Л. Майданевич, О. Войтович, Г. Шелепало

ТЕХНІКО-КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Міністерство освіти і науки України
Вінницький національний технічний університет

Л. Майданевич, О. Войтович, Г. Шелепало

ТЕХНІКО-КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Електронний навчальний посібник

Вінниця
ВНТУ
2025

УДК [343.982.4: 004.946.5.056] (075.8)
М14

Рекомендовано до видання Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 8 від 30.01.2025 р.)

Рецензенти:
О. О. Можаєв, доктор технічних наук, професор
О. О. Кирбят'єв, доктор юридичних наук, професор
В. В. Карпінець, кандидат технічних наук, доцент

Майданевич, Л. О.

М14 Техніко-криміналістичне забезпечення розслідування кіберзлочинів : навчальний посібник [Електронний ресурс] / Майданевич Л. О., Войтович О. П., Шелепало Г. В. – Вінниця : ВНТУ, 2025. – (PDF, 109 с.)
ISBN 978-617-8163-60-0 (PDF)

Навчальний посібник відповідає програмі дисципліни «Техніко-криміналістичне забезпечення розслідування кіберзлочинів» для здобувачів, що навчаються на магістерській програмі за спеціальністю 125 «Кібербезпека та захист інформації» освітньої програми «Безпека інформаційних і комунікаційних систем».

Посібник стане в нагоді здобувачам вищої освіти при вивчені дисципліни, підготовці до іспиту та в практичній діяльності за фахом.

Рекомендується для здобувачів вищої освіти, викладачів, науковців та спеціалістів в сфері кібербезпеки.

УДК [343.982.4: 004.946.5.056] (075.8)

ISBN 978-617-8163-60-0 (PDF)

ЗМІСТ

ВСТУП

Шостий технологічний уклад характеризується стрімким розвитком новітніх технологій, які суттєво впливають на всі аспекти життя, зокрема кібербезпеку та методи розслідування кіберзлочинів. Серед ключових тенденцій слід виділити цифровізацію, роботизацію, прогрес у сфері нано- і біотехнологій, а також впровадження штучного інтелекту. Особливо важливим є розвиток нано- та біотехнологій, які відкривають унікальні можливості, недоступні на попередніх технологічних етапах. Ці досягнення сприяють удосконаленню інформаційно-комунікаційної інфраструктури та суттєво впливають на методи та інструменти криміналістики, що використовуються для розслідування кіберзлочинів.

Зростання складності кіберзлочинів зумовлює потребу вдосконалення криміналістичних методів. Основними напрямами є: цифрова криміналістика, яка забезпечує збирання, аналіз та зберігання цифрових доказів з гарантією їх автентичності; використання машинного навчання для прогнозування кіберзагроз і аналізу поведінкових моделей у кіберпросторі; блокчейн-аналітика, спрямована на дослідження транзакцій у розподілених мережах для виявлення підозрілих операцій; а також розробка нових підходів до захисту даних через шифрування і квантову криптографію, що враховують потенційні ризики використання квантових комп'ютерів для зламу класичних алгоритмів.

Різноманіття апаратних і програмних засобів для обробки інформації в комп'ютерних мережах, їх швидке оновлення та зростання функціональних можливостей, а також використання злочинцями сучасних технологій створюють значні труднощі для працівників правоохоронних органів. Ситуація ускладнюється також недоліками правового, організаційного, тактичного та методичного забезпечення у застосуванні цих технологій у розшуковій та слідчій роботі. Ці тенденції вимагають нових підходів до організації взаємодії кіберполіції та інших поліцейських підрозділів з органами досудового розслідування, особливо під час виконання слідчих доручень. Це також ставить завдання з підготовки фахівців таких підрозділів. Потребує вдосконалення організація та розробка нових методик і тактик для роботи й взаємодії слідчих та оперативних підрозділів, оскільки ефективність їх діяльності значною мірою залежить від оновлення та адаптації методів, які вони використовують.

В посібнику: досліджено апаратні та програмні засоби, що застосовуються для аналізу комп'ютерної техніки та програмного забезпечення; проаналізовано теоретико-множинні моделі кіберінцидентів та ознак кіберзлочинів, передбачених статтями 190, 200, 361–363[1] Кримінального кодексу України; проведено експериментальний аналіз найпоширеніших кіберзлочинів із використанням міждисциплінарного та трансдисциплінарного

підходів, спрямованих на покращення взаємодії між суб'єктами розслідування кіберзлочинів та експертами в галузі інформаційних технологій. Незважаючи на широкі можливості цих інструментів, їх ефективність має обмеження, наприклад: які пов'язані з проблемами визначення формату, методів чи способів створення шкідливого програмного забезпечення та інших факторів.

Цей навчальний посібник спрямований на систематизацію знань і практичних навичок, потрібних для забезпечення ефективного розслідування кіберзлочинів. У ньому розглядаються ключові технікокриміналістичні засоби та методи, що застосовуються для аналізу кіберзагроз, дослідження цифрових слідів, а також організації взаємодії між суб'єктами протидії кіберзлочинності.

Матеріали посібника будуть корисними для здобувачів вищої освіти, викладачів, практикуючих фахівців, а також усіх, хто цікавиться питаннями криміналістики та кібербезпеки. Він покликаний допомогти розвинути навички аналізу цифрових доказів, оцінювання ризиків у кіберпросторі та впровадження інноваційних підходів у протидії злочинності у сфері інформаційних технологій.

РОЗДІЛ 1 КІБЕРПРОСТІР ТА ЗЛОЧИНИ ЯК ОБ'ЄКТ КРИМІНАЛІСТИЧНОГО ДОСЛІДЖЕННЯ

1.1 Кіберзлочинність та її місце в загальній структурі злочинності

Кіберзлочинність стала однією з найсерйозніших загроз для глобальної безпеки у XXI столітті. З розвитком технологій та цифрової інфраструктури, кіберзлочини набувають нових масштабів, що суттєво змінює загальну структуру злочинності. Сьогодні майже всі аспекти життя інтегровані з інформаційними технологіями, що робить кіберпростір ключовим елементом сучасного суспільства.

Збільшення кількості користувачів Інтернету та розширення доступу до мережних технологій створюють нові можливості для злочинців (насамперед, користувачі смартфонами, хмарними сервісами та іншими інформаційними технологіями стають потенційними жертвами кіберзлочинів). Статистика свідчить, що кіберзлочинність зростає швидше, ніж будь-який інший вид злочинності. За даними різних досліджень, фінансові втрати від кіберзлочинності в глобальному масштабі досягли трильйонів доларів, і цей показник продовжує зростати.

Таблиця 1.1 – Соціокультурний портрет «цифрової людини» (за О.Дзьобань, [1])

Ознаки цифрової людини (ЦЛ)	*Примітки*
ЦЛ формується як носій знань та інтерпретатор великого обсягу інформації	- суб'єктивність змісту інформації (залежно від поставленої мети, інформація набуває індивідуального сенсу, стаючи основою для формування знань і стимулом до розвитку); - інформація як ресурс (використовується для реалізації та розвитку розумових здібностей людини); - швидкий доступ до інформації (забезпечується можливість отримувати майже необмежений обсяг інформації за порівняно короткий час)
Для ЦЛ у когнітивній сфері домінує екстенсивність	- пріоритет швидкості над глибиною (у когнітивній сфері зростає значення швидкого сприйняття та обробки інформації, що нерідко відбувається на шкоду її глибокому осмисленню); - поверхневий підхід до знань (знижується

	інтерес до засвоєння фундаментальних основ, натомість перевага надається поверхневому розумінню проблем без критичного аналізу та перевірки досвідом); - розвиток «кліпового» мислення (формується специфічний спосіб мислення, де основний акцент робиться на яскравості та доступності інформації, часто на шкоду її змістовній глибині)
ЦЛ залежна від пристроїв	- передача функцій пам'яті пристроям (зменшується необхідність тренувати оперативну пам'ять, оскільки її функції перекладаються на технічні засоби); - залежність від мобільних пристроїв (мобільні засоби зв'язку стають своєрідним «зовнішнім психічним органом» – у разі їх відсутності людина відчуває себе безпорадною, ніби позбавленою пам'яті та здатності до комунікації)
Становлення ЦЛ відбувається в силу віртуалізації життя	- віртуалізація спілкування (перехід міжособистісних контактів у цифрову площину сприяє спрощенню комунікації, й це створює хибне відчуття легкості й доступності взаємин); - масове переміщення комунікацій в онлайн (більшість форм і способів взаємодії адаптуються до цифрового середовища, стаючи частиною віртуального простору)
ЦЛ є творець нових цінностей, насамперед, моральних	- визначення цільової аудиторії (ідентифікація особи здійснюється через її належність до певного інформаційного, соціального чи віртуального середовища); - онлайн-самопрезентація (людина формує свій образ у мережі за допомогою ніків, аватарів або профілів у соціальних мережах, використовуючи можливості їх творчого оформлення, що приваблює інших користувачів); - зростання соціальних патологій (збільшується кількість проблем, пов'язаних із заздрістю, що виникає через майнову нерівність, різницю в інтелектуальних здібностях та інших аспектах)

Власне, кіберзлочинність охоплює широкий спектр злочинів – від крадіжки особистих даних до атак на критичну інфраструктуру. Зокрема, такі злочини, як кібершахрайство, хакерські атаки, зломи, поширення шкідливого програмного забезпечення та фінансові афери стали буденністю. Ця різноманітність робить кіберзлочини складними для виявлення та розслідування, оскільки вони часто не залишають фізичних доказів і можуть бути вчинені з різних куточків світу.

Кіберзлочинці постійно вдосконалюють свої методи і техніки. Використання штучного інтелекту, машинного навчання, блокчейну та інших сучасних технологій дозволяє створювати нові типи атак, які важко виявити та нейтралізувати. Наприклад, DeepFake технології можуть бути використані для створення фальшивих відео або аудіо, що може призвести до маніпуляцій, шантажу чи навіть політичних криз, а використання анонімайзерів, VPN-сервісів та технологій шифрування ускладнює ідентифікацію злочинців. Також кіберзлочинці можуть використовувати для приховування своєї діяльності посередників (ботнети), що значно ускладнює їх виявлення та притягнення до відповідальності.

Кіберпростір забезпечує високий рівень анонімності, що дозволяє кіберзлочинцям залишатися невловимими протягом тривалого часу. Ця обставина доводить – кіберзлочинність часто має транснаціональний характер, і це робить більш складною боротьбу з нею на рівні окремої держави. Насамперед, через необхідність обміну інформацією, спільних розслідувань і координації дій, що є важливим елементом у протидії таким злочинам.

Однак багато країн не завжди готові оперативно співпрацювати через політичні або правові обмеження. Тобто, незважаючи на децентралізованість, кіберпростір підлягає правовому регулюванню на національному та міжнародному рівнях, хоча і має свої труднощі у створенні єдиних правил через глобальність. Це передбачає наявність міжнародних угод та національних законів для забезпечення прав, боротьби з кіберзлочинністю та захисту даних.

Окрім цього, до проблем у боротьбі з кіберзлочинністю варто віднести й відсутність універсальної правової бази, яка б регулювала ці злочини на глобальному рівні. Кожна держава має власні законодавчі акти, що визначають підхід до боротьби з кіберзлочинністю. Відсутність єдиного стандарту ускладнює міжнародну співпрацю, особливо коли йдеться про розслідування злочинів, вчинених у різних юрисдикціях. Наприклад, злочин може бути вчинений з однієї країни, але вплинути на інші, що створює проблеми у сфері екстрадиції та юрисдикції.

Боротьба з кіберзлочинністю вимагає не лише вдосконалених технічних засобів, але й висококваліфікованих фахівців у сфері кібербезпеки. Нажаль, нині наявний дефіцит кадрів (що мають потрібні навички та досвід) – і це є однією з найбільших проблем для багатьох країн. Багато дер-

жавних органів та приватних компаній не мають достатніх ресурсів для належного захисту своїх мереж та даних, що робить їх вразливими до атак.

Таблиця 1.2 – Аксіоматичне співвідношення систем

Аксіоматика комплексної безпеки соціотехнічних систем (за А. Дудатьєвим [2])	Аксіоматика правопорядку (як соціотехнічної системи)	Аксіоматика злочинності (як незаконної соціотехнічної системи)	Аксіоматика кіберзлочинності (як елемент незаконної соціотехнічної системи)	Примітки
Аксіома 1. *На етапі постановки задачі* рівень безпеки визначається елементами системи, зв'язками між елементами, а також умовами експлуатації майбутньої системи і не може бути меншим допустимого рівня	Сутністю вихідних положень та елементів, що зумовлюють орієнтири безпеки правової системи є: верховенство права; захист прав і свобод людини; рівність перед законом; справедливість; підзвітність та відповідальність; стабільність та адаптивність; дотримання міжнародних стандартів; ефективність; передбачуваність та доступність; підтримання публічного порядку	Сутністю вихідних положень, що зумовлюють орієнтири злочинної системи, є: принципи та закономірності, що пояснюють внутрішню логіку та правила, за якими функціонує злочинне середовище (наприклад, функціонують завдяки співпраці, конспірації та доступу до тіньових ресурсів)	Сутністю вихідних положень, що зумовлюють безпеку системи кіберзлочинності, є: специфічне використання інформаційного ресурсу; можливостей та змін в кіберпросторі	Кіберзлочинці адаптуються до нових технологій, змін в інформаційних ресурсах тощо, постійно вдосконалюючи свої методи і способи
Аксіома 2. *На етапі проєктування* рівень безпеки забезпечується тривіальними методами, засобами та заходами з урахуванням умов експлуа-	Виконання проєктування правової системи та її рівень безпеки забезпечується методами, принципами, механізмами та інституційною структурою, які	Виконання проєктування злочинної системи та її рівень безпеки забезпечується «програмою», яка передбачає відповіді на питання: люди (хто?);	Виконання проєктування злочинної кіберсистеми та її рівень безпеки забезпечується: принципами захисту даних; функціональними можливос-	Можна умовно визначити два типи кібезлочинів: злочини, які повністю базуються на інформаційних технологіях (тобто, неможливі без ІТ); та

тації, які забезпечують виконання проєктування	орієнтовані на захист прав, свобод та правопорядку в суспільстві	цінності (навіщо?); процедури (які?); дії (що?); час (коли?); місце (де?) (відповіді на ці питання забезпечуються методами, засобами та заходами з урахуванням умов експлуатації системи в сфері злочинного інтересу, зокрема: через вразливості в системі правопорядку)	тями інфраструктури; технологічними рішеннями та вразливостями соціальної інженерії	злочини з використанням інформаційних технологій (тобто, ІТ – це лише один із можливих засобів)
Аксіома 3. *На етапі створення системи* рівень безпеки забезпечується реалізацією методів, засобів та заходів, передбачених на етапі проєктування	На етапі створення правової системи її забезпечення рівня безпеки досягається шляхом реалізації конкретних методів, засобів та заходів, передбачених на етапі проектування, зокрема: методи забезпечення безпеки (метод правового регулювання; метод профілактики та превенції; метод контролю та моніторингу; метод підзвітності та відповідальності); засоби забезпечення безпеки (технологічні засоби; інформаційні системи; меха-	На етапі створення в злочинній системі рівень безпеки забезпечується: організаційною структурою; правилами дії та конспірації; ієрархією (мережею) та підпорядкуванням (це дозволяє координувати дії їх учасників, забезпечувати безпеку, захист і досягнення спільних кримінальних цілей)	На етапі створення в системі кіберзлочинності рівень безпеки забезпечується шляхом: 1) безпечної архітектури; 2) застосування сучасних засобів анонімності; 3) застосування технологій захисту від відстеження; 4) шифрування та безпечне збереження даних; 5) маскування фінансових потоків; 6) розробки алгоритмів соціальної інженерії та тестування лояльності учасників; 7) впровадження засобів моніторингу та контролю доступу;	Приклади реалізації методів, засобів та заходів протидії злочинності: створення єдиного реєстру правопорушень (цей засіб дозволяє правоохоронним органам швидко отримувати доступ до інформації про злочини, що значно підвищує ефективність правозастосування); впровадження системи відеоспостереження в громадських місцях (це допомагає попередити правопорушення та сприяє ідентифікації правопорушників у випадках злочинів); організація навчаль-

	нізми захисту персональних даних; системи кібербезпеки); заходи для забезпечення безпеки правової системи (навчання та підвищення кваліфікації працівників; внутрішній аудит та контроль; антикорупційні заходи; громадський контроль та міжнародне співробітництво)		8) планування системи резервних копій та відновлення даних; 9) автоматизації процесів для уникнення помилок через людський фактор; 10) підготовки до адаптації та швидкого реагування на загрози	них програм для працівників правопорядку (це підвищує професіоналізм, особливо у питаннях роботи з технологіями, кібербезпекою та у взаємодії з громадянами; розробка та впровадження антикорупційних програм (охоплює створення системи контролю за діями чиновників, прозорість процедур, аудит фінансових потоків, що дозволяє знижувати ризик зловживань); проведення регулярних аудитів (оцінювання роботи органів правопорядку та судової системи для виявлення недоліків і запровадження коректівів у їхню діяльність)
Аксіома 4. *На етапі експлуатації* безпека системи забезпечується шляхом: оцінвання рівня поточної безпеки; забезпечення потрібного рівня безпеки	На етапі експлуатації правової системи оцінювання рівня її ефективності та забезпечення мінімального рівня безпеки досягається шляхом використання	На етапі експлуатації злочинної системи оцінювання рівня поточної безпеки та забезпечення мінімального рівня її безпеки досягається шляхом постій-	На цьому етапі кіберзлочинець(і) оцінювання рівня поточної безпеки та забезпечення необхідного рівня безпеки створеної системи проводить шляхом:	Кіберзлочинне середовище спрямоване на максимізацію вигоди (прибутку) при мінімізації ризиків (для цього кіберзлочинці намагаються швидко завер-

	технологій для моніторингу, контролю та реагування на правопорушення разом із правоохоронними органами, які застосовують отримані дані для підтримки правопорядку	ного моніторингу та підтримання емоції страху серед її учасників (стейкхолдерів)	використання передових IT; децентралізація мереж та використання хмар; оновлення інфраструктури; мінімізація цифрових слідів; адаптація під нові методи роботи правоохоронних органів; використання криптовалют для відмивання коштів; сегментація доступу для учасників («ланцюг анонімності»); використання фейкових облікових записів	шити операції та зникнути з «цифрового сліду», оскільки правоохоронні органи та технологічні компанії постійно вдосконалюють свої методи протидії)
Аксіома 5. Оцінювання рівня безпеки відбувається <u>в</u> *конкурентному середовищі,* яке охоплює інші антагоністичні системи	Конкурентне середовище для правової системи містить сукупність факторів, установ, структур та інститутів, які впливають на ефективність правової системи та змушують її адаптовуватися, вдосконалюватися та відповідати очікуванням суспільства (конкуренція для правової системи може бути як внутрішньою, так і зовнішньою, зокрема, вона може охоплю-	Злочинна система завжди прагне підлаштовуватися під легальні системи в суспільстві (тримаючись «тіні»)	Конкурентне середовище для системи кіберзлочинності містить: систему міжнародної боротьби з кіберзлочинністю; системи технічних та фінансових обмежень; еволюцію програмних та апаратних засобів кібербезпеки; системи вербування учасників іншими та витоку інформації	Власне, саме конкурентне середовище створює можливості найкраще пізнати структуру, мотивацію, взаємодію і цінності, притаманні тим чи іншим злочинним угрупованням та окремим злочинцям (на контрасті)

	вати інші соціальні інститути, міжнародне право, технологічні інновації, а також тіньові «правові» практики).			
Аксіома 6. *На етапі експлуатації системи* під інформаційним впливом конкуруючої системи може відбутися зміна її структури або зв'язків між елементами, що може призвести до зменшення необхідного рівня комплексної безпеки	Якість інформаційного впливу між системами на контрасті: - згідно з КПК України [3] практична діяльність слідчого має такі тенденції: 1) своєчасне, доцільне та законне застосування влади; 2) надмірне застосування владних повноважень (найперше, зумовлене хибним уявленням про обсяг своїх повноважень або некритичною вірою у всеосяжність закону, норми, розпорядження); 3) нерішуче застосування владних повноважень, що пов'язане з сумнівами, побоюваннями щодо можливої відповідальності за їх застосування (зокрема через те, що законодавець не завжди витримав вимоги принципу юридичної визначеності); 4) дії з елементами корупції (формою цих дій завжди є одна із вказаних вище тенденцій 1–3, а сутнісне наповнення цієї форми зумовлено конкретними обставинами справи) - аксіома «вигода в підтриманні злочинної системи» (наприклад, завжди є неправомірна вигода/корупційна складова в діяльності певних суб'єктів владних повноважень, а також спеціальні інтереси спецслужб)		Згідно зі ст. 364-1 КК України [4] «під неправомірною вигодою слід розуміти грошові кошти або інше майно, переваги, пільги, послуги, нематеріальні активи, будь-які інші вигоди нематеріального чи негрошового характеру, які пропонують, обіцяють, надають або одержують без законних на те підстав»
Аксіома 7. *На етапі експлуатації системи* може відбуватися її знищення антагоністичними системами або знищення антагоністичних систем	Аксіома «латентна корозія правової системи» (приклад, Указ Президента України від 22.10.2024 р. за № 732/2024 Про рішення Ради національної безпеки і оборони України від 22 жовтня 2024 року «Щодо протидії корупційним та іншим правопо-	Аксіома «конфліктності з правовим середовищем» (злочинна система завжди перебуває в конфлікті з правовою системою, в силу дії як «антагоніст»)		Конфлікт між системами: в статиці – це система взаємозалежних структурних елементів/фактів/явищ/ обставин/інформації; а в динаміці – це процес взаємовпливу (в якому кожна сторона приймає рішення в умовах конфлікту та чинника невизначеності за

	порушенням під час встановлення інвалідності посадовим особам державних органів»)		специфічною «стратегією гри»)
Аксіома 8. Кожна система має *закінчення життєвого циклу*	Система правопорядку змінюється в часі через розвиток суспільства, технологічний прогрес, зміни в соціальних нормах і виклики, які з'являються в різних історичних періодах (ці зміни зумовлені необхідністю забезпечити безпеку, справедливість і стабільність у суспільстві, адаптуючи правові норми та структуру правозастосування до нових реалій). Злочинна система змінюється через необхідність адаптації до соціальних, технологічних, економічних і правових змін, які постійно відбуваються у суспільстві (подібно до будь-якої іншої системи, злочинна система прагне виживання і збереження свого впливу, тому змушена розвиватися, щоб залишатися ефективною в нових умовах).		В часі та просторі всі системи перебувають в стані конфлікту та невизначеності (за специфічною «стратегією гри»), що в результаті їх приводить до трансформації, модернізації, ентропії тощо

Варто пригадати, що злочинна поведінка зазвичай має на меті досягнення певної вигоди (будь то матеріальна, соціальна, емоційна або психологічна тощо). Злочинці, найперше, діють з особистих інтересів, намагаючись задовольнити свої потреби або бажання. І хоча ця діяльність є ризикованою (наприклад, бути спійманим та зазнати покарання) цей ризик доволі часто не є стримуючим фактором для злочинців. Їх мотивує «ілюзія потенційної вигоди» (матеріальної чи моральної) та/або «інстинкт гри» з порівняно можливими негативними наслідками. Саме щоб такі «ілюзії» не мали виправдання в статті 68 Конституції України надано чітке визначення: «незнання законів не звільняє від юридичної відповідальності» [5].

Це дає підстави стверджувати, що більшість злочинів мають певний рівень раціонального планування, обдуманості (тобто, злочинці зважують свої шанси на успіх і оцінюють потенційні ризики, обираючи найбільш прийнятні способи досягнення мети). А це, в свою чергу, є ґрунтом для повторюваності злочинних дій (рецидивізм), які в загальній структурі злочинності займають вагоме місце. Кількість інформації в кіберпросторі постійно зростає, створюючи безмежне інформаційне середовище, в якому обсяг даних зберігається, обробляється та передається у великих масштабах. Це веде до нових викликів у зберіганні, обробці та захисті даних.

Кіберпростір за своєю природою є відкритим і доступним, забезпечуючи можливість користування ресурсами, взаємодії і обміну інформацією для широкого кола користувачів. Це дозволяє швидко поширювати інформацію, що робить його важливим інструментом для комунікації, бізнесу та науки. Кіберпростір дозволяє миттєво обмінюватися інформацією,

забезпечуючи надзвичайно високу швидкість комунікації та передачі даних. Це визначає характер інформаційного середовища, де події, новини або дані можуть поширюватися у реальному часі. Користувачі кіберпростору очікують конфіденційності та захисту своїх даних, що є одним із базових принципів, на яких побудовано взаємодію в цифровому середовищі. Проте ця конфіденційність часто піддається ризику через недосконаліть технологічних захистів і недотримання стандартів безпеки.

Кіберпростір постійно розвивається та адаптується до нових технологій і потреб користувачів. Від IoT (інтернету речей) до штучного інтелекту – нові технології безперервно змінюють його функціональні можливості і ризики. Кіберзлочинці швидко адаптуються до нових загроз і протидії, змінюючи методи та інструменти у відповідь на оновлені засоби кіберзахисту, зміни законодавства та інші виклики. Зокрема, використовують сучасні технології, програмне забезпечення та інноваційні методи атак, щоб досягти своїх цілей. Це середовище постійно оновлюється, щоб уникнути виявлення та вдосконалити способи обману.

Як було сказано раніше, більшість кіберзлочинів мають на меті отримання фінансової вигоди, будь то крадіжка даних, фішинг, вимагання або шахрайство. Тому можемо обґрунтовано допустити, що кіберзлочинне середовище має організовану структуру, що охоплює різні угруповання, які співпрацюють, обмінюються ресурсами, інформацією та інструментами для досягнення своїх цілей. Нині певні угруповання об’єднуються в тимчасові альянси для виконання конкретних завдань (наприклад, хакери під керівництвом спецслужб рф та КНДР).

Відтак, соціотехнічний погляд на правопорядок дає можливість: аналізувати, як технології, правові норми та людські фактори разом формують сталу систему, що підтримує безпеку та справедливість у суспільстві; або як сучасні технології дозволяють ефективніше контролювати дотримання законів через автоматизовані системи моніторингу (наприклад, камери відеоспостереження з розпізнаванням обличчя можуть швидко ідентифікувати підозрюваних у правопорушеннях).

Також технології сприяють підвищенню довіри до правопорядку, оскільки автоматизовані системи зберігання і обробки даних мінімізують можливість маніпуляцій. Це підвищує об’єктивність та неупередженість в роботі правоохоронних органів (наприклад, соціальні мережі та інші комунікаційні системи дозволяють громадянам бути більш залученими в забезпечення правопорядку, відслідковувати випадки правопорушень і контролювати роботу державних органів шляхом подання петицій, моніторингу правопорушень тощо). Отже, соціотехнічна система – є складним організмом, що вимагає узгодження технологічних можливостей з людськими потребами, навичками та очікуваннями для ефективного та сталого функціонування. Де правопорядок (як ідеальна соціотехнічна система) є: інтегрованим підходом щодо підтримки законності, безпеки; поєднує традиційні

соціальні механізми з технічними засобами задля ефективного функціонування та адаптації до сучасних викликів; зумовлений балансом інтересів між соціальними потребами та технічними можливостями, щоб забезпечити справедливість, безпеку та захист прав у цифрову епоху.

Проаналізовані тут чинники підтверджують зміну структури злочинності під впливом поширення кіберзлочинності у глобальному масштабі. По-перше, кіберзлочини стали надзвичайно прибутковими для злочинців (що робить їх привабливими як для окремих осіб так і для організованих злочинних угруповань). По-друге, кіберзлочинність значно ускладнює розслідування традиційних злочинів (оскільки в багатьох випадках злочинці використовують кіберпростір для організації, планування та здійснення незаконних дій). В-третіх, кіберзлочинність дедалі частіше застосовується як інструмент для досягнення політичних цілей або впливу на громадську думку (кіберзлочинність стає все більш вагомою частиною сучасної злочинності, і боротьба з нею потребує нових методів, ресурсів і стратегій як на національному, так і на міжнародному рівнях).

1.2 Основи правового регулювання боротьби з кіберзлочинністю

Основи правового регулювання боротьби з кіберзлочинністю – це сукупність законодавчих актів, міжнародних договорів і нормативних документів, які визначають правила та процедури для виявлення, розслідування і запобігання кіберзлочинам. Вони регулюють діяльність правоохоронних органів, захист даних, співпрацю між країнами та встановлюють відповідальність за порушення в кіберпросторі.

В дослідженні (використовуючи, насамперед, трансдисциплінарний та міждисциплінарний підходи) звертаємо більше уваги на практичну сторону проблеми, а саме: на певні правила та процедури щодо виявлення, розслідування та запобігання кіберзлочинам. Залишивши теоретичне дослідження правових принципів, законодавчих актів, міжнародних договорів і нормативних документів (які визначають правила та процедури для виявлення, розслідування і запобігання кіберзлочинам) науковцям у галузі юридичних наук.

Таблиця 1.3 – Класифікація криміналістичних версій (за М. Погорецьким [6])

Види версій	*Означення*	*Примітки*
За суб'єктом висунення	версії слідчі, розшукові, судові, сторони захисту, експертні (різновиди	кожен вид версій має свою специфіку та функцію в розслідуванні справи: *слідчі версії* – це припущення, які формуються слідчим для визначен-

	версій, які висуваються різними суб'єктами кримінального процесу для встановлення обставин злочину і побудови логічної картини події)	ня основних напрямків розслідування (слідчі версії базуються на зібраних доказах, аналізі місця події, показань свідків та інших фактах, що можуть допомогти встановити істину в справі; вони спрямовані на планування слідчих дій і пошук додаткових доказів); *розшукові версії* – формуються оперативними працівниками, які займаються пошуком осіб або предметів, пов'язаних зі злочином (ці версії допомагають організувати розшукові заходи, спрямовані на виявлення прихованих злочинців, свідків або речових доказів, що можуть мати значення для розслідування); *судові версії* – це припущення, які формулюються судом під час розгляду справи (судові версії дозволяють критично аналізувати докази, перевіряти достовірність зібраних матеріалів і визначати винуватість або невинуватість обвинуваченого; вони допомагають суду прийняти об'єктивне рішення на основі доказів, наданих під час судового процесу); *версії сторони захисту* – висуваються адвокатом або обвинуваченим з метою обґрунтування невинуватості підозрюваного або обвинуваченого (такі версії можуть містити альтернативні пояснення подій, критику доказів, наданих слідством, або припущення про можливість вчинення злочину іншими особами; вони спрямовані на захист прав і інтересів підозрюваного чи обвинуваченого); *експертні версії* – формуються експертами, залученими до криміналь-

		ного провадження, для дослідження конкретних питань, що потребують спеціальних знань (наприклад, судово-медичних, криміналістичних, технічних тощо; експертні версії дозволяють дослідити обставини злочину з наукової точки зору та надати об'єктивні висновки, які можуть бути використані як докази)
За змістом	версії, які інтерпретують відомі факти, а також передбачають можливість існування нових, поки що невідомих обставин	у ході розслідування одночасно можуть існувати як перші, так і другі версії; зазвичай версії, що пояснюють невідомі обставини, за своєю суттю є похідними від тих, які висвітлюють уже встановлені факти
За характером	версії – типові та конкретні	типові версії формуються на основі узагальненого практичного досвіду та професійної діяльності слідчих тощо; вони можуть охоплювати злочин у цілому або стосуватися окремих його елементів; ці версії будуються на обмеженій кількості початкових даних і поступово доповнюються/уточнюються з надходженням нової інформації про обставини справи; зрештою, типові версії замінюються конкретними, які формуються з урахуванням особливостей конкретного злочину
Залежно від орієнтації у час	версії – ретроспективні та прогностичні	*ретроспективні версії* – це версії, спрямовані на реконструкцію подій, які вже відбулися, для встановлення обставин злочину (вони базуються на аналізі доказів, свідчень та інших наявних даних, щоб зрозуміти, як саме відбувся злочин, хто брав у ньому участь, якими були мотиви та інші деталі; ретроспективні версії допомагають відновити минулі

		події та встановити послідовність дій); *прогностичні версії* – це версії, що будуються з урахуванням можливого розвитку подій у майбутньому (вони спрямовані на прогнозування подальшої поведінки підозрюваних, можливих місць приховування злочинців, наступних кроків у злочинній діяльності, а також можливого місцезнаходження доказів; прогностичні версії є корисними для планування подальших слідчих дій, розшукових заходів та забезпечення превентивних заходів)
За часом висування	версії – початкові, подальші	існують тому, що в процесі розслідування спершу формуються загальні припущення, які поступово уточнюються з надходженням нових фактів; тобто, початкові версії ґрунтуються на обмеженій інформації, яка є на самому початку розслідування, тоді як наступні версії коригуються та деталізуються відповідно до нових доказів і обставин, що з'являються у ході розслідування; це дозволяє систематично звужувати коло можливих сценаріїв і наближатися до об'єктивної картини події
За обсягом встановлених обставин справи	версії – загальні та окремі	загальні версії розкривають злочин у цілому, тоді як окремі версії охоплюють лише конкретні деталі (такі як спосіб, місце або час скоєння злочину тощо); загальні версії можна розділити на два типи: пошукові (які стосуються обставин, що мають бути підтверджені, та містять припущення про їх можливе існування) і перевірочні (які передбачають встановлення місцезнаходження конкретних осіб або предметів, наявність яких уже відомо); окремі ве-

		рсії можуть бути однорідними (коли стосуються перевірки однієї конкретної обставини) або змішаними (коли охоплюють кілька припущень про різні аспекти злочину)
За обґрунтованістю та логічним взаємозв'язком	версії – основні та контраверсії	з метою запобігання однобічності та необ'єктивності при з'ясуванні обставин злочину кожна основна версія має мати контрверсію (наприклад, у кримінальному провадженні про шахрайство з використанням ЕОМ як основна версія щодо мотиву скоєння злочину може бути збагачення, а контрверсією може бути – помста); спростування контрверсії підвищує імовірність правильності основної версії (хоча цей принцип може мати винятки)
За ступенем вірогідності	версії – вірогідні, ймовірні, малоймовірні, найбільш ймовірні	*вірогідні версії* – це такі версії, які ґрунтуються на значній кількості підтверджувальних фактів і даних, що робить їх дуже близькими до реальності (вони є найбільш обґрунтованими та достовірними); *ймовірні версії* – версії, які мають певну підтримку у вигляді доказів або логічних припущень, але потребують додаткової перевірки (ці версії достатньо обґрунтовані, але ще не мають достатньої доказової бази); *малоймовірні версії* – версії, для яких наразі відсутні суттєві докази або які здаються малоймовірними через відсутність логічного зв'язку з обставинами справи (проте вони не відкидаються повністю та можуть розглядатися за відсутності інших варіантів); *найбільш ймовірні версії* – це версії, що мають найбільшу підтримку фактами та найкраще узгоджуються з обставинами злочину (вони пріоритетні для розгляду та зазвичай

		піддаються глибшому дослідженню з метою підтвердження)
Відносно предмета доказування	версії – які обвинувачують або виправдовують	*обвинувачувальні версії* – це версії, що передбачають винуватість підозрюваного чи обвинуваченого у вчиненні злочину (вони будуються на доказах і припущеннях, які вказують на причетність особи до злочину; обвинувачувальні версії можуть містити інформацію про мотив, спосіб скоєння злочину, участь у злочинній діяльності та інші обставини, що підтверджують вину особи); *виправдовувальні версії* – це версії, які передбачають невинуватість підозрюваного чи обвинуваченого або ж пояснюють обставини, що можуть виправдовувати дії особи (вони ґрунтуються на фактах і припущеннях, які ставлять під сумнів причетність підозрюваного до злочину або доводять, що він не міг бути учасником події через певні алібі, відсутність мотиву, відсутність технічної можливості скоєння злочину тощо)

Структура криміналістичної методики розслідування має відповідати сучасним науковим і практичним вимогам, враховуючи специфіку кожного типу правопорушення. Важливо враховувати законодавчі зміни, які можуть впливати на процес розслідування та вимагати своєчасного корегування методик. Використання цифрових технологій, аналітичних інструментів і штучного інтелекту має значний потенціал для підвищення ефективності криміналістичних методик, але потребує подальших наукових розробок. Отже, розуміння структури криміналістичної методики розслідування правопорушень є основою для забезпечення ефективного і законного проведення розслідувань, а також сприяє підвищенню рівня професійної підготовки слідчих та інших учасників кримінального процесу.

Таблиця 1.4 – Загальна структура криміналістичної методики розслідування злочинів (за О.Ващуком [7])

Етапи	*Зміст*	*Визначення*
Загальна	Криміналістична	криміналістична характеристика

частина	характеристика кримінального правопорушення	кримінального правопорушення (збирання та аналіз інформації про характерні ознаки злочину; опис типових способів вчинення, використовуваних знарядь, механізмів дій злочинця (механізм злочину); залишених слідів (слідова картина); вивчення профілю типових правопорушників та потерпілих)
	Обставини, що підлягають встановленню	обставини, що підлягають встановленню (визначення ключових обставин, що мають бути встановлені в процесі розслідування (факти, події, особи), формування переліку доказів, потрібних для підтвердження або спростування цих обставин)
	Особливості виявлення ознак кримінального правопорушення та початку кримінального провадження	особливості виявлення ознак кримінального правопорушення та початку кримінального провадження (розробка методів виявлення ознак злочину, охоплюючи розшукові заходи, визначення процедур фіксації та документування виявлених ознак)
Початковий етап розслідування	Організація та планування розслідування, взаємодія слідчого з іншими суб'єктами кримінального провадження	організація та планування розслідування, взаємодія слідчого з іншими суб'єктами кримінального провадження (створення детального плану розслідування, встановлення механізмів взаємодії з іншими суб'єктами (експерти, оперативні працівники, прокурори та ін.)
	Типові слідчі ситуації, тактика дій слідчого	типові слідчі ситуації, тактика дій слідчого (розробка типових слідчих ситуацій та версій, визначення тактичних заходів, забезпечувальних дій, тактичних комбінацій і операцій)
	Особливості проведення окремих	особливості проведення окремих слідчих (розшукових) дій, неглас-

	слідчих (розшукових) дій, негласних слідчих (розшукових) дій	них слідчих (розшукових) дій (опис тактик проведення огляду місця події, допитів, обшуків, експертиз, використання негласних методів для збирання доказів тощо)
Основний етап розслідування	Організація та планування розслідування, взаємодія слідчого з іншими суб'єктами кримінального провадження	організація та планування розслідування, взаємодія слідчого з іншими суб'єктами кримінального провадження (продовження планування розслідування з урахуванням отриманих результатів, координація з іншими суб'єктами для уточнення деталей та аналізу нових даних)
	Типові слідчі ситуації, тактика дій слідчого	типові слідчі ситуації, тактика дій слідчого (адаптація слідчих версій та тактики дій на основі нових доказів, проведення додаткових слідчих дій, повторних допитів, експертиз тощо)
	Особливості проведення окремих слідчих (розшукових) дій	особливості проведення окремих слідчих (розшукових) дій, негласних слідчих (розшукових) дій (виконання додаткових слідчих дій з урахуванням специфіки злочину, застосування нових негласних методів для збирання доказів)
Етап криміналістичної профілактики	Тактика криміналістичної профілактики кримінального правопорушення	виявлення причин та умов вчинення злочинів (аналіз причин та умов, що сприяли вчиненню правопорушення, визначення заходів щодо їх усунення або мінімізації); розробка рекомендацій щодо запобігання злочинам (формування рекомендацій для органів державної влади, бізнесу, громадськості, підвищення рівня контролю, проведення просвітницької роботи, удосконалення законодавства); проведення профілактичних заходів (організація семінарів, тренінгів для правоохоронців, проведен-

		ня інформаційних кампаній, розробка систем моніторингу та аналізу криміногенної обстановки); співпраця з іншими організаціями та установам (встановлення партнерських відносин з іншими суб'єктами (місцева влада, громадські організації, медіа), координація дій, обмін інформацією для ефективної профілактики злочинності)

Кримінальний аналіз є специфічним видом інформаційно-аналітичної діяльності, метою якого є виявлення та точне встановлення зв'язків між інформацією, що стосується злочину, та іншими даними, отриманими з різних джерел. Він забезпечує інформаційну підтримку для здійснення оперативно-розшукової і слідчої діяльності, а також аналітичного супроводу.

Таблиця 1.5 – Алгоритм дій слідчого при проведенні аналізу інформації «про зв'язок» [8]

Порядок дій	*Визначення*	*Примітки*
Підготовка клопотання	Слідчий (відповідно до статті 160 КПК України) готує клопотання про тимчасовий доступ до інформації, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, зокрема отримання послуг, їх тривалості, змісту, маршрутів передавання тощо («інформація про зв'язок») та отримує від суду відповідну ухвалу	згідно з КПК України, доступ до інформації, яка містить дані про абонента, надання телекомунікаційних послуг (зокрема, відомості про отримання послуг, їх тривалість, зміст, маршрути передачі тощо), здійснюється через тимчасовий доступ до речей і документів
Отримання інформації	Слідчий (відповідно до статті 165 КПК України) отримує інформацію про зв'язок здебі-	згідно з главою 15 розділу II КПК України, тимчасовий доступ до речей і документів не вважається слідчою (роз-

	льшого на оптичному носії або флеш-накопичувачі	шуковою) дією, а є заходом забезпечення кримінального провадження; однак дії, як-от аналіз інформації про зв'язок та радіотехнічне обстеження, не мають нормативного визначення в КПК України
Аналіз інформації	Слідчий може самостійно здійснити аналіз інформації про зв'язок	кримінальний аналіз є основою моделі «Intelligence Led Policing» («поліцейська діяльність, керована аналітикою»), яка спрямована на ухвалення ефективних управлінських рішень; це досягається завдяки комплексному використанню методів і технік для збирання, обробки, оцінювання та аналізу інформації, її реалізації та обміну в ході кримінального провадження, оперативно-розшукових заходів і розробки тактичних та стратегічних дій для протидії злочинності
Аналіз інформації оперативниками	У разі залучення оперативних підрозділів слідчий готує відповідне доручення щодо проведення аналізу (дослідження) даних про зв'язок, у якому формулює запитання, які потребують відповіді (узгодивши їх попередньо з працівниками оперативних підрозділів та додавши до цього листа носій з електронною копією інформації, отриманою від оператора/провайдера телекомунікацій)	працівник оперативного підрозділу складає довідку за результатами аналізу (яку підписує керівник підрозділу) та надсилає слідчому супровідним листом; у довідці зазначається, що інформація про зв'язки є попередньою і орієнтовною, не може слугувати доказом і потребує додаткової перевірки та підтвердження відповідно до законодавства (оперативні працівники використовують дані про трафік, номери абонентів, інформацію про базові станції та інші відомості з відкритих джерел, включно з картами місцевості); якщо

		інформації багато, довідку можуть надати в електронному вигляді
Фіксація результатів аналізу інформації	Слідчий (відповідно до статті 237 КПК України) проводить огляд електронних документів з інформацією про зв'язок і складає відповідний протокол	якщо застосовуються ресурси оперативних підрозділів, слідчий додатково використовує інформацію з довідки, наданої оперативними підрозділами; у протоколі доцільно зазначити, що інформація, яка є об’єктом цієї слідчої дії, була отримана від операторів і провайдерів телекомунікацій у рамках тимчасового доступу до речей і документів
Аналіз інформації спеціалістами	Слідчий (відповідно до статті 71 КПК України) видає постанову про залучення співробітників, операторів або провайдерів телекомунікацій як спеціалістів (у цій постанові чітко формулюються питання, для вирішення яких необхідні спеціальні знання та навички)	якщо слідчому потрібні кваліфіковані роз’яснення з технічних питань (наприклад, стосовно функціонування базових станцій чи їх розташування), тоді він залучає спеціаліста(ів), який має спеціальні знання та навички і може надати консультації та висновки;
Спосіб уникнення «плодів отруйного дерева»	Слідчий (відповідно до статті 84 КПК України), наприклад, використовує як доказ висновок експерта	якщо в кримінальному провадженні потрібно отримати експертний висновок для використання його як доказу, слідчий залучає відповідного експерта згідно із встановленою процедурою

Таблиця 1.6 – Порівняльний аналіз деяких особливостей діяльності слідчого та адвоката на стадії досудового розслідування

Слідчий	*Адвокат*
Згідно з КПК діяльність слідчого підпорядковується суворо встановленим нормам (правова регламентація).	Згідно зі ст. 20 Закону «Про адвокатуру та адвокатську діяльність» адвокат має право вчиняти будь-які дії, не

Практична діяльність слідчого має такі тенденції: 1) своєчасне, доцільне та законне застосування влади; 2) полягає в надмірному застосуванні владних повноважень (найперше, зумовлене неправильним уявленням про обсяг своїх повноважень або некритичною вірою у всеосяжність закону, норми, розпорядження); 3) проявляється у невпевненому використанні владних повноважень, зумовленому сумнівами та побоюваннями щодо можливої відповідальності за їх реалізацію (зокрема, через те, що законодавство не завжди відповідає принципу юридичної чіткості); 4) полягає в діях з елементами корупції (формою цих дій завжди є одна із вказаних вище тенденцій 1–3, а сутнісне наповнення цієї форми обумовлено конкретними обставинами справи).	заборонені законом, правилами адвокатської діяльності та договором. *Практична діяльність адвоката має такі тенденції*: 1) своєчасне, доцільне вчинення будь-яких необхідних дій, які не заборонені законом; 2) полягає в надмірному застосуванні повноважень в процесі (найперше, у разі низької якості критики/аналізу незаконності дій слідчого або некритичної віри в обсяг права вчиняти будь-які дії, не заборонені законом, правилами адвокатської діяльності та договором за принципом «процес заради процесу»); 3) полягає в нерішучому застосуванні наявних можливостей, що пов'язане з сумнівами, побоюваннями щодо можливої відповідальності, конфліктів із слідчим за їх використання тощо; 4) полягає в діях з елементами корупції (формою цих дій завжди є одна із вказаних вище тенденцій 1–3, а сутнісне наповнення цієї форми зумовлено конкретними обставинами справи).
Особливістю діяльності слідчого є наявність негативних емоцій, що впливають на слідчого. *Компенсація негативної емоційної напруженості може відбуватися:* 1) шляхом усвідомлення великої суспільної корисності роботи; 2) переживання морального задоволення (нового досвіду), що породжується кожним випадком розкриття злочину (як інтелектуальної та організаційної перемоги); 3) через корупційну складову від результату вирішення справи.	Особливістю діяльності адвоката є наявність негативних емоцій, що впливають на адвоката. *Компенсація негативної емоційної напруженості може відбуватися:* 1) шляхом усвідомлення великої суспільної корисності роботи; 2) переживання морального задоволення (нового досвіду) підтриманого матеріальним стимулом, що породжується кожним випадком належного захисту прав, свобод та законних інтересів клієнта (зокрема доведення його невинуватості або справедливого покарання); 3) через корупційну складову від результату вирішення справи.

Особливістю діяльності слідчого є дефіцит часу при формуванні моделей-версій події злочину, за умови дотримання слідчим таких загальних вимог: 1) версія має узгоджуватися з усіма фактами, які її стосуються; 2) для пояснення набору фактів слід пропонувати якомога менше версій, забезпечуючи максимальну кількість зв'язків між ними; 3) серед кількох суперечливих версій пріоритет надається тій, яка найбільш послідовно пояснює всю сукупність фактів; 4) версія має пояснювати подію злочину на основі матеріальних предметних причинно-наслідкових зв'язків, не має мати «фантазійного» характеру.	Особливістю діяльності адвоката є дефіцит часу щодо: 1) критичного аналізу моделі-обставин, яких притримується клієнт; 2) критичного усвідомлення сформованої слідчим моделей-версій події злочину, з аналізом дотримання загальних вимог слідчим при формуванні версії(й) та аналізом особистості слідчого (рівень моральних якостей та принципів; рівень інтелектуально-пізнавальних якостей; характерологічні якості; психофізіологічні якості); 3) напрацювання правової позиції у справі (як цілісної системи), яка з різним ступенем точності відображає багатогранні логічні та пізнавальні зв'язки між вже встановленими фактами і невідомими обставинами, що мають значення для інтересів клієнта у справі. Це важливо, оскільки часто слідчий, оцінюючи ключові факти та обставини, спрямовує інформаційний пошук не за логічною послідовністю, а під впливом емоційно-ціннісного конфлікту; 4) планування та здійснення адвокатської діяльності через завантаженість адвоката в різних процесах (в просторі та часі).

Вищенаведений порівняльний аналіз вибіркових аспектів професійної діяльності адвоката та слідчого дає підстави стверджувати, що діяльність адвоката (на стадії досудового розслідування) напряму обумовлена «професіоналізмом» слідчого (за винятком, у певних випадках).

Криміналістична тактика дій слідчого полягає у використанні таких методів і прийомів, які спрямовані на подолання завад у доступі до джерела інформації, а також на запобігання спотворенню чи приховуванню важливих даних. Цей процес для слідчого є складним і вимагає значного емоційного та інтелектуального напруження. Як наслідок, його діяльність не завжди зводиться до систематизації зібраного доказового матеріалу та ефективного планування розслідування.

Отже, тактика «затягування слідства» зі сторони адвоката, найперше, є результатом «неналежної» діяльності слідчого щодо своєчасного, доцільного та законного застосування влади та вчинення інших дій. Тобто, слідчий, «результатами» своєї діяльності, створює адвокату сприятливі можливості щодо застосовування тактики «затягування слідства» (згідно з законом «тактика захисту»).

Слідча діяльність – це завжди протистояння («єдність та боротьба протилежностей»), а тому скарги слідчого на адвоката щодо «затягування слідства» мають бути підтверджені належними та допустимими доказами (серед яких мають бути докази «своєчасного, доцільного та законного застосування влади» слідчим та «протизаконної» діяльності цьому зі сторони адвоката).

Конкуренція в кримінальному процесі між істиною та правами людини має вирішуватись на користь прав людини. Тобто, важливість балансу між покаранням злочинців та захистом прав невинних осіб можемо показати висловом, який приписують відомому німецькому юристу Рудольфу фон Ієрингу (Rudolf von Jhering): «кримінальне право – це меч, який має вразити злочинця, а кримінальний процес – це щит, який оберігає порядну людину від свавілля та репресій».

1.3 Використання новітніх технологій у розслідуванні злочинів

Новітні технології у розслідуванні злочинів стали ключовим елементом сучасної криміналістики. Вони трансформували традиційний підхід розслідування, надаючи слідчим нові інструменти та методи для збирання, аналізу та інтерпретації доказів. Ці технології не лише пришвидшують розслідування, але й підвищують їхню точність та ефективність, забезпечуючи точне відтворення подій, розкриття та попередження злочинів. Зокрема, вони охоплюють широкий спектр інноваційних інструментів і методів, які підвищують ефективність роботи правоохоронних органів.

Відтак, технологію розслідування злочинів можна визначити як частину функціонального підходу до організації процесу розслідування, яка передбачає можливість структурованого та послідовного виконання дій слідчими, криміналістами та оперативними працівниками у ході розслідування кримінальних правопорушень. Це означає, що діяльність у рамках розслідування можна формалізувати й описати у вигляді чітких алгоритмів або послідовних процедур, що дає змогу забезпечити ефективність і точність на кожному етапі розслідування, мінімізуючи ризики помилок і недоліків. Такий підхід сприяє підвищенню узгодженості та якості роботи усіх задіяних фахівців, що займаються збиранням і аналізом доказів, забезпеченням доказової бази та пошуком винних осіб.

Як зазначає В. Шевчук «сучасний етап розвитку вітчизняної криміналістики та її перспективи характеризуються активними дослідженнями

та застосуванням інноваційних засобів і технологій в усіх її складниках: загальній теорії криміналістики, криміналістичній техніці, криміналістичній тактиці та криміналістичній методиці. Інноваційні напрями розвитку криміналістики тісно пов'язані з розв'язанням її завдань в умовах глобалізації та інформатизації цифрового суспільства та широкого впровадження інноваційних інформаційних технологій» [9].

Тобто, сучасний розвиток української криміналістики та її майбутні перспективи відзначаються активним впровадженням інноваційних технологій та засобів у всі її складові.

У зв'язку з цим виникає потреба в науковому переосмисленні та, у деяких випадках, перегляді низки проблем криміналістики, пов'язаних із дослідженням інноваційних основ цієї науки та практичними аспектами розробки й впровадження інновацій у роботу правоохоронних органів для підвищення ефективності їхньої діяльності.

Таблиця 1.7 – Властивості інноваційного криміналістичного продукту (за В.Шевчуком [9])

Ознака	*Опис*	*Примітки*
Інноваційність (новизна)	ознака інноваційності продукту визначається його новизною, яка відображає створення нових властивостей або значне покращення параметрів, що якісно відрізняються від попередніх аналогів	інноваційність продукту означає, що він є новоствореним, новозастосованим або вдосконаленим, суттєво підвищуючи характеристики об'єкта (важливо, щоб покращення властивостей було істотним, а використання таких продуктів підвищувало якість і ефективність системи)
Упредмеченість	це означає, що продукт є результатом інноваційної діяльності, поданий як новий матеріалізований або нематеріалізований об'єкт	матеріалізований об'єкт може бути реалізований у вигляді нового виробу або технології (науково-технічні засоби, прилади, апаратура, інструменти тощо), маючи фізичну форму; нематеріалізований об'єкт створюється у вигляді нових послуг, рішень та інших нематеріальних складових; отже, «упредметненість» інноваційного продукту означає, що кінцевим результатом цієї діяльності є розробка, впровадження та застосування нових засобів (технічних, тактичних, методичних) – узагальнено «інноваційних

		засобів» – які реалізуються у формі нового конкретного інноваційного рішення
Цілеспрямованість	це означає, що такі продукти мають чітку мету: вони мають сприяти досягненню цілей кримінального провадження, судового розгляду та вирішенню криміналістичних завдань	інноваційні продукти створюються в рамках інноваційного процесу, який охоплює послідовність етапів і дій для досягнення конкретних результатів; цілі цього процесу визначаються як бажані досягнення в діяльності слідчих і судових органів, що містять зменшення помилок, скорочення процесуальних витрат, підвищення ефективності розслідувань та зменшення термінів їх проведення; досягнення цілей інновацій узгоджується з цілями розслідування завдяки створенню та використанню інноваційних криміналістичних інструментів
Суб'єктність	це ознака, що визначає кваліфіковане використання криміналістичних інновацій, що його мають здійснювати спеціально уповноважені особи (слідчий, суддя, експерт тощо)	такі суб'єкти зобов'язані досконало знати та правильно застосовувати інноваційні засоби (лише спеціально підготовлені фахівці, які мають відповідні знання та навички, можуть використовувати ці інновації для вирішення завдань розслідування); важливо, щоб суб'єкти застосування усвідомлювали перспективи використання інноваційних методів і дотримувалися криміналістичних рекомендацій, уникаючи порушень
Затребуваність	це ознака, що вказує на здатність інноваційних продуктів відповідати запитам практики та окремих фахівців, які їх застосовують (вона відображає актуальну потребу в цих продуктах на практиці, а їхню ефективність і придатність перевіряють шляхом	практична потреба зумовлює створення нового продукту (як нового, так і вдосконаленого) з певним рівнем новизни; упровадження інновацій у правозастосовну діяльність пояснюється об'єктивними чинниками, зокрема, змінами в структурі злочинності, що вимагають відповідних криміналістичних засобів із застосуванням інновацій

	апробації в реальних умовах)	
Практична спрямованість	це означає, що новий продукт створено для практичного використання, хоча він ще не впроваджений у роботу	важливо враховувати, що інноваційні криміналістичні продукти подані лише у вигляді нових матеріальних виробів або технологій, тоді як нематеріальні об'єкти (наприклад, послуги чи організаційно-технічні рішення) до цього поняття не належать; практична спрямованість тісно пов'язана з життєвим циклом інновації (новація-нововведення-інновація) та її етапами (розробка, впровадження, застосування); основним у цьому процесі є те, що після впровадження продукт стає криміналістичною інновацією, готовою до використання
Ефективність	це досягнення стабільного позитивного результату у процесі застосування інноваційного криміналістичного продукту, що проявляється в покращенні якості, ефективності та результативності розслідувань, спрямованих на оптимізацію слідчих дій і протидію злочинам	ефективність відображає співвідношення результату до витрат, вкладених у досягнення цього позитивного ефекту; важливо враховувати, який саме ефект досягається: а) підвищення якості розслідувань і результативності слідчих дій; б) зниження витрат ресурсів (процесуальних, кадрових, фінансових, психологічних); в) усунення негативних чинників у процесі розслідування (помилок, конфліктів, корупційних ризиків, професійного вигорання, перевантаження слідчих, психологічного тиску та застосування незаконних методів розслідування)

Обробка великих обсягів інформації стає можливою завдяки інтелектуальним технологіям, які знижують навантаження на слідчого або оперативного працівника та підтримують його в ході здійснення необхідних дій і прийняття процесуальних рішень. Як зазначають Р. Білоус, В. Василинчук та О. Таран, нині «IBM i2 аналітика забезпечує потужний аналіз і надає можливості щодо візуалізації задля підвищення продуктивності аналітики та скорочення часу, необхідного для доставки високого значення інтелекту в межах наборів даних, які швидко зростають в обсязі.

У сфері кримінального аналізу i2 застосовують переважно з програмними продуктами iBase, iBridge, iGlass, Analyst‟s Workstation» [8].

Сучасні технології у сфері розслідування злочинів – це інноваційні методи, технічні засоби, програмне забезпечення та технологічні процеси, що використовуються для збирання, обробки, впорядкування, аналізу, зберігання та застосування інформації криміналістичного, оперативного та процесуального характеру. Їх впровадження спрямоване на автоматизацію і вдосконалення процесу розкриття та розслідування злочинів, а також на підвищення ефективності судового розгляду та якості правозастосовної діяльності.

У сучасному світі технології безперервно еволюціонують і оновлюються: щороку з'являються нові розробки, які з часом стають звичними у повсякденному житті. Так, Р. Благута, А. Мовчан [10] виділяють такі передові технології, що незабаром стануть незамінними у галузі техніко-криміналістичного забезпечення протидії злочинності (табл. 1.8–1.10).

Таблиця 1.8 – Сучасні закордонні розробки та перспективні дослідження в сфері техніко-криміналістичного забезпечення боротьби зі злочинністю

Нові технології	*Опис*	*Примітки*
Розумні окуляри	У 2019 році компанія Google представила нову версію розумних окулярів Google Glass Enterprise Edition 2, відомих як «EE», які працюють на основі технології доповненої реальності (AR). Доповнена реальність об'єднує реальні та комп'ютерні зображення, створюючи для користувача ефект занурення в інший світ. Завдяки легкій і зручній оправі окуляри майже не відчуваються під час носіння, що дозволяє використовувати їх ці-	Слідчі можуть використовувати AR-окуляри для отримання оперативної інформації та як засіб комунікації такої як контрольні списки та інструкції, а також для відправки фото або відео під час розслідування злочину

	лий день як альтернативу смартфону, ноутбуку чи смарт-годиннику	
Розумні дані	це інноваційний підхід, що дозволяє автоматизувати створення й організацію контактної інформації. Завдяки цьому підходу програми на кшталт RelateIQ можуть аналізувати дані з електронної пошти, повідомлень, соціальних мереж і миттєво створювати контакти, нагадування чи важливі списки (у роботі слідчого цей підхід може значно прискорити процес збирання та систематизації даних; у ході розслідування слідчий працює з великими обсягами контактної інформації, повідомлень, зв'язків і звітів)	використання автоматизованих інструментів може допомогти: *ефективно збирати дані* про осіб, що фігурують у справі, з таких різних джерел, як соціальні мережі чи телефонні дані; *зберігати та систематизувати інформацію* про підозрюваних, свідків або інші ключові контакти автоматично, мінімізуючи людські помилки; *проводити порівняльний аналіз* швидше, виявляючи, наприклад, історію спілкування між контактами чи мережу зв'язків підозрюваних
Дисплеї без екранів	це контактні лінзи з можливістю проєктування зображень прямо на сітківку ока (новітня технологія, яка може суттєво змінити роботу слідчого у ході розслідувань, надаючи доступ до інформації без необхідності тримати фізичний пристрій)	ці можливості не тільки полегшують доступ до даних, але й підвищують ефективність та мобільність слідчих дій, скорочуючи час на обробку інформації та прийняття рішень на місці: ось як це може допомогти слідчим: *миттєвий доступ до інформації* (лінзи можуть показувати на сітківці ока важливі дані в режимі реального часу, як-от профілі підозрюва-

		них, картки свідків чи інші документи; це дозволяє слідчому швидко ознайомлюватись із досьє прямо на місці події); *реальні та цифрові підказки одночасно* (слідчий може бачити як фізичні докази, так і цифрові підказки чи схеми (наприклад, аналітичні графіки, карти тощо), не відволікаючись на інші пристрої; це знижує ризик упущення важливих деталей на місці події); *доповнена реальність для аналізу місця злочину* (лінзи з доповненою реальністю можуть підказувати розташування потенційних доказів або візуалізувати траєкторію пострілів, точку входу злочинця або місце розташування інших ключових елементів); *безпечна робота з даними* (проекція даних на сітківку зменшує ризик випадкового розкриття конфіденційної інформації третім особам, оскільки відомості відображаються лише для слідчого); *голосове керування* (слідчий може перегортати документи або отримувати додаткову інформацію за допомогою голосових команд, що звільняє руки для роботи з фізичними доказами)
Нейрокомп'ютерні інтерфейси (НКІ)	такі гаджети можуть стати потужним інструментом для слідчих, дозволяючи їм взаємодіяти з цифровими системами за	потенційно це може допомогти в таких сферах діяльності слідчого: *швидкий доступ до інформації* (слідчі зможуть одразу «викликати» потрібну інформацію, як-от

	допомогою думок, без потреби у фізичних пристроях (ці переваги можуть зробити процеси розслідування швидшими, точнішими та менш залежними від фізичних пристроїв, що розширює можливості слідчих у сучасних та складних умовах роботи)	бази даних, досьє підозрюваних, записи про докази чи записи камер, просто думаючи про них); *миттєве документування доказів і думок* (за допомогою НКІ слідчий може подумки вносити записи або доповнення в документи у ході огляду місця злочину, що зменшить ймовірність упущення важливих деталей і прискорить складання протоколів); *збільшена мобільність* (взаємодія через НКІ дозволяє працювати без додаткових гаджетів, як-от планшети чи ноутбуки, що може бути зручним у процесі польових досліджень або огляду місць із обмеженим доступом); *полегшення роботи з великими обсягами даних* (слідчі, подумки взаємодіючи з інформацією, можуть швидко сканувати великі обсяги даних, аналізувати зв'язки між фактами та вибирати ключову інформацію для розслідування); *аналіз і побудова гіпотез у режимі реального часу* (інтерфейс дозволить оперативно аналізувати сценарії злочинів, переглядати записи, складати схеми та будувати гіпотези, допомагаючи слідчому перевіряти й уточнювати версії на ходу); *захист конфіденційних даних* (оскільки доступ до даних здійснюється через думки, знижується ризик втрати інформації або її потраплян-

		ня в сторонні руки; це особливо корисно при роботі з секретними матеріалами)
Технології Touch ID та Face ID	Touch ID і Face ID можуть суттєво допомогти слідчим у розслідуванні злочинів, забезпечуючи нові можливості для роботи з пристроями, які використовують ці технології; технології Touch ID та Face ID забезпечують можливість швидкого доступу до важливої інформації, яка може бути корисною для слідства. Однак для використання цих даних в розслідуванні слідчі мають дотримуватися юридичних норм, зокрема отримати дозвіл суду, щоб уникнути порушення права на приватність.	ці інновації можуть забезпечити: *доступ до зашифрованих даних* (сканування відбитків пальців (Touch ID) або розпізнавання обличчя (Face ID) можуть бути використані для доступу до мобільних пристроїв, що містять важливу інформацію про злочин або злочинця; наприклад, якщо підозрюваний або потерпілий залишив свій телефон на місці злочину, слідчі можуть спробувати розблокувати пристрій для збору даних, таких як повідомлення, історія дзвінків або фотографії); *встановлення факту використання пристрою* (Touch ID і Face ID зберігають інформацію про відбитки пальців або риси обличчя; це може підтвердити, хто саме використовував пристрій у визначений момент часу; це особливо корисно, якщо потрібно встановити, чи належить телефон, знайдений на місці події, певній особі); *аналіз активності та пересування* (доступ до пристроїв із ввімкненим Touch ID або Face ID може дати доступ до таких даних, як історія пересування (GPS), записи про використання мобільних додатків, фото та відео; це може допомогти відстежити маршрути підозрюваного або зрозуміти його

		дії в часі, що передував злочину); *спростування або підтвердження алібі* (якщо підозрюваний стверджує, що не користувався своїм пристроєм у ході скоєння злочину, перевірка даних про розблокування може надати слідчим інформацію про моменти його доступу до телефону); *використання як цифрових доказів* (дані, отримані з розблокованих пристроїв, можуть бути використані як цифрові докази; наприклад, історія браузера, контакти, геолокація та інші дані можуть підтвердити або доповнити інформацію про злочинні дії або зв'язки підозрюваних); *полегшення пошуку підозрюваного* (Face ID може зберігати інформацію про обличчя користувача)

У криміналістиці особлива увага приділяється використанню спеціалізованих комп'ютерних систем для ідентифікації особи. Ці системи дозволяють отримувати і аналізувати інформацію за кількома пов'язаними параметрами, що може прямо або опосередковано сприяти розкриттю злочину. Останнім часом інформаційно-пошукові системи біометричної ідентифікації стали популярними в діяльності правоохоронних органів.

Біометрична ідентифікація є способом підтвердження особи, що забезпечує зв'язок між людиною та її документом (наприклад, паспортом) шляхом порівняння біометричних характеристик. До них належать колір очей, рисунок сітківки, відбитки пальців, форма руки, риси обличчя тощо, які зберігаються у вигляді біометричних даних і співвідносяться з особистими даними власника.

Таблиця 1.9 – Статичні методи біометричної ідентифікації особи

Методи ідентифікації	*Опис*	*Примітки*
Ідентифікація особи за відбитками	цей метод ґрунтується на унікальності рисунка папілярних ліній на подушечці	в роботі слідчого цей метод дозволяє швидко і точно встановити особу, якщо

пальців	пальця (після отримання зображення відбитка за допомогою спеціального сканера формується цифровий код, який потім порівнюється зі зразковим значенням у базі даних).	її відбитки є у відповідній базі (відбитки пальців, знайдені на місці злочину, можуть бути використані для зіставлення з даними підозрюваних, що допомагає у встановленні причетності або усуненні осіб із кола підозрюваних)
Ідентифікація особи за рисами обличчя	цей метод здійснюється за допомогою камери та спеціального програмного забезпечення (програма виділяє контури таких основних елементів обличчя, як очі, брови, ніс, губи, вуха та підборіддя, і на основі обраного алгоритму вимірює відстані між ними; отримане зображення конвертується у цифровий формат і зберігається в базі даних як еталонний зразок)	в роботі слідчого ця технологія дає змогу швидко і точно ідентифікувати особу підозрюваного чи свідка, навіть якщо вони не мають документів (використовуючи такі еталонні зразки, можна знаходити збіги в наявних базах даних або ідентифікувати особу за записами з камер спостереження, що значно прискорює процес розслідування)
Ідентифікація особи за формою руки	цей метод базується на аналізі унікальної геометрії кисті (у цьому методі отримують тривимірне зображення руки, що враховує розмір долоні, довжину і ширину пальців, висоту та контури суглобів; це зображення фіксується за допомогою спеціальної ПЗЗ-камери з інфрачервоним підсвічуванням, що допомагає чітко відобразити рельєф кисті)	для слідчого такий метод стає корисним, оскільки забезпечує можливість точно ідентифікувати особу на підставі унікальних біометричних даних (це сприяє швидкому підтвердженню або виключенню причетності людини до місця злочину чи до наданих доказів, а також є надійним інструментом для побудови доказової бази у кримінальних справах)
Ідентифікація особи на основі характеристик ока	цей метод ґрунтується на використанні двох унікальних складових: райдужної оболонки та сітківки (їхня структура є настільки ж індивідуальною, як і інші унікальні риси людського тіла)	цей метод допомагає слідчим у розслідуванні злочинів, оскільки сканування райдужної оболонки та сітківки дозволяє точно встановити особу (така ідентифікація може бути особливо корисною у разі переві-

		рки підозрюваних, ідентифікації невідомих осіб або підтвердження наявності особи у базах даних, оскільки ці біометричні дані практично неможливо підробити або змінити)
Ідентифікація особи за розташуванням вен на поверхні долоні	цей метод здійснюється за допомогою інфрачервоної камери, яка зчитує унікальний візерунок вен на зовнішньому боці долоні або пальців (отримане зображення проходить обробку, і на основі схеми розташування вен створюється цифровий відбиток)	для слідчого це має велике значення, оскільки така технологія забезпечує високоточну ідентифікацію особи, навіть якщо традиційні методи, як-от відбитки пальців, не підходять (це особливо корисно в розслідуваннях, де потрібна додаткова перевірка для підтвердження особи, що сприяє прискоренню процесу розкриття злочину)
Ідентифікація особи за допомогою ДНК	цей метод дає можливість встановити особу потерпілого, злочинця за зразками крові, сперми, шкіри, слини або волосся, знайденими на місці події (ДНК-аналіз вважається одним із найбільш точних методів розслідування, який дозволяє майже зі стовідсотковою впевненістю визначити особу та її причетність до злочину; цей метод допомагає слідчому отримати переконливі докази для доведення вини, а також має значний потенціал для розшуку зниклих безвісти осіб, ідентифікації невпізнаних тіл та встановлення особистості жертв у випадках катастроф на транспорті тощо)	слідчому такий аналіз надає точні наукові дані, що зміцнюють доказову базу, дозволяючи ідентифікувати або усунути особу зі списку підозрюваних, встановити зв’язок особи з місцем злочину, а також підтвердити особисті дані, що суттєво прискорює процес розкриття злочинів

Таблиця 1.10 – Динамічні методи біометричної ідентифікації особи

Методи ідентифікації	*Опис*	*Примітки*
Ідентифікація за рукописним почерком	цей метод базується на аналізі почерку (підпису), що охоплює графічні особливо-	ця технологія є інструментом для підтвердження особи або встановлення автен-

	сті, час його виконання, а також силу й динаміку натискання на поверхню, де підпис здійснюється (для цього методу використовують спеціальні планшети або сенсорні екрани)	тичності підпису, що може бути важливим доказом (індивідуальні характеристики, як-от ритм і сила натискання, значно ускладнюють підробку, що підвищує надійність отриманої інформації)
Ідентифікація особи за голосом	цей метод базується на створенні унікального коду, що формується завдяки поєднанню частотних і статичних характеристик голосу людини (коли користувач знову звертається до системи, цей код порівнюється з раніше збереженим зразком голосу, що дозволяє підтвердити його особу)	такий метод особливо корисний для слідчих, оскільки він дозволяє точно ідентифікувати особу навіть на значній відстані (це може бути застосовано у ході перехоплення телефонних розмов, спостереження чи в ході спеціальних операцій, коли важливо визначити, хто саме говорить, без візуального контакту)
Ідентифікація за клавіатурним почерком	цей метод ґрунтується на використанні комп'ютерної клавіатури для введення певного ключового слова (головною характеристикою, що створює унікальний зразок, є динаміка натискання клавіш під час введення цього слова)	ця технологія може допомогти слідчому ідентифікувати підозрюваного за унікальним стилем набору тексту, оскільки ритм і швидкість натискання клавіш є індивідуальними для кожної людини (це може бути корисним у ході розслідування кіберзлочинів, де підозрюваний залишив цифрові сліди або в ході віддаленого спостереження, оскільки навіть при зміні пристрою характерний набір тексту часто залишається сталим)

Також варто зазначити, що використання біометричних систем ідентифікації особи передбачає порівняння раніше збереженого біометричного зразка з новими даними. Принцип роботи таких систем базується на типових алгоритмах, які можна описати такими етапами:

– *запис* (фізичні чи поведінкові характеристики особи фіксуються в системі);

– *виділення шаблону* (зі зразка виокремлюються унікальні характеристики, які формують біометричний шаблон);
– *порівняння* (збережений шаблон зіставляється з новими даними);
– *збіг або незбіг* (система визначає відповідність даних і приймає рішення).

Ця технологія ґрунтується на алгоритмі, наприклад, який переводить зображення в цифровий формат, здійснюючи пошук обличчя в кадрі та виокремлюючи його характерні риси – так звані «реперні точки» (форма очей, лінія вилиць, ширина носа тощо). Унікальна комбінація близько 40 ключових ознак достатня для точної ідентифікації, хоча система аналізує ще більше параметрів, що дозволяє створити точний цифровий опис обличчя. Потім цей опис разом із фотографією зберігається в базі даних для подальшого пошуку.

Для слідчого така система є надзвичайно корисною, оскільки дозволяє швидко і точно ідентифікувати особу, що сприяє встановленню особистості підозрюваних, свідків або інших учасників справи. Завдяки базі біометричних даних та автоматизованому порівнянню, розслідування злочинів значно прискорюється, а ризик помилок в ідентифікації мінімізується. Це робить процес розслідування точнішим та ефективнішим.

РОЗДІЛ 2 ТЕХНІКО-КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

2.1 Поняття та види техніко-криміналістичних засобів, що застосовуються у ході розслідування 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 потрібно використовувати визначальні елементи поняття кіберзлочину, не динамічні, а відносно постійні [11]. Це зумовлено 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 мають спеціальних знань [12].

Наприклад, у ході досудового розслідування кіберзлочинів, пов'язаних із створенням, розповсюдженням або збутом шкідливих програм, криміналістичне версіювання являє собою поєднання кількох видів цього процесу. Це охоплює як версії, що стосуються формату, методів і способів створення шкідливого програмного (технічного) засобу, так і традиційні підходи до версіювання, що охоплюють обставини, події та факти, які спонукали особу до вчинення правопорушення, а також ситуацію, в якій воно відбулося, та інші «позакібернетичні» чинники.

Це доводить, що кіберзлочини мають здебільшого латентний характер та є складними для виявлення та розкриття. Як практичну допомогу (на початковому етапі розслідування) О. Мотлях [13] пропонує враховувати типові слідчі ситуації, що можуть скластися (табл. 2.1).

Таблиця 2.1 – Типові слідчі ситуації при розслідуванні кіберзлочинів

Ситуаційні дані	*Особливі примітки*
Встановлено випадок несанкціонованого доступу до інформації, яка обробляється в банківському або кредитно-фінансовому секторі	проте немає інформації про метод здійснення злочину та осіб, які до нього причетні
Виявлено факт внесення будь-яких коригувань у комп’ютерні дані	за такої умови спосіб доступу до баз даних не встановлено або має непрямий характер, а особа, яка вчинила злочин, залишається невідомою
Виявлено факт внесення будь-яких коригувань у комп’ютерні дані	зафіксовано метод доступу до баз даних та окремих програм, а також встановлено ймовірну особу злочинця

Виявлено факт інтеграції шкідливих або небезпечних вірусних програм у програмне забезпечення або окремі файли	спосіб зараження та особа правопорушника залишаються невизначеними
Зафіксовано випадок знищення інформації в комп'ютерній системі	проте немає інформації про метод здійснення злочину та осіб, які до нього причетні
Зафіксовано випадок викрадення або заволодіння комп'ютерною інформацією	при цьому спосіб доступу до баз даних не встановлено або має непрямий характер, а особа, яка вчинила злочин, залишається невідомою
Зафіксовано випадок модифікації бази даних або зміни інформації в окремих програмних файлах	існують відомості щодо способу вчинення злочину та ймовірного злочинця

Водночас, наведені вище слідчі ситуації (табл. 2.1) мають характер вихідних міркувань. Наприклад, якщо звернути увагу лише на кіберзлочин, передбачений ст. 361-1 КК України, то можна на базі вихідних слідчих ситуацій сформулювати слідчі версії (в межах ознак вказаного злочину).

Таблиця 2.2 – Типові слідчі версії при розслідуванні кіберзлочинів, пов'язаних із ШПЗ [12]

Слідча версія	*Особливі примітки*
виявлено факт ШПЗ	відомі дані про: несанкціоноване втручання комп'ютерних програм у функціонування операційної системи комп'ютера/комп'ютерів або окремих програм; докази такого втручання; підозрюваних, які надають правдиві свідчення
	відомі дані про: несанкціоноване втручання комп'ютерних програм у функціонування операційної системи комп'ютера/комп'ютерів або окремих програм; докази такого втручання; підозрюваних, які заперечують свою вину, і можливість доведення їх провини ускладнена через неможливість перевірити їхні свідчення
	встановлено факт шкідливого впливу програмного забезпечення на операційні системи комп'ютера/комп'ютерів або окремі програми; є докази вчинення злочину; визначені особи, які можуть мати інтерес у здійсненні шкідливого комп'ютерного впливу та відповідальні за забезпечення комп'ютерної безпеки, однак обставини злочину не з'ясовані
	встановлено факт шкідливого програмного впливу на операційні системи комп'ютера/комп'ютерів або окремі комп'ютерні програми; сліди відсутні; особи, підозрювані у вчиненні злочину, не встановлені

Таким чином, обумовлені слідчі ситуації при розслідуванні кіберзлочинів забезпечують способи та методи першочергових слідчих дій: 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 має мати контроверсію. Важливо, щоб як слідча ситуація, так і висунуті версії дозволяли їх об'єктивну перевірку з метою підтвердження або спростування.

Як слушно 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 зберігання, збирання, дослідження можливе лише за допомогою ЕОТ [14].

В сучасній 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 основних цілей (які CAINE прагне гарантувати) відомо, що:

– його операційне середовище розроблено таким чином, щоб забезпечити всі потрібні криміналістичні інструменти для виконання процесів цифрового криміналістичного розслідування, таких як збирання, зберігання, дослідження та аналіз;
– він забезпечує зручний графічний інтерфейс користувача з дружніми криміналістичними інструментами;

– він може завантажуватися з таких знімних носіїв, 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, то 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. 2.3).

Таблиця 2.3 – 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-фільтрацію, - аналітику 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 мовою 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 збирання 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 проведено аналіз певних програмних та апаратних засобів для дослідження комп'ютерної техніки та програмних продуктів (табл. 2.4–2.9).

Таблиця 2.4 – Результати аналізу апаратних засобів мобільної криміналістики

Найменування засобу	*Аналіз засобу*	*Особливі примітки*
Cellebrite UFED Touch 2 [17]	концептуально розділений на дві частини: - планшет Cellebrite UFED Touch 2 (або програмний аналог UFED 4PC, що встановлюється на комп'ютер чи ноутбук фахівця), який використовується виключно для отриман-	- концепція використання обладнання передбачає, що фахівець отримує дані в польових умовах за допомогою Cellebrite UFED Touch 2, а потім проводить їх аналіз у лабораторії з використанням UFED Physical Analyzer;

	ня даних; - UFED Physical Analyzer - програмне забезпечення, призначене для аналізу даних, «витягнутих» з мобільних пристроїв	- лабораторний варіант складається з двох окремих програмних продуктів: UFED 4PC і UFED Physical Analyzer, які встановлені на комп'ютері дослідника; - цей комплекс дозволяє отримувати дані з максимально можливої кількості мобільних пристроїв
MSAB XR / MSAB XRY Field [18]	- аналогічний продукт до Cellebrite, який розробляється шведською компанією MicroSystemation; - на відміну від парадигми Cellebrite, компанія MicroSystemation передбачає, що їхні продукти в основному будуть використовуватися на стаціонарних комп'ютерах або ноутбуках; - до продукту додається фірмовий USB-хаб, який у неформальному середовищі називають «шайбою», а також комплект перехідників і дата-кабелів для підключення різних мобільних пристроїв	- також були розроблені версії апаратних продуктів, що призначені для отримання даних з мобільних пристроїв, у вигляді планшета та кіоску; - MSAB XRY добре зарекомендував себе при отриманні даних із «застарілих» мобільних пристроїв; - завдяки закритій конфігурації та автоматичному веденню журналу аудиту, MSAB Kiosk допомагає виконувати вимоги стандартів ISO 17025 та 27037:2012
Набір адаптерів польської компанії Rusolut [19]	засоби для здійснення chip-off (метод отримання даних безпосередньо з чипів пам'яті мобільних пристроїв).	- за допомогою цього обладнання можна отримувати дані з пошкоджених мобільних пристроїв або пристроїв, захищених PIN-кодом чи графічним паролем; - Компанія Rusolut пропонує кілька комплектів адаптерів для «витягування» даних з певних моделей мобільних пристроїв (наприклад, набір адаптерів для отримання даних з чипів пам'яті, що в основному використовуються в мобільних телефонах китайського виробництва)

Таблиця 2.5 – Результати аналізу програмних засобів мобільної криміналістики

Програмний засіб	Аналіз засобу	Особливі примітки
Мобільний криміналіст	- це одна з найкращих програм для аналізу даних, що були отримані з мобільних пристроїв; - інтегровані переглядачі для баз даних SQLite і plist-файлів дозволяють більш детально досліджувати конкретні SQLite-бази даних та plist-файли вручну	- однією з особливостей програми є сувора прив'язка шляхів, за якими зберігаються файли (бази даних додатків); - тобто, якщо структура бази даних програми не змінилася, але змінився шлях до цієї бази даних у мобільному пристрої, «Мобільний криміналіст» не зможе її виявити у ході аналізу; - тому для дослідження таких баз даних потрібно проводити аналіз вручну, використовуючи файловий браузер «Мобільного криміналіста» і додаткові утиліти
*Magnet AXIOM (*програма канадської компанії) [20] Magnet Forensics *Belkasoft Evidence Center* (розробка компанії Belkasoft) [21]	- у списку програм для мобільної криміналістики ці програми займають гідне місце; - хоча за функціональними можливостями щодо отримання даних з мобільних пристроїв ці програми дещо поступаються програмним та апаратним засобам, згаданим раніше, вони ефективно справляються з аналізом даних і можуть бути використані для перевірки повноти вилучення різних типів даних	- обидві програми активно удосконалюються та швидко розширюють свої можливості в дослідженні мобільних пристроїв

Таблиця 2.6 – Результати аналізу апаратних блокаторів запису

Найменування засобу	Аналіз засобу	Особливі примітки
Tableau T35U [22]	- апаратний блокатор компанії Tableau дозволяє безпечно підключати досліджувані жорсткі диски до комп'ютера дослідника за допомогою шини USB3	- цей блокатор оснащений роз'ємами для під'єднання жорстких дисків через інтерфейси IDE та SATA (а також за допомогою перехідників може підтримувати жорсткі диски з іншими інтерфейсами); - особливістю цього блокатора є здатність емуляції операцій «читання-запис»; - це може бути корисним у ході дослідження накопичувачів, що заражені шкідливим програмним забезпеченням
Wiebitech Forensic UltraDock v5 [23]	- апаратний блокатор компанії CRU має функціонал, аналогічний блокатору Tableau T35U	- цей блокатор також можна підключити до комп'ютера дослідника через більше кількість інтерфейсів; - якщо до блокатора підключено жорсткий диск, доступ до даних якого обмежено ATA-паролем, на дисплеї з'явиться відповідне повідомлення; - крім того, при підключенні жорсткого диска з технологічною зоною DCO (Device Configuration Overlay), ця зона буде автоматично розблокована, щоб фахівець міг скопіювати дані, що знаходяться в ній

Таблиця 2.7 – Результати аналізу програмних засобів комп'ютерної експертизи

Програмний засіб	Аналіз засобу	Особливі примітки
Encase Forensics [24]	- має високу ефективність у випадках, коли потрібно досліджувати комп'ютери з операційною системою MacOS або сервери під керуванням Linux; - допомагає «витягувати» дані з файлів рідкісних форматів, що робить його	- у Encase Forensics макроси Enscripts мають велику бібліотеку готових скриптів, створених як розробниками, так і ентузіастами, які дозволяють проводити аналіз різних операційних та файлових систем

	корисним для таких «нестандартних» ситуацій.	
Access Data FTK [25]	- створює умови для підтримки потрібної функціональності продукту, однак час, потрібний для обробки накопичувачів, значно перевищує розумні межі, які фахівець може дозволити собі витратити на таке дослідження	До особливості Access Data FTK відносять: високий рівень реалізації пошуку за ключовими словами; аналітика кейсів, що дозволяє знаходити взаємозв'язки між даними з різних справ; можливість персоналізації інтерфейсу програми; підтримка таких рідкісних форматів файлів, як бази даних Lotus Notes; Encase Forensics та AccessData FTK здатні обробляти величезні обсяги даних, які можуть досягати сотень терабайт
Magnet AXIOM [20]	- ця програма охоплює цілу низку функціональних можливостей: дослідження мобільних пристроїв, «витягування» даних з хмарних сховищ, аналіз механізмів під управлінням операційної системи MacOS та інше	- програма має інтуїтивно зрозумілий і функціональний інтерфейс, де все необхідне доступне, і може бути використана для розслідування інцидентів інформаційної безпеки, зокрема тих, що пов'язані з зараженням комп'ютерів або мобільних пристроїв шкідливим програмним забезпеченням або витоками даних
Belkasoft Evidence Center [21]	- програма дозволяє «витягати» та аналізувати дані з мобільних пристроїв, хмарних сховищ і жорстких дисків; - у ході аналізу жорстких дисків здійснюється вилучення даних із веббраузерів, чатів, інформації про хмарні сервіси, детектування зашифрованих файлів і розділів, «витягування» файлів за заданим розширенням, даних про геолокацію, електронну пошту, інфо-	Переваги програми Belkasoft Evidence Center такі: - широкий спектр даних із різних носіїв інформації; - вмонтований переглядач баз даних SQLite; - збирання даних із віддалених комп'ютерів і серверів; - інтегрований функціонал для перевірки виявлених файлів на Virustotal. Недоліки програми: - незручний інтерфейс і неочевидність виконання окремих дій; - для ефективного використання

	рмації з платіжних систем і соціальних мереж, мініатюр, системних файлів, системних журналів тощо; - має гнучкий функціонал для вилучення віддалених даних	програми потрібне спеціальне навчання
X-Ways Forensics [26]	- особливістю цієї швейцарської програми є висока швидкість обробки даних порівняно з іншими програмами цієї категорії та оптимальний функціонал, що задовольняє основні потреби фахівців з комп'ютерної криміналістики; - програма має вбудований механізм, який дозволяє зменшити кількість хибнопозитивних результатів (тобто, у разі відновлення файлів із жорсткого диска обсягом 100 Гб, дослідник не бачить 1 Тб відновлених файлів, більшість з яких є хибнопозитивними, як це зазвичай буває з програмами відновлення, а лише файли, що дійсно були відновлені)	За допомогою програми X-Ways Forensics можна: - знаходити та аналізувати дані електронної пошти; - аналізувати історію веб-браузерів, журнали ОС Windows та інші системні артефакти; - фільтрувати результати, залишаючи лише цінні та актуальні відомості; - будувати тимчасову шкалу та переглядати активність у заданий період; - реконструювати RAID; - монтувати віртуальні диски; - перевіряти на наявність шкідливого програмного забезпечення; - програма добре зарекомендувала себе в ручному аналізі жорстких дисків, витягнутих із відеореєстраторів; - завдяки функціоналу X-Tension, є можливість підключення модулів сторонніх розробників До недоліків X-Ways Forensics відносять: - аскетичний інтерфейс; - відсутність повноцінного вбудованого переглядача баз даних SQLite; - необхідність глибокого вивчення програми; - деякі дії, потрібні для отримання результату, не завжди очевидні

Таблиця 2.8 – Результати аналізу апаратних засобів відновлення даних

Апаратний засіб	Аналіз засобу	Особливі примітки
ACELab [27]	- апаратні засоби для аналізу, діагностики та відновлення даних з жорстких дисків містять комплекси, такі як PC-3000 Express, PC-3000 Portable, PC-3000 UDMA та 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)	Лідерство компанії ACELab на ринку апаратних рішень для відновлення даних зумовлене високою якістю її продукції та ціновою політикою, що ускладнює конкуренцію для інших гравців на цьому ринку

Таблиця 2.9 – Результати аналізу програмного забезпечення

Програмне забезпечення	Аналіз забезпечення	Особливі примітки
Autopsy [28]	- зручний інструмент для аналізу комп'ютерів, що працюють на операційній системі Windows, а також мобільних пристроїв на базі операційної системи Android, з графічним інтерфейсом	може бути використаний у розслідуванні комп'ютерних інцидентів
Photorec [29]	- одна з найкращих безкоштовних програм для відновлення даних	
Eric Zimmerman Tools [30]	- набір безкоштовних утиліт, кожна з яких дозволяє досліджувати окремий артефакт Windows; - як показала практика, використання Eric Zimmerman Tools підвищує ефективність роботи фахівця у разі реагування на інциденти в «польових умовах»	Зараз ці утиліти доступні у вигляді пакета програм Kroll Artifact Parser and Extractor (KAPE)

2.2 Теоретико-множинні моделі категорій кіберінцидентів та найпоширеніших кіберзлочинів

У 2021 році Кабінет Міністрів України затвердив Положення про організаційно-технічну модель кіберзахисту [31]. Це Положення було прийнято на виконання статті 8 Закону України «Про основні засади забезпечення кібербезпеки України» [32].

Згідно з цим Положенням 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 [33] базується 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 [34].

Тобто, програмний продукт SIEM (*Security information and event management*) здатний в реальному часі виконувати великий спектр задач, зокрема: отримувати інформацію від мережних пристроїв; здійснювати генерацію звітів про отримані дані задля сумісності з іншими базами даних (табл. 2.10) [35].

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 широке поняття, а кіберпростір – є однією з його ознак.

Кіберзлочини вчиняються у кіберпросторі, і вони є реальними, а не уявними. Сліди кіберзлочинів в кіберпросторі за допомогою ЕОТ стають відомими та досліджуваними.

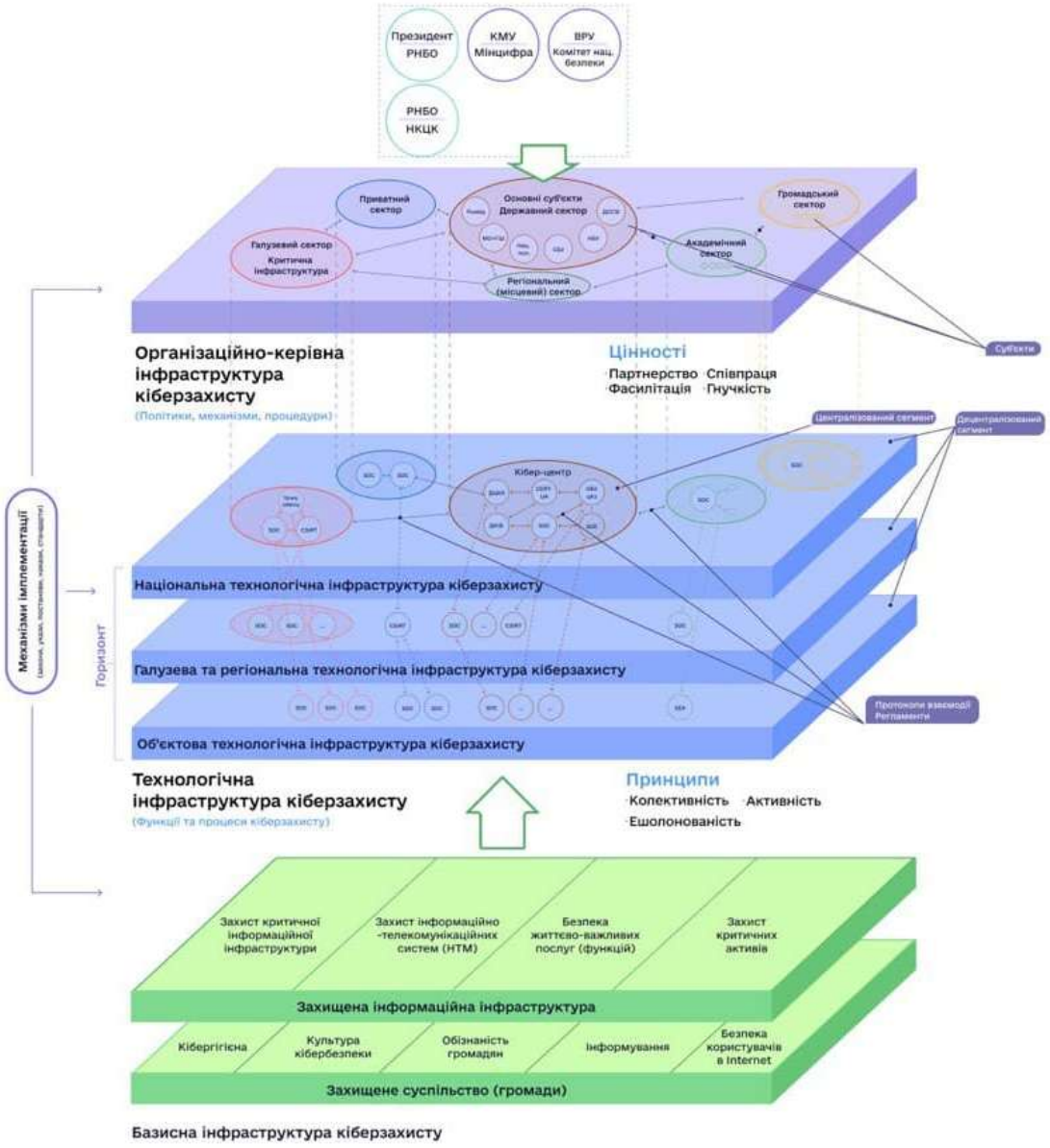

Рисунок 2.1– Архітектура організаційно-технічної моделі кіберзахисту [33]

Таблиця 2.10 – Характеристика SIEM-системи [35]

Структура системи	Задачі системи	Механізми системи
Управління інформаційною безпекою Управління подіями безпеки	збирання, обробка т аналіз подій безпеки що надходять до не з множини різнорід них розподілени джерел	нормалізація, фільтрація, класифіка ція, агрегація, кореляція, пріоритеза ція та аналіз подій і кіберінциденті та їх наслідків, а також генерація рі номанітних звітів, повідомлень і візу ального подання даних для операти ного та обґрунтованого прийнятт рішень

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

- *відмінність в суб'єктному складі* (кіберзлочини – розслідують слідчі та інші особи згідно з кримінально-процесуальним законодавством; кіберінциденти – ідентифікацію, виявлення, захист, відновлення тощо здійснюють команди реагування на комп'ютерні надзвичайні події (п. 6 Положення про організаційно-технічну модель кіберзахисту) [31];
- *не кожен кіберінцидент має ознаки кримінального правопорушення* (до слова, М. Кулешов [36] пропонує кіберінциденти поділяти (залежно від їх природи) на: 1) прості кіберінциденти (наприклад, в силу природних, технологічних факторів тощо); 2) ускладнені (наприклад, обставини, події зумовленні 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* (наприклад, за відсутності звернення потерпілого у формі приватного обвинувачення (ст. 477 КПК України) відсутні правові підстави для розслідування виявлених кіберінцидентів в яких є склади злочину, зокрема, передбачені частиною першої статті 361 та частиною першою статті 362 КК України; водночас, тут потрібно 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) [3; 4];
- *характер об'єкта правопорушення* (визначає підслідність кіберзлочину).

Таблиця 2.11 – Перелік категорій кіберінцидентів [37]

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	Розповсю-дження ШПЗ	Malware distribution	Розповсюдження ШПЗ, наприклад шляхом розсилання повідомлень електронною поштою, що містять вкладення з ШПЗ або посилання на його завантаження
		03	Командно-контрольний центр (C2)	Comma nd & Control (C2)	Система, яка використовується як точка керування та управління ботнетом та/або служить точкою для збору інформації, викраденої ботнетами
		04	Шкідливе під-ключення	Malicio us connecti on	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 інфор-мації зловмисником (Information Gathering)	01	Сканування	Scanning	Збирання інформації про системи або мережі
		02	Сніфінг	Sniffing	Несанкціоноване перехоплення (логічне або фізичне) та аналіз мережного трафіку. Несанкціонований моніторинг та зчитування мережного трафіку
		03	Фішинг	Phishing	Спроба збирання інформації про користувача чи систему за допомогою методів соціальної інженерії (масове розсилання електронною поштою спрямоване на збирання даних, може містити посилання на фішингові сайти)
04.	Спроби втручання (Intrusion Attempts)	01	Спроба експлуатації вразливості	Vulnera bility exploita tion 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 compro mise	Фактичне вторгнення в систему, компонент або мережу шляхом компрометації облікового запису користувача або адміністратора
		02	Компрометація системи	System compro mise	Фактичне вторгнення в систему чи її компоненту, сервісу, застосунку через використання вразливості в компоненті або мережі. Несанкціонований доступ до системи або ком-

					поненту 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 (табл. 2.11) буде мати такі теоретико-множинні моделі категорій та типів інцидентів (КТІ):

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

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

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

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

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

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

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

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

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

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

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

Також вважаємо, що потрібно перевіряти найпоширеніші передумови (обставини) за яких розповсюджуються (здійснюються, реалізуються) найбільш відомі кіберінциденти (кібератаки), наприклад: чи використовувалися комп'ютерні віруси щодо конкретної системи; чи були спроби взнати конфіденційну інформацію за допомогою фішингових листів; чи в інший спосіб була спроба компрометації даних (з метою проникнення в систему) [38].

В Конвенції Ради Європи про кіберзлочинність від 23.11.2001 року встановлено 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) [39].

Згідно з пунктом 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» [32].

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 [40]. Нині в Кримінальному кодексі України [4] передбачено низку злочинів, які вчиняються в кіберпросторі (відомості про найпоширеніші із них наведено в таблицях 2.12–2.19).

Таблиця 2.12 – Характеристика кіберзлочину, передбаченого статтею 190 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
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:

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

де *О.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 згідно з Переліком (див. табл. 2.11)

Таблиця 2.13 – 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 ггрошових 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 з Переліком (див. табл. 2.11)

Окремої уваги заслуговують кіберзлочини передбачені в Розділі XVI Кримінального кодексу України [4].

Таблиця 2.14 – 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	
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 – несанкціонований;	-	прямий умисел до діяння, умисел або необережн. до наслідків	-
ч. 2 ст. 361	те саме	те саме	-	-	спосіб – несанкціонований; обставини – вчинений повторно; або у спосіб - за попередньою змовою групою осіб	-	те саме	-
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 катаст-	те саме	-	те саме	-

				роф, загибелі або масового захворювання населення чи інших тяжких наслідків				
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:

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

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 з Переліком (див. табл.2.11)

Таблиця 2.15 – Характеристика кіберзлочину, передбаченого статтею 361-1 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. 361-1	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 з Переліком (див. табл. 2.11)

Таблиця 2.16 – Характеристика кіберзлочину, передбаченого статтею 361-2 Кримінального кодексу України

	Діяння	Предмет	Потерпілий	Наслідки	Місце, час, спосіб, засоби, знаряддя, обставини, ситуація	Суб'єкт	Форма вини	Мета, мотив, емоц. Стан
1	2	3	4	5	6	7	8	9
	збут або розповсю-	ЕОМ (комп'ю-					прямий уми-	мета –

ч. 1 ст. 361-2	дження інформації з обмеженим доступом	тери), автоматиз. системи, комп'ютерні мережі або носії такої інформації	-	-	спосіб – несанкціонований	-	сел до діяння, умисел або необережн. до наслідків	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'ютери), 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 з Переліком (див. табл. 2.11)

Таблиця 2.17 – Характеристика кіберзлочину, передбаченого статтею 362 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. 362	зміна, знищення або блокування інформації	ЕОМ (комп'ютери), 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 обробляється	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 обробляється	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:

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

де *О.362* – ознаки складу кіберзлочину

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

Пр.362 – предмет злочину – електронно-обчислювальні машини (комп'ютери), 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 з Переліком (див. табл. 2.11)

Таблиця 2.18 – Характеристика кіберзлочину, передбаченого статтею 363 Кримінального кодексу України

Стаття КК України	Ознаки складу злочину							
	Діяння	Предмет	Потерпілий	Наслідки	Місце, час, спосіб, засоби, знаряддя, обстановини, ситуація	Суб'єкт	Форма вини	Мета, мотив, емоційний стан
ч. 1 ст. 363	порушення правил експлуатації	правила експлуатації, порядок або правила захисту інформації	-	заподіяли значну шкоду	-	особ, яка відповідає за експлуптацію	умисел або необережність до діяння, необережність 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:

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

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 з Переліком (див. табл. 2.11)

Таблиця 2.19 – Характеристика кіберзлочину, передбаченого статтею 363-1 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. 363-1	масове розповсюдження повідомлень електрозв'язку	ЕОМ (комп'ютери), автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку	особа	порушення або припинення роботи ЕОМ (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:

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

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'ютери), 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 з Переліком (див. табл. 2.11)	

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

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

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 Моделі розслідування кіберзлочинів

Практичні аспекти дослідження дозволяють сфокусувати увагу на методології та аргументації щодо дослідження обставин із сфери кібернетичних функцій держави, а також, із використанням методів екстраполяції, навести власні підходи до процесу розслідування кіберзлочинів.

Також застосування прогностичного та сценарного підходів, методів моделювання та стратегічного прогнозування розвитку кіберзлочинності надало нам змогу сформулювати основні етапи розслідування кіберзлочинів.

При розслідуванні кіберзлочиннів потрібно враховувати засадниче правило захисту інформації: «*жодна система захисту не може довгий час протистояти цілеспрямованим діям озброєного сучасними технологіями кваліфікованого порушника*» [41]. Іншими словами, це правило має універсальний характер. Воно зумовлює те, що будь-яка система захисту має свої вразливості, і питання полягає: не в тому, чи буде зламана система – а коли це станеться? Отже, мета захисту інформації полягає в тому, щоб максимально віддалити момент потенційного злому. Проблема полягає не в тому, чи зловмисники подолають систему захисту, а в тому, коли саме це станеться. Основне завдання інформаційного захисту – забезпечити, щоб злам системи відбувся якомога пізніше.

При розслідуванні кіберзлочинів вищевказане універсальне правило потрібно враховувати в кореляції з основними завданнями захисту інформації: 1) запобігання витоку інформації з обмеженим доступом; 2) протидія технічним засобам розвідки; 3) охорона інформації з обмеженим доступом від несанкціонованих втручань у процесі її зберігання та обробки; 4) забезпечення захисту від цілеспрямованих впливів на інформацію; 5) гарантування цілісності та доступності відкритої інформації.

Сутність кримінально-правового захисту інформації, що обробляється в комп'ютерах, автоматизованих системах, комп'ютерних мережах або передається через канали електрозв'язку, базується на двох ключових аспектах: 1) з одного боку, така інформація розглядається як об'єкт власності; 2) з іншого боку, важливими є її зміст, корисність та здатність задовольняти інформаційні потреби конкретних користувачів.

Саме ці характеристики, на нашу думку, мають бути основою для визначення комп'ютерної інформації як предмета злочину.

Предметом злочинів, що стосуються використання інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем та мереж, є інформація, яка обробляється або передається через ці системи. Така інформація може бути як пов'язаною з засобами та знаряддями вчинення злочину, так і виступати безпосереднім об'єктом кримінально-правового захисту, характерного для конкретного виду злочину. Іншими словами, предметом злочину в кіберпросторі є інформація, яка має особливі ознаки, що роблять її важливою стосовно кримінального права.

Таблиця 2.20 – Основні етапи інформаційного процесу

Етапи (дії)	Аналіз процесу (змісту)	Примітки
Створення інформації	- процес та/або інтелектуальна діяльність в результаті якої існують відомості, подані у вигляді сигналів, знаків, зву-	- нині термін «Інформація» залишається одним із дискусійних в наукових розвідках та практичній

	ків, рухомих або нерухомих зображень чи в інший спосіб (інформаційний продукт); - цифровізація за своєю суттю є процесом створення інформаційних продуктів або послуг у віртуальному середовищі, де їх відтворення на паперовому носії неможливе без втрати якості чи змісту (це відрізняється від оцифрування, яке полягає у перенесенні інформації на цифровий (електронний) носій)	сфері, а відтак: трактування терміна «Інформація» має різні значення за різних обставин
Збирання (пошук) інформації	- цілеспрямоване виявлення потрібної інформації в таких інформаційних ресурсах, як каталоги, довідники чи пошукові системи; - процес відбору в упорядкованому масиві тих повідомлень, які відповідають запитам користувача або містять потрібні дані (цей процес охоплює сукупність логічних і технічних операцій, спрямованих на пошук документів, відомостей, фактів чи даних, релевантних запиту); - виявлення первинної інформації за допомогою таких методів, як спостереження, вимірювання, опитування, анкетування чи тестування; - аналіз даних для виявлення елементів із заданими характеристиками; - послідовність дій пошуку, що повторюється для кожного елемента даних	- документальний пошук (пошук відомостей про документ, бібліографічний опис, анотація, реферат); - фактографічний пошук (пошук даних, фактів, характеристики приладів, властивостей, матеріалів тощо) ДСТУ 2228-93 Підготовлення та оброблення даних. Терміни та визначення (ISO/IEC 2382-6:1987)
Зберігання інформації	- зберігання *інформації* має гарантувати її захист від втрат, бути організоване та-	

	ким чином, щоб уникнути можливості втрати даних в ІС, що може статися через збої в програмному чи апаратному забезпеченні	
Обробка інформації	- процес виконання операцій з даними (зокрема, систематичне виконання різних маніпуляцій над ними); - процес обробки інформації можна розділити на технічну та наукову обробку (технічна обробка охоплює реєстрацію та облік надходження повідомлень, а також перевірку їх на дублювання в базі даних; наукова обробка передбачає інформаційний аналіз і синтез повідомлень, що є аналітико-синтетичною обробкою інформації)	обробка інформації в системі – це виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів (ЗУ «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 80/94-ВР)
Передавання інформації	- схема передачі інформації (у загальному вигляді): *джерело Інформації –* *канал передачі Інформації –* *приймач Інформації*	- каналами передачі *інформації* може бути будь-яка матерія або поле: електромагнітні поля (радіосигнали, світло тощо); електропровідники (передача електричних сигналів); пружні середовища (передача звукових, інфра-, ультразвукових сигналів); - вакуум або матеріальне середовище (розповсюдження елементарних частинок тощо); - приймачами (споживачами) *інформації* можуть бути люди, тварини, рослини, різного роду обладнання та машини
Поширення (розповсюджен-	- прийнято розрізняти два основні режими розповсю-	- до поточного поширення інформації можемо

ня) інформації	дження інформації (довідковий та поточний); - *довідковий режим* – передбачає доведення до користувача ретроспективної інформації, у відповідь на разовий запит; - *поточне поширення інформації* – надання користувачам інформації про нові надходження в систему, здійснюється масовими, груповими та індивідуальними методами (інформаційне обслуговування)	віднести *вибіркове розповсюдження інформації* – дозволяє оперативно, систематично та диференційовано задовольняти інформаційні потреби фахівців згідно з їх постійними запитами
Використання інформації	- в практиці інформаційної діяльності визначають такі різновиди *системи використання інформації*: диференційоване використання; тематичне обслуговування; проблемно-орієнтоване використання інформації	
Захист інформації	- вжиття заходів для уникнення втрати, пошкодження або несанкціонованого використання інформації	*«захист інформації в системі* – це діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі» (ЗУ «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 80/94-ВР)
Знищення інформації	- це процес, внаслідок якого інформація повністю зникає з усіх матеріальних носіїв і не може бути відновлена	

Таблиця 2.21 – Особливі властивості інформації як об’єкта суспільних відносин

Ознака	*Аналіз процесу (стану)*
Автономність змісту інформації від	- одна й та сама інформація може бути збережена або передана за допомогою різних носіїв, а різні ви-

її носія	ди інформації можуть бути зафіксовані чи поширені через один і той самий носій
Потенціал використання інформації	- одна й та сама інформація може використовуватися багато разів однією особою або необмеженою кількістю осіб протягом невизначеного періоду часу
Збереження інформації	- *цифрова інформація*, що передається через мережу, залишається у володінні того, хто її передає; - цифровізація є процесом *створення* інформаційних продуктів (послуг) у віртуальному просторі, водночас їх перенесення на паперовий носій неможливе без втрати змісту, що відрізняє її від оцифрування – процесу перенесення інформації на цифровий (електронний) носій
Інформація надається (поширюється) як інформаційний продукт	- *інформаційними продуктами* можуть бути різні форми даних (такі як повідомлення, документи, листи, звіти, книги, статті, збірники, фільми, бази даних, бібліотеки, архіви тощо)
Інформація може бути відтворена та поширена у безлічі примірників без змінення її змісту	- один і той самий зміст *інформації* може бути відомий необмеженій кількості осіб одночасно
Одночасності інформації	- *інформація (інформаційний продукт)* є результатом специфічного виду людської діяльності – інтелектуальної (водночас однакові результати можуть бути досягнуті кількома особами незалежно одна від одної та в різних місцях)
Ресурсності інформації	- будь-яка *інформація* може слугувати ресурсом для створення нової інформації (на основі отриманих даних можливо генерувати нові відомості та знання); - водночас *вихідна інформація* не зазнає змін і не зникає (її ресурсні властивості залишаються незмінними; ця особливість інформації є основою пізнавальної діяльності людини)
Змінність споживчих властивостей інформації залежно від умов її використання	- рівень споживчих властивостей інформації є *суб'єктивним* і залежить від новизни, змістовності, актуальності, достовірності та корисності інформації для конкретного споживача в певний момент часу; - споживчі властивості інформації не залежать від кількості осіб, яким вона була передана для використання
Обмеженості доступу до інформації	- *інформація* може мати різні режими доступу залежно від її змісту, що визначає певні обмеження в

	процесах створення, зберігання, поширення, використання, захисту та знищення
Повноти інформації	- споживча властивість інформації полягає в здатності задовольняти потреби споживача щодо обсягу наданих відомостей у конкретний момент часу
Своєчасності інформації	- передача інформації споживачу в потрібний момент часу
Вірогідності інформації	- споживча властивість інформації полягає в її відповідності або несуперечності подіям, явищам та фактам

Таблиця 2.22 – Поширені пастки шахраїв у соцмережах та їх розслідування

Засадничі рекомендації з кібергігієни яких особа має дотримуватися та знати про шахрайські ситуації	*Збирання оперативної інформації в ході розслідування (через відповіді на запитання)*
Критичне ставлення до будь-яких повідомлень, запитань, пропозицій тощо. Наприклад, мають насторожити такі фрази, (на які найчастіше реагують споживачі інтернету): - ваші фінансові рахунки заблоковані, введіть дані картки для розблокування; - збираємо гроші на дрон (каски, одяг, їжу), надішліть певну суму; - вітаємо, як постійний покупець нашого супермаркету, ви виграли телефон/комп'ютер/автомобіль/квартиру за нашою акцією; - система вашого комп'ютера незахищена, оновіть антивірус; - ваші документи на власність видалені з реєстру, завантажте їх заново; - помилка з нарахуванням заробітної плати, для підтвердження вкажіть дані паспорта та банківської картки	- чи надходили будь-які пропозиції від незнайомців (коли, де та які)?
не панікуйте і не поспішайте виконувати те, про що вас просять або навіть вимагають	- чи просили вас робити щось за допомогою гаджета (коли, де та як)?
будьте обережні з незнайомими посиланнями та вкладеннями – не відкривай-	- чи надходили на ваші гаджети підозрілі посилання, вкладення

те їх без вагомої причини	тощо (коли, де та які)?
уникайте роботи з персональними даними в присутності незнайомих осіб, особливо коли йдеться про реквізити карток (номер, термін дії, CVV-код, пін-код), паролі для онлайн-банкінгу чи інші паролі та коди, отримані через СМС	- чи працювали в присутності незнайомців з персональними даними, реквізитами банківських карток тощо за допомогою гаджета (коли, де та як)?
встановіть та оновлюйте антивірус	- якими антивірусними програмами користуєтесь?
створюйте окремі паролі для доступу до особистої та корпоративної електронної пошти, соціальних мереж і банківських додатків тощо	- як часто змінюєте паролі при виході в кіберпростір через соцмережі, електронну пошту, банківську систему тощо?
існують ситуації, коли шахраї заздалегідь надсилають повідомлення з фальшивими номерами телефонів і контактами, що нібито належать службі підтримки; й надалі, вони навмисно викликають проблеми на комп'ютері жертви, чекаючи, коли вона звернеться за допомогою	- чи доводилося вам отримувати повідомлення з телефонами й контактами, нібито від служби підтримки? - чи зверталися ви за отриманими номерами телефонів чи інших контактів? (причини для звернення)

Таблиця 2.23 – Запитання про міждисциплінарні знання підозрюваного (обвинуваченого), свідка при розслідуванні кіберзлочинів

Статус особи	*Орієнтовні питання у процесі збиранні інформації про передумови та вчинення кіберзлочину, а також про способи отримання, приховування інформації*	*Примітки*
Підозрюваний (обвинувачений), свідок	- яку частку у вашій діяльності (роботі) займають інформаційні процеси? - наскільки стандартна та програмована ваша діяльність (робота)? - який рівень абстрактного мислення потрібно мати для вашої праці? - який доступ до інформаційних ресурсів у вас був за останні 6 місяців? - які джерела інформації,	- під інформаційними процесами тут слід розуміти створення, пошук, збирання, зберігання, обробку, використання, поширення, пересилання, захист та знищення інформації; - загальні права та обов'язки підозрюваного (обвинуваченого) передбачені в ст. 42 КПК України;

	на вашу думку, є достовірними та чому? - яке ваше ставлення до інформатизації суспільства та чому?	- права та обов'язки свідка передбачені в ст. 66 КПК України

Таблиця 2.24 – Основні способи захисту інформації та особливості їх дослідження при розслідуванні кіберзлочину

Вид захисту інформації	*Зміст захисту інформації*	*Обставини (факти) зумовлені розслідуванням кіберзлочину*
Технічний захист інформації	- «діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації» [42] - «вид захисту інформації, спрямований на забезпечення, за допомогою інженерно-технічних заходів та/або програмних і технічних засобів, унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації» [43]	- які існують обмеження для автентифікації в комп'ютерній системі в ході розслідування? - чи існують обмеження конкретними апаратними конфігураціями? - який вид програмного забезпечення (власницький чи вільний)? - чи забезпечувала криптосистема належний рівень захищеності інформації, що обробляється, зберігається та/або передається? - які засоби криптографічного захисту інформації зазнали впливу (втручання, пошкодження тощо)?
Криптографічний захист інформації	- «вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо» [44]	
Інженерний (фізичний) захист інформації	- запобігання пошкодженню носія інформації через навмисні дії або природні впливи за допомогою інженерно-технічних засобів (до яких належать обмежуваль-	

	ні конструкції, охоронно-пожежні системи тощо); - застосування різноманітних механічних, електричних або електромеханічних пристроїв спеціального призначення для створення бар'єрів на можливих шляхах проникнення порушників, обмеження їх доступу до компонентів системи та захищеної інформації, а також містить засоби для візуального моніторингу, зв'язку та охоронної сигналізації	
Організаційний захист інформації	- запобігання доступу сторонніх осіб до об'єкта інформаційної діяльності через застосування організаційних заходів	- які організаційні заходи було впроваджено на об'єкті інформаційної діяльності?
Правовий захист інформації	- комплекс правових норм, які регулюють суспільні відносини, пов'язані з інформацією як суспільним ресурсом, та функціонування інформаційних систем з метою задоволення потреб і інтересів людини, суспільства, держави та міжнародної спільноти	- які суспільно небезпечні діяння містять ознаки кіберзлочину та їх попередня кваліфікація? - правові обмеження для з'ясування статусу програмного забезпечення є визначальними (вони містяться в ліцензіях на його використання)

Розслідування кіберзлочину (як дослідження проблеми) завжди розпочинається зі збирання вихідних даних за певними методами (табл. 2.25).

Таблиця 2.25 – 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 кіберп-	

	росторі (обладнання, пристрої, засоби, вузли, маршрутизатори, мережне обладнання, IMEI/IMSI тощо)	
ситуаційні дані	про які відомо електронні/ віртуальні сліди проблеми (інформація, що має сенс у ході розслідування, наприклад: чи є дані з телефонної книги; про SMS/MMS; чи є дані про надіслані 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, у ході огляду гаджета, ноутбука може виникнути потреба фіксації та збирання інформації про кіберзлочин з дотриманням вимог копіювання та зберігання 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 у процесі використання протоколів в сфері/змісті проблеми	топологія мереж та потік даних
програмне забезпечення використані утиліти (на етапі збирання вихідних даних)	важливо, застосовувати правильні засоби, методи, методологію у ході копіювання, досліджені ЕОМ, накопичувачів, трафіку тощо	

Отже, важливо на цьому етапі підготовчих дій – це брати до уваги, яка системоутворювальна сукупність засобів телекомунікації зумовлює про-

блему та які об’єкти беруть участь у інформаційній взаємодії. Тут варто врахувати, що «… кінцем (інтерфейсною точкою) телекомунікаційної мережі є або телекомунікаційний роз’єм, до якого під’єднано пристрій користувача (мережний інтерфейс), або кінцеве мережне обладнання, яке забезпечує з’єднання мереж (міжмережний інтерфейс)» [45]. (рис. 2.2)

Також враховується, що 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.

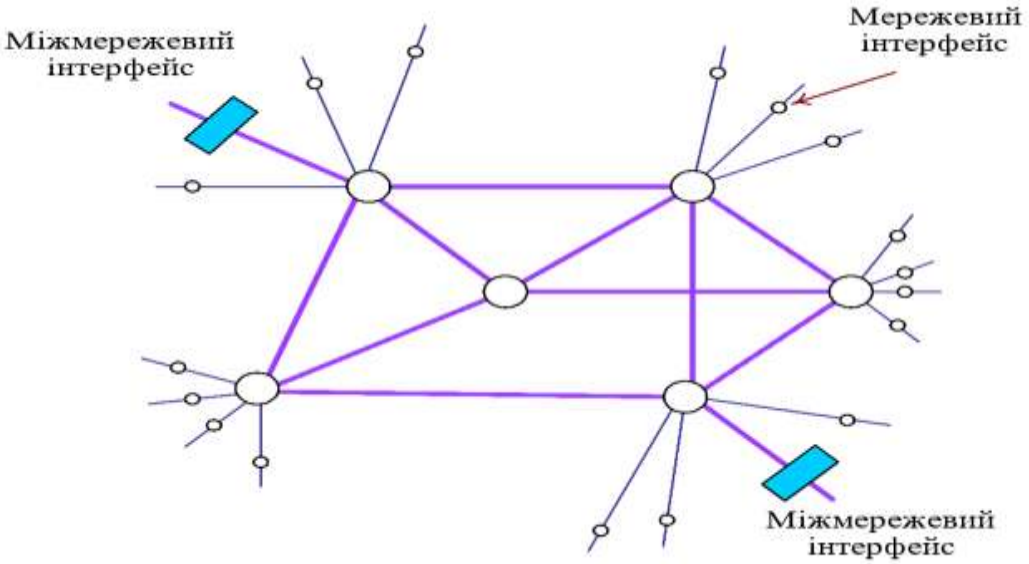

Рисунок 2.2 – Телекомунікаційна мережа [45]

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. 2.26). Перелік понять, які можуть обумовлювати тотожне міркування юристів і спеціалістів в сфері інформаційних технологій запозичений з доробку І. Канта [46].

Таблиця 2.26 – Перелік первісних чистих понять синтезу [46]

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

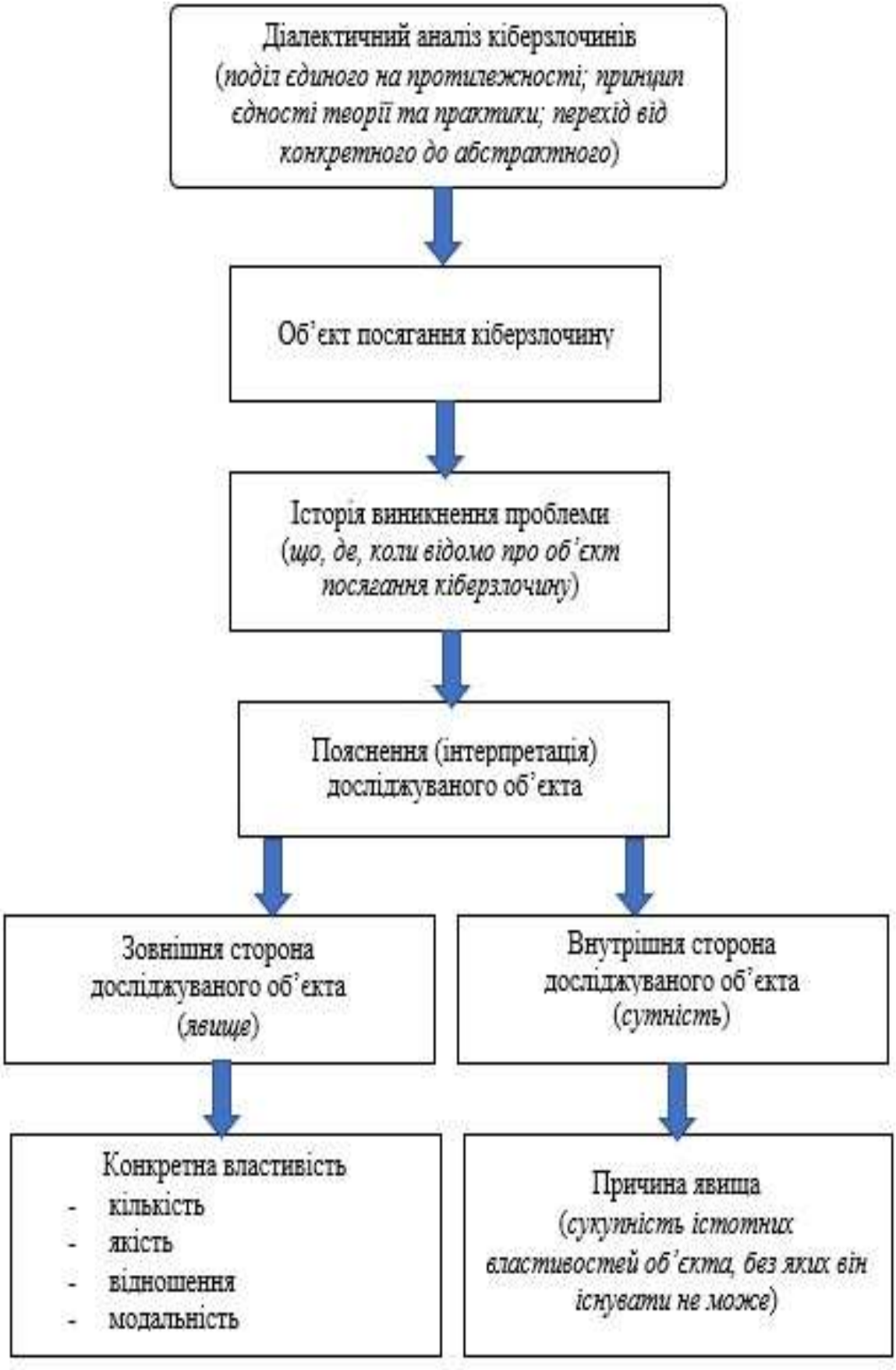

Рисунок 2.3 – Схема діалектичного аналізу кіберзлочинів

Таблиця 2.27 – Модель розслідування кіберзлочинів

Етапи	*Сутність процесу*	*Особливі примітки*
Виявлення проблеми	- з'ясування історії виникнення проблеми, ідентифікації/здобуття, фіксація, збирання та збереження електронних доказів (згідно з ознаками 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; - у ході розслідування, як правило, є протидія у встановленні обставин кіберзлочину	найперше керуються: КПК України
Стадія судового провадження	Особливе завдання, яким є вирішення кримінального провадження за суттю, тобто питання про винуватість обвинуваченого і про ступінь його відповідальності у	найперше керуються: КПК України

	випадку визнання винним (з'ясовуючи ці питання, суд здійснює правосуддя, а тому і завдання судового розгляду збігається з 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)	
Узагальнення досвіду (практичного матеріалу)	- проводять врахування досвіду правозастосування (на основі юридичних фактів, конкретних правових норм) та нової інформації про кіберінциденти від суб'єктів забезпечення кібербезпеки; - готують методичні рекомендації, щоб підвищити ефективність 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» [47].

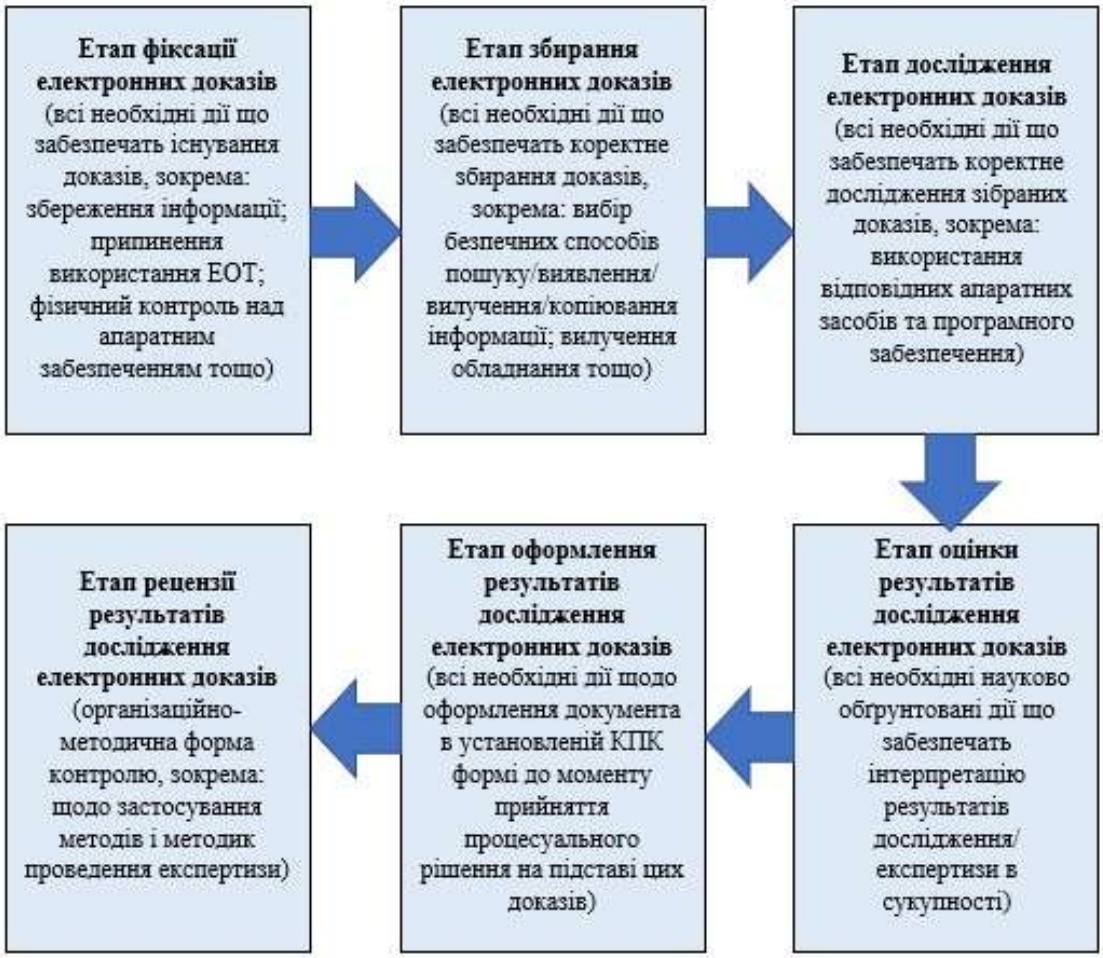

Рисунок 2.4 – Схема моделі роботи з електронними доказами при розслідуванні кіберзлочинів

Рисунок 2.5 – Схема покрокової моделі розслідування кіберзлочинів

РОЗДІЛ 3 ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ У ПРОЦЕСІ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

3.1 Види та можливості судових експертиз у ході розслідування кіберзлочинів

У вітчизняному законодавстві проведення судової експертизи в контексті розслідування кіберзлочинів регулюється такими актами: Кримінальним процесуальним кодексом України (ст. 69, 70, 101, 102, 232, 242-245, 518) [3]; Законом України «Про судову експертизу» від 25.02.1994 № 4038-XII [48]; Інструкцією про призначення та проведення судових експертиз та експертних досліджень, а також Науково-методичними рекомендаціями щодо підготовки та призначення судових експертиз від 08.10.98 № 53/5 [49]; Інструкцією щодо особливостей здійснення судово-експертної діяльності атестованими експертами, що не працюють у державних спеціалізованих установах від 12.12.2011 № 3505/5 [50]; Положенням про Експертну службу МВС України, затвердженим наказом МВС України від 03.11.2015 № 1343 [51].

В ході розслідування кіберзлочинів постає нагальна потреба 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 [52].

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 IT 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 найпоширеніших у ході досудового розслідування злочинів такої категорії. Її проведення дає змогу визначити статус об'єкта посягання (конкретного комп'ютерного пристрою) та детально дослідити його не лише з технічного, а й з функціонального боку, що забезпечує доступ до інформації, яку цей пристрій зберігає або обробляє.

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) [49] ***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)

Основні завдання експертизи	*Орієнтовний перелік вирішуваних питань*	*Особливі примітки*
- відновлення працездатності комп'ютерно-технічних засобів; - визначення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, даних і програмного забезпечення; - виявлення даних і програм, що зберігаються на комп'ютерних носіях; - перевірка відповідності програмних продуктів визначеним версіям або вимогам до їх розробки	- чи зберігається на цьому носії інформація, що стосується розслідуваних обставин (зазначити, яка саме інформація і в якому форматі)? - чи є на носії досліджуваного комп'ютера дані про певні (вказати які саме) дії користувача? - чи проходив досліджуваний накопичувач через процедури, спрямовані на знищення інформації? - чи могла бути створена вказана інформація на цьому комп'ютері, або вона була перенесена з іншого носія? - яким чином інформація (зазначити яка саме) була перенесена на досліджуваний комп'ютер (носій)? - яка технологія та хронологія створення електронного документа (зазначити документ та його зміст)? - які атрибути (час створення, редагування, друк, видалення тощо) файлів, що містять (зазначити зміст)? - чи містить накопичувач комп'ютера цього дослідження певне (зазначити, встановлене чи не встановлене) програмне забезпечення? - які функціональні несправності має це комп'ютерне	- для дослідження інформації, що міститься на комп'ютерних носіях, експерту надається сам комп'ютерний блок, до якого входить досліджуваний носій (комплекс комп'ютерних засобів); - для збереження наданих для дослідження носіїв у робочому стані, вони упаковуються окремо (системні блоки персональних комп'ютерів надаються в упаковках, що перешкоджають доступу до носіїв інформації та підключенню системного блока до джерела живлення); - для встановлення відповідності програмних продуктів певним характеристикам експерту надається носій, що містить копію досліджуваного програмного продукту або програмного коду; - для аналізу робочого стану комп'ютерно-технічних засобів експерту надаються ці засоби, а також відповідна технічна документація; - з метою визначення, які саме об'єкти слід передати експерту в кожному окремому випадку, а також як їх вибирати для дослідження, рекомендується проконсультуватися з фахівцем у

	обладнання або його окремі компоненти, і як це впливає на загальну роботу обладнання? - чи можна виконати певні дії за допомогою цього програмного продукту? - чи можна вирішити певне завдання за допомогою цього програмного продукту? - чи виконуються в цьому програмному продукті (програмному коді) функції, що визначені технічним завданням для його розробки?	галузі комп'ютерної техніки

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

Основні завдання експертизи	*Орієнтовний перелік вирішуваних питань*	*Особливі примітки*
- визначення характеристик та параметрів телекомунікаційних систем і пристроїв; - встановлення фактів і методів передачі або отримання інформації в телекомунікаційних системах; - встановлення фактів і способів доступу до систем, ресурсів та інформації в галузі телекомунікацій; - оцінювання якості надання телекомунікаційних послуг на етапі їх споживання; - встановлення конфігурації та робочого стану телекомунікаційних систем і засобів;	- який тип, марка та модель телекомунікаційного засобу (системи)? - чи знаходиться телекомунікаційний засіб (об'єкт) у робочому стані? - які характеристики під'єднань до мережі має телекомунікаційний засіб? - чи змінював користувач налаштування окремих пристроїв телекомунікаційної мережі, коли і які саме параметри були змінені? - який загальний характер під'єднань до телекомунікаційної мережі здійснював об'єкт (телекомунікаційна система, засіб)? - якими програмними засобами здійснювалось під'єднання до телекому-	- об'єктами експертизи телекомунікаційних систем та засобів є телекомунікаційні системи, засоби, мережі і їх складові частини та інформація, що ними передається, приймається та обробляється

- визначення типу, марки, моделі та інших класифікаційних характеристик телекомунікаційних систем та засобів; - дослідження алгоритмів обробки інформації та її захисту в галузі телекомунікацій.	нікаційної мережі? - яка топологія апаратних засобів, об'єднаних у телекомунікаційну систему? - чи відповідає робота телекомунікаційного засобу (системи) технічній документації? - які технічні характеристики (параметри) має телекомунікаційний засіб (система)? - чи мав місце факт доступу до телекомунікаційної системи та яким чином? - чи було використано ресурси та інформацію в телекомунікаційній системі, і яким чином це сталося? - чи мав місце факт передачі (отримання) інформації в телекомунікаційній системі, і яким чином це відбувалось? - чи є ознаки втручання в роботу телекомунікаційної системи? - чи могли апаратні засоби об'єднуватися в телекомунікаційну мережу, і за якими ознаками це можна визначити? - які шляхи маршрутизації даних використовуються в телекомунікаційній системі? - чи можливе використання телекомунікаційного засобу (обладнання) для зазначених цілей?	

Об'єкт та предмет (експертне завдання) судових експертиз у ході розслідування кіберзлочинів залежать від способу та механізму вчинення і

маскування злочину. Тут також варто враховувати, що «…будь-яка інформація, яка передається за допомогою інформаційно-телекомунікаційних систем, зберігається на спеціальних технічних носіях (серверах) і в спеціальному вигляді (log-файлі). Інтернет-провайдери та інші суб'єкти, які беруть участь у процесі інформаційно-телекомунікаційної передачі даних та у фактичному володінні яких перебувають сервери, мають можливість вилучити необхідні log-файли, засвідчити їхній зміст та надати на вимогу уповноважених учасників кримінального провадження. Такий спосіб збирання доказової інформації, зокрема електронної, використовується під час розслідування кримінальних правопорушень шляхом проведення відповідних НСРД. Зауважимо, що загалом власники серверів досить неактивно співпрацюють з правоохоронними органами або ігнорують запити, апелюючи щодо відсутності технічної можливості зберігання даних. Слід також наголосити, що сучасні месенджери «WhatsApp» і «Viber» містять шифрування end-to-end, що технічно унеможливлює дешифрування листування для компанії, якій належить месенджер, а вся переписка знаходиться під контролем користувачів. Виходить, що правоохоронні органи не зможуть традиційними способами одержати інформацію про листування абонентів» [53].

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

Експертиза комп'ютерної техніки і програмних продуктів Експертиза телекомунікаційних систем та засобів	використання спеціальних знань; проведення дослідження для встановлення важливих для справи обставин; залучення кваліфікованого експерта; дослідження за встановленою формою; оформлення висновків у вигляді процесуального документа (експертного висновку)

3.2 Оцінювання та використання результатів судових експертиз у ході розслідування кіберзлочинів

Призначення судової експертизи на етапі досудового розслідування сприяє забезпеченню об'єктивності, всебічності та повноти розслідування події та обставин злочину завдяки використанню спеціальних знань та отриманню необхідних результатів.

Таблиця 3.4 – Причини які впливають на проведення експертизи у ході розслідування кіберзлочинів

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

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

Таблиця 3.5 – Критерії оцінювання та використання результатів судових експертиз у ході розслідуванні кіберзлочинів

Вид експертизи	*Критерії*
Експертиза комп'ютерної техніки і програмних продуктів Експертиза телекомунікаційних систем та засобів	- власник інформації має встановити умови та правила для отримання та обробки цієї інформації; - власник або розпорядник комп'ютерної техніки, автоматизованих систем чи оператор (провайдер) мереж електрозв'язку зобов'язані розробити та реалізувати заходи для захисту інформації в системі; - власник або розпорядник комп'ютерних систем та оператор (провайдер) мереж мають створити правила для функціонування системи; - має бути укладений договір між власником (оператором, провайдером) системи та володільцем інформації, який визначає заходи захисту інформації в системі; - злочинець здійснив одну з таких операцій: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрацію, приймання, отримання або передавання інформації

Кіберпростір дуже *пластичний,* і його можна описати як *рекурсивний* (платформи на платформах). Платформи можуть відрізнятися в деталях, але їх об'єднує те, що вони є фундаментом для наступної платформи над ними. Д. Кларк писав, що «аналіз контрольних точок – це набір інструментів, які допомагають строго продумати дизайн системи з певного погляду 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 вебсторінки) 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 іншим кутом)» [54].

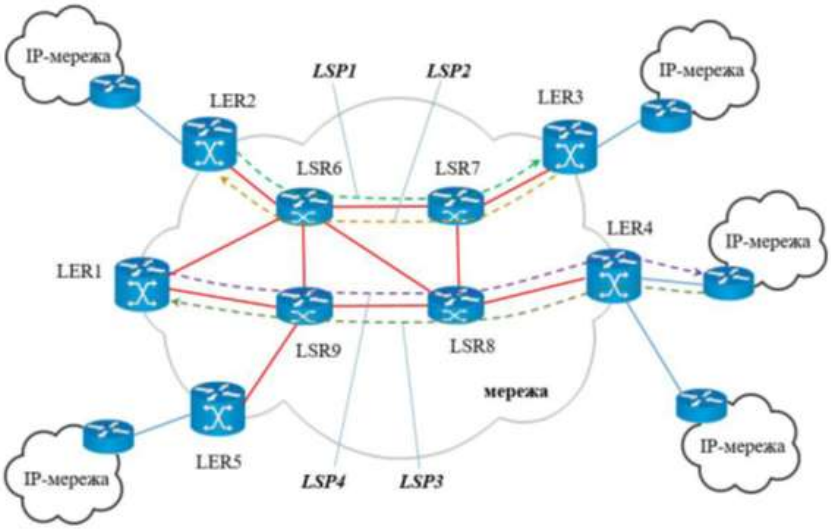

Рисунок 3.1 – Спрощена схема аналізу контрольних точок
(на базі рекурсивних платформ)

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» [3]. 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 отримані результати (у разі необхідності, роз’яснити природу отриманих результатів). Тобто, експерт використовує спеціальні знання у ході проведення судової експертизи задля отримання результатів та їх оцінювання [16].

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» [55].

Таблиця 3.6 – Критерії оцінювання та використання результатів судових експертиз спеціально уповноваженими суб'єктами у ході розслідуванні кіберзлочинів

Спеціально уповноважені суб'єкти	*Аспекти оцінювання*
Слідчі, детективи, прокурори, судді, адвокати	– *перевірка достатності об'єктів для експертизи* (оцінюється, чи надано достатню кількість об'єктів, адже їхній дефіцит, особливо при вирішенні ідентифікаційних питань, може призвести до помилкових висновків або неможливості їх формулювання; – *оцінювання якості об'єктів* (визначається відповідність наданих зразків досліджуваним об'єктам, правильність їх вилучення, упакування, зберігання, транспортування та точність вихідних даних для проведення експертизи); – *аналіз доцільності та правомірності методик* (перевіряється, чи відповідають обрані експертом методики поставленим завданням, чи є вони придатними для встановлення потрібних властивостей об'єктів, а також чи застосовуються вони в експертній практиці і мають наукове обґрунтування); – *оцінювання повноти досліджень* (перевіряється, чи були виконані всі потрібні процедури і дослідження об'єктів проводилось відповідно до затвердженої методики); – *аналіз правильності опису та інтерпретації ознак об'єктів* (визначається, чи всі виявлені ознаки об'єкта детально описані й оцінені з точки зору їх властивостей і значущості для вирішення поставленого питання); – *перевірка обґрунтованості висновків* (оцінюються проміжні та підсумкові висновки, встановлюється, чи вони базуються на результатах дослідження, чи достатньо виявлених ознак для їх формулювання, і чи остаточні висновки є логічним наслідком загальної оцінки проміжних); – *оцінювання компетентності експерта* (аналізується фаховий рівень експерта на основі детального вивчення його висновків)

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 зумовлено 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, що зумовлена обміном інформацією про отримані результати та щодо уточнення завдань перед експертом.

Враховуючи сучасні тенденції розвитку IT-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» [45]. 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. 2.26), та беручи до уваги актуальність їх використання, можна 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 додатка «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 бувши 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 потрібно здобути (згідно з ознаками 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; – у ході аналізу 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 з якого злочинець здійснив вхід до мобільного додатка «NeoBank»		
		характеристика банкомата 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 № 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 (введення, виведення) заборонених електронних грошей шляхом використання забороненої платіжної системи «WebMoney Transfer». ОСОБА_4 з метою отримання незаконного доходу за надання послуг обміну (введення, виведення) заборонених електронних грошей, діючи без ліцензії (дозволу) Національного банку України на обмін та переказ коштів у національній валюті, без відкриття рахунків та не бувши 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, введення, виведення електронних коштів через заборонену платіжну систему «WebMoney Transfer» 20 березня 2023 року здійснив обмін (введення, виведення) 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 № НОМЕР_4. Так, ОСОБА_4 усвідомлюючи протиправність

своїх дій, використав заборонену платіжну систему «WebMoney Transfer» та здійснив обмін (введення, виведення) 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 потрібно здобути (згідно з ознаками 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 access to information)	ч. 1 ст. 200 КК України	характеристики ЕОТ, які забезпечили злочинцю роботу з платіжною системою «WebMoney Transfer»	*Програмний засіб: Belkasoft Evidence Center*	- дозволяє «витягувати» і аналізувати дані з мобільних пристроїв, хмарних сховищ і жорстких дисків; - у ході аналізу 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)		
		характеристика ЕОТ, який забезпечив роботу на веб-ресурсі «OLX» та дані такої роботи		
		характеристики банківських карток з яких перераховувалися гривні і на яку зарахувалися (картка злочинця), дані проведених операцій		
		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 хвороби COVID-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 несанкціоновано 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 потрібно здобути (згідно з ознаками 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; - у ході аналізу жорстких дисків здійснюється вилучення даних із веб-браузерів, чатів, інформації про хмарні сервіси, детектування зашифрованих файлів і розділів, «витягування» 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, з яких перераховувалися 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», бувши 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» «15P5mQNrN4heSJ5iqc4p5FF nb6MXTiHyu4». 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 кваліфікувальними 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	Кібер-злочин	Докази, які потрібно здобути (згідно з ознаками 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 блокатор *Tableau T35U*	дозволяє безпечно під'єднувати 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: - широкий спектр даних із різних носіїв інформації; - вмонтований переглядач баз даних SQLite; - збирання 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 нижчевказаних обставин. Так, ОСОБА_3, бувши 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 інформації, доступ до якої обмежено, діючи за попередньою змовою гру-

пою осіб, розповсюдив інформацію з автоматизованої інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України», яка належить 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 таким текстом: «Пробив Украйна, Анкета физ лица - 20$. За 15 минут. Пробив другой информации. Гарант.+». Згодом, 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 криптовалюти, 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 інтернетгаманець TCxfXEusobtT2n6juch5kdnbkeQVk1Xeqz.

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

Категорія та тип інциденту	Кіберзлочин	Докази, які потрібно здобути (згідно з ознаками 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'ютери 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: - широкий спектр даних із різних носіїв інформації; - вмонтований переглядач баз даних SQLite; - збирання 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 зі 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, бувши 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 таких обставин. Так, 10.07.2022, точного часу в ході досудового розслідування не встановлено, ОСОБА_3, перебуваючи на місці свого проживання за адресою: АДРЕСА_1, діючи умисно, за попередньою змовою 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 обробляється 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 обробляється в автоматизованих системах, вчинені 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	Кібер злочин	Докази, які потрібно здобути (згідно з ознаками 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; - збирання даних із віддалених комп'ютерів і серверів; - інтегрований функціонал щодо перевірки виявлених файлів на Virustotal
		характеристика IP-телефонії (злочинної групи)		
		характеристика банківських карток (кожного зі 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, виконуючи умови 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 обробляється 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	Кібер злочин	Докази, які потрібно здобути (згідно з ознаками 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), у разі 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 зі злочинної групи осіб), дані проведених операцій		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дзьобань О. П. Цифрова людина. *Енциклопедія соціогуманітарної інформології* / коорд. проєкту та заг. ред. проф. К. І. Беляков. Одеса, 2021. Т. 2. С. 177–181.

2. Дудатьєв А. Аксіоматика теорії комплексної безпеки соціотехнічних систем. *Інформаційні технології та комп'ютерна інженерія*. 2013. № 1. С. 22–25.

3. Кримінальний процесуальний кодекс України : *Закон України*, 13.04.2012. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

4. Кримінальний кодекс України : *Закон України*, 05.04.2001. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14

5. Конституція України : *Закон України* від 28 червня 1996 року № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254% D0%BA/96-%D0%B2%D1%80#Text

6. Криміналістична тактика : навч. посіб. / за ред. д-ра юрид. наук, проф. М. А. Погорецького. Київ : Алерта, 2016. 244 с.

7. Ващук О. Структура окремих методик розслідування кримінальних правопорушень. *Юридичний вісник*. 2024. № 3. С. 30–36.

8. Білоус Р., Василинчук В., Таран О. Використання методів кримінального аналізу під час оперативного провадження та досудового розслідування. *Науковий вісник Національної академії внутрішніх справ*. 2021. № 1 (118). С. 131–137.

9. Шевчук В. Інноваційні криміналістичні продукти у правозастосовній діяльності: поняття, ознаки та проблеми впровадження у практику. *Наукові праці НУ «Одеська юридична академія»*. 2020. С. 139–155. URL: https://doi.org/10.32837/npnuola.v26i0.671.

10. Благута Р. І., Мовчан А. В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання : монографія. Львів: ЛьвДУВС, 2020. 256 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 / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2023. 198 с.

12. Журба А. І. Особливості предмета доказування у справах про комп'ютерні злочини : дис. ... канд. юрид. наук : 12.00.09 / Харківський національний університет внутрішніх справ. Харків, 2008. 230 с.

13. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореф. дис. на здобуття наук. степеня канд. юрид. наук : 12.00.09 / Київ, 2005. 20 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: 27.11.2024)

16. 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 / Національна академія внутрішніх справ. Київ, 2021. 268 с.

17. Cellebrite UFED Touch 2. EPOS-ForensicTools. URL : https://forensictools.com.ua/viluchennya-danikh-z-mobilnikh-telefoniv/ufed-touch-2.html (дата звернення: 27.11.2024)

18. MSAB XR / MSAB XRY Field. Mobile Forensics and Data Recovery Software. URL : https://www.msab.com/product/xry-extract/ (дата звернення: 27.11.2024)

19. RUSOLUT. Monolithic Adapters. URL : https://rusolut.com/tag/monolithic-adapters/ (дата звернення: 27.11.2024)

20. Magnet AXIOM. Introduction to Magnet AXIOM. URL : https://www.magnetforensics.com/resources/introduction-magnet-axiom/ (дата звернення: 27.11.2024)

21. Magnet Forensics. Belkasoft Evidence Center. URL : https://belkasoft.com/x (дата звернення: 27.11.2024)

22. Tableau T35U. Opentext Tableau Forensic T35u/T35u-RW SATA/IDE BridgeUser Guide. URL : https://manuals.plus/opentext/tableau-forensic-t35ut35u-rw-sataide-bridge-manual.pdf (дата звернення: 27.11.2024)

23. Wiebitech Forensic UltraDock v5. EPOS-ForensicTools. URL : https://forensictools.com.ua/blokatori-zapisu/wiebetech-forensic-ultradock-v55.html (дата звернення: 27.11.2024)

24. Encase Forensics. EPOS-ForensicTools. URL : https://forensictools.com.ua/search?controller=search&orderby=position&orderway=desc&search_query=Encase+Forensics (дата звернення: 27.11.2024)

25. Access Data FTK. URL : https://www.pluralsight.com/paths/accessdata-forensic-toolkit-ftk (дата звернення: 27.11.2024)

26. X-Ways Forensics: Integrated Computer Forensics Software. URL : https://www.x-ways.net/forensics/ (дата звернення: 27.11.2024)

27. ACELab. URL : https://www.acelab.eu.com/ (дата звернення: 27.11.2024)

28. Autopsy. URL : https://www.autopsy.com/download/ (дата звернення: 27.11.2024)

29. Photorec. Digital Picture and File Recovery. URL : https://www.cgsecurity.org/wiki/photoRec (дата звернення: 27.11.2024)

30. Eric Zimmerman Tools. URL : https://www.sans.org/tools/ez-tools/ (дата звернення: 27.11.2024)

31. Про затвердження Положення про організаційно-технічну модель кіберзахисту : *Постанова Кабінету Міністрів України*; Положення від 29.12.2021 року № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF

32. Про основні засади забезпечення кібербезпеки України : *Закон України* від 05.10.2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

33. 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

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

35. SIEM (Security information and event management). URL: https://uk.wikipedia.org/wiki/SIEM

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

37. 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

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

38. Конвенція про кіберзлочинність : від 23.11.2001 р. *Верховна Рада України. Офіційний вісник України* від 10.09.2007. № 65, С. 107. URL: https://zakon.rada.gov.ua/laws/show/994_575/

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

40. Остапов С. Е., Євсеєв С. П., Король О. Г. Кібербезпека: сучасні технології захисту :. навчальний посібник. Львів : «Новий Світ – 2000», 2024. 678 с.

41. Про Положення про технічний захист інформації в Україні : *Указ Президента України* від 27.09.1999 № 1229/99 (в редакції від 04.05.2008). URL: https://zakon.rada.gov.ua/go/1229/99

42. Про захист інформації в інформаційно-комунікаційних системах : *Закон України* від 05.07.1994 № 80/94-ВР (в редакції від 28.06.2024). URL : https://zakon.rada.gov.ua/go/80/94-%D0%B2%D1%80

43. Про Положення про порядок здійснення криптографічного захисту інформації в Україні : *Указ Президента України* від 22.05.1998 № 505/98 (в редакції від 12.09.2009). URL : https://zakon.rada.gov.ua/go/505/98

44. 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.

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

46. 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.

47. Про судову експертизу : *Закон України* від 25.02.1994 року № 4038-XII (в редакції від 01.01.2024). URL: ttps://zakon.rada.gov.ua/laws/card/4038-12

48. 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. (в редакції від 30.10.2024). URL : https://zakon.rada.gov.ua/laws/show/z0705-98#Text

49. 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 (в редакції від 30.10.2024). URL: https://zakon.rada.gov.ua/laws/show/z1431-11#Text

50. Про затвердження Положення про Експертну службу Міністерства внутрішніх справ України : *Наказ Міністерства внутрішніх справ України* від 03.11.2015 №1343. (в редакції від 25.01.2022). URL:: https://zakon.rada.gov.ua/laws/show/z1390-15#Text

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

52. Судова комп'ютерно-технічна експертиза у кримінальному провадженні : навч. посіб. / Климчук М. П. та ін. Львів : Львівський державний університет внутрішніх справ, 2022. 112 с.

53. 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

54. 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

Електронне навчальне видання

Леонід Олександрович Майданевич
Олеся Петрівна Войтович
Галина Василівна Шелепало

ТЕХНІКО-КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Навчальний посібник

Рукопис оформив *Л. Майданевич*

Редактор *В. Дружиніна*

Оригінал-макет виготовила *Т. Старічек*

Підписано до видання 19.09.2025 р.
Гарнітура Times New Roman.
Зам. № Р2025-132.

Видавець та виготовлювач
Вінницький національний технічний університет,
Редакційно-видавничий відділ.
ВНТУ, ГНК, к. 114.
Хмельницьке шосе, 95,
м. Вінниця, 21021.
press.vntu.edu.ua;
Email: rvv.vntu@gmail.com
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.

МАЙДАНЕВИЧ Леонід Олександрович
кандидат філософських наук, старший викладач кафедри захисту інформації Вінницького національного технічного університету

Сфера наукових інтересів: філософія інформаційного права, організаційно-правові основи забезпечення кібербезпеки, механізми публічного управління, методологія та організація наукових досліджень

Наукові здобутки: кандидат філософських наук (2015), захистив дисертацію з проблеми проведення релігієзнавчої експертизи. Закінчив магістерські програми: в Інституті міжнародних відносин Київського національного університету імені Тараса Шевченка; в Національній академії державного управління при Президентові України; на філософському факультеті Київського національного університету імені Тараса Шевченка; на факультеті інформаційних технологій та комп'ютерної інженерії Вінницького національного технічного університету. Є автором більше 40 публікацій в наукових та інших виданнях

Практична діяльність: адвокат (Рада адвокатів Вінницької області)

Перелік дисциплін: Техніко-криміналістичне забезпечення розслідування кіберзлочинів; Захист інтелектуальної власності в кіберпросторі; Нормативно-правове забезпечення інформаційної безпеки; Законодавство з кібербезпеки критичних систем

ВОЙТОВИЧ Олеся Петрівна
кандидат технічних наук, доцент, доцент кафедри захисту інформації Вінницького національного технічного університету

Сфера наукових інтересів: захист інформації в інформаційно-комунікаційних системах

Наукові здобутки: кандидат технічних наук (2006), захистила дисертацію з питань інформаційно-вимірювальних систем для діагностування на основі нейронечітких алгоритмів. Результатом наукової діяльності є більше 90 наукових праць, серед них: десять у виданнях, що входять до наукометричних баз Scopus і Web of Science, більше 20 статей у фахових виданнях, п'ять монографій, сім навчальних посібників, два патенти на корисну модель, п'ять авторських свідоцтв на комп'ютерну програму

Практична діяльність: доцент кафедри захисту інформації

Перелік дисциплін: Безпека інформаційно-комунікаційних систем; Кібербезпека; Моніторинг та аудит кібербезпеки

ШЕЛЕПАЛО Галина Василівна
кандидат фізико-математичних наук, доцент кафедри захисту інформації Вінницького національного технічного університету

Сфера наукових інтересів: безпека даних (кодування та шифрування) в інформаційно- комунікаційних системах, математичні механізми захисту інформації, методологія та організація наукових досліджень в кібербезпеці

Наукові здобутки: кандидат фізико-математичних наук (2019), захистила дисертацію з питань класифікації квазігрупових функційних рівнянь і тотожностей мінімальної довжини, які застосовуються у криптографії. Є автором 85 наукових праць, з них п'ять у виданнях, що входять до наукометричних баз Scopus і Web of Science, більше 12 статей у фахових виданнях, два навчальні посібники

Практична діяльність: провідний інспектор відділу інформаційних технологій та програмування в центральному регіоні (м. Вінниця) управління інформаційних технологій та програмування Департаменту кіберполіції Національної поліції України

Перелік дисциплін: Криптографія на основі груп; Криптографія на основі квазігруп; Основи наукових досліджень, аналізу та синтезу інформації; Сучасні інформаційні технології в кібербезпеці