МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КРИМІНАЛЬНОГО ПРОЦЕСУ
КАФЕДРА КРИМІНАЛІСТИКИ ТА ДОМЕДИЧНОЇ ПІДГОТОВКИ
КАФЕДРА КРИМІНАЛЬНОГО ПРАВА ТА КРИМІНОЛОГІЇ

РОЗСЛІДУВАННЯ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ ІНФОРМАЦІЙНИХ (АВТОМАТИЗОВАНИХ), ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ, ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖ (ст. 361 КК УКРАЇНИ)

Науково-методичні рекомендації для підрозділів слідства та дізнання Національної поліції України

Дніпро
2025

УДК 343.3.7
Р 64

Схвалено Науково-методичною радою
Дніпровського державного
університету внутрішніх справ
(протокол № 3 від 25.11.2025)

РЕЦЕНЗЕНТИ:

Юрій ВИХОДЕЦЬ – начальник Департаменту кіберполіції Національної поліції України генерал поліції 3-го рангу;

Микола ПОГОРЕЦЬКИЙ – проректор з науково-педагогічної роботи Київського національного університету ім. Т. Шевченка, доктор юридичних наук, професор, заслужений діяч науки і техніки України

УКЛАДАЧІ:

Максим ЦУЦКІРІДЗЕ, перший заступник Голови Національної поліції України - начальник Головного слідчого управління, доктор юридичних наук, професор, заслужений юрист України **Артем ШЕВЧИШЕН**, заступник начальника Головного слідчого управління Національної поліції України, начальник управління організації роботи та методичного забезпечення, доктор юридичних наук, професор, заслужений юрист України **Максим РОМАНОВ**, начальник 3-го відділу (методичної роботи та правового забезпечення) управління організації роботи та методичного забезпечення Головного слідчого управління Національної поліції України, доктор філософії в галузі права **Андрій КРУШЕНИЦЬКИЙ**, старший слідчий в особливо важливих справах 3-го відділу (методичної роботи та правового забезпечення) управління організації роботи та методичного забезпечення Головного слідчого управління Національної поліції України, доктор філософії в галузі праваканідат технічних наук, доцент **Юлія СИНИЦІНА** – т.в.о. завідувача кафедри інформаційних технологій Дніпровського державного університету внутрішніх справ; **Дмитро ДАНЧЕНКО** – начальник 7-го відділу Управління протидії кіберзлочинам в Дніпропетровській області Департаменту КПНП України майор поліції; кандидат юридичних наук, професор **Едуард РИЖКОВ** – професор кафедри інформаційних технологій Дніпровського державного університету внутрішніх справ; кандидат юридичних наук, доцент **Ганна БІДНЯК** – завідувач кафедри криміналістики та домедичної підготовки Дніпровського державного університету внутрішніх справ майор поліції; кандидат юридичних наук, доцент **Андрій ЗАХАРКО** – т.в.о. завідувача кафедри, доцент кафедри кримінального процесу Дніпровського державного університету внутрішніх справ підполковник поліції; кандидат юридичних наук, доцент **Сергій БАБАНІН** – доцент кафедри кримінального права та кримінології Дніпровського державного університету внутрішніх справ.

Р 64 Розслідування несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України) : наук.-метод. рекомендації для підрозділів слідства та дізнання Національної поліції України. / кол. авт. ; за заг. ред. М. С. Цуцкірідзе, перш. заступ. гол. Нац. пол. України, нач. ГСУ, генерала поліції 3-го рангу. Дніпро : Дніпр. держ. ун-т внутр. справ, 2025. 104 с.

ISBN 978-617-560-106-8

Методичні рекомендації призначені для розв’язання актуальних проблем професійної діяльності підрозділів слідства та дізнання Національної поліції України. Розроблені відповідно до листа Головного слідчого управління Національної поліції України від 30.05.2024 № 1/3331 та п. 2.26 плану проведення науково-дослідних та дослідно-конструкторських робіт Дніпровського державного університету внутрішніх справ на 2025 рік, затвердженого 30.12.2024.

ЗМІСТ

ВСТУП

Сучасний світ характеризується стрімкою цифровою трансформацією, що охоплює всі сфери суспільного життя та економіки. Паралельно з перевагами цифровізації невпинно зростає рівень кіберзагроз. Одним із найпоширеніших та найнебезпечніших видів кіберзлочинів є несанкціоноване втручання в роботу комп'ютерних систем та мереж.

В Україні ця проблема набуває особливої гостроти не лише через загальносвітові тенденції, але й у зв'язку з триваючою гібридною агресією та повномасштабним вторгненням російської федерації, що супроводжується цілеспрямованими кібератаками на державні інформаційні ресурси та об'єкти критичної інфраструктури. Ефективне розслідування таких злочинів є ключовим елементом забезпечення національної безпеки, захисту прав громадян та стабільності економіки.

Метою представлених науково-методичних рекомендацій є надання комплексного, науково обґрунтованого та практично орієнтованого посібника для слідчих, дізнавачів, оперативних працівників, кримінальних аналітиків та інших фахівців правоохоронних органів України щодо ефективного виявлення, документування, розслідування та розкриття кримінальних правопорушень, передбачених ст. 361 Кримінального кодексу України (КК України). Досягнення цієї мети передбачає вирішення таких завдань: розкриття базових понять інформаційної сфери; аналіз кримінально-правової кваліфікації НСВ з урахуванням останніх законодавчих змін; деталізація переліку та особливостей проведення слідчих (розшукових) дій; вироблення підходів до фіксації доказів у типових слідчих ситуаціях; окреслення можливостей використання кримінального аналізу та OSINT; висвітлення аспектів міжнародного співробітництва; аналіз специфіки розслідування в умовах воєнного стану; надання практичних алгоритмів та прикладів.

Рекомендації складаються з дев'яти логічно пов'язаних розділів. Починаючи з фундаментальних понять та юридичної кваліфікації, у роботі послідовно розглядаються практичні аспекти розслідування: планування та проведення слідчих дій, фіксація доказів, використання аналітичних інструментів (кримінальний аналіз, OSINT), міжнародна взаємодія та специфіка роботи в умовах воєнного стану. Наводяться типові алгоритми дій для різних суб'єктів розслідування та практичні приклади.

Призначені для широкого кола фахівців, залучених до протидії кіберзлочинності, зокрема: слідчих Головного слідчого управління та інших слідчих підрозділів Національної поліції України, дізнавачів, оперативних працівників Департаменту кіберполіції та інших оперативних підрозділів НПУ та СБУ, прокурорів, співробітників підрозділів кримінального аналізу, експертів комп'ютерно-технічного профілю, суддів, науковців, викладачів, курсантів та студентів юридичних навчальних закладів.

Розділ 1. БАЗОВІ ЗНАННЯ В ІНФОРМАЦІЙНІЙ СФЕРІ В КОНТЕКСТІ СТ. 361 КК УКРАЇНИ

1.1. Визначення ключових понять

Для належного розуміння та застосування ст. 361 КК України критично важливим є чітке визначення ключових термінів, що описують об'єкт та предмет злочинного посягання. Чинне законодавство України, зокрема закони України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про електронні комунікації», «Про основні засади забезпечення кібербезпеки України», оперує низкою понять, як-от:

– *інформаційна система* – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

– *автоматизована система* – система, призначена для автоматизації діяльності або окремих інформаційних процесів, що складається з персоналу і комплексу засобів автоматизації його діяльності. Часто використовується як синонім або близьке поняття до інформаційної системи;

– *електронна комунікаційна система* технічні засоби електронних комунікацій, програмні засоби, споруди електронних комунікаційних мереж, необхідні для надання електронних комунікаційних послуг та/або забезпечення функціонування електронних комунікаційних мереж;

– *інформаційно-комунікаційна система (ІКС)* – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле. Це найбільш узагальнююче поняття;

– *електронна комунікаційна мережа* – комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг (наприклад, Інтернет, мережі мобільного зв'язку).

Також важливими для розуміння об'єктивної сторони злочину є такі поняття:

– *комп'ютерна інформація (дані)* – інформація (відомості) у формі, придатній для зберігання, обробки і передачі за допомогою комп'ютерної техніки;

– *програмне забезпечення* – сукупність програм системи обробки інформації і програмних документів, необхідних для експлуатації цих програм;

– *апаратне забезпечення* – фізичні компоненти комп'ютерної системи (процесор, пам'ять, диски, мережеві карти тощо);

– *втручання* – вплив на процес обробки інформації або на саму інформацію чи систему/мережу, що здійснюється поза встановленим порядком доступу та експлуатації;

– *несанкціонований доступ* – доступ до інформації або ресурсів системи особою, яка не має на це дозволу власника або уповноваженого ним органу, або з порушенням встановлених правил розмежування доступу;

– *витік інформації* – неконтрольоване поширення інформації з обмеженим доступом;

– *втрата інформації* – неможливість доступу до інформації або її фізичне чи логічне знищення;

– *підробка інформації* – внесення в інформацію неправдивих відомостей або зміна існуючих даних;

– *блокування інформації* – унеможливлення доступу до інформації законними користувачами;

– *знищення інформації* – приведення інформації у стан, непридатний для використання;

– *модифікація інформації* – будь-яка зміна інформації, крім знищення;

– *копіювання інформації* – створення дубліката інформації.

Практика свідчить, що певна неузгодженість та подекуди синонімічне використання термінів на кшталт «інформаційна система», «автоматизована система», «інформаційно-комунікаційна система» у різних нормативно-правових актах може створювати труднощі при кваліфікації діяння та точному визначенні предмета злочину за ст. 361 КК України. Слідчим та прокурорам необхідно ретельно аналізувати технічну суть об'єкта, що зазнав втручання, та обирати термінологію, яка найбільш точно відповідає його характеристикам та визначенням, наведеним у профільному законодавстві. Це мінімізує ризики помилок при формулюванні обвинувачення та під час судового розгляду. У перспективі бажаною є уніфікація термінології на законодавчому рівні або вироблення єдиних підходів у судовій практиці.

1.2. Типи систем та мереж як об’єктів посягання

Об’єктами посягання за ст. 361 КК України можуть бути різноманітні системи та мережі. Їх класифікація допомагає зрозуміти потенційні масштаби шкоди та особливості розслідування.

За призначенням розрізняють:

1. Державні інформаційні ресурси: системи, що містять інформацію, яка належить державі або перебуває у її розпорядженні (реєстри, бази даних органів влади). Їх компрометація може мати значні наслідки для функціонування держави;
2. Банківські системи: системи обробки фінансових транзакцій, управління рахунками клієнтів. Атаки на них часто мають на меті викрадення коштів;
3. Системи критичної інфраструктури: системи, що забезпечують життєдіяльність суспільства та держави (енергетика, транспорт, зв’язок, охорона здоров’я). Атаки на такі системи є особливо небезпечними;
4. Корпоративні мережі: внутрішні мережі підприємств, установ, організацій, що містять комерційну таємницю, персональні дані співробітників, фінансову інформацію;
5. Персональні комп’ютери та пристрої: комп’ютери, смартфони, планшети громадян, що можуть бути ціллю для викрадення особистих даних, шантажу, використання у ботнетах.

За типом мереж:

1. Локальні обчислювальні мережі (LAN): мережі, що об’єднують пристрої в межах однієї будівлі або організації;
2. Глобальні мережі (WAN): мережі, що охоплюють великі географічні території (найвідомішим прикладом є Інтернет);
3. Корпоративні мережі (VPN, інтранет): захищені мережі для внутрішнього використання організаціями;
4. Публічні мережі: мережі, доступні широкому загалу (наприклад, публічні Wi-Fi точки).

Розуміння типової архітектури сучасних ІКС (клієнт-серверна модель, хмарні технології, багаторівневі системи захисту) та мереж (маршрутизатори, комутатори, міжмережеві екрани) є важливим для слідчого при плануванні огляду місця події, визначенні місць можливого збереження цифрових слідів та формулюванні питань експерту.

1.3. Поширені вразливості та вектори атак

Несанкціоноване втручання стає можливим через наявність вразливостей у системах та мережах. Вразливості у системах та мережах поділяються на: технічні, програмні, конфігураційні та людський фактор. До технічних вразливостей відносять недоліки в апаратному забезпеченні. До програмних – помилки у коді операційних систем, прикладного програмного забезпечення (включно з вебдодатками). До конфігураційних – неправильні налаштування безпеки систем, мережевого обладнання, прав доступу. До людського фактора потрібно віднести необережність користувачів, використання слабких паролів, недостатню обізнаність щодо загроз (наприклад, фішингу).

Зловмисники використовують ці вразливості через різні вектори атак, релевантні для ст. 361 КК України, як-от:

– *шкідливе програмне забезпечення (ШПЗ (Malware)):* віруси, трояни, програми-вимагачі (ransomware), шпигунське ПЗ (spyware), руткіти, боти;

– *фішинг (Phishing):* виманювання конфіденційної інформації (логіни, паролі, дані платіжних карток) шляхом маскування під довірену особу чи організацію (за допомогою email, месенджерів, підроблених вебсайтів);

– *соціальна інженерія:* маніпулювання людьми з метою отримання доступу до систем або інформації (телефонні дзвінки, видавання себе за співробітника техпідтримки тощо);

– *атаки на відмову в обслуговуванні (Denial of Service, DoS/DDoS):* перевантаження системи або мережевого каналу запитами з метою унеможливлення доступу для легітимних користувачів (блокування інформації або порушення маршрутизації);

– *використання експлойтів (Exploits):* використання відомих або невідомих (0-day) вразливостей у програмному забезпечені (ПЗ) для отримання несанкціонованого доступу або виконання шкідливого коду;

– *атаки типу «людина посередині» (Man-in-the-Middle, MitM):* перехоплення та можлива модифікація комунікацій між двома сторонами;

– *SQL-ін'єкції (SQL Injection):* впровадження шкідливого SQL-коду через вразливості вебдодатків для отримання доступу до баз даних;

– *атаки перебору (Brute-force attacks):* спроби вгадати пароль шляхом перебору всіх можливих комбінацій або за словником.

Важливо усвідомлювати, що вибір вектора атаки часто корелює з типом системи, яка є ціллю. Наприклад, об'єкти критичної

інфраструктури або державні ресурси частіше стають мішенню для складних, цілеспрямованих атак (Advanced Persistent Threats, APT), які можуть тривати довго, використовувати 0-day експлойти та фінансуватися державними структурами. Водночас масові фішингові розсилки або атаки програм-вимагачів зазвичай спрямовані на широке коло користувачів та компаній із метою фінансової вигоди.

Розуміння цього зв’язку вже на етапі отримання первинної інформації про інцидент (наприклад, заяви потерпілого) дозволяє слідчому формувати більш обґрунтовані первинні версії щодо можливого способу вчинення злочину, його мотивів та потенційних зловмисників. Це, в свою чергу, безпосередньо впливає на визначення пріоритетів та планування першочергових слідчих (розшукових) дій, наприклад необхідності термінового запиту даних у певних провайдерів чи залучення вузькопрофільних спеціалістів.

Розділ 2. КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА НЕСАНКЦІОНОВАНЕ ВТРУЧАННЯ В РОБОТУ ІНФОРМАЦІЙНИХ (АВТОМАТИЗОВАНИХ), ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ, ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖ (СТ. 361 КК УКРАЇНИ)

2.1. Юридичний аналіз складу несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж

Частина 1 ст. 361 КК України (кримінальний проступок) передбачає відповідальність за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Обов'язковими ознаками складу цього кримінального правопорушення є: об'єкт, предмет, об'єктивна сторона, суб'єкт та суб'єктивна сторона.

Об'єкт: родовий об'єкт – суспільні відносини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (розділ XVI КК України).

Основний безпосередній об'єкт – встановлений законодавством порядок роботи та безпека функціонування інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, а також безпека інформації, що в них обробляється, зберігається або передається.

Предмет: інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи та електронні комунікаційні мережі як комплекси технічних та програмних засобів (див. підрозділ 1.1). Важливо у кожному кримінальному провадженні чітко ідентифікувати конкретну систему чи мережу, в роботу якої було здійснено втручання, та описати її характеристики у відповідних процесуальних документах.

Об'єктивна сторона: склад кримінального правопорушення (ч. 1 ст. 361 КК України) є формальним, тобто закінченим це правопорушення вважається з моменту вчинення діяння – несанкціонованого втручання у відповідні системи/мережі.

Під несанкціонованим втручанням в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж розуміється активна дія, а саме проникнення будь-яким способом до цих систем чи мереж (будь-який вплив на нормальний режим функціонування системи/мережі або на інформацію в ній) і вчинення дій, які змінюють режим їхньої роботи або ж повністю чи частково припиняють їхню роботу без дозволу (згоди) відповідного власника або уповноважених ним осіб або з порушенням встановлених правил.

Згідно з ч. 6 ст. 361 КК України дії, передбачені ч. 1–4 цієї статті, не вважаються несанкціонованим втручанням в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж.

Суб'єкт: загальний – фізична осудна особа, яка досягла 16-річного віку. Встановлення конкретної особи суб'єкта часто є одним із найскладніших завдань у розслідуванні кіберзлочинів через використання зловмисниками засобів анонімізації (VPN, Tor, проксі-сервери), викрадених облікових записів тощо.

Суб'єктивна сторона: характеризується виключно прямим умислом. Особа усвідомлює суспільно небезпечний характер свого діяння (несанкціоноване втручання) і бажає його вчинити. Мотиви (корисливий, хуліганський, помста, політичний тощо) та мета вчинення кримінального правопорушення не є обов'язковими ознаками основного складу кримінального правопорушення, передбаченого ч. 1 ст. 361 КК України, але можуть враховуватися при призначенні покарання.

2.2. Кваліфікуючі та особливо кваліфікуючі ознаки несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж

У ч. 2–5 ст. 361 КК України передбачені кваліфікуючі та особливо кваліфікуючі ознаки несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

Частина 2 ст. 361 КК України містить такі кваліфікуючі ознаки, як вчинення:

– повторно: вчинення двох або більше кримінальних правопорушень, передбачених ст. 361 КК України;

– за попередньою змовою групою осіб: якщо його спільно вчинили декілька осіб (дві або більше), які заздалегідь, тобто до початку кримінального правопорушення, передбаченого ст. 361 КК України, домовилися про спільне його вчинення.

Частина 3 ст. 361 КК України передбачає відповідальність за дії, передбачені ч. 1 або 2 цієї статті, якщо вони призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації. За конструкцією це матеріальний склад кримінального правопорушення, який вважається закінченим із моменту настання хоча б одного з таких суспільно небезпечних наслідків:

1. Витік інформації: несанкціоноване ознайомлення з інформацією хоча б однією сторонньою особою;
2. Втрата інформації: фізичне або логічне знищення інформації, унеможливлення доступу до неї;
3. Підробка інформації: внесення неправдивих даних або зміна існуючих;
4. Блокування інформації: унеможливлення доступу до інформації для легітимних користувачів;
5. Спотворення процесу обробки інформації: порушення логіки роботи програм, алгоритмів обробки даних;
6. Порушення встановленого порядку маршрутизації інформації: зміна шляхів передачі даних у мережі (наприклад, перенаправлення трафіку).

Обов’язковою ознакою складу кримінального правопорушення, передбаченого ч. 3 ст. 361 КК України, є встановлення причинного зв’язку між несанкціонованим втручанням та одним із зазначених суспільно небезпечних наслідків.

Частина 4 ст. 361 КК України передбачає відповідальність за дії, передбачені ч. 1 або 2 цієї статті, якщо вони:

– заподіяли значну шкоду. Згідно з приміткою до ст. 361 КК України значною шкодою у ст. ст. 361–363-1 КК України вважається така шкода, яка в 300 і більше разів перевищує неоподатковуваний мінімум доходів громадян. При кваліфікації кримінальних правопорушень як один неоподатковуваний мінімум доходів громадян береться одна соціальна податкова пільга, яка у 2025 р. становить 1514 грн. Відповідно,

значною шкодою у 2025 р. визнається шкода у розмірі 454 тис. 200 грн і більше;

– створили небезпеку тяжких технологічних аварій або екологічних катастроф. Під технологічною аварією мається на увазі, зокрема, вихід із ладу, поломка, ушкодження, збій, порушення нормального режиму роботи електрообладнання (п. 3.1 Правил технічної експлуатації електроустановок споживачів, затверджених наказом Міністерства палива та енергетики України від 25.07.2006 № 258); небезпечна подія техногенного характеру, що виникла під час експлуатації джерела небезпеки і за своїми наслідками призвела (може призвести) до загибелі, загрози життю або здоров'ю працівників об'єкта підвищеної небезпеки і населення чи до забруднення навколишнього природного середовища (ст. 1 Закону України «Про об'єкти підвищеної небезпеки»). Екологічною катастрофою слід визнавати надзвичайну екологічну ситуацію, при якій на окремій місцевості сталися негативні зміни в навколишньому природному середовищі, що потребують застосування надзвичайних заходів з боку держави (ст. 1 Закону України «Про зону надзвичайної екологічної ситуації»). При вирішенні питання про тяжкість технологічної аварії або екологічної катастрофи слід враховувати Порядок класифікації надзвичайних ситуацій за їх рівнями, затверджений постановою Кабінету Міністрів України від 24 березня 2004 р. № 368;

– створили небезпеку загибелі або масового захворювання населення, тобто створили реальну загрозу спричинення смерті невизначеній кількості людей чи масового поширення інфекційної хвороби серед населення відповідної території за короткий проміжок часу (епідемії) (ст. 1 Закону України «Про захист населення від інфекційних хвороб»);

– створили небезпеку інших тяжких наслідків. Інші тяжкі наслідки – оціночне поняття. До них можна віднести загрозу спричинення середньої тяжкості або тяжких тілесних ушкоджень невизначеній кількості людей, загрозу суттєвих порушень роботи транспорту, зв'язку, функціонування органів влади тощо.

Частина 5 ст. 361 КК України передбачає відповідальність за дії, передбачені ч. 3 або 4 цієї статті, вчинені під час дії воєнного стану.

Воєнний стан – це особливий правовий режим, що вводиться в Україні або в окремих її місцевостях у разі збройної агресії чи загрози нападу, небезпеки державній незалежності України, її територіальній цілісності та передбачає надання відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам

місцевого самоврядування повноважень, необхідних для відвернення загрози, відсічі збройної агресії та забезпечення національної безпеки, усунення загрози небезпеки державній незалежності України, її територіальній цілісності, а також тимчасове, зумовлене загрозою, обмеження конституційних прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень (ст. 1 Закону України «Про правовий режим воєнного стану»).

2.3. Відмежування несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж від суміжних складів кримінальних правопорушень

НСВ за ст. 361 КК України часто є частиною більш складної кримінальної протиправної діяльності, тому важливо правильно відмежовувати склад цього кримінального правопорушення від суміжних складів.

Розділ XVI КК України:

– ст. 361-1 «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут». Якщо НСВ здійснювалося за допомогою спеціально створеного або придбаного шкідливого ПЗ, дії можуть кваліфікуватися за сукупністю ст. ст. 361 та 361-1 КК України;

– ст. 361-2 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації». Якщо внаслідок НСВ (витоку) інформація з обмеженим доступом була в подальшому збута чи розповсюджена, можлива кваліфікація за сукупністю ст. ст. 361 та 361-2 КК України;

– ст. 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї». Ця стаття стосується дій, вчинених особою, яка має право доступу до системи (наприклад, системним адміністратором). Якщо ж доступ був несанкціонованим, дії особи кваліфікуються за ст. 361 КК України;

– ст. 363 «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється». Відповідальність настає за порушення правил, якщо це спричинило наслідки, передбачені приміткою до ст. 361 КК України, і вчинене особою, відповідальною за експлуатацію комп'ютерів, систем чи мереж;

– ст. 363-1 «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку». Часто перетинається з DDoS-атаками, що також можуть кваліфікуватися як блокування інформації або порушення маршрутизації за ч. 3 ст. 361 КК України. Кваліфікація залежить від конкретних обставин та наслідків.

Кримінальні правопорушення проти власності: якщо НСВ було лише способом вчинення крадіжки (ст. 185 КК України) або шахрайства (ст. 190 КК України), наприклад шляхом отримання доступу до банківського рахунку та викрадення коштів, дії кваліфікуються за сукупністю відповідної частини ст. 361 КК України та статті розділу про кримінальні правопорушення проти власності.

Інші кримінальні правопорушення: НСВ може бути способом вчинення кримінальних правопорушень проти державної таємниці, комерційної таємниці, порушення таємниці листування, терористичного акту тощо. У таких випадках також застосовується кваліфікація за сукупністю кримінальних правопорушень.

Складність сучасних кібератак, які часто є багатоетапними та переслідують кілька цілей (наприклад, спочатку НСВ для отримання доступу, потім розгортання ransomware для блокування даних та вимагання викупу, а паралельно – викрадення конфіденційної інформації для продажу), створює реальний ризик неправильної або неповної кваліфікації кримінальних правопорушень. Якщо слідчий фокусується лише на одному аспекті атаки (наприклад, тільки на факті НСВ), ігноруючи інші склади кримінальних правопорушень (вимагання, несанкціонований збут інформації тощо), це може призвести до неповноти розслідування, притягнення винних до відповідальності не за всі вчинені діяння та, як наслідок, призначення несправедливого покарання. Тому критично важливо аналізувати всю сукупність дій зловмисника та правильно кваліфікувати кожен епізод кримінальної протиправної діяльності.

Розділ 3. ОРГАНІЗАЦІЯ ТА ПРОВЕДЕННЯ СРД, НСРД ТА ІНШИХ ПРОЦЕСУАЛЬНИХ ДІЙ ТА РОЗШУКОВИХ ЗАХОДІВ ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, КВАЛІФІКОВАНИХ ЗА СТ. 361 КК УКРАЇНИ

3.1. Планування досудового розслідування кримінальних правопорушень, кваліфікованих за ст. 361 КК України

Ефективне розслідування кримінальних правопорушень, передбачених ст. 361 КК України, вимагає його ретельного планування з урахуванням специфіки кіберзлочинів. Алгоритмізація є обов'язковою складовою для будь-якого процесу, звичайно, лише в тих випадках, коли у його організатора на меті буде послідовна та цілеспрямована діяльність. Розслідування досліджуваних кримінальних правопорушень не є винятком. Водночас алгоритмізація повинна бути побудована відповідно до певної системи. У цьому розрізі процес розслідування будується на типових слідчих ситуаціях. Адже вказані ситуації можуть акумулювати в собі як криміналістичні версії, так і окремі відомості про подію протиправного діяння та її учасників (потерпілих, свідків, підозрюваних).

Розслідування зазвичай починається з отримання первинної інформації: заяви потерпілої особи (фізичної чи юридичної особи), повідомлення представника компанії, рапорту оперативного працівника про виявлення ознак протиправного діяння, інформації зі ЗМІ або даних моніторингу (наприклад, від CERT-UA). На цьому етапі важливо максимально детально зафіксувати обставини події: час виявлення втручання, характер наслідків, опис атакованої системи, відомі IP-адреси, підозрілі файли тощо.

На основі початкової інформації уповноважена особа висуває такі типові слідчі версії:

– *щодо способу вчинення:* який вектор атаки був використаний (malware, фішинг, експлойт, DDoS тощо)? Чи мав місце фізичний доступ до обладнання?

– *щодо суб'єкта:* чи є підозри щодо конкретних осіб (зовнішні зловмисники, інсайдери)? Який рівень їхньої технічної кваліфікації? Звідки могла здійснюватися атака (географічно)?

– *щодо місця знаходження доказів:* де можуть зберігатися цифрові сліди (логи серверів, комп'ютери користувачів, мережеве обладнання, дані провайдерів, хмарні сховища)?

– *щодо мотивів:* якою була мета атаки (фінансова вигода, шпигунство, дестабілізація роботи, помста)?

Складання плану розслідування. План має бути гнучким та враховувати специфіку кіберзлочинів:

Швидкоплинність цифрових доказів. Необхідність негайного проведення дій для збереження логів, даних трафіку, які можуть швидко видалятися або перезаписуватися.

Транскордонність. Імовірність знаходження зловмисників або серверів за кордоном вимагає планування заходів міжнародної правової допомоги.

Технічна складність. Необхідність залучення спеціалістів (із кіберполіції, експертів) на ранніх етапах.

Великі обсяги даних. Потреба у використанні спеціалізованих інструментів для аналізу логів, трафіку, образів дисків. План повинен визначати послідовність слідчих (розшукових) дій, відповідальних виконавців та строки.

3.2. Типові слідчі ситуації та відповідні їм алгоритми дій працівників правоохоронних органів під час розслідування кримінальних правопорушень, кваліфікованих за ст. 361 КК України

Опитування слідчих працівників Національної поліції України дало підстави сформувати, зокрема, такі типові слідчі ситуації у кримінальних провадженнях, розпочатих за ст. 361 КК України.

1. Дії, пов'язані з *несанкціонованим отриманням доступу до акаунту особи в соцмережах та месенджерах* та *розміщенням у них від імені справжніх користувачів оголошень про збір коштів* на лікування, розсиланням іншим користувачам від їхнього імені повідомлень про нібито скрутну життєву ситуацію чи з проханням надання (перерахування) матеріальної допомоги.

Типовий приклад: 12.01.2025 гр. К. помітила, що втратила доступ до свого акаунту в соцмережі «Фейсбук». Наступного дня їй зателефонувала знайома П. та повідомила, що відреагувала на її прохання про допомогу, яке побачила у «Фейсбук» на сторінці К., та перерахувала на вказаний там рахунок 10 000 грн. Гр. К. пояснила, що

ніяких оголошень не розміщувала, про допомогу не просила. Як пізніше з'ясувалось, невідома особа, скориставшись акаунтом К, розіслала її знайомим прохання про допомогу, на яке відгукнулось 5 осіб, перерахувавши на рахунок зловмисника понад 50 000 грн;

2. Дії, пов'язані з *несанкціонованим отриманням доступу до банківського рахунку* (облікового запису у веббанкінгу) та *викраденням коштів* шляхом їх перерахунку на підконтрольний правопорушнику рахунок.

Типовий приклад: 11.04.2025 гр. А. виявив відсутність на своєму банківському рахунку коштів, які зникли за невизначених обставин. Опитаний/допитаний потерпілий пояснив, що перед зникненням коштів він не спілкувався з правопорушником, не розголошував конфіденційні відомості щодо номера рахунку, тризначного коду безпеки, паролів із sms-повідомлень.

Як пізніше з'ясувалось, невідома особа отримала доступ до його облікового запису у веббанкінгу (номеру рахунку, дати випуску, CVC-коду) та перерахувала кошти (або оформила кредит) на чужий рахунок;

3. Дії, пов'язані з *несанкціонованим отриманням доступу до персонального комп'ютера (смартфона) та програмного забезпечення на ньому* шляхом пересилання повідомлень із шкідливим програмним забезпеченням.

Типовий приклад: 10.03.2025 бухгалтер ТОВ «МИР» гр. А. побачила, що на електронну пошту підприємства надійшло повідомлення від невідомої особи, яке вона відкрила та переглянула. Наступного дня на мобільний телефон керівника товариства почали надходити повідомлення про перерахунок коштів із рахунків товариства. Зайшовши у додаток веббанкінгу, він виявив, що з рахунків підприємства без його відома та згоди перераховано 300 000 грн на сторонні рахунки.

Як пізніше з'ясувалось, на електронну пошту товариства зловмисник направив замасковане під повідомлення шкідливе програмне забезпечення, яке надало віддалений доступ до комп'ютера (забезпечило автоматичний перерахунок коштів на чужий рахунок).

Інший варіант – відомості на комп'ютері було зашифровано, а керівник товариства отримав вимогу про виплату певної суми коштів за розшифровку даних.

Для збору доказів у провадженнях за ст. 361 КК України застосовується комплекс слідчих (розшукових) дій, передбачених КПК України, з урахуванням специфіки цифрових доказів (табл. 3.1).

Таблиця 3.1

Слідчі (розшукові) дії при розслідуванні злочинів за ст. 361 КК України та їхня специфіка

Слідча (розшукова) дія	Мета проведення	Ключові особливості/ Виклики	Норма КПК України	Необхідність залучення спеціаліста/ експерта
Огляд місця події	Фіксація обстановки; виявлення та огляд комп'ютерної техніки, серверів, мережевого обладнання; виявлення первинних цифрових слідів.	Необхідність фіксації стану системи *до* вилучення; ризик втрати даних при вимкненні; важливість правильного документування конфігурації мережі.	ст. 237	Обов'язково (спеціаліст з кіберполіції або ІТ-спеціаліст)
Тимчасовий доступ до речей і документів	Отримання інформації, що становить таємницю (логи провайдерів, дані абонентів, банківські дані, дані з хмарних сервісів тощо).	Необхідність отримання ухвали слідчого судді; чітке формулювання обсягу даних; стислі терміни зберігання логів у провайдерів; транскордонні запити.	ст. ст. 159–166	Зазвичай ні, але консультація може бути корисною
Обшук	Виявлення та вилучення комп'ютерної техніки, носіїв інформації, мобільних пристроїв, паролів, документації, що стосуються втручання.	Правильне вилучення цифрових носіїв (створення образів «на місці» або вилучення для дослідження); ризик віддаленого знищення даних; шифрування дисків.	ст. ст. 234–236	Обов'язково (спеціаліст з кіберполіції або ІТ-спеціаліст)
Допит (потерпілого, свідка, підозрюваного)	З'ясування обставин події; отримання технічних деталей; встановлення можливих	Необхідність використання спеціальної термінології; складність перевірки показань щодо	ст. 224	Бажано (для підготовки запитань та оцінки відповідей)

	мотивів, підозрюваних; з'ясування технічних знань та навичок підозрюваного.	технічних аспектів; можлива неправдива інформація від підозрюваного.		
Зняття інформації з електронних комунікаційних мереж (НСРД)	Отримання даних про з'єднання, трафік, зміст комунікацій підозрюваних у реальному часі або за певний період.	Негласний характер; необхідність отримання ухвали апеляційного суду; технічна складність реалізації; великі обсяги даних.	ст. ст. 263–265	Технічні спеціалісти оперативних підрозділів
Призначення судових експертиз	Дослідження комп'ютерної техніки, носіїв інформації, ПЗ, мережевого трафіку для встановлення механізму втручання, ідентифікації слідів, відновлення даних, аналіз ШПЗ.	Основний вид – комп'ютерно-технічна експертиза (КТЕ); важливість правильного формулювання запитань експерту; тривалість проведення.	ст. ст. 242–245	Експерт відповідної спеціальності
Слідчий експеримент	Відтворення механізму втручання (якщо є можливість); перевірка певних версій щодо способу атаки.	Технічна складність відтворення; необхідність створення безпечного середовища; ризик завдання шкоди.	ст. 240	Обов'язково (спеціаліст/експерт)

На основі вивчення слідчо-судової практики було визначено такі типові слідчі ситуації початкового етапу розслідування кримінальних правопорушень, кваліфікованих за ст. 361 КК України:

1) вчинено кримінальне правопорушення, кваліфіковане за ст. 361 КК України, наявна особистісна доказова інформація, правопорушник відомий;

2) вчинено кримінальне правопорушення, кваліфіковане за ст. 361 КК України, наявна особистісна доказова інформація, правопорушник невідомий;

3) вчинено кримінальне правопорушення, кваліфіковане за ст. 361 КК України, наявна матеріальна та особистісна доказова інформація, правопорушник відомий, але його дії замасковані під вид законних фінансових операцій;

4) вчинено кримінальне правопорушення, кваліфіковане за ст. 361 КК України, наявна заява від потерпілого, відсутня достатня доказова інформація.

Крім того, було окреслено алгоритми вирішення кожної з цих слідчих ситуацій. У першій ситуації (наявна особистісна доказова інформація та правопорушник відомий) уповноважена особа повинна провести комплекс заходів, за допомогою яких необхідно з'ясувати можливі обставини провадження для доказування вини правопорушника, зокрема: огляд засобів електронно-обчислювальної техніки правопорушника під час проведення обшуку (смартфонів, планшетів, ноутбуків, персональних комп'ютерів); допит підозрюваного з приводу обставин обману громадян та законності його діяльності; допит потерпілого щодо обставин вчиненого кримінального правопорушення; витребування відомостей від інтернет-провайдерів та операторів телекомунікаційного зв'язку; з'ясування умов створення фіктивного сайту, створення програм віддаленого доступу, «троянів», «ботів»; пред'явлення підозрюваного для впізнання потерпілому за голосом (у разі спілкування в телефонному режимі) та в натурі (у разі комунікації у режимі відеоконференції); призначення комп'ютерно-технічної та інших видів експертиз.

Друга ситуація є найбільш розповсюдженою у досліджуваній категорії кримінальних проваджень – наявна особистісна доказова інформація, але правопорушник невідомий. Для її вирішення всі зусилля уповноважених осіб повинні бути направлені на встановлення особи, яка вчинила кримінальне правопорушення, кваліфіковане за ст. 361 КК України, а також її місцезнаходження. Для реалізації вказаного потрібно проводити комплекс заходів, спрямованих на встановлення IP-адреси та осіб, які мали доступ до електронно-обчислювальної техніки.

У третій ситуації (наявна матеріальна та особистісна доказова інформація, правопорушник відомий, але його дії замасковані під вид законних фінансових операцій) уповноважені особи повинні спрямувати усі зусилля на опрацювання змісту файлів та аналіз змісту web-браузерів, а також дослідження змісту електронної пошти, журналу вхідних і вихідних дзвінків на всіх доступних гаджетах потерпілого.

Вказана ситуація характеризується обставинами, коли особи не переховуються від правоохоронних органів, водночас заперечуючи свою причетність до вчинення протиправних дій. З огляду на це перед

уповноваженими особами (слідчий, дізнавач, прокурор, оперативний працівник, який виконує доручення слідчого) постає низка завдань, які необхідно вирішити в найкоротші терміни. Зокрема, виявити, зібрати та отримати певну сукупність належних, обґрунтованих та достатніх обвинувальних доказів шляхом з'ясування у потерпілих осіб обставин, за яких розпочиналися та завершилися протиправні дії, а також ролі кожної причетної (підозрюваної) до цього особи. Крім того, варто провести детальний огляд місця події, вилучення слідів, які вказують на факт кримінального правопорушення, та встановити можливих свідків. Провести пред'явлення для впізнання осіб, причетних до протиправних дій. Також необхідно терміново провести обшуки житла та іншого володіння особи з метою виявлення і вилучення електронних носіїв, а також інших предметів і документів, що свідчать про вчинення протиправних дій. Для покращення результативності розслідування доцільно проводити й негласні слідчі (розшукові) дії з метою встановлення протиправних зв'язків злочинця, його образу життя, можливого місця знаходження його, речей, предметів, документів, що підтверджують причетність до кримінального правопорушення, та інших доказів, які цікавлять слідство.

Четверта ситуація (наявна заява від потерпілого та відсутня достатня доказова інформація) вирішується завдяки проведенню максимальної кількості СРД, НСРД та інших розшукових заходів для з'ясування як обставин вчиненого протиправного діяння, так і встановлення особи правопорушника.

Також для розв'язання вказаних слідчих ситуацій запропоновано вирішення таких тактичних завдань:

1) з'ясування механізму кримінальних правопорушень, кваліфікованих за ст. 361 КК України;
2) визначення точок доступу, з яких реалізувалися протиправні дії;
3) перевірка цифрових слідів, які залишені під час проведення електронних операцій;
4) встановлення осіб, які реалізували незаконне втручання в роботу ЕОТ;
5) перевірка мобільних контактів правопорушника та його особистих зв'язків;
6) перевірка банківських і поштових переказів правопорушника;
7) з'ясування всіх епізодів протиправної діяльності;
8) вжиття заходів стосовно попередження протидії розслідуванню.

3.3. Особливості проведення СРД, НСРД та інших процесуальних дій та розшукових заходів під час розслідування кримінальних правопорушень, кваліфікованих за ст. 361 КК України

Огляд місця події проводиться з метою фіксації обстановки, виявлення та огляду ЕОТ, серверів, мережевого обладнання; виявлення первинних цифрових слідів. Після прибуття на місце уповноважена особа (слідчий, дізнавач, прокурор, оперативний працівник, який виконує доручення слідчого) повинна вжити таких попереджувальних заходів, які забезпечують цілісність і незмінність інформації на ЕОТ: захистити і взяти під охорону приміщення, в якому перебувають засоби ЕОТ; віддалити людей від обладнання та джерел живлення; виявити стан комп'ютерної техніки (вимкнена або увімкнена); переконатися, що за жодних обставин вимкнений ЕОТ не буде ввімкнено. Під час проведення огляду спеціаліст безпосередньо надає допомогу уповноваженій особі: у виявленні засобів ЕОТ, її окремих компонентів, документації та інших об'єктів, які можуть містити сліди неправомірних дій; у коректному (з погляду збереження слідів кримінального правопорушення) відключенні засобів ЕОТ від енергопостачання; в описі засобів ЕОТ, її окремих компонентів і документації, що вилучаються, у протоколі та додатках до нього; у вирішенні питання щодо складу комплекту ЕОТ або окремих її компонентів, які підлягають вилученню або ізолюванню від вільного доступу; у підготовці засобів ЕОТ до транспортування (їх упакуванні, опечатуванні). Під час розслідування кримінальних правопорушень, кваліфікованих за ст. 361 КК України, потрібно максимально забезпечити збереження інформації, яка перебуває на флеш-накопичувачах, жорстких дисках, у кеш-пам'яті відповідного пристрою, хмарних сховищах тощо.

Тимчасовий доступ до речей і документів здійснюється для отримання інформації, що становить таємницю (логи провайдерів, дані абонентів, банківські дані, дані з хмарних сервісів тощо).

Обшук проводиться з метою виявлення та вилучення ЕОТ, носіїв інформації, мобільних пристроїв, паролів, документів, що стосуються втручання. Обов'язково до реалізації вказаної СРД залучається спеціаліст із кіберполіції та/або ІТ-спеціаліст. Адже під час проведення обшуку виникає необхідність вилучати як заблоковані, так і розблоковані переносні гаджети (смартфони, smart-годинники, портативні відеореєстратори, GPS-навігатори). Звісно, специфіка їх вилучення

відрізняється, адже з розблокованих пристроїв в принципі достатньо дістати, якщо вони є, SIM-карту та карту пам'яті, тоді як заблоковані потрібно ще розблокувати перед вилученням відповідних слотів.

Із-поміж об'єктів, що їх необхідно вилучати під час обшуку, слід назвати такі:

1) ЕОТ, за допомогою якої здійснювалося втручання в роботу інтернет-мереж для їх дестабілізації (комп'ютери, планшети, ноутбуки, смартфони);

2) реквізити карток, що викрадені з серверів магазинів електронної торгівлі, платіжних і розрахункових систем, із персональних гаджетів користувачів;

3) фотографії, відеозаписи, на яких наявні дані, що мають значення для кримінального провадження;

4) квитанції про здійснення банківських операцій;

5) смартфони або інші гаджети, в яких наявна адресна книга (ПІБ й адреси клієнтів фінансових установ, підприємств та організацій різних форм власності);

6) записні книжки, журнали, рукописні тексти з наявними даними про особу потерпілого або інших зацікавлених осіб та ін.

Допит (потерпілого, свідка, підозрюваного) проводиться для з'ясування обставин події; отримання технічних деталей, встановлення можливих мотивів, підозрюваних, з'ясування технічних знань та навичок підозрюваного.

Під час допиту потерпілого необхідно:

– з'ясувати обставини вчинення протиправного діяння (час, місце, зокрема, з доступом до загальної мережі Wi-Fi, наявність поблизу сторонніх осіб – можливість віддаленого підключення з іншого гаджета);

– проаналізувати його передумови (чи були надіслані на номер потерпілого та прийняті повідомлення – в якому месенджері та якого змісту, чи були наявні дзвінки – в якому месенджері та якого змісту);

– встановити послідовність дій потерпілого після вчинення кримінального правопорушення (одразу повідомив у правоохоронні органи чи своїм знайомим, родичам, що зробив з гаджетом – вимкнув, перезавантажив, продовжив користуватися).

Під час допиту підозрюваних необхідно встановлювати такі факти:

– ЕОТ, яка була застосована для вчинення протиправних діянь;

– програмне забезпечення, яке використовувалось для вчинення кримінального правопорушення (програми віддаленого доступу, «трояни», «боти»);

– логіни та паролі акаунтів, які використовувались для спілкування з потерпілими;

– реквізити банківських карток та рахунків, на які переказували кошти.

Зняття інформації з електронних комунікаційних мереж реалізується з метою отримання даних про з'єднання, трафік, зміст комунікацій підозрюваних у реальному часі або за певний період із обов'язковим залученням технічних спеціалістів оперативних підрозділів.

Призначення судових експертиз проводиться з метою дослідження ЕОТ, носіїв інформації, програмного забезпечення, мережевого трафіку для встановлення механізму втручання, ідентифікації слідів, відновлення даних тощо.

З-поміж судових експертиз варто призначати та проводити такі, як:

1) стосовно ЕОТ: комп'ютерно-технічна експертиза (експертиза технічних комп'ютерних засобів; експертиза даних; експертиза програмного забезпечення), дактилоскопічна експертиза вилучених слідів рук із різних предметів ЕОТ;

2) стосовно телекомунікаційних засобів та систем (експертиза телекомунікаційних систем і засобів);

3) стосовно документів (експертиза документів, які утворюються внаслідок вчинення протиправних дій – криміналістична почеркознавча експертиза; технічна експертиза документів; дактилоскопічна експертиза вилучених слідів рук із документів);

4) стосовно майна, яке було предметом посягання (криміналістична експертиза матеріалів, речовин і виробів; трасологічна експертиза; дактилоскопічна експертиза вилучених слідів рук із різних предметів).

Об'єкти, що направляються на експертизу:

– власні гаджети потерпілого (смартфон, планшет, ноутбук, комп'ютер, модеми, маршрутизатори);

– власні гаджети підозрюваного (смартфон, планшет, ноутбук, комп'ютер, модеми, маршрутизатори);

– флеш-накопичувачі;

– жорсткі диски та ін.

Крім того, варто вказати, що існують такі розповсюджені способи підміни реальної IP-адреси: підключення до проксі-сервера, використання інтернет-браузера TOR, маскування IP-адреси через VPN. Під час комп'ютерно-мережевої експертизи надзвичайно важливо виявити програмне забезпечення, що було встановлене для приховування IP-адреси. Прикладами вищевказаного можуть бути: ProxyCap, Proxyfier, Proxy Switcher – програми для проксі; TOR Browser, Tor Control (anonymity layer) for Firefox; NordVPN, OpenVPN, ExpressVPN, PureVPN

for Teams, ProtonVPN, NetMotion – програми, які забезпечують сервіс VPN. Якщо експертом буде проведено якісне дослідження мережевих слідів та викрито усі ланцюжки IP-адрес, через які проходили транзакції, з великою ймовірністю таке кримінальне правопорушення буде розкрито.

Усі СРД, НСРД та інші процесуальні дії та пошукові заходи повинні ретельно фіксуватися у відповідних протоколах з детальним описом дій, виявлених об'єктів та застосованих технічних засобів.

Особливу увагу слід приділяти процесуальній «чистоті» при роботі з цифровими доказами. Ці докази є надзвичайно чутливими до будь-яких змін, їх легко модифікувати або знищити, навіть ненавмисно. Отримання доступу до них часто пов'язане зі втручанням у сферу приватного життя (доступ до даних на комп'ютері, в телефоні, до листування). Тому будь-які порушення встановленої процедури – неправильне оформлення протоколу огляду чи обшуку, відсутність необхідної ухвали слідчого судді на ТДРД, некоректне копіювання даних без забезпечення їхньої цілісності (наприклад, без фіксації хеш-сум) – можуть стати фатальними. Захист у суді обов'язково використовує такі помилки для обґрунтування клопотання про визнання ключових цифрових доказів недопустимими. Це може призвести до руйнації всієї доказової бази та виправдання винної особи. Отже, бездоганне дотримання процесуальних норм при зборі та фіксації цифрових доказів є не просто формальною вимогою, а запорукою успішного завершення розслідування.

Розділ 4. ФІКСАЦІЯ ФАКТІВ ПРАВОПОРУШЕННЯ НА ПРИКЛАДІ ТИПОВИХ СИТУАЦІЙ

4.1. Ідентифікація та збереження цифрових доказів

Цифрові докази – це будь-яка інформація, що має доказове значення, зберігається або передається в електронній формі. У кримінальних провадженнях за ст. 361 КК вони є основними. До таких належать:

1. Файли системних журналів (логи) операційних систем, вебсерверів, баз даних, мережевого обладнання (маршрутизаторів, міжмережевих екранів), систем виявлення вторгнень (IDS/IPS);
2. Дані системного реєстру (Windows);
3. Історія відвідувань вебсайтів у браузері, кеш, файли cookie;
4. Електронне листування, повідомлення в месенджерах;
5. Файли, створені, змінені або вилучені зловмисником;
6. Дані з пам'яті мобільних пристроїв (журнали дзвінків, SMS, дані додатків);
7. Дані, що зберігаються у хмарних сховищах (Google Drive, Dropbox тощо);
8. Дані про мережевий трафік (NetFlow, PCAP-файли);
9. Конфігураційні файли систем та мережевого обладнання.

Поводження з цифровими доказами вимагає дотримання специфічних правил:

– *мінімізація змін:* уникати будь-яких дій, що можуть змінити оригінальні дані на носії (наприклад, не завантажувати ОС із досліджуваного диска);

– *документування:* ретельно фіксувати всі дії з цифровими доказами (час, місце, виконавець, використані інструменти);

– *забезпечення цілісності:* використовувати криптографічні хеш-функції (наприклад, SHA-256, MD5) для фіксації стану даних до і після копіювання або аналізу. Хеш-сума слугує «цифровим відбитком», що дозволяє перевірити незмінність даних;

– *використання спеціалізованих засобів:* для копіювання даних (створення криміналістично чистого образу диска) та їх аналізу слід використовувати спеціалізоване програмне (наприклад, EnCase Forensic,

FTK Imager, Autopsy) та апаратне забезпечення (блокатори запису). Робота проводиться з копією (образом), а не з оригіналом.

4.2. Типові слідчі ситуації та алгоритми фіксації

Залежно від характеру НСВ першочергові дії зі збору та фіксації доказів можуть відрізнятися. Розглянемо кілька типових ситуацій.

Ситуація 1. Компрометація сервера/вебсайту (наприклад, дефейс, встановлення вебшелу, викрадення бази даних).

Алгоритм дій:

1. Ізоляція (якщо є можливість). Відключити скомпрометований сервер від мережі для запобігання подальшій шкоді та знищенню слідів (з обережністю, щоб не втратити дані з оперативної пам'яті);
2. Зняття образу. Створити повний фізичний образ жорстких дисків сервера за допомогою спеціалізованого ПЗ та блокатора запису;
3. Зняття дампу пам'яті. Якщо сервер ще працює, зробити дамп оперативної пам'яті (може містити цінні артефакти: процеси, мережеві з'єднання, ключі шифрування);
4. Збір логів. Зібрати всі доступні логи: ОС, вебсервера (Apache, Nginx, IIS), СУБД (MySQL, PostgreSQL), FTP-сервера, логи додатків, логи мережевого обладнання (міжмережевий екран, маршрутизатор), що стосуються періоду атаки;
5. Аналіз трафіку. Якщо здійснювався запис мережевого трафіку (PCAP), вилучити та проаналізувати його;
6. Ідентифікація IP. Проаналізувати логи на предмет виявлення IP-адрес, з яких здійснювалася атака;
7. ТДРД. Підготувати та подати клопотання про тимчасовий доступ до даних інтернет-провайдерів щодо власників ідентифікованих IP-адрес.

Ситуація 2. Фішингова атака (розсилка листів із посиланнями на підроблені сайти для викрадення облікових даних або розповсюдження malware).

Алгоритм дій:

1. Збереження доказів. Зберегти оригінал фішингового листа (з усіма заголовками), зробити скріншоти фішингового сайту;
2. Аналіз листа/сайту. Проаналізувати заголовки листа для встановлення IP-адреси відправника (може бути підроблена). Визначити доменне ім'я фішингового сайту;

3. WHOIS та DNS. Здійснити запити WHOIS для отримання інформації про реєстратора домену та власника (часто анонімізовано). Проаналізувати DNS-записи;

4. ТДРД. Подати клопотання про ТДРД до реєстратора домену та хостинг-провайдера фішингового сайту для отримання даних про особу, що замовила послуги, та логів доступу до сайту;

5. Аналіз Malware. Якщо через фішинг розповсюджувалося шкідливе ПЗ, вилучити його зразок та направити на КТЕ.

6. Допит потерпілих. Допитати осіб, які отримали листи або ввели свої дані на фішинговому сайті, щодо обставин події та можливої шкоди.

Ситуація 3. Мережеве вторгнення (сканування мережі, експлуатація вразливостей, отримання доступу до внутрішніх ресурсів без фізичного доступу).

Алгоритм дій:

1. Аналіз логів безпеки. Зібрати та проаналізувати логи міжмережевих екранів, систем виявлення/запобігання вторгненням (IDS/IPS), VPN-концентраторів, контролерів домену (Active Directory);

2. Аналіз мережевого трафіку. Проаналізувати дані NetFlow або повні дампи трафіку (PCAP), якщо вони доступні, для виявлення аномальної активності, несанкціонованих з'єднань, сканування портів;

3. Ідентифікація джерела. Встановити IP-адреси, з яких здійснювалося вторгнення;

4. Ідентифікація скомпрометованих вузлів. Визначити, які комп'ютери або сервери всередині мережі були скомпрометовані. Здійснити їх огляд та вилучення образів дисків/пам'яті;

5. ТДРД. Подати клопотання про ТДРД до інтернет-провайдерів щодо власників зовнішніх IP-адрес, ідентифікованих як джерело атаки.

Ситуація 4. Використання шкідливого ПЗ (Malware) (зараження комп'ютера вірусом, трояном, ransomware).

Алгоритм дій:

1. Ізоляція. Ізолювати заражений комп'ютер від мережі;

2. Вилучення зразка. Зробити образ диска зараженої системи. Спробувати безпечно вилучити зразок шкідливого файлу;

3. Комп'ютерно-технічна експертиза. Призначити КТЕ (дослідження шкідливих програмних засобів) для:

- визначення типу та функціоналу ШПЗ (крадіжка даних, шифрування, віддалене управління тощо);
- встановлення механізму розповсюдження;
- ідентифікації командних центрів (C&C серверів), з якими зв'язувалося ШПЗ;
- виявлення інших артефактів (вбудовані email, IP-адреси);

4. Аналіз мережевої активності. Проаналізувати логи мережевого обладнання на предмет з'єднань зараженого комп'ютера з C&C серверами або іншими підозрілими ресурсами;

5. ТДРД. Подати клопотання про ТДРД щодо IP-адрес C&C серверів (якщо вони встановлені).

Аналіз типових ситуацій свідчить про критичну важливість фактора часу при фіксації цифрових доказів. У багатьох сценаріях, особливо при DDoS-атаках, швидкому шифруванні даних програмами-вимагачами або автоматичному очищенні логів, ключові цифрові сліди можуть існувати дуже нетривалий час – години або навіть хвилини. Слідчо-оперативна група фізично не завжди може прибути на місце події достатньо швидко, щоб зафіксувати такі швидкоплинні докази. Це підкреслює необхідність проведення превентивної роботи з потенційними потерпілими, особливо зі системними адміністраторами та службами безпеки компаній, банків, державних установ та ОКІ. Вони повинні бути проінструктовані щодо алгоритму першочергових дій зі збереження цифрових доказів (наприклад, негайне збереження всіх релевантних логів, зняття дампів оперативної пам'яті критичних серверів, тимчасова ізоляція скомпрометованих систем від мережі, фіксація часу подій) ще до прибуття правоохоронців. Наявність таких внутрішніх процедур реагування на інциденти (Incident Response Plan) та їх дотримання значно підвищує шанси на збереження важливих доказів і, як наслідок, на успішне розслідування злочину.

4.3. Забезпечення ланцюга безперервності доказів (Chain of Custody)

Для того щоб цифровий доказ був визнаний допустимим у суді, необхідно довести, що він є автентичним (тобто тим самим, що був вилучений) і що його цілісність не була порушена протягом усього процесу розслідування. Це забезпечується дотриманням процедури «ланцюга безперервності доказів» (Chain of Custody). Ця процедура передбачає безперервне документування всіх етапів роботи з доказом:

– *виявлення та ідентифікація:* де, коли, ким і за яких обставин був виявлений цифровий доказ (носій інформації);

– *вилучення:* як, ким і за допомогою яких засобів доказ був вилучений (наприклад, створення образу диска). Фіксація початкової хеш-суми;

– *транспортування та зберігання:* як доказ транспортувався та де зберігався, хто мав до нього доступ;

– *передача:* кожна передача доказу між особами (від слідчого до спеціаліста, від спеціаліста до експерта, повернення слідчому) повинна бути задокументована із зазначенням дати, часу, мети передачі та підписами осіб, що передали та отримали доказ;

– *аналіз:* опис дій, що проводилися з доказом (його копією) під час дослідження чи експертизи. Фіксація кінцевої хеш-суми (має збігатися з початковою, якщо аналіз проводився на копії).

Для спрощення та стандартизації цього процесу доцільно використовувати спеціальні форми (протоколи, акти) для документування ланцюга безперервності (табл. 4.1).

Таблиця 4.1

Ланцюг безперервності цифрових доказів (приклад форми)

№ з/п	Опис доказу (тип носія, модель, серійний №, інше)	Хеш-сума (алгоритм, значення)	Дата/час	Місце дії	Дія (вилучення/ передача/ зберігання/ аналіз)	Хто виконав/ передав (ПІБ, посада, підпис)	Хто отримав (ПІБ, посада, підпис)	Мета передачі/ примітки
1	Жорсткий диск Seagate ST1000DM010, S/N: ZN1XXXXX	SHA-256: e3b0c442...	15.10.2023 /14:30	м. Київ, вул. Хрещатик, 1, каб. 5	Вилучення під час обшуку	Слідчий Петренко П.П. (підпис)	Спеціаліст Іваненко І.І. (підпис)	Для створення образу
2	Образ диска ZN1XXXXX.E01	SHA-256: a1b2c3d4... (образу)	15.10.2023 /16:00	м. Київ, вул. Володимирська, 15	Створення образу	Спеціаліст Іваненко І.І. (підпис)	Слідчий Петренко П.П. (підпис)	Образ створено, оригінал опечатано
3	Образ диска ZN1XXXXX.E01	SHA-256: a1b2c3d4...	16.10.2023 /10:00	м. Київ, вул. Володимирська, 15	Передача експерту	Слідчий Петренко П.П. (підпис)	Експерт Сидоренко С.С. (підпис)	Для проведення КТЕ (постанова № 123)
...	...	...	...	...	...	...	...	...

Розділ 5. ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ ПІДРОЗДІЛІВ КРИМІНАЛЬНОГО АНАЛІЗУ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

5.1. Роль та функції підрозділів кримінального аналізу

Підрозділи кримінального аналізу (ПКА) – це відносно нова, але надзвичайно важлива складова системи Національної поліції України, яка забезпечує *аналітичну підтримку оперативно-службової та слідчої (розшукової) діяльності,* сприяючи підвищенню ефективності розслідування кримінальних правопорушень. До функцій ПКА належать:

– *збір інформації.* Агрегація даних із різноманітних джерел, як-от: відомчі бази даних (ІПНП та ін.), матеріали кримінальних проваджень, інформація від оперативних підрозділів, відкриті джерела (OSINT), дані від інших державних органів;

– *обробка та аналіз.* Систематизація зібраної інформації, перевірка її достовірності, виявлення взаємозв'язків, закономірностей, аномалій та тенденцій у злочинній діяльності за допомогою спеціалізованих аналітичних методів та програмного забезпечення (наприклад, IBM i2 Analyst's Notebook);

– *підготовка аналітичних продуктів.* Створення наочних та змістовних аналітичних документів для слідчих та оперативних працівників: аналітичних довідок, звітів, схем зв'язків (між особами, компаніями, телефонними номерами, IP-адресами, фінансовими транзакціями); здійснення геопросторового аналізу, прогнозів розвитку криміногенної ситуації.

5.2. Модель взаємодії «слідчий – кримінальний аналітик».

Ефективність використання потенціалу ПКА безпосередньо залежить від налагодженої взаємодії між слідчим (який здійснює досудове розслідування у відповідному кримінальному провадженні) та кримінальним аналітиком. Ця взаємодія має базуватися на принципах ефективної співпраці та обміну інформацією.

Ініціювання взаємодії: слідчий може звернутися до ПКА з конкретним запитом (дорученням) на проведення аналітичного дослідження. Запит має чітко формулювати завдання для аналітика (наприклад, встановити зв'язки між фігурантами, проаналізувати фінансові потоки, ідентифікувати можливих співучасників за цифровим слідом). Слідчий повинен надати аналітику максимально повну вихідну інформацію з матеріалів провадження. Аналітик також може ініціювати дослідження на основі виявлених ним закономірностей чи загроз.

Спільна робота: важливим є спільне обговорення слідчим та аналітиком отриманих результатів аналізу, висунутих версій, планування подальших слідчих розшукових дій та оперативно-розшукових заходів. Аналітик може допомогти слідчому побачити неочевидні зв'язки або нові напрями розслідування.

Використання результатів: аналітичні продукти (схеми, звіти) використовуються слідчим для:

- планування слідчих дій (визначення осіб для допиту, місць для обшуку);
- формування доказової бази (аналітичні документи можуть долучатися до матеріалів провадження як додатки до протоколів, рапортів);
- підготовки клопотань до суду (наприклад, обґрунтування необхідності ТДРД або обрання запобіжного заходу).

Зворотний зв'язок: рекомендується, щоб слідчий систематично інформував аналітика про результати перевірки наданої інформації та регулярно надавав відомості про поточний стан розслідування, що сприятиме ефективній взаємодії та підвищенню якості аналітичного супроводу кримінального провадження.

5.3. Типи аналітичних продуктів, релевантних для проведення розслідування кримінальних правопорушень, кваліфікованих за ст. 361 КК України

Під час розслідування фактів несанкціонованого втручання підрозділи кримінального аналізу можуть надати слідчому *аналітичні матеріали, що сприяють комплексному розумінню злочинної діяльності. Одним із ключових інструментів є аналіз зв'язків (Link Analysis),* що дає змогу візуалізувати та дослідити взаємозв'язки між різними об'єктами розслідування, зокрема:

- фігурантами справи;

– IP-адресами та їхніми власниками;

– доменними іменами та хостинг-провайдерами;

– фінансовими транзакціями (оплата хостингу, перекази, отримання коштів);

– телефонними номерами та IMEI-пристроями;

– акаунтами у соціальних мережах і нікнеймами на онлайн-платформах.

Застосування такого аналізу дозволяє *встановити можливих співучасників, організаторів, посередників,* а також *визначити структуру та спосіб взаємодії злочинної групи*.

Аналіз цифрового сліду: систематизація та комплексний аналіз великих масивів цифрових даних, отриманих із різних джерел (логи серверів, дані провайдерів, результати КТЕ, дані OSINT). Мета – реконструювати хронологію подій злочину, встановити послідовність дій зловмисника, ідентифікувати використані інструменти та інфраструктуру.

Профілювання (Profiling): на основі аналізу способу вчинення злочину (обраний вектор атаки, рівень технічної складності, тип цілі, залишені сліди) аналітик може спробувати скласти ймовірний профіль зловмисника або групи (рівень кваліфікації, можливі мотиви, належність до певних хакерських угруповань).

Стратегічний аналіз: аналіз серії однотипних злочинів за ст. 361 КК України для виявлення загальних тенденцій, нових схем та способів НСВ, ідентифікації організованих злочинних груп, що спеціалізуються на певних видах кібератак, оцінки загроз для певних секторів (наприклад, банківського чи енергетичного). Результати стратегічного аналізу важливі для вироблення превентивних заходів.

Розслідування кіберзлочинів, особливо складних та масштабних, неминуче пов’язане з обробкою величезних обсягів різнорідної інформації: гігабайти лог-файлів, тисячі IP-адрес та доменних імен, сотні або тисячі фінансових транзакцій, дані з багатьох джерел. Слідчий, навіть досвідчений, фізично не в змозі самостійно «перетравити» такий потік даних, виявити в ньому приховані закономірності та ключові доказові елементи. Саме тут кримінальний аналітик стає незамінним помічником. Використовуючи спеціалізоване програмне забезпечення та аналітичні методики, він може ефективно обробляти великі масиви даних, візуалізувати складні зв’язки, виявляти аномалії та надавати слідчому концентровану, структуровану інформацію, яка є придатною для прийняття обґрунтованих процесуальних рішень. Таким чином, кримінальний аналіз перетворюється з допоміжної функції на ключовий

інструмент розслідування, що дозволяє подолати інформаційне перевантаження слідчого та суттєво підвищити ефективність розкриття складних кіберзлочинів.

Узагальнений перелік типів аналітичних продуктів, які доцільно використовувати під час досудового розслідування кіберінцидентів за ст. 361 КК України, можна поділити на сім основних груп, а саме:

1. Технічна (цифрова) аналітика.

Мета: ідентифікувати механізм, масштаби та джерело втручання.

Приклади продуктів:

Звіт цифрової криміналістики (Digital Forensics Report) – результати аналізу вилучених комп'ютерів, серверів, мобільних пристроїв, логів.

Мета: встановити технічні обставини несанкціонованого втручання, отримати докази маніпуляцій у системах або пристроях.

Зміст звіту: опис об'єктів дослідження: вилучені комп'ютери, сервери, мобільні пристрої, зовнішні носії, хмарні акаунти.

Методика дослідження: зазначаються інструменти (наприклад, FTK Imager, Autopsy, EnCase), порядок копіювання даних (forensic image).

Результати аналізу:

– знайдено файли, створені або змінені під час події;
– виявлено сліди видалення/шифрування інформації;
– здійснено аналіз системних логів (Windows Event Viewer, syslog);
– встановлено історію браузера, листування, обміну файлами;
– знайдено шкідливі програми чи скрипти.

Висновки: підтвердження або спростування факту несанкціонованого доступу.

Значення для слідчого: дає об'єктивні технічні докази втручання (час, користувач, дії, засоби), які можна долучити до матеріалів справи.

Інструменти: Autopsy, EnCase, FTK, Magnet Axiom, X-Ways Forensics.

Мережевий аналіз (Network Traffic Analysis) – карта зв'язків, IP-адрес, маршрутів трафіку, часу активності.

Мета: виявити джерела, напрямки та характер обміну даними між пристроями, встановити факт і спосіб несанкціонованого доступу через мережеві канали.

Зміст аналізу: опис мережевої інфраструктури: локальна мережа, шлюзи, маршрутизатори, сервери, точки доступу Wi-Fi.

Джерела даних: файли журналів (firewall logs, router logs), дампи трафіку (PCAP), NetFlow-звіти, журнали IDS/IPS-систем.

Методика дослідження:

– фіксація мережевого трафіку (tcpdump, Wireshark, Zeek);

– аналіз портів, IP-адрес і протоколів (HTTP, HTTPS, SSH, DNS, FTP);

– побудова графів взаємодії між вузлами (network map);

– фільтрація підозрілої активності (аномальні з'єднання, великі обсяги передачі, підозрілі домени).

Результати аналізу:

– визначено IP-адреси джерел і приймачів трафіку під час події;

– виявлено незвичні з'єднання або комунікації із зовнішніми серверами;

– встановлено час та тривалість підозрілих сесій;

– виявлено використання тунелювання, TOR або VPN;

– здійснено реконструкцію маршрутів передачі даних.

Висновки: дозволяє відтворити мережеву активність у момент інциденту, встановити, які системи були задіяні, хто ініціював підключення та які дані могли бути передані.

Значення для слідчого: надає можливість встановити джерело кібератаки, канали витоку інформації та часову послідовність подій, а також підтвердити або спростувати факт взаємодії між об'єктами розслідування.

Інструменти: Wireshark, Zeek (Bro), NetworkMiner, Splunk, ELK Stack (Elasticsearch, Logstash, Kibana), SolarWinds, NetWitness Investigator.

Хронологія події (Incident Timeline) – реконструкція послідовності дій зловмисника (логіни, запуск шкідливих файлів, зміни в системі).

Мета: відновити повну часову картину події, встановити початковий вектор атаки, розвиток інциденту, дії зловмисника та реакцію системи безпеки.

Зміст аналізу: джерела часових даних: системні журнали подій (Windows Event Logs, syslog), метадані файлів, журнали серверів, дані антивірусів, бекапи, повідомлення SIEM-систем; часові мітки (timestamps) подій: створення/зміна файлів, запуск процесів, підключення до мережі, вхід користувачів у систему.

Методика дослідження:

– синхронізація часових зон різних джерел;

– побудова лінії часу подій (timeline reconstruction);

– класифікація дій за типами: підготовка, проникнення, закріплення, виконання, ексфільтрація, приховування;

– використання інструментів для автоматичного аналізу часових послідовностей.

Результати аналізу:

– встановлено момент первинного доступу до системи;

– виявлено перші ознаки компрометації (підозрілі логіни, зміна прав доступу, встановлення шкідливих файлів);

– відтворено дії користувачів і зловмисників у хронологічному порядку;

– визначено час реакції систем безпеки або персоналу;

– створено часову діаграму розвитку події.

Висновки: хронологічний аналіз надає змогу визначити початкову точку інциденту, послідовність дій, масштаб наслідків і встановити логічні зв'язки між різними цифровими доказами.

Значення для слідчого: дозволяє підтвердити або спростувати показання учасників події, обґрунтувати версію слідства, а також забезпечити доказову безперервність у суді.

Інструменти: Autopsy Timeline, Plaso (log2timeline), Timesketch, ELK Stack (Kibana), Magnet AXIOM Timeline, Sleuth Kit, FTK Imager.

Hash-аналіз – звіт про унікальні цифрові відбитки файлів для виявлення змін.

Мета: перевірити цілісність цифрових об'єктів, виявити ознаки втручання, встановити тотожність чи відмінність файлів, підтвердити автентичність доказів.

Зміст звіту:

– ідентифікація контрольних сум файлів за допомогою криптографічних алгоритмів (MD5, SHA-1, SHA-256, SHA-512);

– порівняння отриманих хеш-значень з еталонними базами даних (наприклад, NSRL, VirusShare, Project VIC);

– виявлення файлів, які зазнали змін у процесі події або після неї;

– підтвердження цілісності цифрових доказів після копіювання чи передачі.

Методика дослідження:

– створення хеш-значень під час копіювання даних (forensic imaging);

– порівняння отриманих хешів оригіналу та копії;

– автоматичний аналіз великої кількості файлів за допомогою спеціалізованих інструментів;

– документування результатів у протоколі для подальшого використання у кримінальному провадженні.

Результати аналізу:

– виявлено файли, що були змінені або підмінені після події;

– підтверджено цілісність цифрових доказів, що долучаються до справи;

– встановлено збіг або розбіжності між хеш-значеннями копії та оригіналу;

– зафіксовано факти знищення або фальсифікації інформації.

Висновки: Hash-аналіз є ключовим елементом цифрової криміналістики, що гарантує доказову достовірність результатів. Він забезпечує можливість перевірити, що жоден цифровий об'єкт не був змінений із моменту його вилучення.

Значення для слідчого: дозволяє підтвердити цілісність і автентичність цифрових доказів, а також спростувати можливі закиди щодо їх підроблення або маніпуляцій.

Інструменти: FTK Imager, Autopsy, HashMyFiles, md5deep / hashdeep, Magnet AXIOM, EnCase, X-Ways Forensics, OSForensics.

Malware Analysis Report – розбір програмного коду шкідливого ПЗ, що використовувався для атаки.

Мета: виявити, дослідити та описати характеристики ШПЗ, яке використовувалося для несанкціонованого втручання, встановити механізми зараження, функції шкідливого коду та джерела походження атаки.

Зміст звіту:

– опис знайдених зразків шкідливих файлів (виконувані файли, скрипти, бібліотеки, макроси тощо);

– визначення типу ШПЗ (троян, бекдор, вірус, криптолокер, шпигунське ПЗ, ботнет-агент);

– аналіз поведінки програми під час виконання;

– опис способів проникнення у систему (через фішингові листи, експлойти, заражені вебсайти, USB-носії);

– оцінка шкоди, завданої системам чи мережам.

Методика дослідження:

– статичний аналіз: дослідження структури файлу без його запуску, аналіз сигнатур, імпортованих бібліотек, функцій, рядків коду, алгоритмів шифрування;

– динамічний аналіз: спостереження за поведінкою зразка у контрольованому середовищі (пісочниці, sandbox);

– гібридний аналіз: поєднання статичних і динамічних методів для визначення повної картини роботи ШПЗ;

– перевірка зразків через бази антивірусних сигнатур (VirusTotal, Hybrid Analysis, Any.Run, Joe Sandbox).

Результати аналізу:

– встановлено джерела зараження та шляхи поширення ПЗ;

– визначено IP-адреси серверів управління (Command & Control);

– виявлено модулі збору даних, кейлогери, елементи приховування (rootkits, obfuscation);

– отримано індикатори компрометації (IoC), які можна використовувати у подальших розслідуваннях;

– виявлено взаємозв'язки між атакою та попередніми кіберінцидентами.

Висновки: Malware Analysis Report дозволяє ідентифікувати ШПЗ, його функціонал та ланцюг атаки, що є ключовим для встановлення винних осіб і запобігання подальшим інцидентам.

Значення для слідчого: надає технічні докази використання ШПЗ, описує механізми атаки, зв'язує кіберінцидент із конкретними технічними артефактами (IP, доменами, хешами, сигнатурами).

Інструменти: IDA Pro, Ghidra, OllyDbg, x64dbg, Cuckoo Sandbox, Any.Run, Wireshark, PEiD, YARA, VirusTotal, Hybrid Analysis.

2. Аналітика поведінкова.

Мета: виявити закономірності, мотиви та можливі профілі кіберзлочинців.

Приклади продуктів:

Профайл зловмисника (Threat Actor Profile) – типова поведінка, часові шаблони, технічні інструменти, зв'язки.

Мета: зібрати та узагальнити інформацію про конкретного зловмисника або групу (Threat Actor) для ідентифікації характерних ознак, можливих мотивів, технік і каналів діяльності, а також для підвищення ефективності виявлення та атрибуції інцидентів.

Зміст звіту (профайлу):

– базова ідентифікаційна інформація: умовна назва групи/актора, відомі псевдоніми, попередні операції;

– мотивація та цілі (кіберзлочинність заради вигоди, кібершпигунство, кібервандалізм, державна підтримка тощо);

– типовий арсенал інструментів (malware families, C2 домени, фреймворки – Metasploit, Mimikatz, Cobalt Strike тощо);

– тактики, техніки й процедури (TTPs) у термінах MITRE ATT&CK (pivoting, lateral movement, credential dumping, data exfiltration);

– часові шаблони активності (години/дні тижня, сезонність, «вікна» активності згідно з часовими зонами);

– зв'язки з іншими акторами/інфраструктурами (спільні IoC, повторювані домени, загальні C2-сервери);

– відомі індикатори компрометації (IoC): хеші файлів, IP-адреси, домени, URL, YARA-правила;

– рівень складності атак і необхідні ресурси (початковий скриптер до державного APT).

Методика дослідження (збору та формування профайлу):

– агрегація даних із відкритих джерел (OSINT), розвідувальних баз (MISP, VirusTotal, AbuseIPDB), звітів постачальників кібербезпеки;

– кореляція технічних артефактів (PCAP, логи, хеші) з відомими TTPs;

– тимчасовий (time-series) і топологічний (graph) аналіз для виявлення патернів;

– використання інструментів для атрибуції: MISP, Maltego, Recorded Future (за наявності).

Результати аналізу:

– сформовано досьє на актора з переліком TTPs та IoC;

– створено часові профілі активності (наприклад, «пік дій – 02:00–06:00 UTC, п’ятниця – неділя»);

– складено перелік інструментів і сервісів, які слід блокувати чи моніторити;

– здійснено оцінку можливих наступних кроків актора (retaliation, lateral movement, data exfiltration).

Висновки: профайл дозволяє прогнозувати поведінку зловмисника, спрямувати моніторинг на релевантні індикатори та пріоритезувати реагування.

Значення для слідчого: дає контекст для розслідування (чи був інцидент спрямований проти конкретного актора), допомагає скласти запити для МПД і коригувати слідчі дії.

Інструменти та джерела: MISP, VirusTotal, AbuseIPDB, Shodan, Threat Intelligence Feeds, Maltego, Recorded Future, MITRE ATT&CK.

Behavioral Pattern Map – модель типових дій у мережі (кібергігієна, обхід захисту, індикатори компрометації).

Мета: створити візуальну та описову модель типової послідовності дій (патернів) зловмисника у мережі, від підготовки до ексфільтрації, з виділенням ключових індикаторів компрометації (IoC) та точок втручання для реагування.

Зміст звіту (карти поведінки):

– етапи атаки (Kill Chain / Cyber Kill Chain / MITRE ATT&CK stages): Reconnaissance → Initial Access → Execution → Persistence → Privilege Escalation → Lateral Movement → Collection → Exfiltration → Impact;

– для кожного етапу – типові техніки і приклади (наприклад, Initial Access: phishing, exploit public-facing app; Lateral Movement: SMB abuse, Pass-the-Hash);

– індикатори компрометації для кожного етапу (підозрілі логіни, незвичні процеси, нестандартний трафік на портах, нові автостарт-записи);

– точки та способи обходу захисту (обфускація, living-off-the-land, тор/VPN, use of cloud services);

– рекомендації щодо детекції (SIEM rules, EDR signatures, network IDS/IPS правила) та миттєвого реагування.

Методика дослідження (створення карти):

– аналіз минулих інцидентів і їхніх логів;

– мапування знайдених IoC на прийоми MITRE ATT&CK;

– побудова візуальних графів (node-edge) мережевих та хостових подій;

– формування списків детекції для SIEM/EDR.

Результати дослідження:

– створено діаграму з етапами атаки та сигналами (наприклад, «якщо з'явився процес werfault.exe з нестандартними параметрами → тригерити перевірку»);

– сформовано набір правил для SIEM/EDR (список детекційних правил і пріоритетів);

– складено перелік превентивних заходів (жорсткі політики паролів, MFA, сегментація мережі).

Висновки: Behavioral Pattern Map допомагає швидко ідентифікувати, на якому етапі знаходиться інцидент, та пріоритезувати заходи для мінімізації шкоди.

Значення для слідчого: забезпечує оперативний чекліст для ідентифікації і блокування активностей, а також набори доказів для подальшого розслідування.

Інструменти: MITRE ATT&CK Navigator, Timesketch, Elastic SIEM/Kibana, Sigma rules, YARA, EDR-платформи (CrowdStrike, SentinelOne), Zeek (Bro), Suricata.

Сценарії атак (Attack Scenarios) – прогноз можливих напрямів подальшого втручання.

Мета: підготувати набір правдоподібних сценаріїв подальших атак або ескалації подій, що ґрунтуються на виявлених TTPs та поточному рівні загрози; забезпечити основу для планування захисних заходів і контрзаходів.

Зміст звіту (сценаріїв):

– короткий опис сценарію (наприклад, «фішинг → RCE → Ransomware deployment»);

– передумови і тригери (що могло б ініціювати сценарій – політичні події, публікація вразливості, сезонність);

– кроки зловмисника (поетапна послідовність дій);

– технічні артефакти, які можуть бути знайдені (IoC: хеші, домени, IP, реєстраційні записи, незвичні користувачі);

– очікувані наслідки (втручання в роботу сервісів, витік даних, фінансові втрати);

– ймовірність реалізації та рівень впливу (Low/Medium/High) з обґрунтуванням;

– заходи виявлення, пом'якшення та відновлення (detect, contain, eradicate, recover).

Методика дослідження (підготовки сценаріїв):

– аналіз існуючих даних про загрозу (Threat Intelligence);

– кореляція з локальними ризиками (вразливі сервера, критична IT-інфраструктура);

– консультації з операційними підрозділами (кіберполіція, адмінсервіси);

– тестування сценарію у контрольованому середовищі (red team/tabletop exercises).

Типові сценарії (приклади):

Phishing → Credential Harvesting → Lateral Movement → Data Exfiltration.

Ймовірність: Medium. Вплив: High.

Детекція: незвичні логіни, підозрілі PowerShell-запити, великі вихідні з'єднання на незнайомі IP.

Заходи: MFA, блокування IP/домена, аналіз пошти, навчання користувачів.

Exploit Public-Facing Application → Web Shell → Ransomware Deployment.

Ймовірність: Medium. Вплив: Critical (якщо сервер – частина критичної інфраструктури).

Детекція: незвичні HTTP POST запити, створення нових файлів у вебкаталогах, аномалії CPU/IO.

Заходи: швидкий патчинг, WAF, бекапи, сегментація.

Supply Chain Compromise → Malicious Update → Broad Compromise.

Ймовірність: Low/Medium. Вплив: Very High.

Детекція: одночасні аномалії на багатьох системах після оновлення; підпис файлів змінено.

Заходи: контроль цілісності оновлень, підпис продуктів, обмеження прав для оновлень.

Insider Threat → Unauthorized Data Access → Leak.

Ймовірність: Low. Вплив: High (конфіденційні дані).

Детекція: незвичні пошукові запити в системах, великі експортні операції, доступ позмінно.

Заходи: DLP, аудит доступу, політика найменших привілеїв.

Висновки: тестовані сценарії дають змогу підготувати превентивні та реагувальні плани, визначити пріоритетні заходи та ресурси для мінімізації ризику.

Значення для слідчого/команд реагування: сценарії використовуються для швидкого прийняття рішень, планування чеклістів і підготовки запитів на МПД або блокувальні заходи.

Інструменти: ATT&CK Navigator, Caldera (MITRE), Cuckoo Sandbox (для тестування зразків), MISP (для IoC), SIEM/EDR платформи.

3. Аналітика джерел відкритої інформації (OSINT).

Мета: підтвердити або спростувати зв'язки, знайти сліди зловмисників у відкритих джерелах.

Приклади продуктів:

OSINT Report/SOCMINT Report – аналіз акаунтів, доменів, Telegram- або Discord-каналів, пов'язаних із атакою.

Мета: зібрати, систематизувати та проаналізувати відкриті джерела інформації (соціальні мережі, месенджери, публічні реєстри, доменні дані) для ідентифікації учасників інциденту, зв'язків між акаунтами/каналами, збору доказової інформації та побудови розвідувальних висновків.

Зміст звіту:

– перелік проаналізованих об'єктів (акаунти в соцмережах, Telegram/Discord-канали, вебсайти, домени, публічні пости);

– зведені профілі підозрілих акаунтів (ім'я/нікнейм, опис, дата створення, активність, зв'язки);

– хронологія публікацій і ключові повідомлення, пов'язані з інцидентом;

– карти зв'язків між акаунтами/каналами (graph of interactions);

– збережені скріншоти, архіви публікацій та метадані;

– ризикові індикатори (поширення шкідливих посилань, заклики до дій, координування атак);

– рекомендації щодо подальших слідчих дій (запити до платформ, блокування контенту, ідентифікація власників).

Методика дослідження:

– збір даних із відкритих джерел (API, вебскрапінг, manual capture);

– застосування трансформацій (розкриття контактів, пов'язаних акаунтів, доменів) та кореляція з технічними IoC;

– часовий та поведінковий аналіз активності (виявлення піків, синхронних публікацій);

– перевірка достовірності (cross-checking, reverse image search, верифікація метаданих);

– збереження доказів у форензічному форматі (скріншоти з часовими мітками, архіви, експорти чатів).

Результати дослідження (приклади):

– виявлено ключові акаунти, які координували розповсюдження шкідливих посилань;

– побудовано мережу зв'язків між акаунтами у Telegram та групами у Discord;

– ідентифіковано домени, пов'язані з поширенням шкідливого контенту;

– збережено архіви публікацій із часовими мітками для процесуальної фіксації.

Висновки: OSINT/SOCMINT-звіт дозволяє встановити цифрові сліди діяльності, визначити канал розповсюдження загрози, знайти потенційних координаторів або «вузлові» акаунти для подальшого аналізу та процесуального реагування.

Значення для слідчого: дає підґрунтя для запитів платформам (одержання IP-логів, метаданих), формує напрям для оперативних заходів (блокування, виклики на допит), слугує джерелом доказової інформації (скріншоти, архіви).

Інструменти: Maltego, oTranscribe, Social Searcher, Telegram API/Telethon, Discord API, CrowdTangle (FB/IG), Google reverse image, Wayback Machine, Archive.is, OSINT-інструментарій (SpiderFoot, Sherlock).

Whois та DNS-аналітика – ідентифікація реєстратора домену, IP, часу створення, змін власника.

Мета: встановити технічну та реєстраційну інформацію про домени, пов'язані з інцидентом, і за допомогою DNS-даних і WHOIS-записів зібрати підстави для ідентифікації власників інфраструктури та маршрутизації трафіку.

Зміст звіту:

– перелік проаналізованих доменів та піддоменів;

– WHOIS-дані: реєстрант, реєстратор, контактні дані (за наявності), дати реєстрації та останніх змін;

– DNS-дані: A/AAAA записи (IP), MX, NS, TXT (включно з SPF, DKIM), CNAME;

– історія змін (WHOIS history, DNS history) – зміни власника, зміни NS, оновлення записів;

– географічне та провайдерське розміщення IP-адрес (AS-номер, провайдер);

– взаємозв'язки між доменами через спільні IP, NS, реєстрантів або хостинг.

Методика дослідження:

– виконання WHOIS-запитів (RDAP/WHOIS), кеш-пошук історичних записів;

– DNS-запити та рекурсивний аналіз (dig, nslookup), збір DNS-зон;

– використання історичних сервісів (DomainTools, SecurityTrails, whoisxmlapi) для відстеження змін;

– кореляція з IP-даними (GeoIP, BGP/AS lookup) та адресними базами (AbuseIPDB).

Результати дослідження (приклади):

– встановлено дату створення домену і періоди реєстраційних змін;

– ідентифіковано хостинг-провайдера й AS-номер, де розміщено C2-сервер;

– виявлено, що кілька підозрілих доменів використовували один хостинг або однакові NS → вказівка на спільну інфраструктуру;

– знайдено TXT-записи, що вказують на фальшиві налаштування пошти (відсутність SPF/DKIM) – ризик фішингу.

Висновки: Whois/DNS-звіт дозволяє звузити коло підозр до конкретних реєстраторів чи хостинг-провайдерів, підготувати запити про надання логів або блокування ресурсів, а також побудувати технічну картину інфраструктури зловмисників.

Значення для слідчого: надає підстави для оформлення запитів провайдерам та адміністраторам доменів, допомагає у встановленні атрибуції й викритті мережевих проміжних вузлів.

Інструменти: whois/RDAP-клієнти, DomainTools, SecurityTrails, whoisxmlapi, dig/nslookup, VirusTotal passive DNS, AbuseIPDB, BGPView, Censys, Shodan.

Geoint-аналіз – визначення геолокацій користувачів чи серверів.

Мета: визначити просторове розміщення серверів, вузлів інфраструктури або (якщо є можливість) користувачів, пов'язаних із

інцидентом; використати просторові дані для кореляції версій слідства, підготовки МПД або оперативних заходів.

Зміст звіту:

– перелік об’єктів для геолокації (IP-адреси серверів, координати з публікацій, метадані фото/відео, геомаркери у постах);

– джерела просторових даних: GeoIP-бази, BGP/WHOIS, EXIF-метадані з файлів, публічні пости із геотегами;

– картографічні візуалізації (мапи з маркерами, теплові карти активності);

– часово-просторовий аналіз: переміщення об’єктів/активності у часі;

– оцінка ступеня точності геолокації та невизначеностей.

Методика дослідження:

– запити до GeoIP-сервісів (MaxMind, IP2Location) та перевірка через кілька баз для підвищення надійності;

– аналіз EXIF/metadata у зображеннях і відео (exiftool) для отримання координат або часових міток;

– кореляція IP-геолокації з BGP/AS-даними та інформацією про провайдера;

– використання OSINT-джерел для підтвердження (публікації у соцмережах, місцеві оголошення, фото з прив’язкою до місця).

Результати дослідження (приклади):

– встановлено географічне розміщення сервера C2 у певній країні/місті (із зазначенням хостинг-провайдера);

– виявлено геотеги у публікаціях, що підтверджують присутність користувача у конкретному місці й часі;

– створено карту активності з позначенням піків та можливих маршрутів ексфільтрації даних.

Висновки: Geoint-звіт дозволяє визначити географічні вектори загрози, пріоритетні юрисдикції для МПД та спрямувати оперативно-слідчі дії. Однак слід враховувати обмеження точності GeoIP і можливість використання проксі/VPN/TOR.

Значення для слідчого: підстава для міжнародних запитів, визначення пріоритетних територій, допомога в атрибуції інциденту та плануванні арештів/обшуків. Також має користь для оцінки потенційного впливу на локальні об’єкти інфраструктури.

Інструменти: MaxMind, IP2Location, GeoIP2, exiftool, Google Maps/OpenStreetMap, Shodan, Censys, MISP (кореляція із IoC), OSINT джерела (пости, фотографії), BGPView.

4. Аналітика ризиків і наслідків.

Мета: оцінити вплив атаки на безпеку системи, установи чи осіб.

Приклади продуктів:

Оцінка інформаційних втрат (Data Breach Assessment) – визначення обсягу викрадених/змінних даних.

Мета: встановити обсяг, тип і рівень критичності даних, що були викрадені, змінені або знищені внаслідок кіберінциденту. Оцінити, які саме інформаційні ресурси зазнали компрометації, і визначити потенційні наслідки для організації чи державного органу.

Зміст звіту:

– опис інциденту (дата, спосіб виявлення, характер втручання);

– перелік постраждалих систем, баз даних, сервісів;

– категорії інформації, що зазнала втрат (персональні дані, службові, фінансові, державні);

– аналіз журналів подій (логів) для визначення періоду доступу зловмисника;

– обсяг викрадених або змінених файлів (кількість записів, таблиць, документів);

– виявлення методів ексфільтрації даних (FTP, TOR, email, cloud storage);

– оцінка ступеня впливу на інформаційну безпеку.

Методика дослідження:

– аналіз логів доступу до баз даних та файлових систем;

– використання SIEM-систем (Splunk, QRadar, ELK Stack) для кореляції подій;

– відновлення видалених або змінених файлів із forensic-копій;

– зіставлення хешів початкових і змінених файлів;

– виявлення з’єднань із зовнішніми IP/доменами для визначення шляхів передачі даних.

Результати дослідження (приклади):

– виявлено несанкціонований експорт даних із бази клієнтів обсягом 50 тис. записів;

– зафіксовано зміну хеш-сум у 12 конфіденційних файлах;

– підтверджено використання зовнішнього FTP для передачі архівів;

– збережено список викрадених файлів та їхні контрольні суми.

Висновки: Data Breach Assessment дозволяє встановити масштаб компрометації, ідентифікувати джерело та обсяг втрат, а також підготувати матеріали для повідомлення постраждалих сторін і подання звіту до регуляторних органів.

Значення для слідчого: дозволяє оцінити ступінь шкоди, визначити потерпілих, підготувати запити для подальшої локалізації джерела витоку та скласти юридично обґрунтовані процесуальні документи.

Інструменти: Splunk, ELK Stack, QRadar, Autopsy, FTK, Magnet Axiom, X-Ways Forensics, LogParser, PowerShell, MISP (для кореляції IoC).

Impact Analysis Report – наслідки для бізнес-процесів, безпеки державних даних чи персональної інформації.

Мета: визначити наслідки кіберінциденту або інформаційної атаки для безперервності бізнес-процесів, державних сервісів, а також захисту персональної чи службової інформації.

Зміст звіту:

– короткий опис події (інцидент, дата, тип атаки);

– виявлені системи або сервіси, що постраждали;

– вплив на бізнес-процеси (зупинка сервісів, втрата продуктивності, порушення SLA);

– наслідки для державної або конфіденційної інформації;

– вторинні ризики – фінансові, репутаційні, юридичні;

– категоризація наслідків за рівнем критичності (низький/середній/високий/катастрофічний);

– оцінка часу відновлення роботи (RTO) та обсягу відновлення даних (RPO).

Методика дослідження:

– збір інформації від відповідальних підрозділів (IT, безпека, управління ризиками);

– аналіз журналів інцидентів, звітів систем моніторингу, SIEM/SOC;

– оцінка відповідності заходів реагування плану безперервності діяльності (BCP/DRP);

– співставлення наслідків із критичними бізнес-функціями.

Результати дослідження (приклади):

– внаслідок атаки призупинено роботу електронного документообігу на 8 годин;

– втрачено 10 % даних CRM-системи, що потребують відновлення з резерву;

– зафіксовано витік особистих даних 120 користувачів;

– фінансові втрати оцінено в 250 тис. грн.

Висновки: Impact Analysis Report дозволяє керівництву визначити реальний вплив інциденту, обґрунтувати необхідність посилення кіберзахисту та оптимізувати план реагування на інциденти.

Значення для слідчого: надає об'єктивні дані для оцінки шкоди, складання процесуальних документів і визначення кваліфікації злочину (економічна шкода, порушення конфіденційності, дестабілізація роботи об'єктів критичної інфраструктури).

Інструменти: Power BI, Excel (Business Impact Matrix), RiskLens, IBM QRadar, Splunk, Tableau, MISP, OpenFAIR, BIA Template (NIST SP 800-34).

Ризик-профіль системи (System Risk Profile) – рекомендації щодо підсилення кіберзахисту.

Мета: оцінити поточний стан безпеки інформаційної системи, виявити слабкі місця, сформувати рекомендації для зниження ризиків та підвищення рівня кіберзахисту.

Зміст звіту:

– загальна характеристика системи (призначення, архітектура, критичні елементи);
– оцінка загроз (внутрішніх і зовнішніх);
– результати сканування вразливостей та аудит безпеки;
– оцінка ймовірності реалізації загроз і потенційного впливу;
– матриця ризиків (Risk Matrix);
– рекомендації щодо підвищення кіберстійкості (оновлення ПЗ, резервування, сегментація мережі, MFA, політики доступу).

Методика дослідження:

– аудит конфігурацій систем безпеки (SIEM, IDS/IPS, Firewall);
– сканування мережі за допомогою Nessus, OpenVAS, Qualys;
– проведення тестування на проникнення (penetration testing);
– аналіз політик користувацьких прав і логів безпеки;
– формування матриці ризиків за ISO/IEC 27005 або NIST 800-30.

Результати дослідження (приклади):

– виявлено 15 критичних і 42 середні вразливості;
– підтверджено відсутність двофакторної аутентифікації для адміністративних акаунтів;
– встановлено недостатній рівень сегментації мережі між виробничим і офісним сегментом;
– підготовлено рекомендації щодо термінів усунення (Remediation Plan).

Висновки: Risk Profile дає змогу визначити поточний рівень захисту, пріоритезувати заходи з підсилення безпеки та створити план модернізації системи.

Значення для слідчого: допомагає оцінити рівень підготовленості системи до кіберінцидентів, виявити порушення політик безпеки, а також

підготувати технічне обґрунтування для керівництва або судово-технічної експертизи.

Інструменти: Nessus, OpenVAS, Qualys, NIST CSF, ISO/IEC 27005, MITRE ATT&CK, OWASP ZAP, CIS Benchmarks, Power BI/Excel для Risk Matrix.

5. Аналітика правова.

Мета: надати юридичну оцінку фактам втручання.

Приклади продуктів:

Аналітична довідка щодо кваліфікації події (визначення ознак відповідної статті КК України).

Мета: встановити, до якого саме складу кримінального правопорушення належить виявлена подія в кіберпросторі, визначити правову кваліфікацію (за ст. ст. 361, 361-1, 362 КК України) шляхом аналізу зібраних доказів, технічних слідів, мотивів і способу дій зловмисника.

Зміст аналітичної довідки:

– опис події: дата, час, місце, характер кіберінциденту (несанкціоноване втручання, створення/розповсюдження шкідливого ПЗ, перевищення доступу до даних);

– первинні технічні ознаки: виявлені канали доступу, IP-адреси, вид трафіку, використані інструменти (Malware, Exploit, Phishing);

– порівняння з нормами КК України;

– встановлення мотиву та мети дій: отримання вигоди, саботаж, шпигунство, підрив довіри до системи;

– визначення ступеня суспільної небезпеки: масштаб втручання, наявність шкоди, вплив на критичні системи.

Методика дослідження:

– аналіз звітів цифрової криміналістики, логів систем, трафіку, даних OSINT;

– порівняння способу дій з типовими шаблонами кіберзлочинів (з бази CERT-UA, Europol EC3);

– експертна оцінка правового складу злочину у співпраці з юристами-криміналістами.

Результати дослідження (приклади):

– встановлено, що втручання здійснено без прав доступу з використанням SSH-брутфорсу;

– підтверджено створення та тестування Python-скрипта для обходу авторизації;

– виявлено, що доступ мав системний адміністратор, який перевищив службові повноваження.

Висновки: аналітична довідка дозволяє обґрунтувати кваліфікацію злочину, уникнути помилок у визначенні статті та забезпечити юридичну точність у формулюванні фабули кримінального провадження.

Значення для слідчого: надає основу для повідомлення про підозру, визначення статті обвинувачення, обґрунтування у процесуальних документах і запобігання дублюванню складів правопорушень.

Інструменти: X-Ways Forensics, Magnet Axiom, FTK, MISP, IBM i2 Analyst's Notebook, CERT-UA CaseBase, правові бази: ЛІГА:ЗАКОН, ZakonOnline, EUR-Lex.

Матриця відповідності доказів складу злочину.

Мета: систематизувати наявні докази у кримінальному провадженні відповідно до елементів складу злочину, що дозволяє об'єктивно оцінити достатність доказової бази для кваліфікації за відповідною статтею КК України.

Зміст звіту:

Елементи складу злочину: об'єкт, об'єктивна сторона, суб'єкт, суб'єктивна сторона.

Типи доказів: цифрові (логи, хеші, мережеві з'єднання), речові (носії, пристрої), свідчення, експертні висновки.

Матриця відповідності:

Елемент складу злочину	**Джерело доказів**	**Вид доказу**	**Рівень підтвердження**	**Коментар/ рекомендації**
Об'єктивна сторона (втручання в систему)	Digital Forensics Report	технічний	високий	підтверджує зміну логів
Суб'єкт (особа з доступом)	OSINT/допит	персональний	середній	необхідна верифікація акаунту
Мотив	аналіз листування	контентний	високий	підтверджує намір отримати вигоду

Критерії оцінки доказів: релевантність, достовірність, допустимість, взаємна кореляція.

Виявлення прогалин: визначення відсутніх або слабких доказів для кожного елемента складу злочину.

Методика дослідження:

– узагальнення доказів із процесуальних документів і технічних звітів;

– використання цифрових таблиць (Excel, Power BI) для побудови візуальної матриці;

– перевірка ланцюга збереження доказів;

– аналіз зв’язків між доказами (i2 Analyst’s Notebook).

Результати аналізу (приклади):

– встановлено повну відповідність доказів об’єктивній стороні злочину, часткову – суб’єктивній;

– виявлено нестачу даних для підтвердження умислу, рекомендовано додаткову експертизу переписки;

– сформовано рекомендації щодо додаткових запитів до провайдерів або банків.

Висновки: матриця дозволяє систематизувати докази, мінімізувати ризик відхилення обвинувального акта судом та підвищити якість доказової бази.

Значення для слідчого: забезпечує контроль за повнотою доказів, виявлення слабких місць розслідування, спрощує підготовку процесуальних документів і виступів у суді.

Інструменти: Excel/Power BI, IBM i2 Analyst’s Notebook, CaseMap, Relativity, FTK, Autopsy, MISP.

Порівняльний аналіз норм міжнародного права у сфері кібербезпеки.

Мета: порівняти українське кримінальне законодавство щодо кіберзлочинів (зокрема, статті КК України) з міжнародними стандартами та практикою (Будапештська конвенція, Європейська директива 2013/40/ЄС, стандарти NIST, ISO/IEC 27037).

Зміст звіту:

1. Огляд нормативної бази: міжнародні конвенції, директиви ЄС, рекомендації ООН, національні акти України.
2. Порівняльна таблиця норм (приклад):

Аспект	**Україна (КК)**	**Міжнародна практика**	**Відмінності/пропозиції**
Визначення «несанкціонованого втручання»	ст. 361 КК України	ст. 2 Будапештської конвенції	уточнення поняття «автоматизована система»

3. Визначення гармонізаційних прогалин: аналіз невідповідностей і пропозиції щодо адаптації українського законодавства до європейських стандартів.
4. Оцінка практики міжнародної співпраці: INTERPOL, Europol EC3, Council of Europe Cybercrime Programme Office (C-PROC).

Методика дослідження:

– контент-аналіз нормативних актів;

– порівняння положень законів та практики застосування;

– узагальнення позицій ЄСПЛ та міжнародних звітів UNODC, ENISA.

Результати дослідження (приклади):

– встановлено часткову гармонізацію українського законодавства з Будапештською конвенцією;

– виявлено потребу у внесенні змін до статей КК України для розмежування дій;

– рекомендовано створення незалежної сертифікаційної системи експертів цифрових доказів за моделлю ENFSI.

Висновки: звіт сприяє уніфікації національного законодавства з міжнародними стандартами та забезпечує основу для розробки пропозицій до МВС України, Кабінету Міністрів України та Верховної Ради України.

Значення для слідчого: дозволяє врахувати міжнародний досвід при кваліфікації кіберзлочинів і підвищити ефективність міжнародного співробітництва у сфері кібербезпеки.

Інструменти: EUR-Lex, UNODC Cybercrime Repository, ENISA Reports, C-PROC Council of Europe, NIST SP 800 Series, ISO/IEC 27001–27037, ЗІР Мін'юсту, LIGA:ЗАКОН.

6. Аналітика зв'язків і співучасті.

Мета: виявити співучасників, замовників, посередників.

Приклади продуктів:

Link Analysis (граф зв'язків) – візуалізація контактів, транзакцій, спільних IP, електронних адрес.

Мета: візуалізувати й проаналізувати мережу контактів/транзакцій/спільних IP і електронних адрес для виявлення ключових вузлів, маршрутів розповсюдження та аномалій.

Зміст звіту.

Короткий огляд мети й контексту розслідування.

Джерела даних (логи пошти, SIEM, Netflow, blockchain-експорти, списки контактів, WHOIS, OSINT).

Опис підготовки даних (нормалізація, дедуплікація, агрегація).

Графова модель: вузли (суб'єкти) і ребра (відносини).

Таблиця з полями: id, тип (IP/email/телефон/BTC-адреса/обліковий запис), атрибути (хеші, часові мітки), джерело.

Візуалізація (зображення графа + інтерактивний артфакт).

Аналітика: центральність, виявлення спільноти, найкоротші шляхи, часовий зріз.

Індикатори компрометації (IoC) і рекомендовані наступні кроки.

Додатки: CSV/JSON експорти, GEXF/GraphML, скрипти для відтворення.

Методика дослідження.

Збір: перетягнути/експорт з джерел (CSV, JSON, Elastic, Splunk).

Обробка: нормалізація ідентифікаторів (нормалізувати електронні листи, IP6→канонічний).

Зв'язування (роздільна здатність суб'єкта): правила та ваги (наприклад, однакова IP+timestamp → зв'язок).

Побудова графа: вузли/ребра з метаданими (time, count, confidence).

Аналітика:

Degree/Betweenness/Closeness centrality (Ступінь/Проміжність/Центральність близькості).

Виявлення спільноти.

Часовий аналіз: вікна Windows, знімки.

Аналіз шляхів: найкоротші/найімовірніші шляхи зараження.

Валідація: вручну перевірити ключові зв'язки, позначити хибнопозитиви.

Результати дослідження (приклад структури).

Ключові висновки (3–5 сторінок): топ-5 вузлів за центральністю; виявлені «мости» між кластерами.

Таблиця найважливіших вузлів: id | тип | degree | betweenness | пов'язані IoC | confidence.

Графічні артефакти: скріншоти основного графа (анотації).

Інтерактивний файл: graph.gexf або graph.graphml (відкрити в Gephi/Cytoscape).

Тимчасова хронологія зв'язків: таблиця з подіями.

Висновки: список пріоритетних дій (блокувати IP-адреси, карантинувати облікові записи, зберігати докази).

Значення для слідчого: показує ланцюжки комунікацій і потенційні зв'язки з іншими інцидентами; дає цілеспрямовані IoC та пріоритети для подальших технічних/правових дій.

Інструменти: Gephi, Neo4j + Bloom, Maltego, Cytoscape, Graph-tool, NetworkX (Python), Kumu.

Communication Map – карта взаємодії підозрюваних у кіберпросторі.

Мета: візуалізувати та проаналізувати комунікації підозрюваних у кіберпросторі (електронна пошта, месенджери, форуми, соціальні мережі) для виявлення ключових осіб, зв'язків, каналів обміну інформацією та потенційних групових структур.

Зміст звіту:

Вступ: контекст розслідування: мета створення карти взаємодії; перелік джерел даних.

Джерела даних: логи електронної пошти (SMTP, IMAP, Exchange):; мессенджери (Telegram, WhatsApp, Signal, Discord); соціальні мережі та форуми (OSINT, API, scraping); додаткові джерела (Netflow, VPN, DNS-запити).

Підготовка та нормалізація даних: дедуплікація контактів (один користувач – кілька акаунтів); часові мітки в єдиному форматі; валідація достовірності контактів; агрегація повідомлень за типом (email, chat, post, comment).

Структура карти:

– вузли: підозрювані, акаунти, IP-адреси, email;

– ребра (edges): тип взаємодії (листування, дзвінок, коментар), частота, час останньої взаємодії; атрибути вузлів: роль, географія, пов'язані IoC;

– атрибути ребер: позначка часу, кількість контактів, засіб (електронна пошта/чат/форум).

Візуалізація: статичні графи: скріншоти основних кластерів; інтерактивні графи: формат GEXF/GraphML для Gephi/Cytoscape; використання кольорів/розміру вузлів для виділення центральних осіб або активних каналів.

Методика дослідження:

1. Збір: агрегування логів та повідомлень;
2. Об'єднання контактів: зв'язування акаунтів одного користувача;
3. Побудова графа: вузли → особи/акаунти, ребра → взаємодії;
4. Аналітика: центральність (ступінь, проміжність, близькість) → ключові підозрювані; виявлення спільноти → групи підозрюваних; часовий аналіз → активні періоди комунікацій; аналіз шляху → виявлення ланцюгів передачі інформації; валідація: ручна перевірка ключових зв'язків та аномалій.

Результати дослідження:

1.Таблиці ключових вузлів та ребер:

ID	Ім'я/ник	Тип вузла	Центральність	Пов'язані IoC	Кількість контактів

2. Виявлені групи та підгрупи підозрюваних;
3. Частотні патерни комунікацій;
4. Аномалії або «мости» між різними групами;
5. Зв'язок із попередніми інцидентами або відомими загрозами.

Висновки: ідентифіковано ключових комунікаторів та визначено їхню роль у мережі; виявлено потенційні групи, що координують дії.

Значення для слідчого: надає наочну картину взаємодії підозрюваних; визначає пріоритетні особи для детального розслідування; підтримує кореляцію з іншими кіберінцидентами.

Інструменти: Gephi, Neo4j + Bloom, Maltego, Cytoscape, NetworkX (Python), Kumu.

7. Аналітика превентивна (прогностична).

Мета: запобігти подальшим атакам.

Приклади продуктів:

Threat Intelligence Bulletin – інформація про актуальні кіберзагрози.

Мета: оперативно повідомити про актуальні кіберзагрози, TTPs, IoC.

Зміст звіту.

Заголовок: дата, рівень критичності (низький/середній/високий/критичний), таргетована індустрія/регіон.

Короткий дайджест (1–3 абзаци) – найважливіше.

Деталі загроз:

Нові CVEs/експлойти, що використовуються в природі.

Malware families observed (ім'я, версія).

APT (спостереження за учасниками загрози).

TTPs (mapped to MITRE ATT&CK): техніки з прикладами інцидентів.

Індикатори компрометації (IoC): хеші, IP, домени, email-адреси, YARA rules.

Технічний аналіз (коротко): вектор атаки, тип експлуатації.

Оцінка ризику для організації (конкретно: фінанси, доступність, репутація).

Методика дослідження:

1. Джерела: CERTs, канали постачальників, MISP, VirusTotal, abuse.ch, розвідувальна інформація з відкритим кодом;

2. Валідація: підтвердження з кількох джерел; позначення помилок/ненадійних сигналів;

3. Оцінювання: ймовірність + вплив → рівень ризику.

Приклад короткого запису (шаблон).

Назва загрози: „Phish-X campaign".

Дата виявлення: 2025-11-10.

TTPs: Spearphishing Attachment (T1566.001) → Macro droppers.

IoC: domain example-mal[.]com, SHA256: abcd...

Значення для слідчого: надає слідчому актуальні відомості про нові кіберзагрози, зловмисні кампанії та атакуючі групи; дозволяє швидко орієнтуватися у пріоритетності реагування на інциденти; надає конкретні

технічні артефакти: IP-адреси, домени, хеші файлів, YARA-правила, електронні адреси.

Інструменти: MISP, OpenCTI, VirusTotal, Recorded Future (якщо є), Elastic Stack, SIEM, STIX/TAXII clients.

Predictive Risk Analysis – прогноз уразливостей у системах організації.

Мета: проаналізувати й передбачити, які слабкі місця в інфраструктурі організації мають найбільший шанс бути використаними в найближчому періоді, і надати пріоритезований план дій.

Зміст звіту:

1. Мета та охоплення (які підсистеми, дата аналізу);
2. Методи і дані: сканування вразливостей (Nessus/Qualys), інвентаризація активів, канали загроз, конфігурації, бізнес-критичність;
4. Модель ризику: формула/підхід (наприклад, Ризик = Ймовірність × Вплив). Рейтинги: CVSS + експлойт-статус (експлойт доступний/у публічній базі даних експлойтів) + exposure (internet-facing (експлойт доступний/у публічній базі даних експлойтів) + вплив (вихід на Інтернет));
5. Heatmap/ризик-матриця (активи × ризики);
6. Пріоритетні завдання та дорожня карта пом'якшення.

Методика дослідження:

1. Сканування вразливостей + ручна перевірка конфігурації + інформація про загрози;
2. Визначення: CVE → доступність експлойтів → зіставлення з MITRE → власник бізнесу;
3. Оцінювання: оцінка ймовірності (0–10) – на основі доступності експлойтів, вразливості, активності загроз; оцінка впливу (0–10) – на основі чутливості даних, вимог до часу безвідмовної роботи;
4. Аналіз сценаріїв «що – якщо»: наприклад, успішне RCE на вебсервері → латеральний рух → витік бази даних;
5. Прогнозування: короткострокове (30 днів), середньострокове (90 днів) – використання трендів потоків загроз.

Висновки: топ-10 вразливостей/активів із рекомендованими діями (patch/mitigate/compensate); Heatmap (графічна) + таблиця з датами завершення дій; ризикові сценарії з ймовірністю реалізації.

Значення для слідчого: дозволяє слідчому визначити, які системи або активи організації найбільш уразливі і можуть бути потенційними точками компрометації; допомагає спрямувати ресурси на перевірку критичних компонентів інфраструктури.

Інструменти: Nessus/Qualys/OpenVAS, Kenna, Tenable.io, Elastic, BI tool для візуалізацій.

Розділ 6. ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ OSINT СЛІДЧИМ ТА ОПЕРАТИВНИМ ПРАЦІВНИКОМ

6.1. Принципи та правова допустимість OSINT

OSINT (Open Source Intelligence) – це процес збору та аналізу інформації з відкритих, загальнодоступних джерел для отримання розвідувальних даних або доказової інформації. В контексті розслідування кіберзлочинів OSINT є потужним інструментом, доступним як для слідчих, так і для оперативних працівників. Джерела OSINT надзвичайно різноманітні:

1. Загальнодоступні вебсайти (включно з «глибокою павутиною» – Deep Web, доступною через звичайні браузери);
2. Соціальні мережі (Facebook, Instagram, LinkedIn, Twitter, Telegram та ін.);
3. Форуми, блоги, сервіси запитань та відповідей;
4. Відкриті бази даних та публічні реєстри (реєстри юридичних осіб, судових рішень, транспортних засобів, нерухомості тощо);
5. Засоби масової інформації (онлайн-видання, новини);
6. Кеш пошукових систем (Google Cache, Yandex Cache);
7. Метадані файлів (EXIF у фотографіях, дані про автора в документах);
8. Картографічні сервіси (Google Maps, OpenStreetMap);
9. Публічні записи DNS, WHOIS;
10. Спеціалізовані пошукові системи для Інтернету речей (Shodan, Censys).

Правова допустимість: Використання інформації, отриманої з відкритих джерел, у кримінальному провадженні є цілком законним, оскільки доступ до цих джерел не потребує спеціальних дозволів чи негласних методів. Однак для того щоб така інформація могла бути використана як доказ або орієнтуюча інформація, необхідно дотримуватися певних правил:

– *належне документування.* Джерело інформації (URL-адреса вебсторінки, назва бази даних тощо), дата та час отримання даних, а також сама інформація (скріншоти, роздруківки, витяги) повинні бути у належний спосіб зафіксовані у відповідному процесуальному документі

(найчастіше – у рапорті оперативного працівника або протоколі огляду вебсайту/документа);

– *перевірка та валідація.* Інформація з відкритих джерел не завжди є достовірною. Її необхідно ретельно перевіряти та, якщо це можливо, підтверджувати іншими доказами, отриманими процесуальним шляхом (наприклад, даними ТДРД, результатами експертиз).

6.2. Інструменти та техніки OSINT для проведення розслідування кримінальних правопорушень, кваліфікованих за ст. 361 КК України

Існує велика кількість інструментів та технік OSINT, які можуть бути корисними при розслідуванні НСВ (табл. 6.1).

Таблиця 6.1

Основні інструменти та техніки OSINT для розслідування кіберзлочинів

Категорія	**Інструмент/техніка (приклад)**	**Призначення**	**Можливе застосування у кримінальних провадженнях за ст. 361 КК України**
Загальний пошук	Google, Bing, DuckDuckGo (з використанням розширених операторів пошуку – «Google Dorks»)	Пошук інформації за ключовими словами, іменами, нікнеймами, email, IP, доменами.	Виявлення згадок про інцидент, пошук інформації про підозрюваних, виявлення пов'язаних ресурсів.
Пошук пристроїв та сервісів	Shodan, Censys, ZoomEye	Пошук комп'ютерів, серверів, мережевих пристроїв, підключених до Інтернету, за IP, портами, банерами сервісів.	Ідентифікація інфраструктури зловмисника (C&C сервери, проксі), виявлення вразливих систем.
Аналіз доменів та IP-адрес	WHOIS-сервіси (who.is, domaintools.com), DNS-реєстрації (dnsdumpster.com), сервіси IP-геолокації (MaxMind, ipinfo.io), аналіз історії домену (Wayback Machine, RiskIQ)	Отримання інформації про власника домену, дату реєстрації, хостинг-провайдера, пов'язані IP-адреси та субдомени, історію змін сайту.	Встановлення власника домену, використаного для фішингу або C&C; ідентифікація хостинг-провайдера для подальшого запиту; визначення приблизного місцезнаходження IP-адреси.

Аналіз соціальних мереж	Вбудований пошук соцмереж, Maltego, SpiderFoot, OSINT Framework	Пошук профілів за іменем, нікнеймом, email, телефоном; аналіз списку друзів/контактів, публікацій, фотографій, геолокаційних даних.	Ідентифікація особи за цифровим слідом; встановлення зв'язків між співучасниками; збір інформації про спосіб життя, інтереси, місцезнаходження підозрюваного.
Пошук за нікнеймом, email, телефоном	Namechk, Epieos, Have I Been Pwned?	Перевірка використання нікнейму на різних платформах; пошук пов'язаних акаунтів за email або телефоном; перевірка наявності даних у витоках.	Деанонімізація зловмисника; виявлення інших онлайн-ідентичностей; отримання додаткових контактних даних.
Аналіз вебсайтів	BuiltWith, Wappalyzer, Wayback Machine, інструменти розробника в браузері	Визначення технологій, використаних на сайті (CMS, фреймворки, бібліотеки); пошук прихованих файлів та директорій; перегляд архівних копій сайту.	Виявлення вразливостей на атакованому сайті; аналіз фішингових сайтів; реконструкція вигляду сайту до/після атаки.
Аналіз метаданих	ExifTool, FOCA	Вилучення та аналіз метаданих з файлів (фото, відео, документи), що можуть містити інформацію про автора, дату створення, геолокацію, використане ПЗ.	Отримання додаткової інформації про походження файлів, знайдених під час розслідування.

6.3. Практичне застосування OSINT

Інформація, отримана за допомогою OSINT, може бути використана на різних етапах розслідування за ст. 361 КК України:

– *ідентифікація особи.* Часто зловмисники залишають цифрові сліди у вигляді нікнеймів, email-адрес, IP-адрес. За допомогою OSINT можна спробувати пов'язати ці сліди з реальними профілями в соцмережах, на форумах, що може допомогти встановити особу підозрюваного або звузити коло пошуку;

– *встановлення інфраструктури.* OSINT дозволяє зібрати інформацію про домени, IP-адреси, хостинг-провайдерів, які

використовуються зловмисниками для розміщення фішингових сайтів, командних центрів (C&C) для управління ботнетами або шкідливим ПЗ;

– *збір інформації про потерпілого.* Аналіз відкритих джерел може допомогти зрозуміти мотиви атаки (наприклад, виявити конфлікти, в які була залучена компанія-жертва), а також виявити можливих інсайдерів, які могли сприяти втручанню;

– *виявлення зв'язків:* аналіз списків друзів у соцмережах, учасників форумів, коментарів може допомогти виявити зв'язки між відомими підозрюваними та потенційними співучасниками;

– *моніторинг:* відстеження активності підозрюваних осіб або груп у відкритих джерелах (нові публікації, реєстрація нових доменів, продаж викрадених даних на тіньових форумах).

Важливо розуміти, що інформація, отримана виключно за допомогою OSINT, рідко може слугувати самостійним та достатнім доказом вини особи в суді. Основні проблеми полягають у складності достовірної автентифікації інформації (наприклад, доведення, що конкретний профіль у соцмережі належить саме підозрюваному) та забезпеченні її допустимості з процесуального погляду. Однак OSINT відіграє надзвичайно важливу роль як інструмент оперативної розвідки та наведення. Інформація, знайдена у відкритих джерелах (наприклад, зв'язок між IP-адресою, використаною під час атаки, та нікнеймом на хакерському форумі, який, у свою чергу, пов'язаний з певним email, що згадується у профілі соцмережі), може стати ключовою для: а) висування обґрунтованих слідчих версій; б) планування обшуку за ймовірним місцем проживання або роботи особи, попередньо ідентифікованої за допомогою OSINT; в) підготовки більш предметних питань для допиту. Таким чином, OSINT дозволяє ефективно збирати первинну, орієнтуючу інформацію, яка потім перевіряється та закріплюється за допомогою процесуальних інструментів збору доказів, що значно підвищує ефективність та цілеспрямованість розслідування.

Розділ 7. ОРГАНІЗАЦІЯ МІЖНАРОДНОЇ СПІВПРАЦІ ПРИ РОЗКРИТТІ ЗЛОЧИНІВ ЗА СТ. 361 КК УКРАЇНИ

7.1. Важливість міжнародного співробітництва

Кіберзлочинність за своєю природою є транскордонним явищем. Зловмисники, їхні жертви, а також технічна інфраструктура, що використовується для вчинення злочинів (сервери, проксі, ботнети, хостинг-провайдери), дуже часто знаходяться у різних країнах та юрисдикціях. Наприклад, атака на український банк може здійснюватися хакерською групою з однієї країни через сервери, орендовані в іншій країні, а викрадені кошти виводитися через фінансові установи в третій країні. Це створює фундаментальну проблему для національних правоохоронних органів: їхні повноваження щодо проведення слідчих (розшукових) дій (обшук, вилучення, допит, отримання даних) обмежуються територією власної держави. Проведення будь-яких примусових заходів на території іншої країни без її офіційної згоди є порушенням державного суверенітету та міжнародного права. Тому ефективне розслідування транскордонних кіберзлочинів, зокрема НСВ за ст. 361 КК, неможливе без налагодженого міжнародного співробітництва України.

7.2. Механізми міжнародної правової допомоги

Основним інструментом міжнародної співпраці у кримінальних провадженнях є міжнародна правова допомога, що здійснюється на підставі міжнародних договорів та національного законодавства (Розділ IX КПК України).

Міжнародні договори: Україна є учасницею низки ключових багатосторонніх та двосторонніх договорів у цій сфері, як-от:

1. Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) ETS No. 185. Це основний міжнародний документ, що регулює співпрацю у боротьбі з кіберзлочинами. Вона встановлює спільні кримінально-правові стандарти, процесуальні інструменти (зокрема, транскордонний доступ до даних, збереження даних) та механізми співробітництва;

2. Європейська конвенція про взаємну допомогу у кримінальних справах 1959 р. та додаткові протоколи до неї – загальний договір Ради Європи, що регулює широкий спектр питань МПД;

3. Двосторонні договори про правову допомогу. Україна має низку двосторонніх договорів з різними країнами, які можуть деталізувати або доповнювати положення багатосторонніх конвенцій.

Порядок звернення із запитом про МПД:

– *компетентні органи:* центральними органами України, відповідальними за направлення та отримання запитів про МПД у кримінальних справах, є Офіс Генерального прокурора (у межах досудового розслідування) та Міністерство юстиції України (на стадії судового розгляду та виконання вироків);

– *вимоги до запиту:* запит про МПД повинен бути складений письмово, містити детальну інформацію про кримінальне провадження, опис обставин справи, відповідні статті КК України, чітке формулювання прохання (які саме дії необхідно провести), дані про осіб, щодо яких запитується допомога, та іншу необхідну інформацію згідно з вимогами відповідного міжнародного договору та КПК України. Запит та додані матеріали зазвичай потребують перекладу на офіційну мову запитуваної держави або одну з офіційних мов Ради Європи/ООН;

– *процедура:* слідчий або прокурор готує проєкт запиту, який потім направляється через відповідний центральний орган (ОГП) до компетентного органу іноземної держави;

– *види МПД:* запити можуть стосуватися широкого кола дій: проведення окремих слідчих дій на території іншої держави (допит свідків, потерпілих, підозрюваних; обшук; вилучення речей і документів, у тому числі комп'ютерної техніки); тимчасовий доступ до комп'ютерних даних, що зберігаються на території іншої держави (наприклад, отримання логів іноземного провайдера);

– *вручення документів;*

– *передача предметів та інформації;*

– *видача осіб (екстрадиція) для притягнення до кримінальної відповідальності або виконання вироку;*

– *мережа контактних пунктів 24/7:* стаття 35 Будапештської конвенції передбачає створення мережі цілодобово діючих контактних пунктів (24/7 Network) у кожній країні-учасниці. В Україні функції такого пункту виконує Департамент кіберполіції НПУ. Ця мережа призначена для забезпечення термінової взаємодії між правоохоронними органами різних країн, насамперед для швидкого збереження комп'ютерних даних (наприклад, логів провайдера, даних про трафік), які можуть бути швидко видалені. Запит через мережу 24/7 дозволяє

«заморозити» дані на певний період, поки готується та надсилається офіційний запит про МПД.

7.3. Роль Національного центрального бюро Інтерполу в Україні

Міжнародна організація кримінальної поліції (Інтерпол) є важливим каналом міжнародного поліцейського співробітництва. В Україні його представляє НЦБ Інтерполу, що діє у складі Національної поліції України.

Функції НЦБ Інтерполу:

– забезпечення обміну кримінальною інформацією між правоохоронними органами України та країн-членів Інтерполу через захищену комунікаційну систему I-24/7;

– надання доступу до міжнародних баз даних Інтерполу (розшукувані особи, викрадені транспортні засоби, втрачені/викрадені документи, відбитки пальців, ДНК тощо);

– обробка та направлення міжнародних запитів та повідомлень Інтерполу (наприклад, Red Notice – розшук з метою арешту та екстрадиції, Blue Notice – встановлення місцезнаходження особи, Green Notice – попередження про осіб, що становлять загрозу).

Взаємодія слідчого/оперативного працівника з НЦБ Інтерполу. Слідчі та оперативні працівники можуть звертатися до НЦБ Інтерполу для:

1. Перевірки осіб, транспортних засобів, документів за базами даних Інтерполу;
2. Отримання інформації про наявність кримінальних проваджень щодо певних осіб в інших країнах;
3. Встановлення ймовірного місцезнаходження підозрюваних або свідків, які перебувають за кордоном;
4. Оголошення особи у міжнародний розшук;
5. Отримання іншої оперативної інформації, що може бути корисною для розслідування.

Запити до НЦБ Інтерполу направляються у встановленому порядку через відповідні підрозділи НПУ. Важливо розуміти, що Інтерпол є каналом обміну поліцейською інформацією, а не механізмом МПД у процесуальному сенсі (тобто через Інтерпол не можна отримати дозвіл на обшук за кордоном). Однак інформація, отримана каналами Інтерполу, може бути критично важливою для планування подальших дій, у тому числі для підготовки запиту про МПД.

7.4. Практичні аспекти взаємодії

Незважаючи на наявність міжнародних механізмів, міжнародна співпраця у справах про кіберзлочини часто стикається з практичними труднощами:

– *тривалість процедур.* Формальна процедура МПД через центральні органи може бути дуже тривалою (від кількох місяців до року і більше), що є неприйнятним для збереження швидкоплинних цифрових доказів;

– *різниця в законодавстві.* Правові системи різних країн відрізняються, зокрема, щодо визначення кіберзлочинів, вимог до отримання доказів (наприклад, стандартів отримання судового дозволу на доступ до даних), правил допустимості доказів. Це може ускладнити виконання запитів;

– *подвійна злочинність.* Багато договорів вимагають дотримання принципу подвійної злочинності (діяння має визнаватися злочином в обох країнах);

– *мовний бар'єр.* Необхідність перекладу запитів та матеріалів справи;

– *брак ресурсів.* Недостатнє кадрове та технічне забезпечення підрозділів, відповідальних за МПД, як в Україні, так і в запитуваних країнах.

З огляду на ці виклики особливого значення набувають інструменти, що дозволяють прискорити взаємодію. Формальна процедура МПД, хоч і є необхідною для отримання процесуально допустимих доказів, часто виявляється занадто повільною для динамічного середовища кіберзлочинів. Тому слідчим та оперативним працівникам необхідно активно використовувати паралельні, більш швидкі канали, як-от:

1. Мережа 24/7. Як зазначалося, це ключовий інструмент для термінового запиту на збереження даних (preservation request). Це дозволяє виграти час, поки готується повний запит про МПД;

2. Неформальна співпраця. Якщо існують прямі контакти між слідчими підрозділами України та інших країн (наприклад, встановлені під час спільних навчань чи операцій), їх можна використовувати для попереднього обміну інформацією та координації дій (звісно, з подальшим формальним оформленням через МПД);

3. Канали Інтерполу – для швидкого обміну оперативною інформацією та перевірки даних.

Для підвищення ефективності формальних запитів про МПД важливо готувати їх максимально якісно: чітко формулювати прохання, надавати детальне обґрунтування необхідності запитуваних дій, посилатися на відповідні статті міжнародних договорів та національного законодавства, надавати повну контактну інформацію.

Розділ 8. ОСОБЛИВОСТІ ДОКУМЕНТУВАННЯ, РОЗКРИТТЯ ТА РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРОВАДЖЕНЬ ЗА СТ. 361 КК УКРАЇНИ В УМОВАХ ПОВНОМАСШТАБНОГО ВТОРГНЕННЯ рф

8.1. Виклики та адаптації в роботі слідчих підрозділів

Повномасштабне вторгнення російської федерації в Україну 24 лютого 2022 р. створило безпрецедентні виклики для всіх сфер життя країни, включно з діяльністю правоохоронних органів. Розслідування кіберзлочинів, зокрема за ст. 361 КК України, в умовах воєнного стану має свою специфіку та стикається з низкою проблем:

– *різке зростання кількості та інтенсивності кібератак.* Україна стала головною мішенню для кібератак, спонсорованих або здійснюваних державою-агресором та пов'язаними з нею хакерськими угрупованнями (APT-групи, «хактивісти»). Ці атаки спрямовані на державні інформаційні ресурси, об'єкти критичної інфраструктури, ЗМІ, фінансовий сектор, а також на поширення дезінформації та здійснення психологічних операцій;

– *ускладнення проведення слідчих (розшукових) дій.* Ведення бойових дій, тимчасова окупація частини території України, руйнування інфраструктури, переміщення населення та підприємств суттєво ускладнюють або унеможливлюють проведення таких слідчих дій, як огляд місця події, обшук, допит свідків на відповідних територіях;

– *пріоритезація розслідувань.* В умовах обмежених ресурсів та великої кількості інцидентів виникає необхідність пріоритезації розслідувань. На перший план виходять справи, пов'язані із загрозами національній безпеці та обороні, функціонуванню критичної інфраструктури, а також ті, що можуть кваліфікуватися як воєнні злочини;

– *процесуальні особливості.* Хоча КПК України і зазнав певних змін у зв'язку зі введенням воєнного стану, вони переважно стосуються строків розслідування, порядку обрання запобіжних заходів, можливості проведення окремих дій за відсутності підозрюваного. Специфічних змін, що стосувалися б безпосередньо методики розслідування за ст. 361 КК України, не відбулося, однак загальні умови воєнного стану впливають на тактику проведення слідчих дій;

– *посилення відповідальності.* Введення ч. 5 ст. 361 КК України, що встановлює підвищену відповідальність за НСВ, вчинене в умовах воєнного стану, вимагає від слідчих доведення цієї обставини.

8.2. Пріоритезація кіберзагроз, пов'язаних з агресією

В умовах війни зусилля правоохоронних органів, зокрема Департаменту кіберполіції НПУ та відповідних підрозділів СБУ, мають бути сконцентровані на розслідуванні кібератак, що становлять найбільшу загрозу для держави та суспільства. Пріоритетними є атаки, спрямовані на:

– *об'єкти критичної інфраструктури:* енергетичні компанії, системи водо- та теплопостачання, транспортні вузли, телекомунікаційні мережі, фінансові установи, заклади охорони здоров'я. Атаки на ОКІ можуть призвести до катастрофічних наслідків;

– *державні інформаційні ресурси:* урядові портали, бази даних реєстрів, системи електронного документообігу органів влади. Метою таких атак може бути як порушення роботи державних органів, так і викрадення чутливої інформації;

– *військові системи:* системи управління військами, зв'язку, розвідки. Такі атаки становлять пряму загрозу обороноздатності країни;

– *системи життєзабезпечення:* системи, що забезпечують надання гуманітарної допомоги, роботу рятувальних служб, оповіщення населення.

Розслідування таких атак вимагає тісної взаємодії між різними суб'єктами сектору безпеки та оборони: Національною поліцією України (кіберполіція, слідство), Службою безпеки України, Державною службою спеціального зв'язку та захисту інформації України (зокрема, урядовою командою реагування на комп'ютерні надзвичайні події CERT-UA), розвідувальними органами.

8.3. Особливості документування та збору доказів

Війна вносить корективи і в процес документування та збору доказів у справах про НСВ.

Атрибуція атак. Одним із ключових завдань стає не лише встановлення факту НСВ та його наслідків, але й атрибуція атаки – тобто встановлення її джерела, зокрема зв'язку зі спецслужбами рф або

контрольованими нею хакерськими угрупованнями (наприклад, Sandworm, Fancy Bear/APT28, Gamaredon/Armageddon). Це вимагає глибокого технічного аналізу шкідливого ПЗ, інфраструктури атаки, тактик, технік та процедур (TTPs), використовуваних зловмисниками, а також співставлення цих даних із інформацією розвідувальних органів та міжнародних партнерів.

Використання даних розвідки. Інформація, отримана розвідувальними (в тому числі кіберрозвідувальними) органами, може мати вирішальне значення для атрибуції атак та встановлення організаторів. Однак її використання у кримінальному провадженні пов'язане з проблемою легалізації та розсекречення, що потребує окремих законодавчих та процедурних рішень.

Документування воєнних злочинів. Деякі кібератаки, особливо ті, що спрямовані на цивільну інфраструктуру та призводять до значних руйнувань, людських жертв або гуманітарних криз, можуть розглядатися як воєнні злочини, вчинені у кіберпросторі. Збір та належне документування доказів таких атак є важливими для притягнення винних до відповідальності, зокрема у міжнародних судових інстанціях (наприклад, Міжнародному кримінальному суді).

Міжнародна співпраця. В умовах, коли переважна більшість атак походить із території рф або інших недружніх країн, можливості традиційної МПД з цими країнами відсутні. Тому критично важливим стає співробітництво з країнами-партнерами (США, Великою Британією, країнами ЄС) для отримання доказів, що знаходяться в їхній юрисдикції (наприклад, даних американських технологічних компаній, хостинг-провайдерів), а також для обміну розвідувальною інформацією та координації зусиль із протидії російській кіберагресії.

Війна призвела до певної зміни парадигми розслідування кібератак, особливо тих, що спрямовані проти держави та критичної інфраструктури. Якщо раніше основний фокус був зосереджений на ретроспективному аналізі факту розслідування НСВ та притягненні до відповідальності конкретного виконавця (що часто було ускладнено з огляду на анонімність та транскордонність), то зараз акценти зміщуються. По-перше, зростає важливість проактивного реагування та тісної взаємодії з CERT-UA та іншими структурами для якнайшвидшої локалізації атаки та мінімізації шкоди. По-друге, ключовим завданням стає атрибуція атаки – встановлення її зв'язку з державою-агресором або підконтрольними їй структурами. По-третє, збір доказів розглядається не лише в контексті національного кримінального провадження, але й із перспективою їх можливого використання у міжнародних механізмах правосуддя (Міжнародному кримінальному суді, спеціальному

трибуналі) або для обґрунтування міжнародних санкцій проти агресора. Це вимагає від слідчих більш широкого, стратегічного погляду на розслідування, тісної координації з розвідувальними та контррозвідувальними органами, а також глибокого розуміння міжнародного права та механізмів міжнародної співпраці.

8.4. Процесуальні аспекти в умовах воєнного стану

Загалом порядок проведення слідчих (розшукових) дій, передбачений КПК України, залишається чинним і під час воєнного стану. Однак слід враховувати певні особливості та можливі зміни:

– *строки досудового розслідування.* Законом можуть встановлюватися особливості обчислення та продовження строків досудового розслідування в умовах воєнного стану;

– *особливий режим досудового розслідування.* Стаття 615 КПК України передбачає можливість застосування особливого режиму досудового розслідування в умовах воєнного стану, якщо відсутня технічна можливість доступу до ЄРДР. Це може стосуватися порядку початку розслідування, фіксації дій, повноважень керівника органу прокуратури;

– *проведення слідчих (розшукових) дій за відсутності учасників.* Можливі ситуації, коли проведення певних дій (наприклад, обшуку) ускладнюється через відсутність власника приміщення або інших учасників, які перебувають на окупованій території або в зоні бойових дій. КПК України передбачає певні процедури для таких випадків, але їх застосування вимагає обережності та ретельної фіксації;

– *безпека.* При плануванні та проведенні слідчих дій у регіонах, наближених до зони бойових дій, необхідно враховувати підвищені ризики для життя та здоров’я учасників слідчої групи та вживати відповідних заходів безпеки.

Слідчі мають уважно відстежувати зміни до КПК України та інших нормативних актів, що регулюють кримінальне провадження в умовах воєнного стану, та керуватися відповідними роз’ясненнями Верховного Суду та Офісу Генерального прокурора.

Розділ 9. ТИПОВІ ПРАКТИЧНІ ПРИКЛАДИ ТА АЛГОРИТМИ ДІЙ

Цей розділ пропонує узагальнені алгоритми дій для ключових учасників розслідування злочинів за ст. 361 КК України та ілюстративні приклади. Наведені алгоритми не є вичерпними, але можуть слугувати базовим орієнтиром у типових ситуаціях.

9.1. Алгоритм дій слідчого (дізнавача) на початковому етапі

Крок 1: Реєстрація та первинна оцінка. Отримавши заяву, повідомлення про злочин або рапорт, слідчий (дізнавач) невідкладно реєструє відомості в ЄРДР. Проводить первинний аналіз інформації для визначення наявності ознак злочину, передбаченого ст. 361 КК України, та його можливої кваліфікації.

Крок 2: Невідкладний огляд місця події. За наявності підстав організовує та проводить невідкладний огляд місця події (офіс, серверна, житло). Обов'язково залучає спеціаліста (з кіберполіції або ІТ-фахівця). Під час огляду фіксується обстановка, стан комп'ютерної техніки, мережевого обладнання, вилучаються або копіюються первинні цифрові дані (логи, образи дисків – див. Розділ IV).

Крок 3: Допит потерпілого/заявника. Проводить детальний допит потерпілого (власника системи, адміністратора) або заявника для з'ясування всіх обставин події, технічних деталей, можливих підозрюваних, розміру завданої шкоди.

Крок 4: Визначення попередньої кваліфікації. На основі зібраних первинних даних визначає найбільш імовірну кваліфікацію діяння за відповідною частиною ст. 361 КК України (з урахуванням наслідків, кваліфікуючих ознак).

Крок 5: Планування першочергових дій. Складає план першочергових слідчих (розшукових) дій, який може містити:

5.1. Підготовку та направлення запитів інтернет-провайдерам, операторам зв'язку, хостинг-провайдерам (спочатку можливі запити на збереження даних через мережу 24/7, потім – клопотання про ТДРД);

5.2. Підготовку та подання до суду клопотань про тимчасовий доступ до речей і документів (логи, дані абонентів тощо);

5.3. Підготовку та подання до суду клопотання про дозвіл на обшук (за наявності даних про місцезнаходження підозрюваного або доказів);

5.4. Призначення комп’ютерно-технічної експертизи вилученої техніки або даних.

Крок 6: Взаємодія. Налагоджує взаємодію з оперативним підрозділом (надання доручень на встановлення осіб, проведення ОРЗ) та підрозділом кримінального аналізу (постановка завдань на аналіз даних, перевірку зв’язків).

9.2. Алгоритм дій оперативного працівника (Департамент кіберполіції, інші оперативні підрозділи)

Крок 1: Збір первинної інформації. Здійснює первинний збір інформації про можливе вчинення НСВ (з агентурних джерел, моніторингу мережі Інтернет, заяв громадян). Виявляє ознаки злочину.

Крок 2: Застосування OSINT. Активно використовує інструменти та техніки OSINT (див. Розділ VI) для:

2.1. Спроби ідентифікації зловмисників (за IP-адресами, нікнеймами, email);

2.2. Встановлення використовуваної ними інфраструктури (домени, хостинг, сервери);

2.3. Виявлення зв’язків між можливими співучасниками;

2.4. Збору іншої орієнтуючої інформації.

Крок 3: Інформування та взаємодія зі слідчим. Доповідає про виявлені ознаки злочину слідчому (рапорт). Надає зібрані матеріали (зокрема задокументовані у належний спосіб результати OSINT). Узгоджує подальші спільні дії.

Крок 4: Виконання доручень. Виконує письмові доручення слідчого, прокурора щодо:

4.1. Встановлення місцезнаходження осіб, причетних до злочину;

4.2. Встановлення свідків;

4.3. Проведення оперативно-розшукових заходів (ОРЗ), дозволених законом.

Крок 5: Проведення НСРД (за наявності підстав та дозволу). У випадках, передбачених законом, та за відповідним дорученням слідчого/прокурора і на підставі ухвали суду проводить негласні слідчі (розшукові) дії (зняття інформації з транспортних телекомунікаційних мереж, контроль за листуванням тощо).

9.3. Алгоритм дій кримінального аналітика

Крок 1: Отримання завдання/ініціативний аналіз. Отримує завдання (доручення) від слідчого або оперативного працівника щодо проведення аналітичного дослідження у конкретному кримінальному провадженні. Може також проводити ініціативний аналіз на основі наявних даних для виявлення прихованих загроз або зв'язків.

Крок 2: Збір даних. Здійснює збір необхідної інформації з доступних джерел, як-от: інформаційні системи НПУ (ІПНП та ін.), матеріали кримінального провадження (надані слідчим), відкриті джерела (OSINT), дані від інших підрозділів.

Крок 3: Обробка та аналіз. Систематизує та аналізує зібрані дані за допомогою спеціалізованого ПЗ (наприклад, IBM i2) та аналітичних методів:

3.1. Побудова схем зв'язків (особи, IP, телефони, фінанси);

3.2. Аналіз фінансових транзакцій;

3.3. Часовий аналіз подій (timeline analysis);

3.4. Геопросторовий аналіз;

3.5. Виявлення аномалій та патернів.

Крок 4: Підготовка аналітичного продукту. Готує аналітичний документ (довідку, звіт, схему) з чіткими висновками та візуалізацією результатів аналізу.

Крок 5: Представлення результатів та взаємодія. Представляє результати аналізу слідчому/оперативному працівнику. Бере участь у спільному обговоренні версій, надає рекомендації щодо подальших дій. Забезпечує зворотний зв'язок.

9.4. Алгоритм взаємодії з представником НЦБ Інтерполу

Крок 1: Визначення потреби. Слідчий або оперативний працівник визначає необхідність звернення до каналів Інтерполу (наприклад, підозрюваний, імовірно, перебуває за кордоном; необхідно перевірити особу за міжнародними базами даних; потрібно встановити власника іноземного транспортного засобу, що фігурує у справі).

Крок 2: Підготовка запиту. Готує запит до НЦБ Інтерполу відповідно до встановлених форм та вимог МВС України та НПУ. Запит має містити всю необхідну інформацію для його обробки (дані про особу/об'єкт, суть справи, мета запиту).

Крок 3: Направлення запиту. Направляє запит до НЦБ Інтерполу через відповідний структурний підрозділ НПУ згідно з відомчими інструкціями.

Крок 4: Отримання відповіді. Отримує відповідь/інформацію від НЦБ Інтерполу.

Крок 5: Використання інформації. Використовує отриману інформацію в оперативно-розшуковій діяльності або для планування слідчих (розшукових) дій. Важливо пам'ятати, що інформація, отримана каналами Інтерполу, зазвичай має орієнтуючий характер і потребує подальшої процесуальної легалізації, якщо її планується використовувати як доказ у суді (наприклад, шляхом направлення запиту про МПД).

9.5. Ілюстративні (знеособлені) приклади з практики (наведені приклади є узагальненими та знеособленими ілюстраціями застосування описаних підходів)

Приклад 1: Розслідування фішингової атаки на клієнтів банку.

Ситуація: Масова розсилка фішингових листів нібито від імені банку з посиланням на підроблений сайт інтернет-банкінгу. Клієнти вводять логіни/паролі – зловмисники отримують доступ до рахунків та викрадають кошти.

Дії: Слідчий розпочинає досудове розслідування, допитує потерпілих, проводить огляд фішингового сайту (із залученням спеціаліста кіберполіції). Оперативний працівник за допомогою OSINT встановлює реєстратора домену та хостинг-провайдера фішингового сайту (наприклад, зареєстрований на підставну особу через іноземного реєстратора, хостинг в іншій країні). Слідчий готує клопотання про ТДРД до українських банків щодо руху коштів по рахунках потерпілих та рахунках, на які виводилися кошти («дропи»). Кримінальний аналітик аналізує фінансові транзакції, виявляє спільні точки виведення коштів, можливих організаторів та «дропів». Через мережу 24/7 направляється запит на збереження даних хостинг-провайдера, паралельно готується запит про МПД для отримання логів доступу до фішингового сайту та даних про замовника хостингу. Через НЦБ Інтерполу перевіряються особи, на яких зареєстровані рахунки «дропів».

Приклад 2: Розслідування DDoS-атаки на урядовий портал.

Ситуація: Масована DDoS-атака на офіційний вебпортал одного з міністерств, що призводить до його недоступності (блокування інформації).

Дії: CERT-UA фіксує атаку та повідомляє правоохоронні органи. Проводиться огляд серверного обладнання порталу (із залученням спеціалістів CERT-UA та кіберполіції), вилучаються логи мережевого обладнання (міжмережевих екранів, балансувальників навантаження). Кримінальний аналітик аналізує логи для ідентифікації джерел атаки (велика кількість IP-адрес, що належать до ботнету). Оперативний працівник за допомогою OSINT та спеціалізованих сервісів (Shodan) намагається ідентифікувати командні центри (C&C) ботнету. Якщо C&C знаходяться за кордоном, готуються запити через мережу 24/7 та МПД для їх блокування та отримання даних. В умовах воєнного стану особлива увага приділяється атрибуції атаки (пошук зв'язку з рф).

Приклад 3: Розслідування НСВ в корпоративну мережу з метою шпигунства.

Ситуація: Невідомі особи отримують несанкціонований доступ до внутрішньої мережі великої компанії, тривалий час непомітно перебувають у мережі та викрадають комерційну таємницю (креслення, бізнес-плани).

Дії: Слідчий проводить огляд комп'ютерів та серверів компанії (із залученням спеціаліста), призначає комплексну КТЕ для аналізу образів дисків та логів. Експертиза встановлює вектор проникнення (наприклад, фішинг із цільовим мм), виявляє сліди активності зловмисників (використані облікові записи, IP-адреси C&C серверів, перелік викрадених файлів). Кримінальний аналітик аналізує часову шкалу подій, будує схему переміщення зловмисників у мережі, аналізує зв'язки з C&C серверами. Оперативний працівник перевіряє IP-адреси C&C, використовує OSINT для пошуку інформації про ШПЗ та можливі хакерські угруповання (APT), що його використовують. Якщо є підозри щодо інсайдера, проводяться відповідні ОРЗ та слідчі (розшукові) дії щодо співробітників компанії.

Приклад 4: Розслідування НСВ щодо об'єкта критичної інфраструктури в умовах воєнного стану.

Ситуація: Спроба НСВ в систему управління технологічним процесом на енергетичному об'єкті (ОКІІ) з метою виведення її з ладу. Атаку вдалося заблокувати на початковому етапі.

Дії: Розслідування проводиться у тісній взаємодії з СБУ та Держспецзв'язку. Слідчий кваліфікує дії за ч. 3 та ч. 5 ст. 361 КК України. Проводиться ретельний аналіз логів систем безпеки, мережевого трафіку. Призначається КТЕ для аналізу використаного ШПЗ та інструментів атаки. Основний акцент робиться на атрибуції атаки – встановленні зв'язку її з державними структурами рф. Використовуються дані кіберрозвідки (з дотриманням процедур легалізації). Активно задіюються канали міжнародної співпраці з країнами-партнерами для обміну інформацією та отримання доказів із іноземних юрисдикцій. Зібрані докази

документуються також із урахуванням можливості їх використання у міжнародних судах як доказів агресії та воєнних злочинів.

Надання чітких, покрокових алгоритмів дій для різних учасників процесу розслідування (слідчого, оперативного працівника, аналітика) сприяє стандартизації підходів, особливо в умовах високого навантаження та необхідності швидкого реагування. Це допомагає знизити кількість помилок, особливо у менш досвідчених співробітників, та прискорити процес розслідування. Анонімізовані приклади з практики ілюструють, як теоретичні знання, методики та алгоритми застосовуються в реальних ситуаціях, та роблять ці рекомендації більш зрозумілими та легкими для засвоєння і застосування на практиці.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

Підсумок ключових аспектів. Розслідування несанкціонованого втручання в роботу інформаційних систем та мереж (ст. 361 КК України) є складним процесом, що вимагає від правоохоронців глибоких знань як у галузі права, так і у сфері інформаційних технологій. Ключовими аспектами успішного розслідування є: чітке розуміння технічної термінології та правильна кримінально-правова кваліфікація діяння (з урахуванням останніх змін законодавства, зокрема щодо ОКІІ та воєнного стану); ретельне планування розслідування; кваліфіковане проведення специфічних слідчих (розшукових) та процесуальних дій (огляд, ТДРД, обшук, КТЕ) з належною фіксацією швидкоплинних цифрових доказів та дотриманням ланцюга їхньої безперервності; ефективне використання аналітичних інструментів (кримінальний аналіз, OSINT) для обробки великих обсягів даних та виявлення прихованих зв'язків; активне залучення механізмів міжнародної правової допомоги та інших каналів міжнародної співпраці (Інтерпол, мережа 24/7) для подолання транскордонного характеру кіберзлочинності; адаптація тактики розслідування до викликів, пов'язаних із повномасштабною агресією рф, із акцентом на атрибуцію атак та документування воєнних злочинів у кіберпросторі.

Системні проблеми. Незважаючи на значний прогрес у розбудові спроможностей України у сфері протидії кіберзлочинності, залишається низка системних проблем, що ускладнюють розслідування кримінальних правопорушень за ст. 361 КК України:

1. Недосконалість законодавства: потребує подальшого вдосконалення термінологія, вимагають уточнення процедури отримання та використання цифрових доказів (особливо транскордонних), необхідною залишається гармонізація з міжнародними стандартами (зокрема, Другим додатковим протоколом до Будапештської конвенції);
2. Кадрові питання: брак достатньої кількості висококваліфікованих слідчих, прокурорів, експертів та суддів, що спеціалізуються на кіберзлочинах; необхідність постійного підвищення їхньої кваліфікації з урахуванням швидкого розвитку технологій;
3. Матеріально-технічне забезпечення: потреба у сучасному програмному та апаратному забезпеченні для збору, аналізу цифрових доказів та проведення експертиз;

4. Міжнародна співпраця: тривалість та бюрократичність формальних процедур МПД, проблеми з виконанням запитів деякими країнами;

5. Взаємодія: необхідність подальшого покращення координації та обміну інформацією між різними правоохоронними органами (НПУ, СБУ, прокуратура), Держспецзв'язку та приватним сектором.

Рекомендації. На основі проведеного аналізу пропонуються такі рекомендації:

законодавчі:

1. Продовжити роботу над уніфікацією та уточненням термінології у сфері кібербезпеки та кіберзлочинності в національному законодавстві;

2. Розглянути можливість імплементації положень Другого додаткового протоколу до Будапештської конвенції для спрощення процедур транскордонного доступу до доказів;

3. Удосконалити процесуальні норми щодо фіксації, вилучення та дослідження цифрових доказів, забезпечивши їхню відповідність сучасним технологічним реаліям та міжнародним стандартам;

4. Розробити чіткіші критерії для визначення «тяжких наслідків» у ч. 4 ст. 361 КК України;

організаційні:

1. Посилити спеціалізацію слідчих, прокурорів та суддів, що займаються розслідуванням та розглядом справ про кіберзлочини. Забезпечити їх безперервне навчання та підвищення кваліфікації;

2. Зміцнити матеріально-технічну базу підрозділів кіберполіції, слідства та експертних установ, забезпечивши їх сучасними інструментами для роботи з цифровими доказами;

3. Покращити механізми взаємодії та обміну інформацією між НПУ, СБУ, ОГП, Держспецзв'язку (CERT-UA), розвідувальними органами та приватним сектором (провайдери, банки, IT-компанії);

4. Розвивати потенціал підрозділів кримінального аналізу, забезпечуючи їх необхідними ресурсами та інтегруючи їхню роботу у процес розслідування на ранніх стадіях;

методичні:

1. Регулярно оновлювати та поширювати методичні рекомендації для слідчих, прокурорів, оперативних працівників та аналітиків щодо розслідування різних видів кіберзлочинів, зокрема НСВ, з урахуванням нових векторів атак, інструментів та законодавчих змін;

2. Розробляти типові алгоритми дій та поширювати успішні практики розслідування;

3. Активніше використовувати можливості OSINT, проводячи відповідні тренінги для персоналу;

щодо міжнародної співпраці:

1. Активізувати використання «швидких» каналів міжнародної взаємодії (мережа 24/7, прямі контакти, Інтерпол) паралельно з формальними процедурами МПД;

2. Підвищувати якість підготовки запитів про МПД для прискорення їх розгляду іноземними партнерами;

3. Поглиблювати співпрацю з міжнародними організаціями (Рада Європи, ООН, Інтерпол, Європол) та країнами-партнерами у сфері обміну інформацією, проведення спільних розслідувань та навчань;

4. Продовжувати роботу щодо притягнення рф до відповідальності за кіберагресію на міжнародному рівні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Біленчук П. Д., Кравчук В. В., Кравчук О. В., Кулик В. М. Комп'ютерний тероризм : практика запобігання, протидії, розслідування: навч. посібник / за заг. ред. П. Д. Біленчука. Хмельницький : Хмельн. ЦНТЕІ, 2008. 258 с.
2. Довженко О. Ю. Основи методики розслідування кіберзлочинів : дис. … канд. юрид. наук : 12.00.09 / Харківський національний університет внутрішніх справ. Харків, 2020. 229 с.
3. Європейська конвенція про взаємну допомогу у кримінальних справах від 20.04.1959. Ратифікована із заявами і застереженнями Законом України від 16.01.1998. URL : https: // zakon.rada.gov.ua/laws/show/995_036#Text.
4. Єфімов М. М., Павлова Н. В., Чучко С. В. Методика розслідування шахрайств, пов'язаних із купівлею-продажем товарів через мережу Інтернет : теоретичні та праксеологічні засади : монографія. Одеса : Видавничий дім «Гельветика», 2022. 200 с.
5. Захарова Г. В. Теоретичні засади методики розслідування шахрайства у сфері туризму, вчиненого організованою групою : дис. … канд. юрид. наук : 12.00.09 / ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом»». Київ, 2021. 246 с.
6. Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 Право / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2022. 234 с.
7. Конвенція про взаємодопомогу в кримінальних справах між державами-членами Європейського Союзу. URL : https://zakon.rada.gov.ua/laws/show/994_238#Text.
8. Конвенція про кіберзлочинність від 23.11.2001. Ратифікована із застереженнями і заявами Законом України від 07.09.2005. URL : https://zakon.rada.gov.ua/laws/show/994_575#Text.
9. Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. … д-ра філос. : 081 Право / Національна академія внутрішніх справ. Київ, 2021. 255 с.
10. Криміналістика : підруч. / за заг. ред. В. В. Пясковського. 2-е вид., перероб. і доп. Харків : Право, 2020. 752 с.
11. Криміналістика : підруч. : у 2 т. Т. 2 / за заг. ред. А. Ф. Волобуєва, Р. Л. Степанюка, В. О. Малярової. Харків : МВС України ; Харків. нац. ун-т внутр. справ, 2018. 312 с.

12. Кримінальний кодекс України : Закон України від 05.04.2001. URL : https://zakon.rada.gov.ua/laws/show/2341-14#Text.

13. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012. URL : https://zakon.rada.gov.ua/laws/show/4651-17#Text.

14. Про внесення змін до Кримінального кодексу України щодо посилення відповідальності за злочини проти основ національної безпеки України в умовах дії режиму воєнного стану : Закон України від 03.03.2022. URL : https://zakon.rada.gov.ua/laws/show/2113-20#Text.

15. Про електронні комунікації : Закон України від 16.12.2020. URL : https://zakon.rada.gov.ua/laws/show/1089-20#Text.

16. Про затвердження Порядку класифікації надзвичайних ситуацій за їх рівнями : постанова Кабінету Міністрів України від 24 березня 2004 р. № 368. URL : https://zakon.rada.gov.ua/laws/show/368-2004-п#Text.

17. Про затвердження Правил технічної експлуатації електроустановок споживачів : наказ Міністерства палива та енергетики України від 25.07.2006 № 258. URL : https://zakon.rada.gov.ua/laws/show/z1143-06#Text.

18. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994. URL : https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

19. Про захист населення від інфекційних хвороб : Закон України від 06 квітня 2000 р. URL : https://zakon.rada.gov.ua/laws/show/1645-14#Text.

20. Про зону надзвичайної екологічної ситуації : Закон України від 13 липня 2000 р. URL : https://zakon.rada.gov.ua/laws/show/1908-14#Text.

21. Про інформацію : Закон України від 02.10.1992. URL : https://zakon.rada.gov.ua/laws/show/2657-12#Text.

22. Про об’єкти підвищеної небезпеки : Закон України від 18.01.2001. URL : https://zakon.rada.gov.ua/laws/show/2245-14#Text.

23. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

24. Про правовий режим воєнного стану : Закон України від 12 травня 2015 р. URL : https://zakon.rada.gov.ua/laws/show/389-19#Text.

25. Сисолятін В. В. Розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу : дис. … канд. юрид. наук : 12.00.09 / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2024. 230 с.

26. Чаплинський К. О., Єфімов М. М., Жилін А. Е. Методика розслідування шахрайства у сфері використання банківських електронних платежів : монографія. Одеса : Видавництво «Юридика», 2024. 218 с.

ГЛОСАРІЙ

Експлойт (exploit) – програмний код, метод або послідовність дій, які використовують вразливість у програмному забезпеченні, апаратному забезпеченні чи інформаційній системі для отримання несанкціонованого доступу або порушення нормальної роботи.

Кеш (cache) – це спеціальна ділянка пам'яті або сховище, де тимчасово зберігаються дані, щоб прискорити доступ до них у майбутньому.

Нікнейм (від англ. nickname) – псевдонім або ім'я користувача, що його людина використовує в мережі Інтернет, онлайн-іграх, соціальних мережах або на форумах замість свого реального імені.

Файли cookie (кукі) – це невеликі текстові файли, які вебсайт зберігає на пристрої користувача через браузер. Вони містять дані, що допомагають сайту «розпізнавати» користувача й полегшують роботу сервісу.

DDoS (Distributed Denial of Service) – тип кібератаки, під час якої зловмисники масово надсилають велику кількість запитів до сервера, сайту чи мережевого ресурсу з різних пристроїв, щоб перевантажити систему і зробити її недоступною для законних користувачів.

NetFlow – технологія та протокол мережевого моніторингу, розроблений компанією Cisco, для збору, аналізу та відстеження інформації про трафік у мережі.

WHOIS – сервіс та протокол для отримання інформації про реєстрацію доменних імен та IP-адрес.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЕОМ – електронно-обчислювальна машина.
ЕОТ – електронно-обчислювальна техніка.
ЗМІ – засоби масової інформації
ІКС – інформаційно-комунікаційна система.
ІПНП – інформаційний портал Національної поліції України.
КК України – Кримінальний кодекс України.
КМЕ – комп'ютерна медіаекспертиза.
КПК України – Кримінальний процесуальний кодекс України.
КТЕ – комп'ютерно-технічна експертиза.
МВС України – Міністерство внутрішніх справ України
МПД – міжнародна правова допомога.
НПУ – Національна поліція України
НСВ – несанкціоноване спрямоване втручання.
НСРД – негласні слідчі (розшукові) дії
НЦБ Інтерполу – Національне центральне бюро Інтерполу.
ОГП – Офіс Генерального прокурора.
ОКІ – об'єкти критичної інфраструктури.
ОКІІ – об'єкт криміналістичного ідентифікаційного інтересу.
ОРЗ – оперативно-розшукові заходи.
ОС – операційна система.
ПЗ – програмне забезпечення.
ПКА – підрозділи кримінального аналізу.
СБУ – Служба безпеки України
СРД – слідчі (розшукові) дії
СУБД – система управління базами даних.
ТДРД – технічне дослідження розслідування доказів.
ТДРД – тимчасовий доступ до речей і документів.
ШПЗ – шкідливе програмне забезпечення.
APT – Advanced Persistent Threat (розвинена постійна загроза).
DNS – Domain Name System (система доменних імен).
IMEI – International Mobile Equipment Identity (міжнародний ідентифікатор мобільного обладнання).
OSINT – Open Source Intelligence (аналітика на основі відкритих джерел інформації).

ДОДАТКИ

Додаток 1
Клопотання про тимчасовий доступ
до речей і документів

ГОЛОВНЕ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ
В ДНІПРОПЕТРОВСЬКІЙ ОБЛАСТІ
СЛІДЧЕ УПРАВЛІННЯ
пр. Слобожанський, м. Дніпро, 49101, тел: 725-01-83, факс 725-01-82

Слідчому судді
Індустріального районного
суду м. Дніпропетровська

КЛОПОТАННЯ
про тимчасовий доступ до речей і документів

м. Дніпро «__» липня 20__ року

Слідчий відділу розслідування особливо важливих справ та злочинів, вчинених організованими групами та злочинними організаціями слідчого управління Головного управління Національної поліції в Дніпропетровській області старший лейтенант поліції Петров Юрій Юрійович, розглянувши матеріали досудового розслідування кримінального правопорушення, відомості про яке внесено до Єдиного реєстру досудових розслідувань №42000000000000293 від 05.01.20__ за ознаками кримінального правопорушення, передбаченого ч. 3 ст. 190, ч. 5 ст. 361 КК України, -

В С Т А Н О В И В:

У провадженні СУ ГУНП в Дніпропетровській області перебуває кримінальне провадження № 42000000000000___ від 05.01.20__ за ознаками кримінального правопорушення, передбаченого ч. 3 ст. 190, ч. 5 ст. 361 КК України.

Нагляд за додержанням законів під час проведення досудового розслідування у формі процесуального керівництва досудовим розслідуванням здійснюється групою прокурорів Дніпропетровської обласної прокуратури.

Відповідно до ст. 12 КК України склад злочину, передбаченого ч. 5 ст. 361 КК України, належить до особливо тяжкого злочину.

В ході досудового розслідування встановлено, що до Управління протидії кіберзлочинам в Дніпропетровській області Департаменту кіберполіції Національної поліції України звернувся із заявою гр. С, ____ року народження, мешкає _____, про те, що 13.02.20__ року невстановлені особи здійснили несанкціоновані входи до його веббанкінгів «Ощад24/7» та «Raiffeisen Online» та в подальшому шахрайським шляхом, з його банківських рахунків № _____, емітованого в АТ «Райфзен Банк Аваль», та _____, емітованого в АТ «Ощад Банк», викрали грошові кошти.

Встановлено, що до вказаного злочину причетні наступні особи, а саме гр. Д, К, Х, П, О та Д.

Так, останні вступили в злочину змову, розподіливши ролі, маючи єдність, спільність намірів та цілей на незаконне збагачення, створили стійку ієрархічну групу, яка має за ціль шахрайським шляхом заволодівати грошовими коштами громадян України.

Останні на початку 20__ року задля досягнення своїх цілей підготувались до вчинення тяжких злочинів проти власності громадян, а саме організували свій офіс, який розташували в одноповерховому будинку за адресою _____. В мережі Інтернет (Дарк-нет) здійснили закупівлю баз даних (клієнтські бази банківських установ, де є повна інформація про клієнтів банку), оформили за грошову винагороду банківські рахунки на осіб із низьким соціальним достатком, які вони повністю контролюють, вказані рахунки використовують для того щоб переводити на них викрадені грошові кошти та в подальшому безперешкодно їх переводити в готівку через мережу банкоматів на території міста. Закупили мобільні телефони та сім-картки мобільних операторів стільникового зв’язку та в подальшому почали вчиняти протиправні діяння.

Так, 13.02.20__ року, маючи розподілені ролі між собою, гр. Д, К, Х, П, О та Д здійснили з невідомого номеру телефонний дзвінок на номер мобільного телефону _____, який належить гр. С, _____ року народження.

Піднявши слухавку, С почав розмову з особою жіночої статі, яка представилася як працівник служби безпеки АТ «Райфазен Банк Аваль». Продовжуючи вести бесіду, один з фігурантів, який видавав себе за працівника служби безпеки банку, повідомив С, про те, що з його особистого банківського рахунку № _____, емітованого в АТ «Райфазен Банк Аваль», невідомі особи намагаються викрасти грошові

кошти та для запобігання цьому йому потрібно провести декілька онлайн-операцій та підтверджень.

С, маючи довіру до вказаної особи, так як вона надала повну інформацію про нього, такі як номер паспорта, реєстраційний номер облікової картки платника податків, кодове слово, яке використовується для підтвердження ідентифікації клієнта банківської установи, продовжив вести діалог із одним із фігурантів**.**

Так, вступивши в довіру до потерпілого, шахрайським шляхом під приводом перевірки мобільного телефону на вірусні програми та для попередження викрадення шляхом списання грошових коштів, належних потерпілому, вмовили С встановити мобільний додаток «AnyDesk» (вказана програма використовується для відділеного доступу та користування до персональних комп'ютерів та інших пристроїв, таких як мобільні телефони). Після встановлення вказаного мобільного додатку, будучи впевненим у законних діях невідомої особи, С надав доступ до вказаного додатку, тим самим дозволив віддалено користуватись своїм мобільним телефоном третім особам.

Заволодівши доступом до мобільного телефону, гр. Д, К, Х, П, О та Д, за раніше обговореним планом, продовжили вести бесіду з С під приводом захисту грошових коштів, які належать потерпілому та які знаходились на банківському рахунку № _____, емітованому в АТ «Райфазен Банк Аваль», вмовили С здійснити авторизацію в дистанційному банківському обслуговуванні, а саме «Raiffeisen Online», яке було встановлено на мобільному телефоні потерпілого для власного віддаленого користування банківським рахунком. Маючи доступ до вказаного мобільного телефону, через мобільний додаток «AnyDesk» вищевказані особи відразу ж отримали повний доступ до авторизованого Степаненком О. О. онлайн-банкінгу «Raiffeisen Online».

Продовжуючи розмову з С, маючи авторизований доступ до онлайн-банкінгу, використовуючи опції вказаного інтернет-сервісу, в тайні від потерпілого перевели грошові кошти, належні останньому, на підконтрольний банківський рахунок, тим самим незаконно ними заволоділи.

В подальшому, перебуваючи в діалозі по мобільному телефону з потерпілим, шахрайським шляхом, маючи повну довіру від потерпілого, діючи за попереднім обумовленим планом, вмовили С здійснити авторизацію в дистанційному банківському обслуговуванні «Ощад 24/7», де С мав відкритий банківський рахунок № _____. Так, ідентичним способом, як і минулий, використовуючи опції вказаного «Інтернет сервісу», в тайні від потерпілого перевели грошові кошти, належні останньому, на підконтрольну банківську карту № _____, тим самим незаконно заволоділи грошовими коштами потерпілого у сумі 47 780 гривень.

Заволодівши вказаними грошовими коштами, маючи вільний доступ до банківського рахунку № _____, в подальшому перевели частину викрадених коштів на банківський рахунок № _____, емітований в ПАТ

«Восток» та відкритий на ім’я К _____ року народження, після чого перевили його в готівку та території міста Р.

Так, у ході досудового розслідування було встановлено, що шахраї використовують для обготівкування банківські рахунки, а саме:

_____ – «Конкорд Банк»,
_____ – «Акцент банк»,
_____ – «Акцент банк»,
_____ – «ПУМБ»,
_____ – «Банк Восток»,
_____ – «УкраГаз банк».

Вищевказана інформація підтверджується проведеними в ході розслідування слідчими (розшуковими) та процесуальними діями, а саме: допитом потерпілого, інформуванням, протоколами пред’явлення особи для впізнання за фотознімками, допитом свідка, стенограмою розмови потерпілого с представниками злочинного угруповання тощо.

Враховуючи те, що в матеріалах досудового розслідування знаходяться достатні дані про те, що гр. Д, К, Х, П, О та Д вчиняють особливо тяжке кримінальне правопорушення, з метою отримання додаткових доказів його вчинення вказаними особами виникла необхідність у проведенні слідчих (розшукових) дій.

Під час досудового розслідування виникла необхідність в отриманні інформації, яка містить банківську таємницю, а саме інформації щодо розрахункових рахунків, із метою встановлення всіх обставин кримінального правопорушення та подальшого проведення судової економічної експертизи.

Відповідно до ст. 159 КПК України тимчасовий доступ до речей і документів полягає у наданні стороні кримінального провадження особою, у володінні якої знаходяться такі речі і документи, можливості ознайомитися з ними, зробити їх копії та вилучити їх (здійснити їх виїмку). Тимчасовий доступ до речей і документів здійснюється на підставі ухвали слідчого судді, суду.

Статтею 160 КПК України передбачено, що сторони кримінального провадження мають право звернутися до слідчого судді під час досудового розслідування чи суду під час судового провадження із клопотанням про тимчасовий доступ до речей і документів.

Частиною 5 ст. 163 КПК України слідчий суддя, суд постановляє ухвалу про надання тимчасового доступу до речей і документів, якщо сторона кримінального провадження у своєму клопотанні доведе наявність достатніх підстав вважати, що ці речі або документи: 1) перебувають або можуть перебувати у володінні відповідної фізичної або юридичної особи; 2) самі собою або в сукупності з іншими речами і документами кримінального провадження, у зв’язку з яким подається клопотання, мають суттєве значення для встановлення важливих обставин у кримінальному провадженні; 3) не становлять собою або не включають речей і документів, які містять охоронювану законом таємницю.

Згідно зі ст. 165 КПК України особа, яка зазначена в ухвалі слідчого судді, суду про тимчасовий доступ до речей і документів як володілець речей або документів, зобов'язана надати тимчасовий доступ до зазначених в ухвалі речей і документів особі, зазначеній у відповідній ухвалі слідчого судді, суду. Зазначена в ухвалі слідчого судді, суду особа зобов'язана пред'явити особі, яка зазначена в ухвалі як володілець речей і документів, оригінал ухвали про тимчасовий доступ до речей і документів та вручити її копію. Особа, яка пред'являє ухвалу про тимчасовий доступ до речей і оригіналів або копій документів, зобов'язана залишити володільцю речей і оригіналів або копій документів опис речей і оригіналів або копій документів, які були вилучені на виконання ухвали слідчого судді, суду.

На вимогу володільця особою, яка пред'являє ухвалу про тимчасовий доступ до речей і документів, має бути залишено копію вилучених оригіналів документів. Копії документів, які вилучаються або оригінали яких вилучаються, виготовляються з використанням копіювальної техніки, електронних засобів володільця.

Зважаючи на викладене, з метою встановлення відомостей про обставини кримінального правопорушення, які можуть бути використанні як речові докази, а також мають суттєве значення для встановлення істини у справі, виникла необхідність в отриманні інформації, яка містить банківську таємницю, а саме інформації щодо розрахункових рахунків:

– особистого банківського рахунку № _____, емітованого в АТ «Райфазен Банк», який належить потерпілому – С, _____ року народження;

– особистого банківського рахунку № ___, емітованого в АТ «Ощад Банк», який належить потерпілому – С, _____ року народження;

– _____ – «Конкорд Банк»;

– _____ – «Акцент банк»;

– _____ – «Акцент банк»;

– _____ – «ПУМБ»;

– _____ – «Банк Восток»;

– _____ – «УкраГаз банк»

, з метою встановлення всіх обставин кримінального правопорушення та подальшого проведення судової економічної експертизи.

Інформація, що знаходиться у вказаних документах, має суттєве значення для подальшого розслідування даного кримінального правопорушення, у тому числі для встановлення кола осіб, причетних до скоєння злочину.

Згідно з п. 2 ст. 62 Закону України «Про банки та банківську діяльність» інформація щодо юридичних та фізичних осіб, яка містить банківську таємницю, зокрема стосовно операцій за рахунками конкретної юридичної особи або фізичної особи – суб'єкта підприємницької діяльності за конкретний проміжок часу, розкривається банками за рішенням суду. Крім цього, відповідно до ст. 91 КПК України сама подія кримінального правопорушення підлягає доказуванню, яке полягає у збиранні, перевірці та оцінці доказів з метою встановлення обставин, що

мають значення для кримінального провадження. Беручи до уваги вищевикладене та враховуючи, що у матеріалах кримінального провадження вбачається наявність достатніх підстав вважати, що вказані документи мають суттєве значення для встановлення важливих обставин у кримінальному провадженні, а також керуючись ст. ст. 36, 131, 132, 159-166 КПК України,-

ПРОШУ СУД:

1. Надати тимчасовий доступ до інформації та оригіналів документів з можливістю вилучення (виїмки) їх копій, в тому числі на лазерних дисках для оптичних систем зчитування, слідчому відділу розслідування особливо важливих справ та злочинів, учинених організованими групами і злочинними організаціями СУ ГУНП в Дніпропетровській області старшому лейтенанту поліції Петрову Юрію Юрійовичу, що перебувають у володінні АТ «Райфазен Банк» (код ЄДРПОУ_____), юридична адреса:_____, а саме:

1. Довідок-інформації про рух грошових коштів по платіжним пластиковим карткам з зазначенням анкетних даних про особу, на яку оформлено картковий рахунок, повних даних про контрагентів і призначення платежів за період з 01.01.20__ року до теперішнього часу: **№_____**;
2. Документів на відкриття зазначених карткових рахунків;
3. Даних систем відеоспостереження і фотофіксації зняття грошових коштів із банківських терміналів при оформленні та одержанні грошових коштів за рахунками за період з 01.01.20__ року до теперішнього часу: **№_____**;
4. IP-адрес підключення до інтернет-банкінгу за зазначеними платіжними картками, з інформацією про MAC-адреси комп'ютерів, з яких відбувалося з'єднання з системою, із зазначенням дати та часу за київським часом у форматі: день, місяць, рік, години, хвилини, секунди таких з'єднань за відповідні періоди;
5. Інформації, отриманої банком під час обслуговування зазначених платіжних карток, а саме: номери телефонів, адреси проживання, місце роботи, рід занять, родинні зв'язки, особи, які надають поруку, довірені (довірителі) особи;
6. Надати інформацію стосовно наявних відкритих в АТ «Райфазен Банк» додаткових банківських рахунків у осіб, власників наступних карток: **№_____**, з наданням довідок-інформації про рух грошових коштів за період з 01.01.2022 до теперішнього часу; даних систем відеоспостереження і фотофіксації зняття грошових коштів з банківських терміналів при оформленні та одержанні грошових коштів за наявними у вказаної особи рахунками з 01.01.20__ до теперішнього часу;
7. Інформації про всі відкриті рахунки у АТ «Райфазен Банк» фізичною

особою **С, _____ р.н.**;

8. Довідок-інформації про рух грошових коштів по всім відкритим рахункам **С, _____ р.н.**, з зазначенням анкетних даних про особу, на яку оформлено картковий рахунок, повних даних про контрагентів і призначення платежів за період з 01.01.20__ року до теперішнього часу;
9. Даних систем відеоспостереження і фотофіксації зняття грошових коштів з банківських терміналів при оформленні та одержанні грошових коштів по всім відкритим рахункам **С, _____ р.н.** за період з 01.01.20__ року до теперішнього часу;
10. IP-адрес підключення до інтернет-банкінгу за всіма відкритими рахунками **С, _____ р.н.**, з інформацією про MAC-адреси комп'ютерів, з яких відбувалося з'єднання з системою, з зазначенням дати та часу за київським часом у форматі: день, місяць, рік, години, хвилини, секунди таких з'єднань за відповідні періоди.

2. З метою недопущення знищення або спотворення вказаної інформації та документів, які мають суттєве значення для кримінального провадження, керуючись ч. 2 ст. 163 КПК України, розглянути дане клопотання без виклику представників АТ «Райфазен Банк».

Додаток:

1) витяг з кримінального провадження №42000000000000___ від 05.01.20__;
2) копії матеріалів кримінального провадження.

Слідчий
відділу РОВС та ЗУ ОГ і ЗО
СУ ГУНП в Дніпропетровській області
старший лейтенант поліції **Юрій ПЕТРОВ**

«ПОГОДЖЕНО»
Прокурор відділу
обласної прокуратури **Сергій ІВАНОВ**

Додаток 2
Постанова про призначення
комп'ютерно-технічної експертизи

ГОЛОВНЕ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ
в Дніпропетровській області
слідче управління

49083, Дніпропетровська область, м. Дніпро, проспект Слобожанський, 40, тел. (056) 376-05-42

ПОСТАНОВА
про призначення комп'ютерно-технічної експертизи

Слідчий відділу розслідування особливо важливих справ та злочинів, вчинених організованими групами та злочинними організаціями слідчого управління Головного управління Національної поліції в Дніпропетровській області старший лейтенант поліції Петров Юрій Юрійович, розглянувши матеріали кримінального провадження, внесеного до Єдиного реєстру досудових розслідувань за №42000000000000___ від 05.01.20__ року, за ознаками кримінального правопорушення, передбаченого ч. 3, 4 ст. 190, ч. 2, 5 ст. 361 КК України, -

ВСТАНОВИВ:

Слідчим управлінням Головного управління Національної поліції в Дніпропетровській області проводиться досудове розслідування у кримінальному провадженні за №42000000000000___ від 05.01.20__ року, за ознаками кримінального правопорушення, передбаченого ч. 3, 4 ст. 190, ч. 2, 5 ст. 361 КК України.

Нагляд за додержанням законів під час проведення досудового розслідування у формі процесуального керівництва досудовим розслідуванням здійснюється групою прокурорів Дніпропетровської обласної прокуратури.

Досудовим розслідуванням встановлено, що група осіб у складі: гр. Д, К, Х, П, О та Д, яка діє на території міста Кривий Ріг, здійснює несанкціоновані входи до веббанкінгів банківських установ потерпілих та в подальшому шахрайським шляхом з їхніх банківських рахунків викрадає грошові кошти.

Так, гр. Д, К, Х, П, О, Д та У, діючи умисно, з корисливих мотивів, за попередньою змовою групою осіб, шляхом незаконних операцій з використанням електронно-обчислювальної техніки:

– 13.02.20__ у період часу з 19:40 год. до 20:40 год. шляхом обману заволоділи грошовими коштами С на загальну суму 47 980 гривень, чим спричинили останньому майнову шкоду;

– 11.08.20__ у період часу з 14:57 год. до 15:50 год. шляхом обману заволоділи грошовими коштами О на загальну суму 67 180 гривень, чим спричинили останній майнову шкоду;

– 30.01.20__ у період часу з 19:20 год. до 15:50 год. шляхом обману заволоділи грошовими коштами К на загальну суму 3 237 гривень, чим спричинили останній майнову шкоду.

Отже, враховуючи вищевикладене, гр. Д, К, Х, П, О, Д та У підозрюються у заволодінні чужим майном шляхом обману (шахрайстві), вчиненому повторно, за попередньою змовою групою осіб шляхом незаконних операцій з використанням електронно-обчислювальної техніки, тобто у тяжкому злочині, за яке передбачено покарання у виді позбавлення волі строком до 8 років.

Під час досудового розслідування за вказаним кримінальним провадженням, враховуючи об’єктивні обставини вчиненого кримінального правопорушення, проведено слідчі дії, направлені на встановлення осіб, причетних до вказаного кримінального правопорушення. Під час проведення таких заходів працівниками Управління протидії кіберзлочинам в Дніпропетровській області ДКП НПУ, в ході виконання доручення ст. 40 КПК України, були встановлені відповідні особи.

01.03.20__ органом досудового розслідування отримано ухвали слідчого судді Індустріального районного суду м. Дніпропетровська щодо надання дозволу на проведення обшуків в квартирах, домоволодіннях та автотранспорті, інших приміщеннях фігурантів на території м. Кривий Ріг Дніпропетровської області.

Так, 12.03.20__ слідчими слідчого управління ГУНП в Дніпропетровській області за оперативним супроводженням Управління протидії кіберзлочинам в Дніпропетровській області ДКП НПУ проведено санкціоновані Індустріальним районним судом м. Дніпропетровська обшуки.

За результатами яких вилучені речові докази, які мають важливе значення у кримінальному провадженні, зокрема за адресою: Дніпропетровська область, м. Кривий Ріг, вул. _____ буд. ___, за місцем мешкання Д, К та У, виявлено та вилучено: персональний комп’ютер білого кольору, без назви та марки.

Враховуючи вищевикладене, а також те, що у даному кримінальному провадженні виникла необхідність у проведенні комп’ютерно-технічної експертизи, для якої потрібні спеціальні знання, керуючись статтями 2, 36, 91, 93, 110, 242, 243 КПК України, -

ПОСТАНОВИВ:

1. Призначити у кримінальному провадженні №42000000000000___ від 05.01.20__ року, комп'ютерно-технічну експертизу, до проведення якої залучити експертів Дніпропетровського НДЕКЦ МВС України.

2. На вирішення експерта поставити наступні запитання:

2.1. Чи міститься на персональному комп'ютері білого кольору, без назви та марки програмне забезпечення для віддаленого керування «AnyDesk»? Якщо так, то прошу зазначити метадані виконуючого файлу та надати в електронному вигляді файли статистики використання цього програмного забезпечення (log файли);

2.2. Чи міститься на наданих на дослідження предметах файли графічних та текстових форматів, в тому числі файли із розширенням «.pdf»? Якщо так, то прошу надати файли та їх список в електронному вигляді;

2.3. Чи міститься на наданих на дослідження предметах будь-яка інформація про ідентифікатори номерів мобільних операторів у вигляді: «_____» – та інформація про номери банківських карт у вигляді: «_____»? Якщо так, то прошу надати інформацію в електронному вигляді.

3. Для дослідження експерту направити один опечатаний сейф-пакет Національної поліції України **№**_____, який містить у собі персональний комп'ютер білого кольору, без назви та марки, вилучений 12.03.20__ в ході проведеного обшуку за адресою: Дніпропетровська область, м. Кривий Ріг, вул. Г, буд. 10, за місцем мешкання Д., К, та У.

4. Відповідно до ст. 5 Закону України «Про судову експертизу» дозволити часткове або повне пошкодження об'єктів дослідження у тій мірі, в якій це необхідно для експертного дослідження.

5. За необхідності надати експертам для ознайомлення матеріали кримінального провадження.

6. Копію даної постанови направити директору Дніпропетровського НДЕКЦ МВС України.

Слідчий
відділу РОВС та ЗУ ОГ і ЗО
СУ ГУНП в Дніпропетровській області
старший лейтенант поліції **Юрій ПЕТРОВ**

Додаток 3
Постанова про призначення
комп'ютерно-технічної експертизи

ГОЛОВНЕ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ
В ХАРКІВСЬКІЙ ОБЛАСТІ
СЛІДЧЕ УПРАВЛІННЯ
вул. Весніна, м. Харків, 61023, тел. (057)705-9077, факс (057)700-0271

ПОСТАНОВА
про призначення судової комп'ютерно-технічної експертизи

м. Харків 22 квітня 20__ року

Слідчий СУ ГУНП в Харківській області капітан поліції Ткачов Владислав Юрійович, розглянувши матеріали кримінального провадження, внесеного до Єдиного реєстру досудових розслідувань за № 12000000000000000 від 20.01.20__ за ч. 5 ст. 361, ч. 3 ст. 28 ч. 5 ст. 361 КК України,

ВСТАНОВИВ:

Слідчим управлінням Головного управління Національної поліції в Харківській області (далі – СУ) проводиться досудове розслідування у кримінальному провадженні № 12000000000000000 від 20.01.20__ за ознаками вчинення кримінальних правопорушень, передбачених ч. 5 ст. 361, ч. 3 ст. 28 ч. 5 ст. 361 КК України.

14.03.20__ на підставі ухвали Київського районного суду м. Харкова проведено обшук за місцем мешкання Іваненка Петра Івановича, за адресою: м. Київ, вул. І., буд. 1, кв. 1, у ході якого, зокрема, вилучено: системний блок комп'ютера «Vinga».

Враховуючи, що для з'ясування питань, необхідність у вирішенні яких виникла під час досудового розслідування, керуючись ст. ст. 69, 110, 242, 243 КПК України, –

ПОСТАНОВИВ:

1. Призначити у кримінальному провадженні № 12000000000000000 від 20.01.20__ за ознаками вчинення кримінальних правопорушень, передбачених ч. 5 ст. 361, ч. 3 ст. 28 ч. 5 ст. 361 КК України, судову комп'ютерно-технічну

експертизу, проведення якої доручити судовим експертам Національного наукового центру «Інститут судових експертиз» ім. Засл. проф. М. С. Бокаріуса (далі – ННЦ «ІСС» ім. Засл. проф. М. С. Бокаріуса).

2. На вирішення експерта поставити питання:

– Чи міститься на наданому на дослідження системному блоці комп'ютера «Vinga», зокрема в файлах, які містяться у папці «Этот компьютер» та прокладаємо маршрут до остаточної папки: «Новий том (D:)»/»[7.9.11.56] Private Keeper», – програмні забезпечення Checker, PrivateKeeper? У разі наявності даного програмного забезпечення чи можна його ідентифікувати як шкідливе? Якщо так, то якого воно типу та яку функцію виконує?

– Чи наявні на наданому на дослідження системному блоці комп'ютера «Vinga» текстові документи із авторизаційними даними до електронних сервісів (електронні поштові скриньки, соціальні мережі, електронні платіжні системи тощо) та паролі до них? Якщо так, то чи могли вони бути застосовані як інструмент до шкідливого програмного забезпечення? Також, у разі наявності таких файлів, чи можливо за їх допомогою здійснити авторизацію до електронних сервісів із техніки, яка була надана на дослідження, та в який спосіб?

– Чи наявні на наданому на дослідження системному блоці комп'ютера «Vinga» додатки для приватного листування або передачі файлів? Якщо так, то які ідентифікатори вони мають? У разі наявності таких додатків чи наявні спільноти в таких додатках (приватні повідомлення, групи), в яких є пересилка текстових файлів, програмних застосунків між учасниками, обговорення теми збуту, або застосування шкідливого програмного забезпечення зазначеного вище? У разі наявності фактів надсилання таких файлів іншим користувачам чи можуть ці файли бути ідентифіковані як шкідливі?

3. Для проведення технічної експертизи документів експертам ННЦ «ІСС» ім. Засл. проф. М.С. Бокаріуса направити:

системний блок комп'ютера «Vinga», який поміщено до полімерного пакета та скріплено биркою з пояснювальним написом, та, в разі необхідності, матеріали кримінального провадження № 12000000000000000 від 20.01.20__.

4. Копію даної постанови направити для виконання експертам ННЦ «ІСС» ім. Засл. проф. М.С. Бокаріуса за адресою: м. Харків, вул. Залютинська, 4.

5. Попередити судових експертів ННЦ «ІСС» ім. Засл. проф. М.С. Бокаріуса про кримінальну відповідальність, передбачену ст. ст. 384, 385, 387 КК України, за надання завідомо неправдивого висновку, відмову без поважних причини від виконання покладених обов'язків у суді, невиконання інших обов'язків або розголошення даних досудового розслідування.

6. Дозволити експерту в разі необхідності повне або часткове знищення об'єкта дослідження згідно з методикою дослідження.

Слідчий СУ
ГУНП в Харківській області
капітан поліції **Владислав ТКАЧОВ**

Додаток 4
Постанова про призначення
комп'ютерно-технічної експертизи

ГОЛОВНЕ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ
В ХАРКІВСЬКІЙ ОБЛАСТІ
СЛІДЧЕ УПРАВЛІННЯ
вул. Весніна, м. Харків, 61023, тел. (057)705-9077, факс (057)700-0271

ПОСТАНОВА
про призначення судової комп'ютерно-технічної експертизи

м. Харків 10 листопада 20__року

Слідчий відділу розслідування особливо важливих справ та злочинів, учинених організованими групами, злочинними організаціями СУ ГУНП в Харківській області капітан поліції Ткачов Владислав Юрійович, розглянувши матеріали кримінального провадження, внесеного до Єдиного реєстру досудових розслідувань за № _____ від 28.08.20__ за ознаками складу кримінального правопорушення, передбаченого ч. 3 ст. 28, ч. 2 ст. 361 КК України,

ВСТАНОВИВ:

Досудовим розслідуванням встановлено, що організована злочинна група, до складу якої входять _____, займалася втручанням в роботу електронно-обчислювальних систем з метою отримання доступів до особистих даних сторонніх осіб,

08.10.20__ проведено обшуки за місцем мешкання _____, під час яких вилучено комп'ютерну техніку.

Враховуючи, що для з'ясування питань, необхідність у вирішенні яких виникла під час досудового розслідування, керуючись ст. ст. 69, 110, 242, 243 КПК України, –

ПОСТАНОВИВ:

1. Призначити у кримінальному провадженні, внесеному до єдиного реєстру досудових розслідувань 28.08.20__ за номером 12019220490000000 за ознаками кримінальних правопорушень, передбачених ч. 3 ст. 28 ч. 2 ст. 361 КК України, судову комп'ютерно-технічну експертизу, проведення якої доручити експертам Харківського НДІСЕ ім. засл. проф. М. С. Бокаріуса.

2. На вирішення експерта поставити питання:

1) _____ браузерів, інстальованих в операційній системі, наданих на дослідження пристроїв, а також вказати, чи наявні авторизації на вебресурси https://bhf.io, https://exploit.in, https://wwh-club.cc, https://www.blockchain.com, https://qiwi.com , https://webmoney.ru;

2) чи збережена в інтернет-браузерах інформація щодо реквізитів авторизації – логінів та паролів, що застосовувалися для доступу до сайтів? якщо так, то надати їх;

3) чи встановлені розширення VPN-сервісів, PROXY сервісів, що призначені для уникнення обмеження доступу до Web-ресурсів або приховання своєї IP-адреси у наявній на дослідження техніці?

4) чи міститься на наданій на дослідження техніці програмне забезпечення All-one-checker, Mailbrut checker, Mail List Validator 2.0, twitter_checker, emailtools software?

5) у разі наявності даного програмного забезпечення чи можна його ідентифікувати як шкідливе? Якщо так, то якого воно типу та яку функцію виконує?

6) чи наявні на техніці, наданій на дослідження, текстові документи із авторизаційними даними до електронних сервісів (електронні поштові скриньки, соціальні мережі, електронні платіжні системи тощо) та паролі до них? Якщо так, то чи могли вони бути застосовані як інструмент до шкідливого програмного забезпечення? Також, в разі наявності таких файлів, чи можна допустити, що за їх допомогою було здійснено авторизацію до електронних сервісів з техніки, яка була надана на дослідження, та в який спосіб?

7) чи наявні на наданій на дослідження техніці месенджери, додатки для приватного листування або передачі файлів. Якщо так, до які ідентифікатори мають? В разі наявності таких додатків чи наявні спільноти в таких додатках (приватні повідомлення, групи), в яких є пересилка текстових файлів між учасниками, обговорення теми збуту, або застосування шкідливого програмного забезпечення, зазначеного вище?

3. Дозволяю часткову або повну зміну досліджуваного об'єкта.

4. Для дослідження експертам надати полімерний пакет, опечатаний биркою з відбитком печатки УПК в Харківській області ДКП НПУ, в якому знаходиться мобільний телефон _____ з зарядним пристроєм, вилучені під час проведення обшуку за місцем мешкання _____ за адресою: м. Харків, вул. К., 111, полімерний пакет

опечатаний биркою з відбитком печатки УПК в Харківській області ДКП НПУ, в якому знаходиться ноутбук «Packorbell» model _____ з зарядним пристроєм, вилучені під час проведення обшуку офісу за адресою: м. Харків, вул. С., 1, оф. 101.

5. Після проведення дослідження висновок експерта та об'єкт дослідження видати слідчому СУ ГУНП в Харківській області Дерію О. М. або за довіреністю іншій уповноваженій особі.

6. Для ознайомлення експерта надати матеріали кримінального провадження (у разі необхідності, на вимогу експерта).

Старший слідчий СУ ГУНП
в Харківській області
капітан поліції **Владислав ТКАЧОВ**

Додаток 5
Супровідний лист

ГОЛОВНЕ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ В ДНІПРОПЕТРОВСЬКІЙ ОБЛАСТІ
Слідче управління
пр. Слобожанський, 40, м. Дніпро, 49101,тел.
факс (056) 376-04-05, 376-04-39
_____ №
_____ _____

Директору
Дніпровського
НДЕКЦ МВС України

Направляю Вам для організації виконання постанову слідчого про призначення експертизи у кримінальному провадженні №42000000000000000 від 05.01.20__ року за ознаками кримінального правопорушення, передбаченого ч. 3, 4 ст. 190, ч. 2, 5 ст. 361 КК України.

Додаток:

- постанова про призначення комп'ютерно-технічної експертизи на 3 арк.;
- копія протоколу обшуку від 12.03.20__ року, за адресою: Дніпропетровська область, м. Кривий Ріг, вул. Г., буд. 1, за місцем мешкання Д., К, та У на ____ арк.;
- один опечатаний сейф-пакет Національної поліції України **№_____**, який містить у собі персональний комп'ютер білого кольору, без назви та марки.

Слідчий
відділу РОВС та ЗУ ОГ і ЗО
СУ ГУНП в Дніпропетровській області
старший лейтенант поліції **Юрій ПЕТРОВ**

контактний номер моб. тел.

Додаток 6
Клопотання про дозвіл на проведення
негласної слідчої (розшукової) дії

Прим.___

Слідчому судді Харківського
Апеляційного суду

КЛОПОТАННЯ
про дозвіл на проведення негласної слідчої (розшукової) дії – зняття інформації з транспортної телекомунікаційної мережі

м. Харків ___.___.20__

Слідчий СУ ГУНП в Харківській області капітан поліції Петренко С. М., розглянувши матеріали досудового розслідування, внесеного до Єдиного реєстру досудових розслідувань за № 1201900000000000 від 28.08.20__ за ознаками складу кримінального правопорушення, передбаченого ч. 2 ст. 361 КК України,-

ВСТАНОВИВ:

Відділом розслідування особливо важливих справ та злочинів, учинених організованими групами, злочинними організаціями СУ ГУНП в Харківській області здійснюється досудове розслідування у кримінальному провадженні, відомості у якому внесені до Єдиного реєстру досудових розслідувань 28.08.20__ за номером № 1201900000000000, за ознаками кримінального правопорушення, передбаченого ч. 2 ст. 361 КК України.

Протягом тривалого часу з 20__ року група невстановлених осіб з використанням електронно-обчислювальної техніки, шляхом застосування шкідливого програмного забезпечення втручалась в роботу електронних систем та мереж громадян України, що призвело до витоку конфіденційної інформації.

Таким чином, в діях вказаних осіб вбачаються ознаки кримінального правопорушення, передбаченого ч. 2 ст. 361 КК України – несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж, що призвело до витоку інформації.

Згідно з матеріалами УПК в області ДКП НПУ, за результатами проведення комплексу оперативно-розшукових заходів, спрямованих на встановлення осіб, які вчинили вказане кримінальне правопорушення, встановлено особу: _____, який причетний до вчинення зазначеного кримінального правопорушення та який брав безпосередню участь у його вчиненні.

Під час досудового розслідування було встановлено, що _____ користується мобільними пристроями та комп'ютерною технікою, що підключені до телекомунікаційних мереж провайдера _____ IP адреса

_____ MAC адреса _____,
в пам'яті яких в електронному вигляді зберігаються відомості про обставини скоєння злочину та осіб, причетних до його скоєння, які можуть бути використані як докази у зазначеному кримінальному провадженні.

З метою документування участі в скоєнні злочинної діяльності гр. _____, встановлення її злочинних зв'язків, місцезнаходження речових доказів, отримання інформації, яка має важливість для органів Національної поліції України, були проведені оперативні заходи.

Враховуючи те, що відомості про злочин та осіб, які його вчиняють, неможливо отримати в інший спосіб, для подальшого документування злочинної діяльності гр._____ необхідно провести негласну слідчу (розшукову) дію – зняття інформації з транспортної телекомунікаційної мережі з IP-адреси _____ інтернет-провайдера _____, якою постійно користується _____

Ураховуючи викладене, з метою пошуку, фіксації відомостей про гр._____, встановлення його злочинних зв'язків, місцезнаходження речових доказів, отримання інформації, яка має важливість для органів національної поліції, встановлення інших осіб, причетних до скоєння тяжкого злочину, та для встановлення інших обставин, у зв'язку з тим, що вказані відомості неможливо отримати в інший спосіб, крім як зняття інформації з транспортної телекомунікаційної мережі, керуючись вимогами статей 246, 248, 249, 263 КПК України,-

ПРОШУ:

Надати дозвіл на проведення негласної слідчої (розшукової) дії, а саме зняття інформації з транспортної телекомунікаційної мережі з IP-адреси _____ інтернет-провайдера _____, якою постійно користується _____, із застосуванням відповідних технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, спостереження, відбору та фіксації змісту інформації та сигналів (SMS, MMS, факсимільний зв'язок, модемний зв'язок тощо), які передаються каналом зв'язку, що контролюється, на строк два місяці.

Додаток: Витяг з Єдиного реєстру досудових розслідувань за № 1201900000000000 від 28.08.2024 року.

Слідчий СУ ГУНП
в Харківській області
капітан поліції **Сергій ПЕТРЕНКО**

ПОГОДЖЕНО
Прокурор відділу прокуратури
Харківської області _____
___.____. 20__

Наукове видання

Колектив авторів
За загальною редакцією
першого заступника Голови Національної поліції України,
начальника Головного слідчого управління,
генерала поліції 3-го рангу
М. С. Цуцкірідзе

РОЗСЛІДУВАННЯ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ ІНФОРМАЦІЙНИХ (АВТОМАТИЗОВАНИХ), ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ, ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖ
(ст. 361 КК України)

Науково-методичні рекомендації
для підрозділів слідства та дізнання Національної поліції України

Редактор, оригінал-макет, дизайн – *А. В. Самотуга*
Редактор *О. Ю. Чижевська*

Підп. до друку 15.12.2025. Формат 60х84/16. Друк – цифровий.
Гарнітура – Times New Roman. Ум.-друк. арк. 6,05. Обл.-вид. арк. 6,50. Зам. № 04/25/мр

Надруковано у Дніпровському державному університеті внутрішніх справ
49005, м. Дніпро, просп. Науки, 26, sed@dduvs.edu.ua
Свідоцтво про внесення до державного реєстру ДК № 8112 від 13.06.2024