

АЛГОРИТМ ОТРИМАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ В УМОВАХ ПОТЕНЦІЙНОГО САМОЗНИЩЕННЯ ЕЛЕКТРОННИХ (ЦИФРОВИХ) СЛІДІВ

Майданевич Леонід Олександрович

канд. філос. наук, старший викладач кафедри захисту інформації
факультету інформаційних технологій та комп'ютерної інженерії

Вінницького національного технічного університету,
адвокат (Рада адвокатів Вінницької області), м. Вінниця

Кирбят'єв Олег Олександрович

доктор юридичних наук, професор,

старший оперуповноважений з оперативного пошуку
та партнерства у сфері інформаційних технологій управління протидії
кіберзлочинам в Запорізькій області Департаменту кіберполіції

Національної поліції України, м. Запоріжжя

Тарасюк Микола Борисович

студент групи ІБС-24М кафедри захисту інформації
факультету інформаційних технологій та комп'ютерної інженерії
Вінницького національного технічного університету, м. Вінниця

Кіберзлочинність в XXI столітті є найнебезпечнішою глобальною загрозою. Це обумовлено стрімким розвитком інформаційних технологій та інформаційної інфраструктури. Власне, «кіберзлочинність ... завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат. Набуває поширення використання кіберпростору для вчинення злочинів проти основ національної безпеки України, а також кримінальних правопорушень, пов'язаних із легалізацією доходів, одержаних злочинним шляхом, торгівлею людьми, незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами, незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інших предметів і речовин, які загрожують життю та здоров'ю людей тощо» [1].

Задля підвищення ефективності боротьби із кіберзлочинністю, найперше, необхідно дослідити закономірності побудови її як системи. Для цього ми враховуємо, що «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 зберігання даних; 5) маскуванню фінансових потоків; 6) розробки алгоритмів соціальної інженерії та тестування лояльності учасників кіберзлочинної групи; 7) впровадження засобів моніторингу та контролю доступу; 8) планування системи резервних копій та відновлення даних; 9) автоматизації процесів для уникнення

помилки через людський фактор; 10) підготовки до адаптації та швидкого реагування на загрози» [2, 11-12].

Враховуючи вказані особливості «безпеки системи кіберзлочинності» та використовуючи стандарти надані в NIST SP 800-101 Rev.1 [3], ДСТУ ISO/IEC 27037:2017 [4] ми вибудовуємо алгоритм вилучення цифрових доказів в умовах потенційного самознищення із 9 етапів: 1) підготовчий етап (попередня оцінка слідчої ситуації); 2) фіксація поточного стану; 3) ізоляція мережових комунікацій; 4) визначення підходу до збереження стану пам'яті; 5) зняття живлення; 6) захист і вилучення носіїв інформації; 7) первинне клонування (forensic imaging); 8) аналіз копій у контрольованому середовищі; 9) документування та оформлення електронних доказів.

Таблиця 1. Алгоритм отримання електронних доказів в умовах потенційного самознищення електронних (цифрових) слідів

Етап	Зміст	Примітки
1. Підготовчий етап (попередня оцінка слідчої ситуації)	На початковому етапі важливо визначити безпечність роботи на місці проведення розслідування та оцінити ризики, пов'язані з потенційним використанням механізмів самознищення. Слід здійснити ідентифікацію всіх наявних цифрових пристроїв, їхнього поточного стану (увімкнено / вимкнено), а також характеру мережових підключень і периферійного обладнання. Хоча застосування вибухових пристроїв є надзвичайно радикальним засобом протидії розкриттю інформації, в окремих випадках зловмисники можуть вдаватися до такого методу, якщо втрата даних або їх потрапляння до рук правоохоронних органів може призвести до	Ризики: Існує ймовірність використання спеціалізованих пристроїв або механізмів, що реагують на фізичне втручання середовище (відкриття корпусу зміна температури, переміщення), що може спричинити як знищення даних так і загрозу фізичній безпеці персоналу. До непрямих індикаторів наявності вибухових пристроїв або підозрілих модифікацій корпусу системного блоку належать: - сторонні елементи кріплення, що не відповідають оригінальній конструкції пристрою (наприклад, додаткові шурупи, герметики, пломби); - підозрілі електронні або механічні компоненти, прикріплені до корпусу або внутрішніх елементів (наприклад, додаткові плати, дроти, які ведуть до жорсткого диска або кнопок живлення); - наявність звукових або візуальних сигналів, що не

	серйозних юридичних або матеріальних наслідків, або розкриття критично важливої інформації (наприклад, компрометація розгалужених кіберзлочинних мереж, державна зрада, промислове шпигунство тощо)	характерні для штатної роботи пристрою (клацання, тікання, миготіння індикаторів тощо); - поява сторонніх запахів (наприклад, запах пластику, що плавиться або хімікатів); - підключення до нетипових джерел живлення або батареї, які можуть свідчити про автономні тригери; - агресивна або підозріла поведінка осіб, пов'язаних із пристроєм, включно з погрозами щодо його відкриття або використання
2. Фіксація поточного стану	Необхідно виконати повну фото- та відеофіксацію усіх пристроїв, стану екранів, індикаторів живлення, підключень кабелів, типу з'єднань та інших деталей. Усі маніпуляції повинні супроводжуватись відповідною документацією з позначенням місця, часу та відповідальної особи	Ризики: Недостатня деталізація фіксації або помилки у маркуванні можуть спричинити відтворення некоректної конфігурації під час лабораторного дослідження, що своєю чергою, може активувати ворожі скрипти. Відсутність належної документації може бути підставою для відхилення доказу у суді
3. Ізоляція мережевих комунікацій	З метою запобігання дистанційному впливу на пристрій або передачі даних слід здійснити негайну ізоляцію від зовнішніх мереж: - фізично вилучити мережеві кабелі; - помістити мобільні пристрої у Faraday-бокси; - деактивувати бездротові модулі (Wi-Fi, Bluetooth) за допомогою апаратних перемикачів	Ризики: Для певного класу анти-форензичного програмного забезпечення втрата мережевої з'єднаності може бути тригером для запуску процедур знищення або шифрування даних. Однак, з огляду на вищий пріоритет запобігання несанкціонованому дистанційному втручанням, ізоляція є необхідною
	Для увімкнення	Ризики: Завантаження

4. Визначення підходу до збереження стану пам'яті	пристроїв: доцільним є виконання процедури live acquisition (тобто, зняття вмісту оперативної пам'яті (RAM), інформації про активні процеси, мережеві сесії, кеш браузера тощо). Для вимкнених пристроїв: - слід уникати вмикання без підготовки; - рекомендується безпосередньо вилучити носії інформації для подальшого аналізу у контрольованому середовищі (дод. див. етап 6)	сторонніх програм на пристрої може активувати шкідливі скрипти. Підключення накопичувача до іншої системи без write-blocker'a може ініціювати автозапуск руйнівних процесів
5. Зняття живлення	Цей крок застосовується лише у випадках, коли live acquisition неможливий або небезпечний. Перевагу слід надавати апаратному відключенню (наприклад, вилучення акумулятора або кабелю живлення), попередньо переконавшись у відсутності джерел резервного живлення	Ризики: Втрата всіх volatile-даних, активація скриптів самознищення, що реагують на завершення роботи системи (stop-задачі, команди на вихід, системні події завершення живлення)
6. Захист і вилучення носіїв інформації	Носії слід вилучати обережно, із дотриманням вимог електростатичної безпеки, та упаковувати у спеціальні антистатичні пакети	Ризики: SSD накопичувачі можуть автоматично виконувати команди очищення (TRIM), що унеможливає відновлення частини даних. Деякі USB-носії можуть бути модифіковані апаратно (BadUSB, USB Killer), що створює як інформаційні, так і фізичні загрози

7. Первинне клонування (forensic imaging)	З метою уникнення змін в оригінальному носії створюються побітові копії із застосуванням write-blocker-ів. Клонування виконується у відповідності до методичних стандартів збереження цифрових доказів	Ризики: Відсутність блокування запису може призвести до модифікації вмісту, зміни хеш-сум та втрати достовірності доказів
8. Аналіз копій у контрольованому середовищі	Усі процедури аналізу здійснюються в ізолюваному лабораторному середовищі, з використанням спеціалізованого ПЗ	Слід здійснити пошук: - ознак антифорензичних дій (wipe-utility, rootkits, приховані розділи); - тригерів самознищення (скрипти, cron-задачі, сигнали таймерів, механізми автоформатування); - змін у таблицях розділів, файлових системах або MBR/GPT
9. Документування і оформлення доказів	На всіх етапах необхідно: - фіксувати дії за допомогою відео, аудіо, журналів логів тощо; - здійснювати цифрове підписування створених копій; - використовувати хеш-функції (MD5, SHA-256) для підтвердження цілісності; - забезпечити ланцюг зберігання (chain of custody)	

Запропонований алгоритм дозволяє уніфікувати підхід до обробки інформації в умовах потенційного самознищення електронних (цифрових) слідів. Запропоновані етапи є орієнтирами, та мають бути уточненні слідчим під конкретні обставини слідчої ситуації, слідчої версії. Результати дослідження можуть бути використанні для подальшого теоретичного та

практичного осмислення способів протидії анти-криміналістичним засобам, насамперед, застосовуючи трансдисциплінарний та міждисциплінарний підходи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». Указ Президента України від 26.08.2021 року № 447/2021. URL: <https://zakon.rada.gov.ua/go/447/2021> (дата звернення: 11.05.2025)
2. Техніко-криміналістичне забезпечення розслідування кіберзлочинів : навчальний посібник / Л. Майданевич, О. Войтович, Г. Шелепало. Вінниця : ВНТУ, 2025. 117с.
3. NIST SP 800-101 Rev.1 URL: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf> (дата звернення: 11.05.2025)
4. ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=74978 (дата звернення: 11.05.2025)

ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ МЕРЕЖНИХ СПІВТОВАРИСТВ

Манжай Олександр Володимирович

к.ю.н., професор, завідувач кафедри протидії кіберзлочинності
ННІ № 4 Харківського національного університету внутрішніх справ

На круглому столі «Роль OSINT-досліджень у підвищенні рівня національної безпеки України», який відбувся на базі Львівського державного університету внутрішніх справ 07 травня 2025 року, нами було презентовано спосіб аналізу даних співтовариств в Telegram з використанням зв'язки програм Telegram-Desktop+Excel+Gephi. У результаті аналізу файлу в форматі JSON, який містить інформацію про групу Telegram, зокрема повідомлення та відповіді на них, нам вдалося досить швидко створити схему, на якій відображені найбільш активні учасники групи, однаковим кольором позначені користувачі, які входять до одного співтовариства, розмір вузлів відображає інтенсивність написання повідомлень в групі, товщина стрілок та їх напрями відображають кількість та напрям надсилення повідомлень (рис. 1).