіберінцидентів та кібератак підрозділами СБ України // Інформація і право. 2019. №2 (29). С. 115-122.

23. Кримінальний процесуальний кодекс України : Закон України, 13.04.2012. № 4651-VI. Голос України від 19.05.2012 . № 90-91. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 01.09.2023)

24. Перелік категорій кіберінцидентів : схвалений Національним координаційним центром кібербезпеки при РНБО України (протокол №18 від 28.10.2021 №16/320/21 дск). URL: https://cert.gov.ua/recommendation/16904 (дата звернення: 08.09.2023)

25. Киричок Р.В. Тест на проникнення як імітаційний підхід до аналізу захищеності корпоративних інформаційних систем // Сучасний захист інформації. 2018. №2 (34). С. 53 – 58.

26. Конвенція про кіберзлочинність : від 23.11.2001р. / Верховна Рада України. Офіційний вісник України від 10.09.2007. №65, стор.107. URL: https://zakon.rada.gov.ua/laws/show/994_575/ (дата звернення: 02.03.2020).

27. Хавронюк М.І. Довідник з Особливої частини Кримінального кодексу України. Київ : Істина, 2004. 504 с.

28. Кримінальний кодекс України : Закон України, 05.04.2001. № 2341-III. Голос України від 19.06.2001. №107. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 01.09.2023)

29. Телекомунікаційні системи та мережі : навчальний посібник для студентів спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» / Укладачі : Микитишин А.Г., Митник М.М., Стухляк П.Д. Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2017. 384 с.

30. Кант Іммануїл. Критика чистого розуму / Пер. з нім. та приміт. І. Бурковського. Київ : Юніверс, 2000. 504 с.

31. ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» // Кіберзлочинність та електронні докази : навч. посібник. Львів : ЛНУ ім. Івана Франка, 2022. С.212 – 278.

32. Кіберзлочинність та електронні докази : навч. посібник. Львів : ЛНУ ім. Івана Франка, 2022. 298 с.

33. Про судову експертизу : Закон України від 25.02.1994 року № 4038-XII. Відомості ВРУ від 12.07.1994, № 28, стаття 232. URL: ttps://zakon.rada.gov.ua/laws/card/4038-12 (дата звернення: 06.10.2023)

34. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : Наказ Мін'юст України від 08.10.1998. № 53/5.

Офіційний вісник України від 03.12.1998. №46. Ст.172. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 08.09.2023)

35. Про затвердження Інструкції про особливості здійснення судово-експертної діяльності атестованими судовими експертами, що не працюють у державних спеціалізованих експертних установах : Наказ Мін'юст України від 12.12.2011. № 3505/5. Офіційний вісник України від 26.12.2011. №98. Ст.134. URL: https://zakon.rada.gov.ua/laws/show/z1431-11#Text (дата звернення: 08.09.2023)

36. Про затвердження Положення про Експертну службу Міністерства внутрішніх справ України : Наказ Міністерства внутрішніх справ України від 03.11.2015 №1343. Офіційний вісник України від 27.11.2015. №92. Ст.342. URL: https://zakon.rada.gov.ua/laws/show/z1390-15#Text (дата звернення: 08.09.2023)

37. Пашнєв Д.В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : автореф. дис. ... канд. юрид. наук : 12.00.09. Харків, 2007. 19 с.

38. Про судову експертизу в кримінальних та цивільних справах: Постанова Пленуму Верховного Суду України № 8 від 30.05.1997 р. (із змінами) URL: https://zakon.rada.gov.ua/laws/show/v0008700-97#Text (дата звернення: 06.10.2023)

39. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. Вінниця : ВНТУ, 2021. 42 с.

40. Дудатьєв А., Куперштейн Л., Войтович О. Інформаційне протиборство: моделі реалізації та оцінювання інформаційних операцій // Кібербезпека: освіта, наука, техніка. 2023. № 4(20). С. 72–80. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/468 (дата звернення: 08.10.2023)

41. Майданевич Л. Діалектичний аналіз кіберзлочинів // Інформаційні технології та комп'ютерна інженерія. Молодь в науці: дослідження, проблеми, перспективи (МН-2024). URL: https://conferences.vntu.edu.ua /index.php/mn/mn2024/paper/view/19505

42. Майданевич Л. Кіберпростір: основні аспекти // Інформаційні технології та комп'ютерна інженерія. 2023.черв.18. URL: https://conferences.vntu.edu. ua/index.php/mn/mn2023/author/submission/18743

43. Можаєв М.О. Моделі та методи синтезу спеціалізованої комп'ютерної системи для забезпечення судово-експертної діяльності : дис. ... д-ра техн. наук : 05.13.05. Черкаси. 2021. 324 с.

Додаток А

ПРОТОКОЛ ПЕРЕВІРКИ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Модель криміналістичного розслідування кіберзлочинів
Автор роботи: Майданевич Леонід Олександрович
Тип роботи: магістерська кваліфікаційна робота

Підрозділ кафедра захисту інформації ФІТКІ
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність – 81,9 %. Схожість – 18,1 %.

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

□ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

□ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку (підпис) Валентина КАПЛУН

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи (підпис) Леонід МАЙДАНЕВИЧ

Керівник роботи (підпис) Олеся ВОЙТОВИЧ

Додаток Б
Методичні рекомендації юристам (схеми, алгоритми)

Сутність вчиненого кіберзлочину, найперше, пізнається на межі між правом і технічною сферою. Відтак, для вірного пізнання вчиненого кіберзлочину, спеціально уповноваженим суб'єктам необхідно послуговуватися загальними положеннями про основні види кіберінцидентів (кібератак) (рис.Б.1).

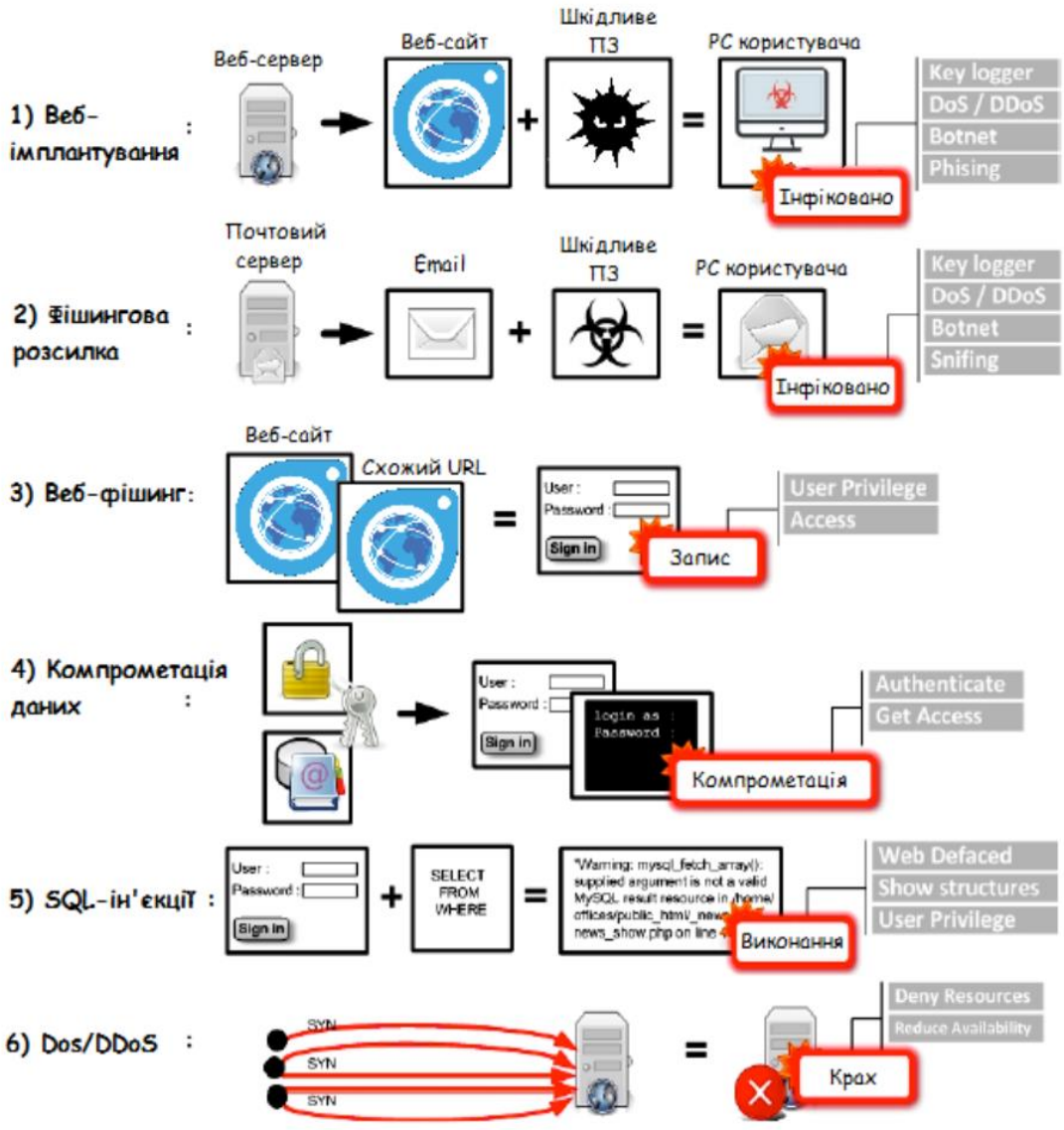


Рисунок Б.1 – Основні види кібернетичних атак [25]

Відповідно до наказу Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ») від 6 грудня 2017 року № 400 «Про прийняття національних нормативних документів, гармонізованих з європейськими та міжнародними нормативними документами, скасування національних нормативних документів, змін до національних нормативних документів» з 1 січня 2019 року в Україні набрав чинності державний стандарт ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» [31].

Рекомендації, що викладені в стандарті, стосуються специфічної діяльності з оброблення потенційних цифрових доказів, а саме процесів: ідентифікації, збирання, здобуття та збереження цифрових доказів. Ці процеси потрібні під час слідства для підтримання цілісності цифрових доказів – прийнятна методологія отримання цифрових доказів, яка буде забезпечувати їхню допустимість у законодавчих та дисциплінарних судових процесах, а також інших потрібних інстанціях.

Цей стандарт надає настанови для таких пристроїв та/або функцій, використовуваних за різних обставин: носій для зберігання цифрових даних, використовуваний у стандартних комп’ютерах, подібний жорстким дискам, гнучким дискам, оптичним і магнітооптичним дискам, цифровим пристроям з подібними функціями; мобільні телефони; персональні цифрові помічники (PDAs); персональні електронні прилади (PEDs); карти пам’яті; мобільні навігаційні системи; цифрові фото- та відеокамери (зокрема CCTV); стандартний комп’ютер з мережевими з’єднаннями; мережі, які ґрунтовані на TCP/IP та інших цифрових протоколах, а також прилади з функціями, подібними до наведених вище (тут вище наведений перелік не є вичерпним).

Відтак, на етапі «виявлення проблеми» та «стадії досудового розслідування», в ході «фіксації електронних доказів» та їх «збирання/здобуття», доречно враховувати вказані нижче алгоритми вказані (див. рис. Б.2 – Б.4).

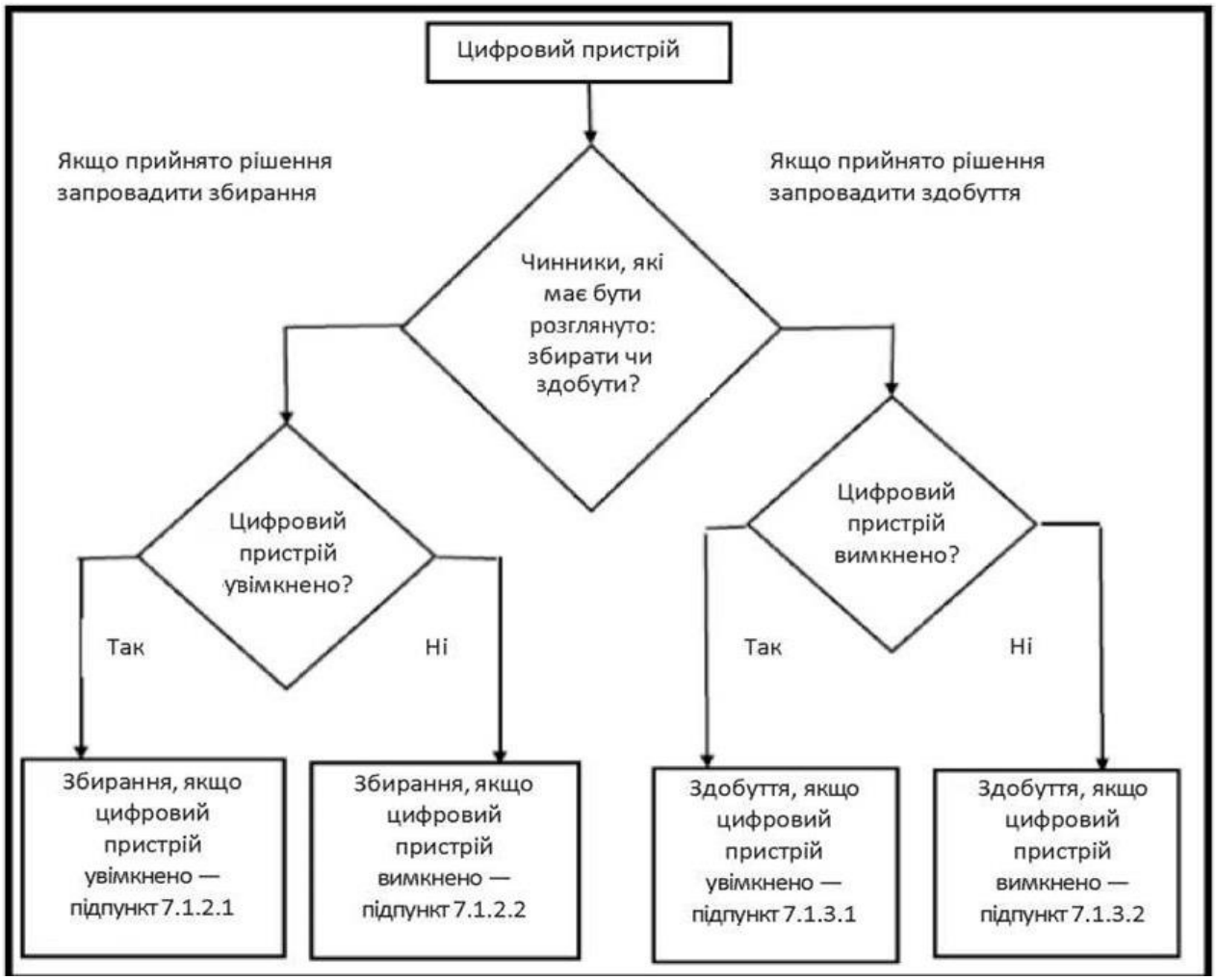


Рисунок Б.2 – Схема процесу прийняття рішення щодо збирання електронних доказів з дотриманням п.7 ДСТУ ISO/IEC 27037:2017 [31]

Під *збиранням* розуміється – процес складання фізичних об’єктів, які містять потенційні цифрові докази.

Під *здобуття* розуміється – процес створення копії даних у межах визначеного набору (результатом здобуття є копія потенційних цифрових доказів).

Також варто враховувати, що електронні (цифрові) докази мають різну доказову силу при розслідуванні конкретного кіберзлочину, а тому: сценарії їх фіксації, збирання (здобуття) можуть передбачати першочергові та інші дії (з дотриманням принципів: *важливості, надійності та достатності*).

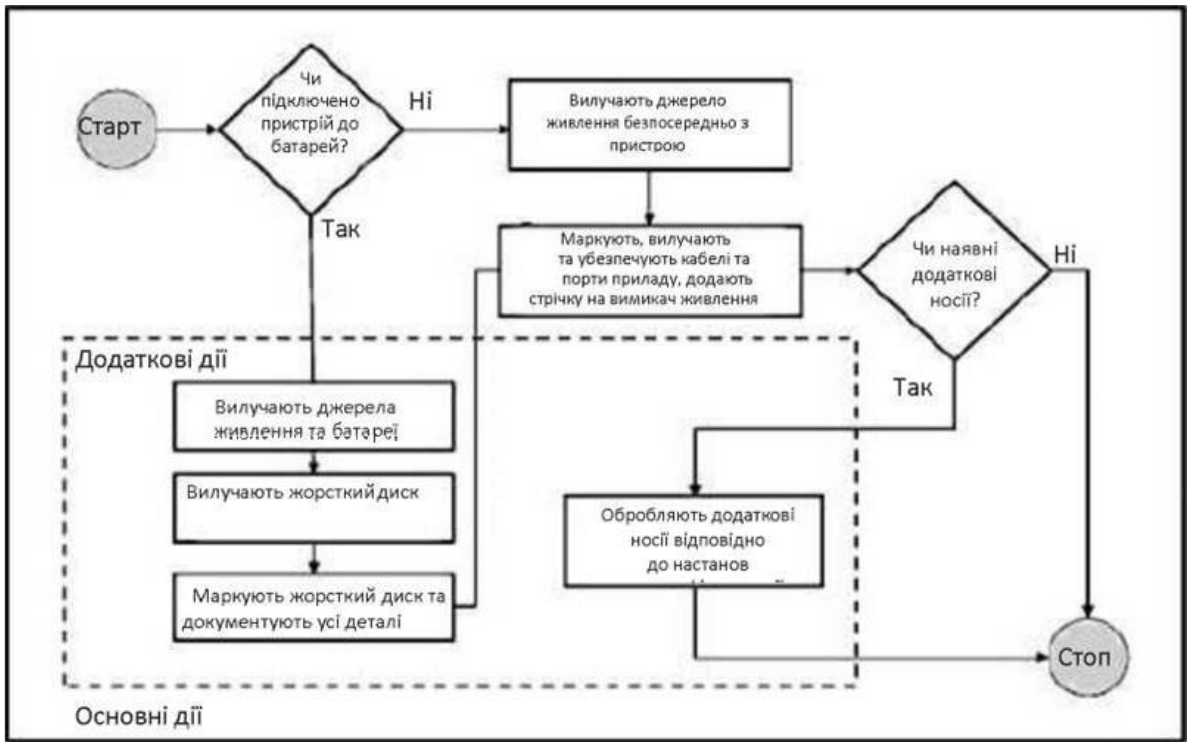


Рисунок Б.3 – Схема збирання доказів на вимкнених цифрових пристроях [31]

Загальні настанови щодо *збирання* доказів на вимкнених цифрових пристроях: важливо вилучити кабель живлення так – з початку вилучити кінець, підключений до цифрового пристрою, а не кінець, підключений до розетки; вилучити та убезпечити всі кабелі від цифрових пристроїв та помістити позначки на портах так, щоб систему можна було відновити пізніше; помістити стрічку на вимикачі живлення, за потреби, для уникнення зміни стану вимикача (упевнитися чи стан вимикача було правильно задокументовано перед тим, як він був закритий стрічкою або відкритий).

Загальні настанови щодо *здобуття* доказів на ввімкнених цифрових пристроях: провести здобуття доказів, які можуть бути потенційно втраченими (якщо цифровий пристрій буде вимкнено зникнуть несталі дані, як мережевих з’єднань, установках дати/часу, статус мережі, декодовані прикладні програми та паролі тощо);

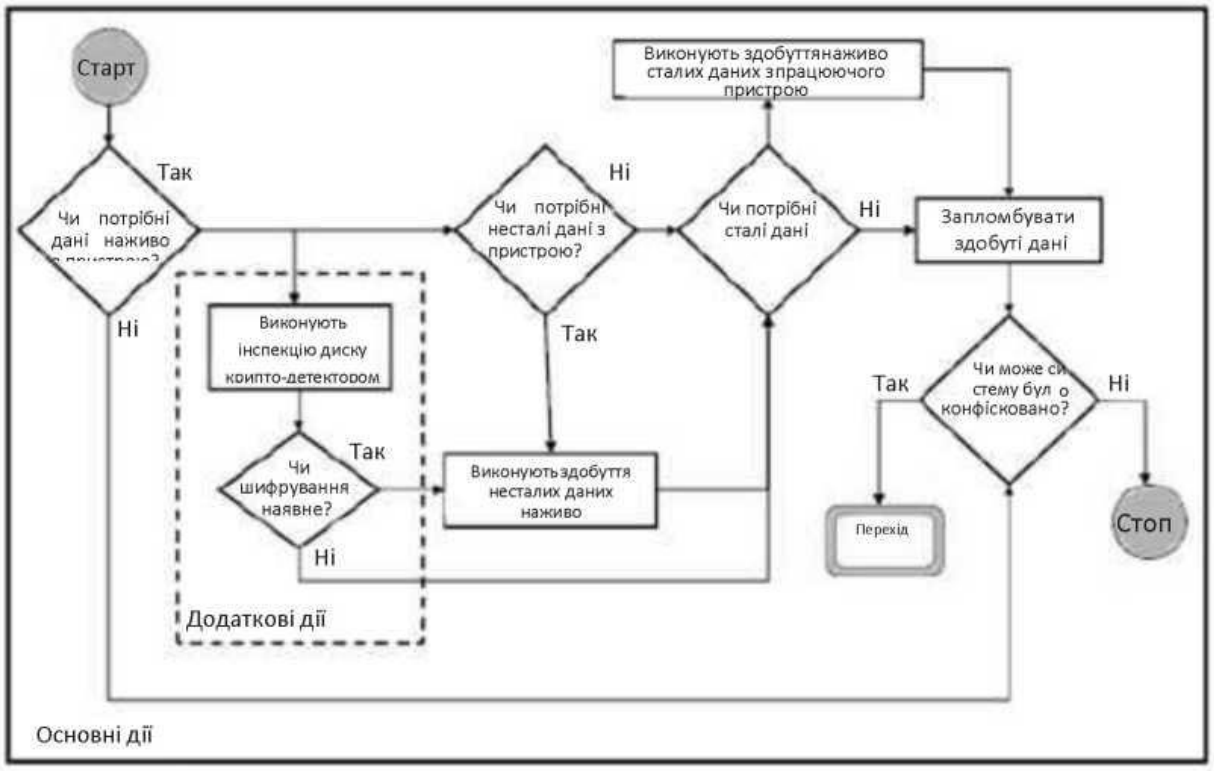


Рисунок Б.4 – Схема здобуття доказів на ввімкнених цифрових пристроях [31]

Отже, дотримання вказаних тут алгоритмів зменшать ризики втрати інформації на етапі фіксації електронних доказів та на етапі їх збирання (див. рис. 2.4 Схеми моделі роботи з електронними доказами при розслідуванні кіберзлочинів в Розділі 2).

А також, дотримання вищевказаних рекомендацій дозволить ефективно використовувати теоретико-множинні моделі ознак кіберзлочинів (формули 2.12 – 2.20, які наведені в Розділі 2), в частині розслідування кіберзлочинів на підставі належних та допустимих доказів (порядком статей 84 – 90 КПК України).

Принагідно тут вказати на відмінність міждисциплінарного та трансдисциплінарного підходів при дослідженні кіберзлочинів: міждисциплінарний підхід обумовлюється такою ситуацією, за якої відбувається перенесення знання з однієї дисциплінарної області в іншу, зі збереженням дисциплінарних поділів (тобто, міждисциплінарність методологічно додатково збагачує те, що визначено у «просторі» дисципліни); трансдисциплінарний

підхід передбачає порушення жорстких дисциплінарних поділів наукового знання, вони стають «прохідними», і це сприяє створенню різного роду систем «поверх-дисциплінарного» поділу, «між-системних» утворень тощо.

Наприклад, трансцендування в комп'ютерній експертизі обумовлює шлях за межі вже відомих даних і конструює алгоритм дослідження електронних (цифрових) доказів задля досягнення мети слідства: всебічного, повного і неупередженого дослідження всіх обставин кіберзлочину. Ситуація трансдисциплінарності в комп'ютерній експертизі передбачає порушення жорстких дисциплінарних поділів наукового знання, що забезпечує створення різних нових систем, які отримують лише відносний статус автономного існування від дисциплінарних поділів наукового знання (в межах криміналістичного розслідування конкретного кіберзлочичну).

Необхідність міждисциплінарних та трансдисциплінарних підходів при дослідженнях кіберзлочинів виникає в тому випадку, коли знання про проблеми мають не чітко визначений характер і конкретна природа обговорюваних проблем є дискусійна (існує визнання принципової складності реальності, яка обумовлюється зануренням різних її рівнів один в одного).

НАЦІОНАЛЬНА АСОЦІАЦІЯ АДВОКАТІВ УКРАЇНИ
РАДА АДВОКАТІВ ВІННИЦЬКОЇ ОБЛАСТІ
вул. Соборна, 53, місто Вінниця, Вінницька область, 21050, Україна

АКТ
ВПРОВАДЖЕННЯ

Рада адвокатів Вінницької області в особі голови Ради ТЕРЕЩЕНКО Ольги Василівни цим актом підтверджує, що результати магістерської кваліфікаційної роботи на тему «МОДЕЛЬ КРИМІНАЛІСТИЧНОГО РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ», яку виконано МАЙДАНЕВИЧЕМ Леонідом Олександровичем (студентом групи 1 БС 22М Вінницького національного технічного університету, за спеціальністю 125 «Кібербезпека», яка виконувалася з 01.09.2023 року по 01.12.2023 року) впроваджено, як методичні рекомендації для адвокатів при розслідуванні кіберзлочинів.

Цей документ не є підставою для фінансових розрахунків.

Голова Ради **О.В.ТЕРЕЩЕНКО**

РАДА АДВОКАТІВ ВІННИЦЬКОЇ ОБЛАСТІ
Ідентифікаційний код
38512163

ІЛЮСТРАТИВНА ЧАСТИНА

Перелік категорій кіберінцидентів

Код хх	Категорія інциденту	Код хх	Тип інциденту	Тип інциденту англійською	Опис типу інциденту
01.	Шкідливий (образливий) вміст (Abusive content)	01	Спам	Spam	Надсилання небажаних повідомлень або великої кількості повідомлень (флуд)
02.	Шкідливий програмний код (Malicious Code)	01	Зараження шкідливим програмним забезпеченням (далі – ШПЗ)	Malware infection	У системі виявлено ШПЗ.
		02	Розповсюдження ШПЗ	Malware distribution	Розповсюдження ШПЗ, наприклад шляхом розсилки повідомлень електронної пошти, що містять вкладення з ШПЗ або посилання на його завантаження
		03	Командно-контрольний центр (C2)	Command & Control (C2)	Система, яка використовується як точка керування та управління ботнетом та/або служить точкою для збору інформації, викраденої ботнетами
		04	Шкідливе підключення	Malicious connection	Спроби з'єднання від/до IP/URL - адреси, пов'язаної з відомим ШПЗ, наприклад C2C або ресурсом розповсюдження компонентів, пов'язаних із активністю певної бот-мережі
03.	Збір інформації зловмисником (Information Gathering)	01	Сканування	Scanning	Збір інформації про системи або мережі
		02	Снiфінг	Sniffing	Несанкціоноване перехоплення (логічне або фізичне) та аналіз мережевого трафіку. Несанкціонований моніторинг та зчитування мережевого трафіку
		03	Фішинг	Phishing	Спроба збору інформації про користувача чи систему за допомогою методів соціальної інженерії (масова розсилка електронною поштою спрямована на збір даних, може містити посилання на фішингові сайти)
04.	Спроби втручання (Intrusion Attempts)	01	Спроба експлуатації вразливості	Vulnerability exploitation attempt	Спроба вторгнення з використанням вразливості у системі, компоненті чи мережі
		02	Спроби авторизації/входу в систему	Login attempts	Спроба входу до служб або механізмів автентифікації / доступу. Невдала спроба підбору автентифікаційних даних чи використання раніше скомпрометованих вже не актуальних даних
05.	Втручання (Intrusion)	01	Компрометація облікового запису	Account compromise	Фактичне вторгнення в систему, компонент або мережу шляхом компрометації облікового запису користувача або адміністратора
		02	Компрометація системи	System compromise	Фактичне вторгнення в систему чи її компоненту, сервісу, застосунку через використання вразливості в компоненті або мережі. Несанкціонований доступ до системи або компоненту в обхід системи контролю доступу
06.	Порушення доступності (Availability)	01	Атака на відмову в обслуговуванні	DoS/DDoS	Вплив на нормальне функціонування системи чи сервісу що досягається направленням з одного чи багатьох джерел до цільового ресурсу запитів для перенасичення пропускної здатності чи системних ресурсів

		02	Саботаж / шкідливі дії	Sabotage	Дії (навмисні або ненавмисні), спрямовані на пошкодження системи, переривання процесів, зміну або видалення інформації тощо
		03	Збій	Outage, no malice	Збій в роботі системи чи її компоненту без зловмисного втручання
07.	Порушення властивостей інформації (Information Content Security)	01	Несанкціонований доступ до інформації	Unauthorised access to information	Несанкціонований доступ до інформації. Несанкціонований обмін конкретним набором інформації
		02	Несанкціонована модифікація	Unauthorised modification of info	Несанкціонована зміна або видалення певного набору інформації.
08.	Шахрайство (Fraud)	01	Шахрайський сайт	Fraudulent site	Створення фішингових сайтів для збору автентифікаційних чи інших даних користувачів. Використання ресурсів установи для цілей, відмінних від передбачуваних
09.	Відома вразливість (Vulnerable)	01	Вразливість	Vulnerability	Наявність в системі чи її компонентах відомих вразливостей, відкритих для експлуатації
		02	Некоректна конфігурація	Misconfiguration	Недоліки в налаштуваннях, що можуть бути використані зловмисником (налаштування за замовчуванням тощо)
10.	Інше (Other)	01	Невизначений інцидент	Undetermined incident	Недостатньо даних для обробки інциденту

Теоретико-множинні моделі категорій кіберінцидендів

$$КТІ = \{ КТІ.01; КТІ.02; КТІ.03; КТІ.04; КТІ.05; КТІ.06; КТІ.07; КТІ.08;; КТІ.09; КТІ.10\}, \quad (2.1)$$

$$КТІ.01 = \{ КТІ.01.01\}, \quad (2.2)$$

$$КТІ.02 = \{ КТІ.02.01; КТІ.02.02; КТІ.02.03; КТІ.02.04\}, \quad (2.3)$$

$$КТІ.03 = \{ КТІ.03.01; КТІ.03.02; КТІ.03.03\}, \quad (2.4)$$

$$КТІ.04 = \{ КТІ.04.01; КТІ.04.02\}, \quad (2.5)$$

$$КТІ.05 = \{ КТІ.05.01; КТІ.05.02\}, \quad (2.6)$$

$$КТІ.06 = \{ КТІ.06.01; КТІ.06.02; КТІ.06.03\}, \quad (2.7)$$

$$КТІ.07 = \{ КТІ.07.01; КТІ.07.02\}, \quad (2.8)$$

$$КТІ.08 = \{ КТІ.08.01\}, \quad (2.9)$$

$$КТІ.09 = \{ КТІ.09.01; КТІ.09.02\}, \quad (2.10)$$

$$КТІ.10 = \{ КТІ.10.01\}, \quad (2.11)$$

Характеристика підготовчих дій на початковому етапі розслідування кіберзлочинів

Вихідні дані	Аналіз процесу	Особливі примітки
історія виникнення проблеми	що, де, коли відомо про проблему	
засоби електронних комунікацій	про які відомо елементи технічної інфраструктури, що забезпечують віртуальне існування проблеми в кіберпросторі (обладнання, пристрої, засоби, вузли, маршрутизатори, мережне обладнання, IMEI/IMSI тощо)	
ситуаційні дані	про які відомо електронні/ віртуальні сліди проблеми (інформація яка має сенс при розслідуванні, наприклад: чи є данні з телефонної книги; про SMS/MMS; чи є дані про надісланні повідомлення; чи є дані з електронної пошти; чи відомо історію відвідування ресурсів в кіберпросторі; чи є дані про геолокацію; чи є видалена інформація тощо)	так, під час огляду гаджета, ноутбука може виникнути необхідність фіксації та збирання інформації про кіберзлочин з дотриманням вимог копіювання та збереження в ході процесуальної дії; збирання інформації може відбуватися, як із дисків, браузерів, чатів, хмар, платіжних систем, журналів тощо.
реєстратор-реєстрант (IP/доменні імена/сайти/сторінки)	способи встановлення власників (офіційних користувачів) IP/доменних імен що в сфері/змісті проблеми	
провайдер	хто провайдер (и) та які послуги провайдера забезпечували (ють) формування/існування проблеми в кіберпросторі	Вид хостингу: віртуальний хостинг; віртуальний сервер; виділений сервер; хмарний хостинг тощо
технічна інфраструктура	яка комунікаційна система обумовлювала (є) проблему	
архітектура протоколів *(попередні висновки)*	які стандарти було порушено при використанні протоколів в сфері/змісті проблеми	топологія мереж та потік даних
програмне забезпечення використані утиліти *(на етапі збору вихідних даних)*	важливо, застосовувати правильні засоби, методи, методологію при копіюванні, дослідженні ЕОМ, накопичувачів, трафіку тощо.	

Модель розслідування кіберзлочинів

Етапи	Сутність процесу	Особливі примітки
Виявлення проблеми	- з'ясування історії виникнення проблеми, ідентифікації/здобуття, фіксація, збирання, та збереження електронних доказів (згідно ознак ситуації); -вирішення питання про залучення консультанта (спеціаліста, експерта в сфері комп'ютерних наук) до моменту внесення відомостей в ЄРДР	Найперше керуються: - рекомендаціями щодо поводження з електронними (цифровими) доказами, які викладені в ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів»; - Переліком категорій кіберінцидентів (*який схвалений НКЦК при РНБО України 28.10.2021; в редакції на час звернення*)
Стадія досудового розслідування	ця стадія має специфічні функції, критерії, задачі: – нормативно визначена процесуальна діяльність; – процесуальну діяльність здійснюють виключно спеціально уповноважені суб'єкти; – коло засобів доказування обмежене; – розслідування має ретроспективний характер; – при розслідуванні, як правило, є протидія у встановленні обставин кіберзлочину.	Найперше керуються: КПК України
Стадія судового провадження	Особливе завдання, яким є вирішення кримінального провадження по суті, тобто питання про винуватість обвинуваченого і про ступінь його відповідальності у випадку визнання винним (з'ясовуючи ці питання, суд здійснює правосуддя, а тому і завдання судового розгляду співпадають, звичайно, із завданнями кримінального судочинства загалом); - коло суб'єктів провадження, до якого окрім суду і вказаних у п.26 ст.3 КПК України учасників судового провадження долучаються свідки, експерти, спеціалісти тощо; - процесуальною формою здійснення судового розгляду є судове засідання, в межах якого, насамперед, допускається вчинення процесуальних дій (особливо тих, що спрямовані на дослідження доказів); - прийняття судового рішення, яке є завершальним не лише для даної стадії, але й для провадження загалом (вироку, ухвали про закриття тощо)	Найперше керуються: КПК України
Узагальнення досвіду (практичного матеріалу)	- проводять врахування досвіду правозастосування (на основі юридичних фактів та конкретних правових норм) та нової інформації про кіберінциденти від суб'єктів забезпечення кібербезпеки; - готують методичні рекомендації для підвищення ефективності розслідування кіберзлочинів	Найперше керуються: відомчими інструкціями

Схема моделі роботи з електронними доказами при розслідуванні кіберзлочинів

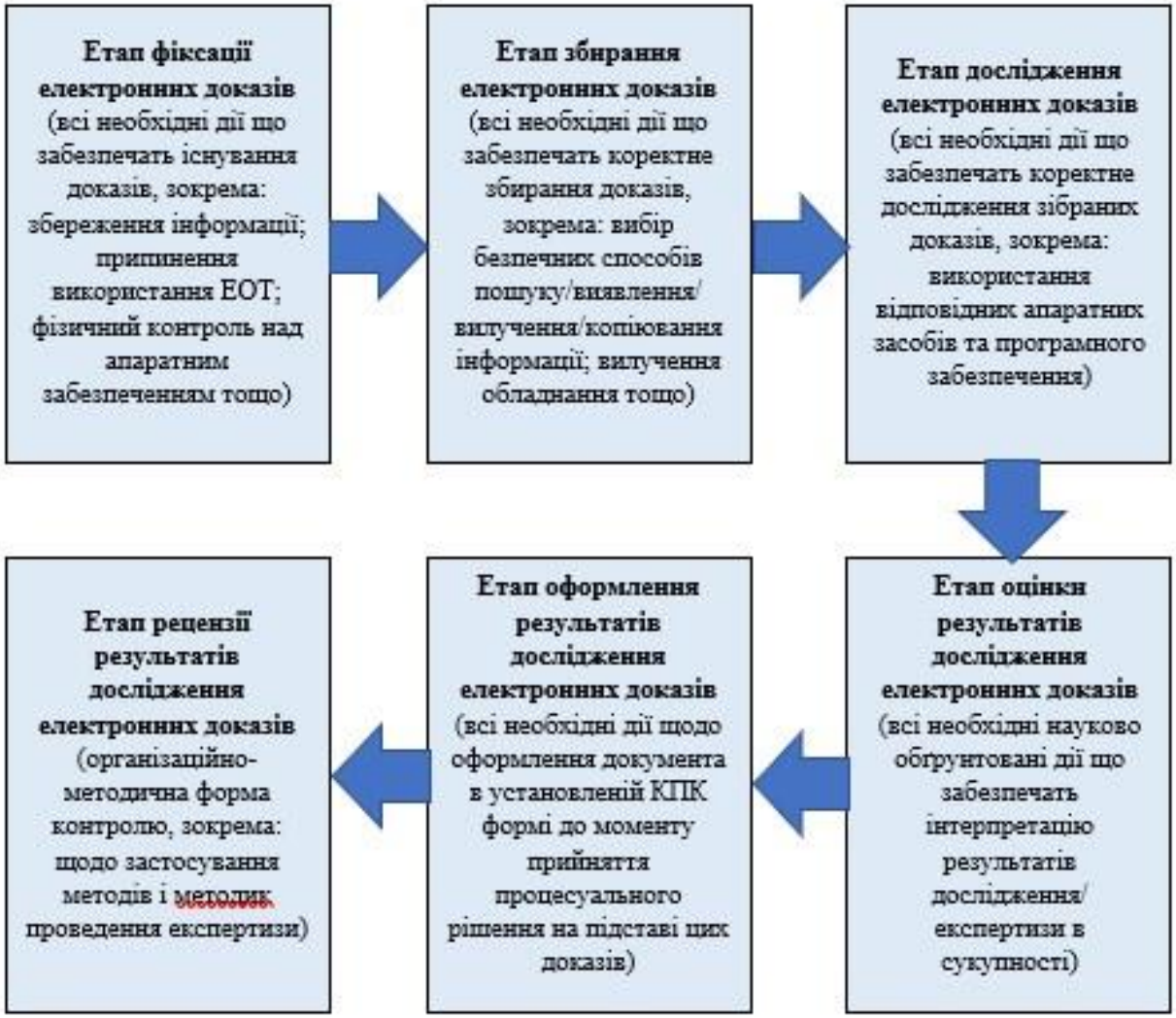
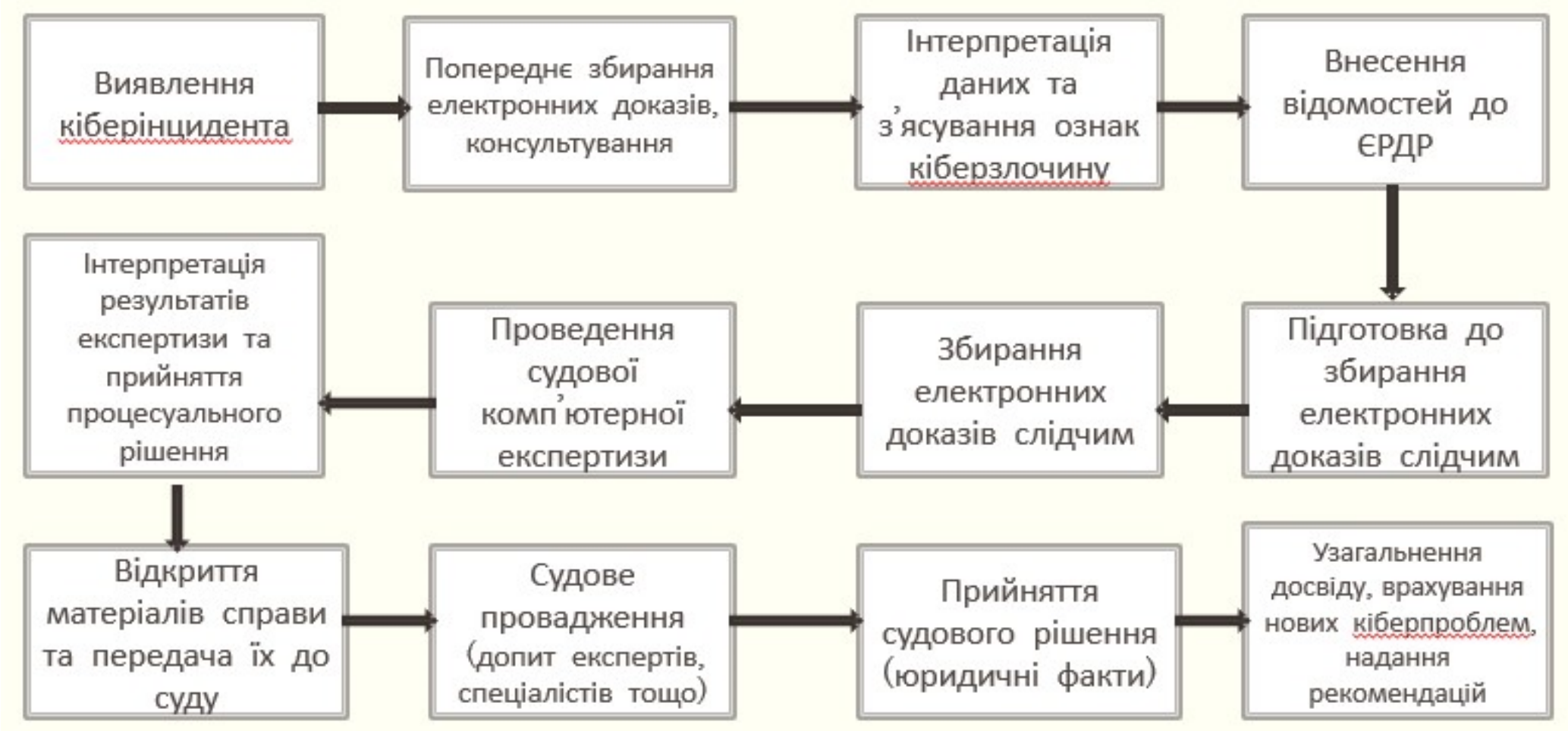


Схема покрокової моделі розслідування кіберзлочинів



Сутнісні ознаки комп'ютерно-технічної та телекомунікаційної експертизи

Експертиза комп'ютерної техніки і програмних продуктів Експертиза телекомунікаційних систем та засобів	1) використання спеціальних знань; 2) проведення дослідження з метою встановлення обставин, які мають значення для провадження; 3) наявність спеціального суб'єкта експертизи; 4) визначену процесуальну форму; 5) оформлення результатів у процесуальному документі – висновку експерта

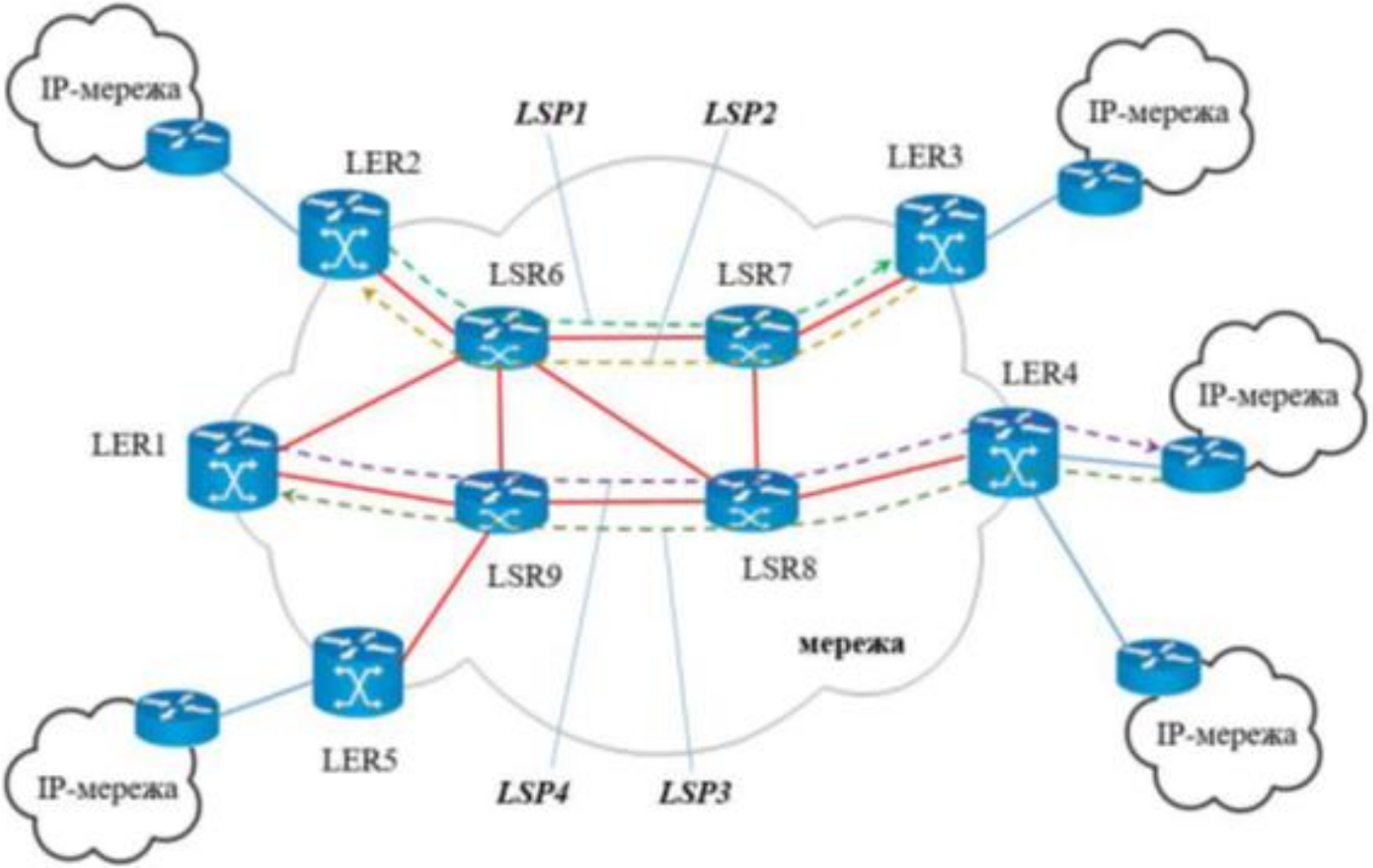
Причини які впливають на проведення експертизи при розслідуванні кіберзлочинів

Об’єктивні причини	особливості слідів ЕОТ, комп’ютерних мереж і мереж електрозв’язку, які обумовлюють складність процесу розслідування
Суб’єктивні причини	відсутні належні знання, навички та вміння в сфері комп’ютерних наук щодо усвідомлення сутності кіберпростору та його особливостей, що стає причиною нецілеспрямованого та неефективного розслідування кіберзлочинів спеціально уповноваженими суб’єктами (найперше, слідчими, прокурорами, суддями)

Критерії оцінки та використання результатів судових експертиз при розслідуванні кіберзлочинів

Вид експертизи	Критерії
Експертиза комп'ютерної техніки і програмних продуктів Експертиза телекомунікаційних систем та засобів	- володільцем інформації повинні бути визначені умови та правила отримання і обробки інформації; - власник (розпорядник) ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи оператор (провайдер) мереж електрозв'язку повинні розробити та впровадити заходи захисту інформації в системі; - власник (розпорядник) комп'ютерів, систем та оператор (провайдер) мереж повинні розробити правила роботи системи; - між власником (оператором, провайдером) системи та володільцем інформації повинен бути укладений договір щодо захисту інформації в системі; - злочинець виконав хоча б одну із операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання інформації

Спрощена схема аналізу контрольних точок (на базі рекурсивних платформ)



Критерії оцінки та використання результатів судових експертиз

спеціально уповноваженими суб'єктами при розслідуванні кіберзлочинів

Спеціально уповноважені суб'єкти	Аспекти оцінки
Слідчі, детективи, прокурори, судді, адвокати	- перевірка достатності наданих для експертизи об'єктів (оскільки недостатня їх кількість, особливо у випадку вирішення ідентифікаційного питання, може стати причиною помилкового висновку чи відмови від його дачі); - якість об'єктів, що визначається відповідністю зразків для експертного дослідження досліджуваним об'єктам, належними способами вилучення, упакування, збереження, транспортування об'єктів експертизи, правильності вихідних даних для експертного дослідження; - перевірка доцільності, правомірності застосованих експертом методики, методів дослідження та оцінку їх наукової обґрунтованості (з цією метою визначається: чи відповідає використана експертом методика поставленим перед ним питанням, чи придатна вона для виявлення необхідних властивостей наданих об'єктів, чи знаходить ця методика застосування в експертній практиці); - перевірка повноти проведених досліджень, встановлення всіх ознак об'єктів судової експертизи (для чого визначається: чи всі процедури і види досліджень стосовно об'єкта виконані згідно з обраною методикою); - перевірка правильності опису та інтерпретації встановлених ознак об'єктів (в даному випадку визначається: чи кожна виявлена в перебігу експертного дослідження ознака детально описана та оцінена експертом, як з точки зору відображення властивостей об'єкта, так і з точки зору його значущості для вирішення поставленого питання); - перевірка наукової обґрунтованості проміжних і підсумкових висновків, що є логічним завершенням оцінки (для цього встановлюється: чи зроблені проміжні висновки за результатами проведених досліджень, чи достатньо виявлених ознак для цих висновків, чи є остаточні висновки наслідком сукупної оцінки проміжних); - визначення фахової компетентності експерта на підставі всебічного аналізу висновку

Приклад криміналістичного дослідження кіберзлочину передбаченого ч.1 ст. 361-1 КК України

Категорія та тип інциденту	Кіберзлочин	Докази, які необхідно здобути (згідно ознак за формулою 2.15)	Інструменти	Примітки до використання інструменту
категорія інциденту – 02. Шкідливий програмний код (Malicious Code); тип інциденту – 02. Розповсюдження ШПЗ (Malware distribution)	ч. 1 ст. 361-1 КК України	характеристики ЕОТ (зокрема персонального комп'ютера «SpiderMan» та інші засоби електронної комунікації), які забезпечили злочинцю роботу на веб-ресурсів тіньової тематики	апаратний блокіратор *Tableau T35U*	дозволяє безпечно підключати досліджувані жорсткі диски до комп'ютера дослідника по шині USB3 (це буває корисним у дослідженні накопичувачів, заражених шкідливим програмним забезпеченням)
		характеристика ШПЗ «brut-force» (характеристика методу пошуку паролів)	Програмний засіб *Belkasoft Evidence Center*	Переваги програми Belkasoft Evidence Center такі: - широкий спектр даних із різних носіїв інформації; - вмонтований переглядач баз даних SQLite; - збір даних із віддалених комп'ютерів і серверів; - інтегрований функціонал щодо перевірки виявлених файлів на Virustotal.
		характеристика IP-телефонії (злочинця),		
		характеристика ЕОТ, який забезпечив роботу в месенджері «Telegram», дані такої роботи		
		характеристика банківських карток (картки злочинця), дані проведених операцій		
		характеристика електронного гаманця електронних платежів Bitcoin, та дані проведених операцій		