Всеукраїнська науково-практична конференція

Актуальні питання проведення науково-технічних та судових експертиз щодо виявлення і дослідження сучасних способів і засобів вчинення кримінальних правопорушень в умовах війни

5 грудня 2025 року

Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України

Національний науковий центр «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України

Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України Міністерства оборони України

Київський науково-дослідний інститут судових експертиз Міністерства юстиції України

Всеукраїнська науково-практична конференція

Актуальні питання проведення науково-технічних та судових експертиз щодо виявлення і дослідження сучасних способів і засобів вчинення кримінальних правопорушень в умовах війни

5 грудня 2025 року

Мета конференції

Обмін науковими і практичними результатами у сфері науково-технічних та судових експертиз, пов’язаних із виявленням і дослідженням сучасних способів і засобів вчинення кримінальних правопорушень в умовах війни.

Обговорення тенденцій щодо розробки і впровадження нових підходів, методів дослідження наслідків вчинення кримінальних правопорушень, що вчиняються в умовах війни, а також викликів, що виникають під час проведення таких експертиз, розробка рекомендацій для підвищення їх ефективності та достовірності в умовах воєнного стану.

Об’єднання зусиль науковців, судових експертів та представників правоохоронних і оборонних структур задля удосконалення методології розслідування кримінальних правопорушень в умовах війни.

Встановлення творчих контактів, розвиток міжвідомчої співпраці та розширення наукових і професійних зв’язків у науково-технічній та судово-експертній галузі.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Почесні голови оргкомітету

Потій Олександр Володимирович	д-р техн. наук, професор, Голова Державної служби спеціального зв'язку та захисту інформації України
Трофименко Володимир Михайлович	д-р юрид. наук, професор, заступник Голови Державної служби спеціального зв'язку та захисту інформації України

Голова організаційного комітету

Павліков Володимир Володимирович	д-р техн. наук, професор, начальник Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України

Співголови організаційного комітету

Чепков Ігор Борисович	д-р техн. наук, професор, начальник Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України
Купріянова Анастасія Олександрівна	канд. юрид. наук, в.о. директора Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М.С. Бокаріуса» Міністерства юстиції України
Кисельов Максим Євгенович	доктор філософії в галузі права, директор Київського науково-дослідного інституту судових експертиз Міністерства юстиції України

Заступники голови

Чабанець Тетяна Миколаївна	заступник директора-завідувач Київського відділення Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М.С. Бокаріуса» Міністерства юстиції України
Васьківський Михайло Іванович	д-р техн. наук, полковник Збройних сил України, заступник начальника Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України

Жила Семен Сергійович	д-р. техн. наук, доцент, перший заступник начальника Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України
Агапова Олена Валеріївна	д-р юрид. наук, заступник директора з наукової роботи Київського науково-дослідного інституту судових експертиз Міністерства юстиції України

Члени оргкомітету

Сімакова-Єфремян Елла Борисівна	д-р юрид. наук, професор, заступник директора з наукової роботи Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М.С. Бокаріуса» Міністерства юстиції України
Алєксєйчук Вікторія Іванівна	канд. юрид. наук, доцент, заступник завідувача відділення з науково-методичної роботи та післядипломної освіти Київського відділення Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М.С. Бокаріуса» Міністерства юстиції України
Демидова Євгенія Євгеніївна	канд. юрид. наук, доцент, старший науковий співробітник відділу науково-методичної роботи та післядипломної освіти Київського відділення Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М.С. Бокаріуса» Міністерства юстиції України
Ткаченко Юрій Володимирович	канд. економ. наук, доцент, завідувач відділу науково-методичної роботи та післядипломної освіти Київського відділення Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М.С. Бокаріуса» Міністерства юстиції України
Тимко Євген Валентинович	завідувач лабораторії досліджень цифрових доказів Київського науково-дослідного інституту судових експертиз Міністерства юстиції України
Мунчак Володимир Миколайович	завідувач відділу вибухотехнічних досліджень та досліджень ракетної, артилерійської зброї лабораторії військових

	досліджень Київського науково-дослідного інституту судових експертиз Міністерства юстиції України
Панасюк Євген Володимирович	Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України
Бондаренко Дмитро Михайлович	Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України
Лисенко Сергій Станіславович	Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України
Кальченко Юрій Олександрович	Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України
Сущенко Віталій Анатолійович	Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України
Комаров Максим Юрійович	Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України
Дирда Олександр Вікторович	Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України
Іщук Максим Володимирович	Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України

ЗМІСТ

УДК 621.3.083

ОСНОВНІ ПІДХОДИ ДО РОЗРОБЛЕННЯ МЕТОДИКИ ВИЯВЛЕННЯ НЕДОКУМЕНТОВАНОГО ВТРУЧАННЯ У РОБОТУ ПРИСТРОЇВ IoT

Дмитро БОНДАРЕНКО[1], e-mail: d.bondarenko@cip.gov.ua, ORCID: 0009-0007-7355-4433
Олександр ЛИПСЬКИЙ[1], e-mail: o.lypskyi@cip.gov.ua, ORCID: 0009-0007-7355-4433
Ярослав СТЕФАНИШИН[1], e-mail: yaroslavstf513@gmail.com, ORCID: 0000–0002–8317–4131

[1]Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України

Вступ. Бурхливий розвиток технологій Internet of Things (IoT) призводить до широкого впровадження «розумних» пристроїв у побуті, промисловості та критичній інфраструктурі. Однак розширення функціональності та взаємне підключення величезної кількості електронних пристроїв створює нові виклики у сфері кібербезпеки. Наразі, однією із найбільш актуальних проблем є недокументоване (без відома розробника чи користувача) втручання в IoT-пристрої шляхом модифікації програмного чи апаратного забезпечення. Це втручання може включати надання програмному забезпеченню прихованих шкідливих функцій, зокрема, зміну прошивки з метою примушення IoT-пристрою до неанонсованих вразливостей. У багатьох випадках несанкціоноване втручання в IoT-пристрій має наслідком серйозні кримінальні правопорушення, які потребують (для запобігання і профілактики протиправних дій) втручання правоохоронних і судових органів. Важливим елементом роботи судових органів є судові експертизи. Згідно із статтею 8 Закону України [1] судові експертизи проводяться у відповідності до атестованих методик, які мають державну реєстрацію. Тому дослідження можливих принципів і каналів несанкціонованого впливу на IoT-пристрої є актуальним кроком на шляху розроблення Методики судової експертизи щодо виявлення недокументованого втручання у роботу пристроїв IoT (далі – Методика).

Далі представлені основні підходи до вирішення проблеми формування засад розроблення Методики, яка, загалом, видається достатньо складною і потребує значних дослідницьких та випробувальних зусиль наукової спільноти.

Результати. На поточний час найбільш вразливими щодо несанкціонованого втручання вважаються IoT-пристрої, створені із використанням чипів Field-Programmable Gate Array (FPGA) – програмованих логічних матриць [2]. Цей тип мікросхем набув широкого застосування у телекомунікаціях (зокрема, у мережевому устаткуванні), оборонному та промисловому устаткуванні та IoT-пристроях, які широко застосовуються у багатьох інших галузях економіки держави. Одним із основних переваг цього типу мікросхем є перепрограмованість (можливість змінювати логіку роботи чипа). Саме ця властивість і створює широкі можливості для несанкціонованого втручання у роботу IoT-пристроїв, при чому, як на етапах виробництва чи постачання так і на етапах експлуатації.

Наразі, розповсюдженими вважаються інвазивні та неінвазивні методи шкідливого втручання (атак) у роботу чипів FPGA.

При неінвазивному методі атаки на IoT-пристрій фізичне втручання не передбачається, а використовуються побічні канали втручання. Зокрема, аналіз певної поведінки IoT-пристрою, яку можна зафіксувати (наприклад, вимірювання енергоживлення IoT-пристрою для підбору ключа алгоритму шифрування). Іншим прикладом неінвазивного втручання побічними каналами втручання можна вважати вплив тим чи іншим чином на IoT-пристрій з метою отримання збоїв у його роботі, що інколи дає можливість увести в оману системи безпеки (наприклад, сильний електромагнітний імпульс може вимкнути перевірку пароля [2]). Ці методи можуть застосовуватися зловмисниками, переважно, при експлуатації IoT-пристроїв. До неінвазивних методів можна віднести також і пряме несанкціоноване втручання у програмне забезпечення IoT-пристрою перед його постачанням користувачу.

Одними із ефективних методів захисту інформації, для запобігання неінвазивному втручанню у чипи FPGA є шифрування конфігурації (bitstream) за допомогою симетричних алгоритмів (зазвичай AES) із зберіганням ключа розшифрування у захищеному контейнері. При цьому, підміна bitstream (бітового потоку) виявляється за допомогою хеш–функцій (математичного алгоритму, який перетворює дані будь-якого розміру на коди фіксованої довжини). При цьому, кожний унікальний набір вхідних даних генерує унікальний хеш, який має властивості односторонності (необоротності) та детермінованості (для одного і того ж набору вхідних даних формується однаковий результат). Хеш-суми дозволяють швидко перевірити цілісність даних (відсутність несанкціонованого втручання).

Для інвазивних методів характерне приховане (завуальоване) втручання (фізичний доступ) до кристалу з метою впливу на нього (наприклад, вплив на структуру активної зони (кристалу) чипа за допомогою випромінювання). При цьому кристал чипа залишається роботоспроможним. Якщо ж інвазивний метод застосовується для реверс-інжинірингу чипу FPGA (встановлення принципу його функціонування), то для цього чип аналізується при руйнівному процесі зняття шару за шаром. Після такого дослідження чип втрачає роботоспроможність. Шари чипа знімаються, зазвичай, методом шліфування. Технологічно такі операції доволі складні, бо потребують декапсуляції корпусу чипа FPGA чи його частини (наприклад хімічними чи механічними методами) та використання спеціального, зазвичай, достатньо громіздкого технологічного обладнання. До цього обладнання, наприклад, належить: прецизійне шліфувальне обладнання для зняття шарів мікросхем, лазерне обладнання та інші джерела випромінювання (наприклад, радіоактивного) для фізичного створення у кристалі джерел збоїв при штатній роботі чипів FPGA. Наприклад, часто інвазивні атаки включають редагування (шліфування, різання та травлення) кристалу чипу сфокусованим іонним променем, видалення окремих зв’язків між активними елементами в кристалі та створення нових контактів для підключення контрольних зондів, растрове сканування чипа за допомогою сканувального електронного мікроскопа (який дає можливість побачити, навіть, окремі транзистори та з’єднання між ними [3]). При цьому, робота технологічного обладнання підтримується специфічним програмним забезпеченням і вимагає висококваліфікованого персоналу. Реалізація інвазивних методів впливу на IoT-пристрої можлива, переважно, на етапі їх виробництва або на етапі передпродажної підготовки.

Виявлення факту інвазивного втручання у фізичну структуру чипів IoT-пристроїв також вимагає залучення високотехнологічного обладнання (у тому числі і спеціалізованого програмного забезпечення) та персоналу високої кваліфікації.

Висновки. Наведені результати досліджень свідчать про реальність і можливість розроблення Методики, яка може (після атестації та державної реєстрації) використовуватися при проведенні судових експертиз. При цьому, створення Методики потребує значних дослідницьких та випробувальних зусиль наукової спільноти, залучення спеціалістів найвищої кваліфікації та широкого спектру спеціального обладнання.

Для створення умов практичного використання Методики при проведенні судових експертиз подальші дослідження мають бути спрямовані на формалізацію і розроблення основних положень Методики та методів її атестації і державної реєстрації у Міністерстві юстиції України.

Література

1. Про судову експертизу: Закон України від 01.01.2025 р. № 4059-IX, Відомості Верховної Ради України, 1994, № 28, ст.232.

2. Борода А. В. Атаки за побічними каналами на реалізації криптосистем: навчальний посібник / А. В. Борода. – К. : СЗР України, 2018. – 106 с.

3. https://habr.com/ru/companies/piter/articles/737622/ Книга «Аппаратный хакинг: взлом реальны.

УДК 004.738.5

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙНУ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДЕРЖАВНИХ ТА ПРИВАТНИХ РЕЄСТРІВ В УКРАЇНІ

Микола КОНДРАТЕНКО[1], email: mkond.95@gmail.com, ORCID: 0009-0009-0979-2626
Людмила КОВАЛЬЧУК[2], д-р техн. наук., проф., email: lusi.kovalchuk@gmail.com, ORCID: 0000-0003-2874-7950
Наталія ЛИСЕНКО[2], natalka.lsnk@ukr.net, ORCID: 0009-0008-9935-7646

[1]Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України
[2]Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України

Вступ. В Україні триває процес активної цифровізації та створення державних електронних реєстрів, які охоплюють практично всі сфери суспільного життя. До них належать реєстри юридичних осіб, фізичних осіб-підприємців, судових рішень, виборців, земельний кадастр тощо. Вони містять критично важливу інформацію — персональні дані громадян, майнові права, документи дозвільного характеру, відомості про бізнес та ресурси держави [1].

Однак сучасна модель функціонування цих реєстрів має низку недоліків. По-перше, інформація зберігається централізовано, що робить систему вразливою до кібератак та технічних збоїв. По-друге, відсутній єдиний механізм контролю, який би унеможливив підміну даних або їх приховане редагування. Саме тому поширеними залишаються випадки зловживань — так звані «чорні нотаріуси» використовують слабкі місця системи для незаконного перепису прав власності, підробки документів та інших маніпуляцій [2]. Також проблема полягає у низькому рівні довіри громадян до державних інституцій. Якщо інформація, зафіксована у реєстрі, може бути змінена без відома власника, то сам інститут електронних реєстрів втрачає легітимність. У цьому контексті впровадження інноваційних технологій, здатних забезпечити незмінність та прозорість даних, є ключовим завданням.

Технологія блокчейн розглядається як одна з найбільш перспективних. Її принципи — децентралізація, криптографічний захист, неможливість ретроспективної зміни даних та відкритість для перевірки — дозволяють подолати основні проблеми, притаманні традиційним централізованим базам даних [3; 4]. Вже сьогодні в Україні робляться кроки в цьому напрямі: прикладом є використання блокчейну в системі «Дія» та оновленому земельному кадастрі, створеному за участі міжнародних партнерів.

У цьому контексті постає завдання розробки каскадної моделі державних реєстрів, побудованої на основі блокчейн-технологій. Такий підхід дозволить не лише забезпечити захист від атак на підміну інформації, а й створить основу для суспільного контролю та зниження рівня корупційних ризиків. При цьому основний блокчейн, який забезпечує стійкість до основних атак, повинен бути незалежним від другорядного блокчейну і гарантовано стійким до цих атак. За таких умов, можливо створити чіткий алгоритм проведення науково-технічної експертизи, яка буде забезпечувати такі властивості:

1) однозначне виявлення факту підміни інформації в реєстрі;

2) однозначне виявлення особи, яка здійснила цю підміну;

3) за умови надання коректних даних власником цих даних – однозначне відновлення відповідної інформації у реєстрі.

Результати. У дослідженні обґрунтовано доцільність використання блокчейн-технології для побудови багаторівневої (каскадної) системи державних реєстрів. Основні переваги такого рішення:

1. **Захист від підміни інформації.** Дані у блокчейні після включення у блок стають незмінними. Це унеможливлює маніпуляції з реєстраційними даними, навіть якщо зловмисник має доступ до локальної бази.

2. **Прозорість і контроль.** Кожен запис підтверджується та фіксується в загальному ланцюзі, що дозволяє громадянам та інституціям перевіряти достовірність даних у будь-який момент [3].

3. **Розподіленість та відмовостійкість.** На відміну від централізованих серверів, блокчейн функціонує у вигляді розподіленої мережі. Навіть при виведенні з ладу окремих вузлів система зберігає працездатність.

4. **Каскадна структура реєстрів.** Модель передбачає існування основного державного блокчейну (mainchain), який синхронізує незалежні реєстри-сайдчейни. Для їх взаємодії використовується протокол консенсусу Proof-of-Proof (PoP), що дозволяє забезпечити надійність нижчих рівнів за рахунок властивостей вищого рівня [3].

5. **Протидія шахрайству та можливість експертизи.** Завдяки протоколу Proof-of-Proof навіть при спробах «чорних нотаріусів» змінити дані на локальному рівні остаточне підтвердження відбувається через головний державний блокчейн, що робить вірогідність успіху атаки вкрай низькою [5]. Також науково-технічна експертиза, зазначена вище, дає можливість однозначно виявити підміну даних, особу, що здійснила цю підміну, та відновити спотворену інформацію – за умови, що заінтересована сторона, що є власником коректних даних, надасть ці дані у визначеному форматі та разом з відповідними забезпечуючими матеріалами (номер блоку, геш-значення блоку, підпис особи, що його створила, шлях у відповідному дереві Меркля)

Висновки. Блокчейн-технологія здатна радикально підвищити стійкість та достовірність державних реєстрів України. Основні результати:

- усувається можливість підміни даних та зловживань при роботі з реєстрами;
- створюється прозорий механізм контролю за інформацією, що підвищує довіру суспільства;
- каскадна модель на основі Proof-of-Proof поєднує переваги незалежності локальних реєстрів із централізованим гарантом достовірності;
- зменшується ризик корупційних практик і незаконних дій приватних нотаріусів.

Запровадження блокчейну у державні реєстри стане важливим кроком у напрямі цифрової трансформації України, сприятиме розвитку електронної демократії та зміцненню кібербезпеки.

Література

1. Єдині та державні реєстри [Електронний ресурс]. – Офіційний сайт Міністерства юстиції України. – Режим доступу: https://minjust.gov.ua/m/str_22253 (дата звернення: 12.10.2025).

2. Закон України «Про публічні електронні реєстри» [Електронний ресурс]. – Офіційний вебпортал Верховної Ради України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1907-20#Text (дата звернення: 12.10.2025).

3. Proof-of-Proof and VeriBlock Blockchain Protocol Consensus Algorithm and Economic Incentivization Specifications [Електронний ресурс]. – Veriblock Documentation. – Режим доступу: https://www.veriblock.org/wp-content/uploads/2019/06/Proof-of-Proof_and_VeriBlock_Blockchain_Protocol_Consensus_Algorithm_and_Economic_Incentivization_v1.0.pdf (дата звернення: 12.10.2025).

4. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System [Електронний ресурс]. – Режим доступу: https://bitcoin.org/bitcoin.pdf (дата звернення: 12.10.2025).

5. Back, A. Hashcash – A Denial of Service Counter-Measure [Електронний ресурс]. – Режим доступу: http://hashcash.org/papers/hashcash.pdf (дата звернення: 12.10.2025).

УДК 004.056

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ ТА НАВЕДЕНЬ У СУДОВІЙ ЕКСПЕРТИЗІ

Іван ЦМОКАНИЧ[1], д-р філософії, e-mail: ivakobor@ukr.net, ORCID: 0000-0002-5085-8457

[1]Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України

Вступ. В умовах воєнного стану та зростання кіберзагроз питання технічного захисту інформації набуває особливого значення. Одним із найменш очевидних, але вкрай небезпечних каналів витоку інформації залишаються побічні електромагнітні випромінювання та наводення (ПЕМВН). Вони виникають у процесі роботи електронних пристроїв і можуть нести відображення оброблюваної інформації. Для зловмисників це — потенційне джерело конфіденційних даних, а для експертів — об'єкт технічного аналізу та джерело доказової інформації.

З кожним роком кількість електронних засобів, що генерують ПЕМВН, зростає — від побутової техніки до військових комунікаційних систем. Унаслідок цього експертам доводиться працювати з великими обсягами сигналів, часто — у зашумлених і складних умовах. Традиційні методи аналізу не завжди дозволяють своєчасно виявляти закономірності чи аномалії, особливо коли йдеться про малопомітні витоки або навмисно модифіковані пристрої.

У таких ситуаціях перспективним напрямом стає застосування штучного інтелекту (ШІ), здатного автоматизувати процеси збору, фільтрації, класифікації та інтерпретації сигналів. ШІ може навчатися на великих масивах експериментальних даних і з високою точністю розрізняти типи пристроїв, визначати джерела ПЕМВН і навіть прогнозувати ризики витоку. Це не лише підвищує якість проведення судової експертизи, а й скорочує час аналізу, що має особливе значення в оперативних умовах воєнного часу [1].

Результати. Методи ШІ дозволяють вирішувати кілька ключових завдань, з якими стикаються фахівці під час аналізу побічних електромагнітних випромінювань [2]:

1. Класифікація сигналів: згорткові нейронні мережі (CNN) здатні розпізнавати характерні спектральні ознаки різних типів технічних пристроїв, що дає змогу точно ідентифікувати джерело ПЕМВ.
2. Виявлення аномалій: моделі глибинного навчання — такі як автокодувальники чи LSTM-мережі дозволяють виявляти нетипові відхилення в структурі сигналів, які можуть свідчити про спробу несанкціонованого зняття або передачі інформації.
3. Прогнозування ризиків: на основі накопичених даних системи ШІ можуть оцінювати рівень потенційної загрози, моделювати сценарії витоку та формувати рекомендації щодо технічних і організаційних заходів захисту.

Такі алгоритми можуть працювати як у лабораторних умовах, так і в складі мобільних систем технічного контролю. У ході судової експертизи вони здатні аналізувати великі обсяги даних, виявляти приховані зв'язки між сигналами різних частотних діапазонів та визначати джерело випромінювання з високою точністю.

Застосування ШІ у судовій експертизі дозволяє суттєво підвищити ефективність роботи експертів [3]:

1. Автоматизувати аналіз великих масивів спектральних даних, що значно скорочує час обробки.
2. Створювати бази електромагнітних «підписів» типових технічних засобів, які можуть використовуватися для подальшої ідентифікації.
3. Генерувати аналітичні звіти, придатні як доказова база у кримінальних провадженнях.

4. Підвищувати об’єктивність експертних висновків завдяки алгоритмічній обробці без впливу людського фактору.

Практичні дослідження свідчать, що нейронні мережі здатні відновлювати закономірності в сигналах навіть за низького співвідношення «сигнал/шум». Наприклад, під час експертизи вилученого обладнання ШІ може допомогти визначити, чи було воно модифіковане для несанкціонованого зняття даних, чи спостережувані ПЕМВ є результатом технічних несправностей. Це суттєво підвищує точність і доказову силу експертних висновків.

Крім того, інтеграція систем ШІ із засобами цифрової криміналістики дозволяє поєднувати результати електромагнітного аналізу з іншими даними — мережевими журналами, цифровими артефактами, часовими мітками. Такий підхід створює комплексну картину події, що особливо важливо для кримінальних проваджень у сфері кіберзлочинів.

Висновки. Застосування штучного інтелекту для аналізу побічних електромагнітних сигналів відкриває новий етап розвитку технічного захисту інформації та судової експертизи. Інтелектуальні системи забезпечують високу точність виявлення каналів витоку, пришвидшують обробку сигналів і сприяють формуванню більш обґрунтованих експертних висновків.

Результати досліджень свідчать, що використання ШІ дозволяє істотно розширити межі традиційного експертного аналізу. Завдяки здатності систем машинного навчання працювати з великими обсягами даних, виділяти приховані закономірності та кореляції між параметрами сигналів, експерти отримують нові можливості для ідентифікації технічних пристроїв, оцінки їхнього стану та реконструкції подій. Це особливо важливо у випадках, коли фізичні докази частково втрачені, а електромагнітні сліди залишаються єдиним джерелом інформації.

Подальший розвиток цього напряму пов’язаний не лише з удосконаленням алгоритмів, але й з формуванням нормативно-методичної бази, яка регламентуватиме використання ШІ в судових експертизах. Необхідним є також створення централізованих баз даних електромагнітних «підписів» пристроїв, накопичення навчальних вибірок для алгоритмів і забезпечення сумісності державних методик із міжнародними стандартами технічного захисту інформації.

Окрему увагу варто приділити підготовці фахівців нового покоління, які володітимуть знаннями не лише в галузі електромагнітної сумісності, а й у сфері ШІ, обробки сигналів і цифрової криміналістики. Такі експерти зможуть ефективно поєднувати традиційні методи вимірювань із аналітичними можливостями інтелектуальних систем.

У ширшому контексті, впровадження ШІ в аналіз ПЕМВ є важливим елементом національної системи інформаційної безпеки. Це підсилює здатність держави протидіяти технічним каналам розвідки, забезпечувати цілісність критичної інфраструктури та захищати конфіденційні дані в умовах гібридної війни. Таким чином, інтеграція технологій ШІ в експертну практику є не лише інноваційним, а й стратегічно необхідним кроком для зміцнення безпеки України в інформаційному просторі.

Література

1. Sayakkara, A., Le-Khac, N.-A., Oren, Y. Cross-device portability of machine learning models in electromagnetic side-channel analysis for forensics / A. Sayakkara, N.-A. Le-Khac, Y. Oren // Journal of Universal Computer Science. – 2024. – Vol. 30, №10. – P. 1389–1422. DOI: 10.3897/jucs.109788.

2. Hameed, F., Alkhzaimi, H. Deep learning-based profiling side-channel attacks in SPECK cipher / F. Hameed, H. Alkhzaimi // Scientific Reports. – 2025. – Vol. 15. – Article 26149. DOI: 10.1038/s41598-025-08888-1.

3. Sayakkara, A., Le-Khac, N.-A., Oren, Y. A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics / A. Sayakkara, N.-A. Le-Khac, Y. Oren // Digital Investigation. – 2019. – Vol. 29. – P. 43–56. DOI: 10.1016/j.diin.2019.03.002.

УДК 004.056

ПРОБЛЕМИ СУДОВОЇ ЕКСПЕРТИЗИ ЗАСОБІВ ЗВ'ЯЗКУ ТА ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ З ПОЗИЦІЇ ЕЛЕКТРОМАГНІТНОЇ БЕЗПЕКИ

Іван ЦМОКАНИЧ[1], д-р філософії, e-mail: ivakobor@ukr.net, ORCID: 0000-0002-5085-8457

[1]Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України

Вступ. У сучасному світі засоби зв'язку та обчислювальна техніка стали невід'ємною частиною будь-якої державної, комерційної та особистої діяльності. Їхнє широке впровадження забезпечує швидкий обмін інформацією, доступ до хмарних сервісів, управління технологічними процесами та функціонування критично важливих об'єктів інфраструктури. Разом із тим, зростання обсягів цифрової інформації та її передача через електронні канали підвищують ризики несанкціонованого доступу, перехоплення та модифікації даних. Одним із ключових джерел таких ризиків є побічні електромагнітні випромінювання (ПЕМВ), що виникають під час роботи електронних пристроїв і можуть бути використані для витоку конфіденційної інформації.

Проблематика електромагнітної безпеки (ЕМБ) набуває особливої актуальності в умовах сучасних воєнних конфліктів, кібератак та активного розвитку цифрових технологій, включаючи Інтернет речей (IoT), мобільні мережі п'ятого покоління та високопродуктивні обчислювальні системи. Це створює нові виклики для судової експертизи, яка повинна не лише відновлювати факти злочинів, а й оцінювати потенційні канали витоку, їхні характеристики та загрози, пов'язані з електромагнітними сигналами.

Судова експертиза з позиції ЕМБ включає оцінку рівня побічних випромінювань, визначення їх спектральних та часових характеристик, а також аналіз можливостей несанкціонованого зчитування даних. Це дозволяє не тільки встановити технічну природу загрози, а й розробити практичні рекомендації щодо підвищення захищеності пристроїв. В умовах сучасної технічної еволюції та зростання обсягів даних особливо перспективним є використання методів штучного інтелекту та машинного навчання, що дозволяє автоматизувати аналіз великих обсягів сигналів, виявляти аномалії та класифікувати джерела випромінювань.

Таким чином, дослідження проблем судової експертизи засобів зв'язку та обчислювальної техніки з позиції електромагнітної безпеки є надзвичайно актуальним. Воно поєднує аспекти захисту інформації, цифрової криміналістики та сучасних аналітичних технологій, забезпечуючи комплексний підхід до оцінки ризиків, виявлення загроз і підвищення ефективності експертних висновків.

Результати. Проведений аналіз засобів зв'язку та обчислювальної техніки з позиції електромагнітної безпеки дозволив виділити ключові аспекти, що впливають на ефективність судово-технічної експертизи [1]:

1. Оцінка електромагнітної безпеки пристроїв.

Судово-технічна експертиза передбачає детальне вимірювання спектральних характеристик побічних електромагнітних випромінювань засобів зв'язку та обчислювальної техніки. Такі дослідження дозволяють визначити рівень потенційної загрози витоку інформації та встановити, які конкретні компоненти пристрою можуть бути джерелом ПЕМВ. Особливу увагу приділяють портативним і мобільним пристроям, які через компактну конструкцію та високу функціональність зазвичай мають менший рівень електромагнітного захисту.

2. Аналіз побічних сигналів як джерела доказів.

Побічні сигнали несуть інформацію про внутрішні процеси пристроїв, включаючи виконувані обчислення, стан пам'яті та взаємодію з периферійними модулями. Використання спектрального аналізу, кореляційних методів та алгоритмів машинного навчання дозволяє

реконструювати дії користувача або пристрою, що надає додаткові докази у кримінальних провадженнях. Зокрема, дослідження показують, що навіть короткочасні операції залишають електромагнітний слід, який можна відтворити за допомогою високочутливих вимірювальних систем.

3. Основні проблеми експертної діяльності.

Серед ключових проблем, що ускладнюють судово-технічну експертизу:

- наявність шумових факторів та зовнішніх інтерференцій у реальному середовищі;
- різноманітність конструкцій та електронних компонентів сучасних пристроїв, що ускладнює стандартизацію методик;
- відсутність централізованих баз даних електромагнітних «підписів» пристроїв, що значно ускладнює класифікацію сигналів;
- швидке оновлення технологій, що створює нестандартні та нові ПЕМВ, для яких ще немає досліджень і методик аналізу.

4. Застосування штучного інтелекту [2].

Методи глибинного навчання, включаючи нейронні мережі, автокодульники і LSTM-моделі, дозволяють автоматизувати обробку великих масивів сигналів, виділяти аномалії та класифікувати джерела випромінювань. Це підвищує об'єктивність експертних висновків, скорочує час аналізу та дозволяє прогнозувати потенційні загрози. Алгоритми ШІ також дозволяють створювати адаптивні моделі для різних типів пристроїв, що забезпечує гнучкість і масштабованість експертиз.

5. Практичні аспекти експертизи:

- створення та підтримка баз електромагнітних підписів відомих пристроїв, що дозволяє швидко ідентифікувати джерело ПЕМВ;
- використання аналітичних систем для оцінки ризику витоку інформації через побічні сигнали;
- розробка методик контролю та зниження побічних випромінювань у засобах зв'язку та обчислювальній техніці;
- інтеграція сучасних алгоритмів ШІ для автоматизації процесів класифікації та аналізу сигналів, що підвищує ефективність і точність експертних висновків.

Висновки. Судова експертиза засобів зв'язку та обчислювальної техніки з позиції електромагнітної безпеки є критично важливою у сучасних умовах цифровізації та зростання кіберзагроз. Аналіз побічних електромагнітних сигналів дозволяє виявляти приховані канали витоку інформації та оцінювати реальні загрози для конфіденційності даних.

Основні виклики включають шумові фактори, різноманітність пристроїв та відсутність централізованих баз даних. Використання штучного інтелекту підвищує ефективність і об'єктивність експертизи, автоматизуючи процеси класифікації та аналізу сигналів.

Подальший розвиток напряму потребує стандартизації методик, формування навчальних баз для алгоритмів і підготовки фахівців, здатних поєднувати традиційні методи експертизи із сучасними аналітичними технологіями. Це забезпечить надійний захист інформації та об'єктивність судових висновків.

Література

1. Теплицький, Б. Б. Актуальні питання призначення експертизи комп'ютерної техніки і програмних продуктів під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку. Current Issues an Examination Computer Hardware and Software Products during the Investigation of Crimes in the Use of Computers (Computer) Systems, Computer Networks and Telecommunication Networks. 2021.

2. Sayakkara, A., Le-Khac, N.-A., Oren, Y. A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics / A. Sayakkara, N.-A. Le-Khac, Y. Oren // Digital Investigation. – 2019. – Vol. 29. – P. 43–56. DOI: 10.1016/j.diin.2019.03.002.

УДК 343.98:004.056.5

СУДОВІ ЕКСПЕРТИЗИ З ПИТАНЬ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ТЕХНІЧНІ КАНАЛИ В УМОВАХ БОЙОВИХ ДІЙ

Євген ПАЩИН[1], e-mail: projectevgen91@gmail.com, ORCID: 0009-0007-2978-5699

[1]Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України

Вступ. Сучасні воєнні конфлікти характеризуються широким використанням інформаційно-комунікаційних технологій, що зумовлює підвищену увагу до питань захисту інформації та недопущення її витоку. В умовах бойових дій інформація про дислокацію військових частин, пересування військової техніки, управління підрозділами та логістичне забезпечення набуває критичного значення. Будь-який її витік через технічні канали може призвести до значних втрат та загроз національній безпеці. У цих умовах судові експертизи з питань витоку інформації є важливим інструментом для встановлення фактів компрометації даних та оцінки ефективності застосованих заходів технічного захисту [1; 2].

Результати. Проведення судових експертиз у сфері витоку інформації через технічні канали дозволяє вирішувати низку важливих завдань. Передусім, експерти встановлюють наявність чи відсутність небезпечних каналів витоку інформації. До них належать:

- електромагнітні канали (побічні випромінювання технічних засобів, які можуть бути перехоплені противником за допомогою спеціальних приймачів [3]);
- акустичні та віброакустичні канали (витік мовної інформації через стіни, вентиляційні системи або за допомогою високочутливих датчиків та лазерних мікрофонів [1]);
- оптичні канали (лазерні та інфрачервоні системи знімання інформації з приміщень);
- інформаційно-телекомунікаційні канали (несанкціонований доступ до комп'ютерних мереж, атак на системи зв'язку та канали передачі даних [4]).

Особливістю проведення таких експертиз у воєнний час є наявність додаткових факторів ризику. Активне застосування засобів радіоелектронної боротьби, створення завад, руйнування інфраструктури зв'язку та нестабільність енергозабезпечення суттєво ускладнюють завдання експерта. Водночас ці умови стимулюють розвиток нових методик виявлення та дослідження каналів витоку [5].

У процесі дослідження експерти використовують:

- вимірювальну апаратуру для фіксації побічних електромагнітних випромінювань;
- спеціальні акустико-вібраційні комплекси для моделювання та перевірки витоку мовної інформації;
- методики тестування каналів бездротового та супутникового зв'язку на наявність загроз перехоплення;
- комп'ютерно-технічний аналіз цифрових слідів у мережах [3; 4].

Важливою складовою є не лише виявлення факту витоку, але й оцінка його масштабу та потенційних наслідків. Наприклад, експерт може визначити, чи достатній рівень сигналу для реального знімання інформації на заданій відстані, чи є ймовірність дешифрування перехоплених даних противником.

До проблематики проведення експертиз у цій сфері належать:

- відсутність уніфікованих методик для умов воєнного часу;
- складність відтворення реальних умов роботи технічних систем на полі бою;
- недостатня кількість сучасних технічних засобів у експертних установах;
- потреба у швидкому проведенні досліджень через оперативний характер інформації [5].

Шляхи вирішення зазначених проблем полягають у:

- впровадженні новітніх технологій аналізу сигналів;
- створенні мобільних експертних груп з необхідним обладнанням;
- розробці нормативно-методичного забезпечення для експертиз у воєнних умовах [1; 3];

- налагодженні співпраці між експертними установами, військовими підрозділами та структурами кіберзахисту [5].

Таким чином, результати судових експертиз не лише сприяють розслідуванню конкретних кримінальних проваджень, але й виконують превентивну функцію — дозволяють удосконалювати системи захисту інформації, знижуючи ризик компрометації у майбутньому.

Висновки. Судові експертизи з питань витоку інформації через технічні канали є одним із ключових інструментів забезпечення інформаційної безпеки держави в умовах війни. Вони дозволяють об’єктивно оцінювати рівень загроз, підтверджувати факти компрометації даних та надавати слідчим і судовим органам вагомі докази [2; 4]. Подальший розвиток методів таких експертиз, оснащення експертів сучасними технічними засобами та вдосконалення правового регулювання сприятимуть підвищенню ефективності протидії витоку інформації та зміцненню національної безпеки України [5].

Література

1. ДСТУ 3396.0–96. Захист інформації. Технічний захист інформації. Основні положення. – Київ: Держстандарт України, 1996. – 28 с.

2. Закон України «Про інформацію». Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650 (зі змінами станом на 2023 рік). – 36 с.

3. Методичні рекомендації з виявлення та аналізу каналів витоку інформації. – Київ: ДССЗЗІ, 2020. – 64 с.

4. ISO/IEC 27001:2022. Information Security Management Systems — Requirements. – Geneva: ISO/IEC, 2022. – 35 p.

5. Ліпкан В. А. Національна безпека України: навчальний посібник. – Київ: КНТ, 2021. – 312 с.

УДК 004.056

АКТУАЛЬНІ ПИТАННЯ ПРОВЕДЕННЯ НАУКОВО-ТЕХНІЧНИХ ТА СУДОВИХ ЕКСПЕРТИЗ ЩОДО ВИЯВЛЕННЯ І ДОСЛІДЖЕННЯ СУЧАСНИХ СПОСОБІВ І ЗАСОБІВ ВЧИНЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ В УМОВАХ ВІЙНИ

Юрій СУКАЧ[1], e-mail: ysukach79@gmail.com

[1]Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України

Вступ. Сучасні умови збройної агресії проти України характеризуються активним використанням новітніх технологій для вчинення кримінальних правопорушень. Військові дії суттєво ускладнюють діяльність правоохоронних органів, а кримінальні прояви набувають нових форм, пов'язаних із застосуванням безпілотних літальних апаратів (БпЛА), кібератак, криптовалютних операцій, поширенням дезінформації та використанням deepfake-технологій. У цих умовах особливої актуальності набуває розвиток науково-технічних і судових експертиз, які дозволяють виявляти, досліджувати та документувати факти вчинення кримінальних правопорушень із застосуванням новітніх засобів.

Результати Однією з ключових проблем є швидкий розвиток технологій, який випереджає традиційні методи експертної діяльності. Наприклад, використання криптовалют унеможливлює класичне відстеження фінансових потоків, а кіберзлочини потребують застосування спеціалізованого програмного забезпечення та алгоритмів штучного інтелекту.

Для систематизації напрямів проведення експертиз в умовах війни доцільно виділити основні категорії сучасних методів і засобів. Результати наведенні в таблиці 1.

Таблиця 1 – Класифікація сучасних методів експертиз щодо виявлення кримінальних правопорушень

Напрям експертизи	Приклади застосування	Основні інструменти
Кіберфорензіка	Аналіз зламаних систем, відновлення видалених даних, дослідження шкідливого ПЗ	спеціалізоване ПЗ, блокчейн-аналіз
Експертиза БпЛА	Встановлення траєкторії польоту, аналіз «чорних скриньок», ідентифікація каналів зв'язку	технічні комплекси перехоплення
Фінансово-економічна	Розслідування криптовалютних операцій, відмивання коштів, електронні платежі	блокчейн-сканери, аналітичні системи
Інформаційно-психологічна	Виявлення deepfake, бот-мереж, маніпулятивного контенту	системи штучного інтелекту, OSINT

Крім того, необхідно розвивати методики комплексних експертиз, коли для розслідування одного правопорушення одночасно залучаються спеціалісти в галузі кібербезпеки, криміналісти, експерти з психології та інформаційних технологій.

Висновок. Таким чином, проведення судових та науково-технічних експертиз в умовах війни потребує адаптації існуючих методик до сучасних реалій та використання новітніх інструментів, особливу увагу слід приділяти кіберзлочинам, використанню БпЛА, фінансовим правопорушенням у сфері криптовалют та інформаційно-психологічним впливам. Для підвищення ефективності експертиз необхідне створення єдиних методичних підходів, міжвідомчої взаємодії та впровадження систем штучного інтелекту.

Література

1. *Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI.*

2. Шевчук О. М., Кузьменко О. В. Кібербезпека та кіберзлочинність: сучасні виклики для України. – Київ: НАВС, 2022. – 215 с.

3. Грищук В. К. Судові експертизи в умовах воєнного стану: проблеми та перспективи. // Вісник криміналістики. – 2023. – №1. – С. 15–23. 4. OSCE. Guidelines on Digital Evidence. – Vienna: OSCE, 2021. 5. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2022. – The Hague: Europol, 2022.

УДК 004.62

ЕВОЛЮЦІЯ КІБЕРВІЙНИ ПРОТИ УКРАЇНИ: АНАЛІТИКА ЗРОСТАННЯ КІБЕРАТАК, ГІБРИДНІ ІНСТРУМЕНТИ ВПЛИВУ ТА НАПРЯМИ ВДОСКОНАЛЕННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ

Максим КОМАРОВ[1], канд. техн. наук, e-mail: maxkom32@gmail.com, ORCID: 0000-0002-5739-8959
Ірина КАЛЬЯН[1], e-mail: i.harbovska@cip.gov.ua, ORCID: 0009-0009-5535-4475

[1]Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України

Вступ. З початку повномасштабного вторгнення кібервимір набув системного характеру, що супроводжує військові операції, впливає на інформаційний простір і має безпосередній ефект на функціонування критичної інфраструктури. У сучасних умовах цифровізації, коли інформаційні системи забезпечують стабільність державного управління, економіки та соціальної сфери, кібератаки дедалі частіше використовуються як інструмент стратегічного тиску, дестабілізації та психологічного впливу.

Особливої актуальності набуває питання захисту автоматизованих систем управління критичною інфраструктурою, на які все частіше спрямовуються скоординовані атаки, що мають на меті порушення безперервності їх функціонування. У відповідь на зростаючі кіберзагрози Україна активно розбудовує національну систему кібербезпеки, удосконалює механізми кіберзахисту та нарощує кіберстійкість держави як складової національної безпеки.

В даній роботі висвітлено результати дослідження, що ґрунтуються на наукових статтях, аналітичних матеріалах та статистичних даних з відкритих джерел, наведено тенденції розвитку кібератак проти України в умовах війни та визначено напрями розвитку національної системи кібербезпеки з урахуванням сучасних гібридних викликів.

Результати. Поняття «кібервійна» включає в себе декількох складових: кібератака, кібероборона, кіберрозвідка [1]. У ході ведення кібервійни, кібератаки в основному спрямовані на інформаційні системи, що забезпечують функціонування енергетичних, промислових, військових та інших критично важливих об'єктів. В свою чергу кібероборона полягає у можливості усунення (нейтралізації) кібератак противника, а кіберрозвідка має на меті здобуття корисної інформації шляхом проникнення в інформаційну систему (ІС) противника.

За даними аналітичних матеріалів CERT-UA [2], у першому півріччі 2025 року в Україні зафіксовано 3018 кіберінцидентів, що на 17% більше, ніж за 2 півріччя 2024 року. Найбільша кількість кібератак були спрямовані проти місцевих органів влади (34%), сектору безпеки та оборони (23%) та урядових організацій (19%). Серед основних типів кіберінцидентів переважають: розповсюдження ШПЗ (33%); фішинг (27%); зараження ШПЗ (21%). Зростання активності спостерігається з боку угруповань, пов'язаних із російськими спецслужбами: UAC-0002 (Sandworm, APT44), UAC-0218 та UAC-0219, UAC-0226, UAC-0227, UAC-0001 (APT28), UAC-0125, Gamaredon (UAC-0010), які системно адаптують свої методи шляхом зміни тактик, технік та процедур відповідно до заходів кібероборони України. Їх діяльність характеризується високим рівнем автоматизації, використанням обфускації та легітимних сервісів (GitHub, Telegram, OneDrive) для передачі команд і ексфільтрації викрадених даних.

Зростає частка операцій кібершпигунства, націлених на здобуття розвідданих, що частково пояснює зменшення кількості критичних інцидентів у 2023–2024 роках (367 – у 2023 та 59 – у 2024 році), попри загальне зростання числа всіх зареєстрованих кіберінцидентів (2194 – у 2022 році, 2543 – у 2023 році та 4315 – у 2024 році) [3].

Порівняльний аналіз свідчить про еволюцію атак – від масових фішингових кампаній до цільових операцій проти окремих державних установ і критичної інфраструктури, зокрема кібератаки проти ПрАТ «Київстар» (2023), проти державних реєстрів ДП «НАІС» (2024) та «Укрзалізниці» (2025). Зростає частота застосування шкідливих фреймворків типу PowerShell-

скриптів, Cobalt Strike Beacon, Metasploit. Також спостерігається поєднання технічних і психологічних методів впливу: використання Zero-click вразливостей, фішингові повідомлення, застосування методів соціальної інженерії та використання deepfake-технологій. Це підтверджує, що гібридна війна набуває системного характеру.

Зауважимо, що сучасна кібервійна часто інтегрована з інформаційно-психологічними операціями, що застосовуються з метою деструктивного впливу проти національної інформаційної безпеки України та спрямовані на підрив стійкості суспільства та інформаційної дестабілізації держави, дискредитації України, розсіювання паніки або деморалізацію населення. Такий підхід відповідає доктрині гібридної війни, де кібератаки є лише одним з елементів ширшої стратегії.

Україна активно посилює спроможності у розвитку національної системи кібербезпеки, зокрема ухвалення Закону України № 4336 «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» визначає функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагроз, функціонування системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та передбачає створення галузевих та регіональних команд реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT), а також визначає CERT-UA як національну команду реагування на кіберінциденти, кібератаки та кіберзагрози. Водночас Україна нарощує міжнародну взаємодію в сфері кібербезпеки, інтегруючись у європейські та глобальні механізми обміну інформацією про кіберзагрози. Зауважимо, що синхронізація зусиль між державним та приватним сектором, а також інтеграція з міжнародними структурами безпеки, зокрема шляхом налагодження співпраці з розвідувальними органами (NSA, CIA), цивільними інституціями (CISA, DHS, ENISA), а також з міжнародними альянсами (НАТО, QUAD, Five Eyes) сприятиме формування спільних алгоритмів дій на транскордонні кіберзагрози.

Реалізація наступальних проактивних спроможностей, створення системи кібероборони, а також розбудова мережі CSIRT сприятиме розвитку національної системи кібербезпеки, нарощування кіберстійкості та можливостей кіберзахисту для протидії російській кіберагресії, як складової частини гібридної війни.

Висновки. Таким чином, статистичні дані та характер кібератак доводять, що Україна залишається основною ціллю у глобальній гібридній війні. Кібератаки виступають не лише засобом технічного впливу, а й складовою інформаційної війни, спрямованої на дестабілізацію держави. Україна повинна системно розвивати власну кіберстійкість (кіберрезильєнтність) та готовність до реагування на кризові ситуації в сфері кібербезпеки на національному рівні.

У цьому контексті розвиток національної системи кібербезпеки передбачає централізоване управління кібероперaціями на стратегічному, оперативному та тактичному рівнях, а також розвиток наступальних, оборонних і розвідувальних кіберспроможностей, інтегрованих у загальну систему національної безпеки. Впровадження механізмів міжвідомчої координації дозволить не лише ефективно протидіяти поточним кіберзагрозам, але й формувати превентивні стратегії для виявлення потенційних атак.

Література

1. Когут, Ю. І. Кібервійна та безпека об'єктів критичної інфраструктури: практичний посібник / Ю. І. Когут; за ред. док-ра тех. наук, проф. А.С. Довгопологo. – Київ : Консалтингова компанія «СІДКОН»; ВД Дакор, 2021. – 332 с.

2. Державна служба спеціального зв'язку та захисту інформації України російські кібероперації [Електронний ресурс]. — Режим доступу: https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=71278&embedded=true&a=bi (дата звернення: 13.10.2025). — Назва з екрана.

3. WAR AND CYBER: THREE YEARS OF STRUGGLE AND LESSONS FOR GLOBAL SECURITY [Електронний ресурс]. — Режим доступу: https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=69131&embedded=true&a=bi (дата звернення: 13.10.2025). — Назва з екрана.

УДК 004.056

СТАТИЧНИЙ АНАЛІЗ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЯК ОДИН ІЗ МЕТОДІВ ДОСЛІДЖЕННЯ ПРИ ПРОВЕДЕННІ СУДОВОЇ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ

Максим КОМАРОВ[1], канд. техн. наук, e-mail: maxkom32@gmail.com, ORCID: 0000-0002-5739-8959
Ірина КАЛЬЯН[1], e-mail: i.harbovska@cip.gov.ua, ORCID: 0009-0009-5535-4475

[1]Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України

Вступ. З початку повномасштабного вторгнення в умовах зростаючої кількості кібератак на державні установи, енергетичний сектор, сектор безпеки та оборони та критичну інфраструктуру України в цілому, питання ефективного виявлення, аналізу та дослідження шкідливого програмного забезпечення (ШПЗ) набуває особливої актуальності.

В більшості зловмисних операцій, спрямованих проти України, для зараження пристроїв потенційних жертв використовується розповсюдження різних типів ШПЗ, що, в залежності від функціональності та векторів атаки, призводить як до викрадення конфіденційної інформації та отримання несанкціонованого доступу до систем жертви, так і порушення роботи систем в цілому. В таких умовах проведення експертизи комп'ютерної техніки і програмних продуктів набуває особливого значення, оскільки від її результатів залежить ідентифікація спроможностей ШПЗ, поширення відомих тактик, методів та процедур (TTP), визначення індикаторів компрометації (IoC) та збереження цифрових доказів.

Для комплексної оцінки кіберінцидентів з метою визначення характеристик та оцінки впливу ШПЗ на систему можуть використовуватись різні методи аналізу, серед яких має місце статичний аналіз (СА), що дозволяє виявити закономірності у великій кількості зразків ШПЗ, визначити вектори атак та методи обфускації даних, а також встановити взаємозв'язки у використанні технік атак та підвищити точність експертних висновків.

В даній роботі наведено результати дослідження можливостей застосування методу статичного аналізу при вивченні ШПЗ у межах проведення судової комп'ютерно-технічної експертизи.

Результати. Статичний аналіз у дослідженні ШПЗ дозволяє отримати метадані, що пов'язані з підозрілим двійковим файлом без його виконання, та визначити кількісні характеристики, які відображають закономірності у структурі та поведінці програмного забезпечення (ПЗ) [1]. Завдяки СА можливо виявити приховані патерни у випадках, коли код зашифрований, обфускований чи пошкоджений.

Початковий етап аналізу включає визначення типу двійкового файлу в результаті якого можна ідентифікувати операційну систему (ОС), на яку націлено ШПЗ, та її архітектуру [2]. Даний аналіз можна здійснити шляхом визначення розширення файлу, аналізу цифрового підпису файлу з використанням HEX-редактора, утиліт Linux (file) або Windows (CFF Explorer), модуля Python-magic.

Метод зіставлення інформації за допомогою цифрових відбитків включає в себе генерацію значень хеш-суми (використання алгоритмів MD5, SHA1, SHA256) для двійкового файлу на основі вмісту шкідливого файлу. Хеш-сума є унікальним ідентифікатором образу файлу. Створення бази статистичних ознак дозволяє зіставити невідомі зразки з існуючими профілями.

Наявність сигнатур шкідливого коду можна виявити використовуючи антивірусні сканери, наприклад VirusTotal, що дозволяє здійснювати пошук по власній базі даних, використовуючи хеш-суму, URL домен чи IP адресу, або альтернативні інструменти такі як: PeStudio, PPEE (puppy), IDA FindCrypt/FindCrypt2, FindCrypt-Ghidra, findcrypt-yara. Результати можна класифікувати як: TP (true positive), TN (true negative), FN (false negative), FP (false positive).

Аналіз послідовності символів ASCII/Unicode надає уявлення про індикатори: URL, IP, шляхи, назви функцій, рядки конфігурацій. Статистичні параметри рядків, зокрема їх довжина та частота використання спеціальних символів, виступають індикаторами, що дають змогу розмежовувати автентичні сигнатурні ознаки програмного коду від артефактів, зумовлених застосуванням методів обфускації. Для автоматичної ідентифікації та вилучення рядків з шкідливої програми може використовуватись інструмент FLOSS (FireEye Labs Obfuscated String Solver), що дозволяє визначити рядки, які були приховані автором ШПЗ.

Зауважимо, що для ускладнення процесу аналізу зловмисники здійснюють обфускацію ШПЗ з використанням пакувальників та крипторів, які стискають або шифрують виконуваний файл. Для їх виявлення можна скористатись інструментом Exeinfo PE, що дозволяє отримати інформацію про імпорти, експорти, секції PE, рівень ентропії та ознаки обфускації файлу.

Перевірка інформації про PE-заголовок є одним із ключових етапів дослідження у межах судово-комп'ютерної експертизи, оскільки містить критичні метадані, що визначають структуру та функціонування виконуваного файлу. Аналіз імпорту дозволяє визначити зовнішні залежності та можливі способи взаємодії з ОС, а перевірка експорту виявляє функції, які файл надає іншим модулям, що може свідчити про створення шкідливих API. Водночас дослідження ресурсів PE-файлу (рядки, сертифікати, іконки) допомагає виявити ознаки маскування чи соціальної інженерії.

На основі аналізу зібраних даних можна ідентифікувати та класифікувати ШПЗ. Існує декілька способів ідентифікації пов'язаних зразків, зокрема: метод хешування імпорту (imphash), нечітке хешування (алгоритм ssdeep) [3] та правила YARA (застосування правил, що базуються на сигнатурах, структурних особливостях та шаблонах). YARA дозволяє виявляти не лише відомі зразки, а й їх модифіковані варіанти, зокрема з використанням обфускації чи поліморфізму. Зокрема, YARA формалізує характеристики файлу у вигляді правил, що полегшує пошук подібних зразків у великих масивах даних. Це робить її важливим інструментом у СА та підвищує достовірність експертних висновків у судових дослідженнях.

Висновки. Таким чином, впровадження методів статичного аналізу у практику проведення судової комп'ютерно-технічної експертизи розширює можливості експертів у визначенні функціонального призначення та належності досліджуваних зразків, а також підвищує об'єктивність і точність судових експертиз. Такий підхід забезпечує отримання інформації про функціональні можливості та потенційні загрози, закладені в програмі.

Запропонований підхід дозволяє не лише підвищити ефективність виявлення та атрибуції шкідливого коду, але й забезпечує систематизацію цифрових доказів, що має важливе значення для кримінального провадження в умовах сучасної кіберзлочинності. Подальші дослідження у цій сфері мають бути спрямовані на вдосконалення алгоритмів статичного аналізу, розширення можливостей автоматизації та інтеграцію з існуючими системами кіберзахисту.

Література

1. Лисенко, С.М. Аналіз методів виявлення шкідливого програмного забезпечення в комп'ютерних системах / С.М. Лисенко, Р.В. Щука // Вісник Хмельницького національного університету – 2020. – 2 (283). – Режим доступу: https://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/01/17-4.pdf (дата звернення: 02.10.2025). — Назва з екрана.

2. Педяш, В. Сучасні методи виявлення шкідливого програмного забезпечення / В. Педяш, Є. Ледовський, В. Ткач // Вісник Хмельницького національного університету – 2024. – 2 (333). – Режим доступу:https://heraldts.khmnu.edu.ua/index.php/heraldts/article/view/164/148 (дата звернення: 02.10.2025). — Назва з екрана.

3. Єремізін, О.С. Перспективи використання нечіткого хешування в антивірусному захисті / О. С Єремізін, І. В. Стьопочкіна // Фізико-технічний інститут «НТУУ «КПІ» – 2016. – 1 (31). – Режим доступу: https://ela.kpi.ua/server/api/core/bitstreams/36e76527-d105-4f88-84c5-422539227031/content (дата звернення 02.10.2025). — Назва з екрана.

УДК 623-1/-8

СПЕЦІАЛІЗОВАНА АПАРАТНА ПЛАТФОРМА ЯК КЛЮЧОВИЙ ІНСТРУМЕНТ У СФЕРІ ДОСЛІДЖЕННЯ ЗРАЗКІВ ОВТ

Артем КАРПИНСЬКИЙ[1], e-mail: a.karpinsky@ws.cip.gov.ua
Максим ІЩУК[1], e-mail: m.ishchuk@cip.gov.ua, ORCID: 0009-0008-1132-8665

[1]Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України

Вступ. Ефективний аналіз трофейних зразків озброєння та військової техніки (ОВТ) є критичним завданням для підвищення обороноздатності держави. Такий аналіз вимагає наявності спеціалізованої апаратної платформи, що дозволяє досліджувати ворожі технології на мікрорівні. Зазвичай, дослідження обмежується програмним аналізом, тоді як фізичний реверс-інжиніринг потребує значно складнішого обладнання та компетенцій.

Передова лабораторна база, що включає стенд для аналізу побічних каналів, лазерну станцію та системи прецизійної підготовки зразків, дозволяє проводити унікальні дослідження, які неможливо виконати за допомогою стандартних засобів. Такий комплекс забезпечує високу точність та достовірність отриманих даних, що має вирішальне значення для ідентифікації прихованих вразливостей і розробки ефективних контрзаходів.

В даній роботі наводяться результати практичного застосування унікального лабораторного комплексу, що включає спеціалізоване обладнання для аналізу побічних каналів, фізичних атак та прецизійної підготовки зразків.

Результати. Для досягнення поставленої мети було задіяно багатокомпонентну лабораторну базу з такими ключовими характеристиками:

Стенд для аналізу побічних каналів (SCA) та атак впровадження несправностей (FI):

Використовуються високошвидкісні осцилографи:

Picoscope 3206D: має смугу пропускання 200 МГц та частоту дискретизації 1 ГВиб/с, що дозволяє з високою роздільною здатністю знімати побічні сигнали.

LeCroy Waverunner 9104M: забезпечує смугу пропускання до 1 ГГц та частоту дискретизації 5 ГВиб/с, що є критично важливим для аналізу високочастотних сигналів.

Current Probe та Power Tracer: дозволяють знімати точні струмові та енергетичні характеристики криптомодуля.

High precision EM probe та EM-FI Transient Coils: використовуються для виявлення електромагнітного випромінювання на мікрорівні.

Лазерна станція для фізичних атак та реверс-інжинірингу:

Laser Station 2: основна платформа, що забезпечує функціональність лазерної системи.

Діодні лазери: використовуються джерела випромінювання з різними довжинами хвиль (1064 нм NIR (30 Вт), 808 нм (20 Вт), 445 нм Blue (3 Вт)), що дозволяє впливати на різні матеріали та шари мікросхем.

Об'єктиви для мікроскопа: 5X, 20X, 50X забезпечують точне фокусування та візуальний аналіз об'єкта.

Glitch Amplifier: дозволяє генерувати контрольовані імпульсні збої для аналізу стійкості систем.

Системи прецизійної підготовки зразків:

Allied High Tech Products Inc – X-PREP Precision Milling/Polishing/Grinding System: використовується для механічного прецизійного фрезерування, шліфування та полірування.

Allied High Tech Products Inc – MULTIPREP SYSTEM 8": забезпечує напівавтоматичну хіміко-механічну підготовку зразків, що дозволяє досягти найвищої якості поверхні для мікроскопічних досліджень.

Аналіз побічних каналів (SCA) проводився з використанням високошвидкісних осцилографів, зокрема Picoscope 3206D і LeCroy Waverunner 9104M, а також зондів Current

Probe та Power Tracer. Це дозволило з високою роздільною здатністю знімати точні струмові та енергетичні характеристики під час виконання криптографічних операцій.

Паралельно, для фізичного доступу та ініціювання збоїв (FI) використовувалась Laser Station 2 з набором потужних лазерів з різними довжинами хвиль. Для підготовки мікросхем використовувалися стенди Allied High Tech Products Inc – X-PREP та MULTIPREP SYSTEM, призначені для високоточного механічного та хіміко-механічного шліфування. Це забезпечило фізичний доступ до внутрішніх шарів мікросхем, що є критично важливим для реверс-інжинірингу.

Усі отримані дані збиралися та аналізувалися на центральних обчислювальних платформах, що дозволило інтегрувати інформацію з різних джерел. Наявність у персоналу глибоких знань з електроніки, криптографії та аналізу даних дозволила не лише отримати, а й правильно інтерпретувати результати, виявляючи навіть найменші аномалії, що свідчили про потенційні вразливості.

Висновки. Наявний інструментарій створює унікальний комплекс для всебічного дослідження електронних компонентів ОВТ. Його можливості виходять за рамки простого тестування, дозволяючи проводити глибокий зворотний інжиніринг та виявляти неявні вразливості, що має пряме практичне значення для підвищення національної обороноздатності та створення перспективних зразків озброєння. Ця лабораторна база є ключовим активом, що забезпечує технологічну перевагу в умовах сучасних військових конфліктів.

Література

1. Fault Injection for Device Security [Електронний ресурс]. — Режим доступу: http://www.keysight.com/us/en/products/network-test/device-vulnerability-analysis/inspector-fj2-fault-injection-system.html — Назва з екрана.

2. Side Channel Analysis for Device Security [Електронний ресурс]. — Режим доступу: http://www.keysight.com/us/en/products/network-test/device-vulnerability-analysis/inspector-sc4-side-channel-analysis.html— Назва з екрана.

3. Allied High Tech Products Inc – MULTIPREP SYSTEM 8" [Електронний ресурс]. — Режим доступу: http://www.alliedhightech.com/Equipment/multiprep-polishing-system-8 — Назва з екрана.

УДК 623-1/-8

СИНЕРГІЯ ВИСОКОТЕХНОЛОГІЧНОЇ ЛАБОРАТОРНОЇ БАЗИ ТА ЕКСПЕРТНИХ КОМПЕТЕНЦІЙ: КЛЮЧ ДО УСПІШНОГО РЕВЕРС-ІНЖИНІРИНГУ ТРОФЕЙНИХ ЗРАЗКІВ ОВТ

Артем КАРПИНСЬКИЙ[1], e-mail: a.karpinsky@ws.cip.gov.ua
Максим ІЩУК[1], e-mail: m.ishchuk@cip.gov.ua, ORCID: 0009-0008-1132-8665

[1]Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України

Вступ. У сучасних умовах військово-технічного протистояння реверс-інжиніринг трофейних зразків озброєння та військової техніки (ОВТ) є ключовим інструментом для розуміння технологій противника. Ефективність цього процесу залежить від синергії трьох компонентів: передової апаратної бази, експертних знань персоналу та чіткої методології. Лише поєднання цих факторів дозволяє отримати повне уявлення про архітектуру, логіку роботи та існуючі вразливості ворожих систем.

Зазвичай, дослідження обмежуються програмним аналізом, тоді як фізичний реверс-інжиніринг потребує значно складнішого обладнання та компетенцій. Подолати це обмеження можливо за рахунок створення комплексної лабораторної бази, що дозволяє досліджувати як логічні, так і фізичні аспекти систем, а також використання мультидисциплінарної команди фахівців.

В даній роботі наводяться результати практичного застосування унікального лабораторного комплексу, що включає спеціалізоване обладнання для аналізу побічних каналів, фізичних атак та прецизійної підготовки зразків.

Результати. Для досягнення поставленої мети було задіяно багатокомпонентну лабораторну базу. Аналіз побічних каналів та атак впровадження несправностей проводився з використанням високошвидкісних осцилографів, зокрема LeCroy Waverunner 9104M, а також зондів Current Probe та Power Tracer. Це дозволило з високою точністю знімати та аналізувати струмові та енергетичні характеристики під час виконання криптографічних операцій.

Паралельно, для фізичного доступу та ініціювання збоїв, використовувалась Laser Station 2 з різними джерелами лазерного випромінювання. Експерти, що мають навички роботи з хіміко-механічним шліфуванням (Allied High Tech Products Inc), підготовлювали мікросхеми, забезпечуючи доступ до їхніх внутрішніх шарів для подальшого аналізу.

Усі отримані дані збиралися та аналізувалися на центральних обчислювальних платформах, що дозволило інтегрувати інформацію з різних джерел. Наявність у персоналу глибоких знань з електроніки, криптографії та аналізу даних дозволила не лише отримати, а й правильно інтерпретувати результати, виявляючи навіть найменші аномалії, що свідчили про потенційні вразливості.

Висновки. Таким чином, ефективність реверс-інжинірингу трофейних зразків ОВТ досягається завдяки повному використанню можливостей сучасної лабораторної бази. Ключовим фактором є синергія між передовим обладнанням та мультидисциплінарними навичками персоналу, який може одночасно працювати з фізичними, електронними та програмними аспектами дослідження. Ця комбінація дозволяє переходити від простого аналізу до глибокого розуміння технологій противника, що є критично важливим для підвищення рівня національної безпеки та розробки перспективних зразків ОВТ.

Література

1. Fault Injection for Device Security [Електронний ресурс]. — Режим доступу: http://www.keysight.com/us/en/products/network-test/device-vulnerability-analysis/inspector-fj2-fault-injection-system.html — Назва з екрана.

2. Side Channel Analysis for Device Security [Електронний ресурс]. — Режим доступу: http://www.keysight.com/us/en/products/network-test/device-vulnerability-analysis/inspector-sc4-side-channel-analysis.html— Назва з екрана.

3. Allied High Tech Products Inc – MULTIPREP SYSTEM 8" [Електронний ресурс]. — Режим доступу: http://www.alliedhightech.com/Equipment/multiprep-polishing-system-8 — Назва з екрана.

УДК 343.9.004

ОСОБЛИВОСТІ ПРОВЕДЕННЯ КОМП'ЮТЕРНО-ТЕХНІЧНИХ ЕКСПЕРТИЗ З ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ СТВОРЕННЯ ФАЙЛІВ ФОРМАТУ *.PDF ІЗ ВСТАНОВЛЕННЯ ОЗНАК КОМП'ЮТЕРНОГО МОНТАЖУ

Ольга БРЕНДЕЛЬ[1], *д-р філософії, e-mail: olgabrenda@ukr.net, ORCID:* 0000-0002-1723-0203
Олена СЕЛЕЗНЬОВА[1], *e-mail: seleznova.olena@nncise.org.ua, ORCID: 0009-0001-9940-6291*

[1]Національний науковий центр «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України

Вступ. Сучасна інформаційна епоха формує нові виклики для судово-експертної практики, адже цифрові документи дедалі частіше виступають носіями доказової інформації. Одним із найпоширеніших форматів електронних документів є Portable Document Format, відомий як PDF (із 1 липня 2008 року PDF є відкритим стандартом ISO 32000-1:2008 [1]). Його популярність пояснюється зручністю зберігання, сумісністю з різними операційними системами та здатністю відтворювати зміст і структуру незалежно від програмного середовища. Водночас універсальність формату робить його потенційним об'єктом маніпуляцій, коли підроблення може здійснюватися шляхом непомітного редагування або комп'ютерного монтажу.

В останні роки в Україні спостерігається суттєве зростання кількості злочинів, пов'язаних із підробкою електронних документів, насамперед файлів формату *.PDF. В умовах цифровізації державного управління та активного впровадження електронного документообігу у владних, судових, фінансових та освітніх структурах такі злочини набули системного характеру й становлять серйозну загрозу інформаційній безпеці держави. Особливо небезпечним це явище стає в період воєнного стану, коли більшість службових комунікацій, звітності та фінансових операцій здійснюється дистанційно, що полегшує створення і розповсюдження фальсифікованих PDF-документів – наказів, довідок, договорів, платіжних документів тощо. Такі файли часто використовуються для введення в оману державних органів, легалізації незаконних операцій, отримання персональних даних або дискредитації інституцій влади. У кіберпросторі поширюються випадки створення фальшивих сертифікатів, судових рішень, наказів чи довідок, які не лише вводять громадян в оману, а й сприяють поширенню дезінформації та дестабілізації суспільно-політичної ситуації. У складніших випадках підроблені PDF-документи стають елементами інформаційно-психологічних операцій, спрямованих на підрив довіри до державних органів, провокування панічних настроїв і здійснення інформаційних диверсій.

Проведення спеціальних комп'ютерно-технічних експертиз дозволяє виявляти ознаки підроблення PDF-документів, які через використання сучасних інструментів редагування часто мають високий рівень візуальної достовірності.

Результати. В експертній практиці найчастіше виявляються випадки комп'ютерного монтажу PDF-документів – вставки сторонніх фрагментів тексту, підписів, печаток або графічних елементів тощо. Такі дії залишають цифрові сліди у вигляді змінених метаданих, різних часових міток, ознак повторного конвертування чи різнорідної структури файлу. Їх виявлення можливе лише за допомогою спеціалізованого експертного аналізу в межах комп'ютерно-технічних експертиз.

Комп'ютерно-технічна експертиза PDF-документів – це складний аналітичний процес, спрямований на встановлення структури створення, редагування та можливого втручання у структуру PDF-файлів, виявлення непритаманних певній структурі файлу фрагментів, виявлення «накладання» зображень тощо. На відміну від звичайної перевірки візуального вмісту, експертне дослідження передбачає глибокий аналіз внутрішніх об'єктів, метаданих, системних відомостей, часових міток і програмного коду, який керує структурою документа,

бо саме ці елементи містять об’єктивні ознаки, що свідчать про зміну документа після його початкового створення.

Особливе значення має аналіз метаданих, які містять службову інформацію у стандартних полях (CreationDate, ModDate, Author) або у вбудованих XMP-блоках. Виявлення невідповідності дат створення та редагування, різних часових зон чи використання кількох програм редагування є типовими ознаками втручання. Дослідження графічних компонентів також має доказове значення: різниця у форматах стиснення, роздільній здатності або кольорових профілях зображень може свідчити про комп’ютерний монтаж кількох документів.

У процесі дослідження експерти використовують широкий спектр програмних інструментів – Autopsy, FTK Imager, X-Ways Forensics, Magnet AXIOM, ExifTool тощо, а також спеціалізовані скрипти, які дозволяють аналізувати структуру PDF, вилучати метадані, виявляти приховані об’єкти та фіксувати історію змін. У складних випадках застосовується порівняльний аналіз контрольних сум MD5 і SHA-256 об’єктів, що дає змогу встановити навіть незначні відмінності, непомітні користувачу.

Ознаками комп’ютерного монтажу PDF-документів є:

– накладання шарів поверх первинного тексту/зображень, різнорідність шрифтів/кодових підмножин у межах однієї сторінки;

– заміна/вставка зображень із відмінними параметрами стиснення чи роздільної здатності;

– наявність нетипових часових міток шрифтів або поява нових у пізніх версіях файлу;

– структурні порушення у формах і анотаціях, пізнє додавання полів чи коментарів.

Враховуючи наведене, особливого значення набуває підготовка висококваліфікованих фахівців у галузі комп’ютерно-технічної експертизи, розвиток методик виявлення фактів втручання у зміст цифрових документів (зокрема щодо дослідження PDF-документів), а також створення національних баз зразків автентичних цифрових документів для порівняльного аналізу. У сучасних умовах саме експертно-криміналістичне забезпечення здатне стати ключовим інструментом протидії фальсифікаціям, спрямованим проти інформаційного суверенітету України. Перспективним напрямом є створення автоматизованих систем аналізу, що зможуть самостійно виявляти аномалії у структурі файлу, аналізувати послідовність змін і порівнювати отримані результати з базою типових шаблонів підроблення. Використання технологій машинного навчання дозволить суттєво скоротити час експертного аналізу та підвищити його об’єктивність.

Висновки. Результати експертного аналізу PDF-документів мають велике судово-експертне значення. Вони дозволяють зробити обґрунтований висновок про внесення змін у зміст електронного документа, визначити спосіб та інструмент втручання, а також підтвердити чи спростувати відповідність файлу вихідному електронному оригіналу. Проте для того, щоб висновок мав юридичну силу, необхідно забезпечити належне зберігання об’єкта дослідження, дотримання ланцюга передачі цифрових доказів і застосування сертифікованих методик, схвалених Міністерством юстиції України. Таким чином, проведення комп’ютерно-технічних експертиз з дослідження технологій створення PDF-документів із встановлення ознак комп’ютерного монтажу вимагає від експерта високого рівня технічної компетентності, знання внутрішніх механізмів функціонування формату та вміння інтерпретувати цифрові артефакти.

Отже, судова експертиза є одним з унікальних способів отримання цінної доказової інформації, а її висновки як джерело доказів значною мірою підвищують надійність і доказову силу зібраних у справі матеріалів, забезпечують встановлення об’єктивної істини [2].

Література

1. ISO 32000-1:2008: Управління документами / Portable document format. Частина 1: PDF 1.7. [Електронний ресурс]. – Режим доступу: https://opensource.adobe.com/dc-acrobat-sdk-docs/pdfstandards/PDF32000_2008.pdf (дата звернення: 10.11.2025).

2. Попович, І. М. Проблемні питання призначення та проведення судової експертизи в господарському судочинстві // Теорія та практика судової експертизи і криміналістики. – 2019. – № 20. – С. 190–206.

УДК 344.1

БОЙОВИЙ ІМУНІТЕТ ЯК ЧИННИК УДОСКОНАЛЕННЯ ЗАВДАНЬ СУДОВОЇ ВІЙСЬКОВОЇ ЕКСПЕРТИЗИ

Олександр КОТЛЯРЕНКО[1], канд. юрид. наук, e-mail: lida_oleg@ukr.net, ORCID: 0000-0001-8776-2515

[1]Київський науково-дослідний інститут судових експерти Міністерства юстиції України

Вступ. Новий етап повномасштабної збройної агресії російської федерації проти України, який розпочався 24 лютого 2022 року, спричинив запровадження воєнного стану та фактичний початок воєнних (бойових) дій, а також введення в дію низку актів надзвичайного правового регулювання. Йдеться про наявність безпрецедентних до того часу політико-правових рішень, ухвалених органами державної влади, які спрямовані на відсіч збройної агресії.

Вказані події зумовили значне збільшення чисельності Збройних Сил України та інших утворених відповідно до законів України військових формувань, діяльність яких безпосередньо пов'язана із застосування зброї та бойової техніки. Довготривале ведення воєнних (бойових) дій на території України негативно позначилося на стані злочинності у воєнній сфері, призвело до суттєвого зростання кількості зареєстрованих кримінальних правопорушень, передбачених розділами XIX, XX Кримінального кодексу України.

Результати. Як відомо, запорукою ефективного, швидкого, повного та неупередженого досудового розслідування згаданих кримінальних правопорушень є використання спеціальних знань та можливостей судової експертизи, зокрема військової: щодо застосування видів та окремих родів військ (сил) Збройних Сил України, тимчасового оперативного підпорядкування підрозділів, порядку віддання та виконання наказів, управління військами, тощо.

З огляду на виклики сьогодення, пов'язані з постійно триваючою збройною агресією російської федерації, а саме прийняття військовими службовими особами усіх рівнів нестандартних управлінських рішень в умовах воєнного стану, перебування значної кількості підрозділів Збройних Сил України на лінії безпосереднього зіткнення із переважаючими силами противника, де ситуація постійно змінюється, для органів досудового розслідування під час розслідування у кримінальних провадженнях за фактами подій, що призвели до втрати особового складу, військової техніки та озброєння в процесі ведення воєнних (бойових) дій або проведення оборонних чи наступальних операцій, існує постійна потреба у проведенні саме судових військових експертиз. При цьому, під час проведення таких експертиз виникає необхідність у наданні оцінки діям (бездіяльності) військового командування, а також управлінських рішень як безпосередньо командирів підрозділів нижчої ланки, так і вищого військового командування.

Для аналізу і оцінки прийнятих начальниками органів військового управління управлінських рішень потрібно залучати судових експертів, які мають досвід проходження військової служби в органах військового управління на посадах старшого (вищого) офіцерського складу, експертно-аналітичні здібності, як правило, мають науковий ступінь (вчене звання), допуск до державної таємниці та оперативний (стратегічний) рівень військової освіти, яких катастрофічно не вистачає сьогодні в існуючих державних спеціалізованих експертних установах.

Із набрав чинності Законом України «Про внесення змін до Кримінального кодексу України та інших законодавчих актів України щодо визначення обставин, що виключають кримінальну протиправність діяння та забезпечують бойовий імунітет в умовах дії воєнного стану» від 15 березня 2022 року № 2124-IX, зокрема із введенням поняття «бойовий імунітет», виникла також потреба у проведенні експертної оцінки обстановки, в якій відбувалися втрати особового складу бойової техніки та іншого військового майна, настали негативні наслідки

застосування озброєння та військової техніки під час відсічі збройної агресії, можливості передбачити їх під час планування таких завдань (дій), а також виправданості їх настання.

Варто відмітити, що саме визначення поняття «бойовий імунітет» є складним для правозастосування у військово-юридичній спільноті, адже такі його категорії як «розумна обачність» та «виправданий ризик» досить важко застосувати через їх оціночний характер, оскільки їх тлумачення завжди має «суб'єктивний відтінок», а також є такими, що не сприймаються однаково будь-яким суб'єктом застосування. На нашу думку, на етапі планування операції (бойових дій) командири (начальники) змушені передбачати втрати особового складу, бойової техніки чи іншого військового майна, але спрогнозувати їх кількісні показники, а тим більше здійснити процедуру оцінки прийнятих командиром рішень з позиції прояву ним «розумної обачності» та охоплення заподіяної шкоди «виправданим ризиком» на практиці може виявитися дуже складним завданням, що підтверджується актуальною судовою практикою.

У цьому контекст вбачаємо доречною тезу, висловлену директором Одеського НДІСЕ Дмитром Кішком у вітальній промові до учасників конференції, у якій ним виснувано, що «військова експертиза – це синтез технічного, юридичного, криміналістичного, а часто – і гуманітарного напрямків. Це та сфера, де точність стає моральним обов'язком, а методика – питанням національної безпеки» [1].

Відтак, розширення меж людського розсуду під час аналізу прийнятих командиром рішень крізь призму правової категорії «бойовий імунітет» не приносить очікуваної ясності і недвозначності, не забезпечує передбачуваності застосування правових норм, та, як наслідок, визначення стандарту розумної та обачливої поведінки особистості може попадати в залежність від суб'єктивної оцінки судового експерта.

Варто відмітити, що нещодавно на базі Національної асоціації адвокатів України було проведено професійне обговорення з порушеного нами питання. За результатами дискусії модератор заходу Олексій Шевчук резюмував, що «бойовий імунітет і судова експертиза є невіддільними категоріями» [2].

Необхідність експертних висновків із цих питань обумовлена потребою застосування спеціальних знань відповідних фахівців у військовій (воєнній) сфері, оскільки саме існування поняття «бойовий імунітет» **є не підставою** для звільнення від кримінальної відповідальності, **а обставиною**, що виключає протиправність діяння, адже заподіяння шкоди суб'єкту кримінально-правової охорони при виконанні завдань із відсічі збройної агресії іншої держави проти України є правомірним.

Так, кримінальна відповідальність наставатиме, якщо загибель особового складу, втрата бойової техніки, захоплення ворогом наших територій сталися у зв'язку з бездіяльністю військової влади або перевищенням військовою посадовою (службовою) особою влади чи службових повноважень.

Досліджувати подібні обставини надзвичайно складно, адже під час оцінювання рішень командувачів (командирів) потрібно брати до уваги спеціальні, специфічні лише для конкретної воєнної ситуації обставини. Наприклад, чи були досконало вивчені наявні розвідувальні дані, чи під час ухвалення рішення було проведено рекогносцировку, виконано інші вимоги бойових (оперативних, планувальних) документів, чи були військовослужбовці забезпечені необхідною зброєю та всіма засобами особистого захисту. Належну оцінку таким обставинам можуть дати лише судові військові експерти, які мають спеціальні знання не лише у військовій сфері, а й у інших суміжних сферах (воєнній, правовій, тощо).

Висновки. Підсумовуючи викладене, вважаємо необхідним наголосити, що враховуючи наявність беззаперечних чинників, які, насамперед, спричинені довготривалою збройною агресією російської федерації проти України, на теперішній час потреба в удосконаленні визначених «Інструкцією про призначення та проведення судових експертиз та експертних досліджень» завдань судової військової експертизи є надто гострою та вкрай необхідною, адже очевидно, що в осяжному майбутньому кількість, обсяги та різновиди судових військових (а можливо і воєнних) експертиз, зокрема для з'ясування наявності обставин, що

виключають протиправність діяння (бойовий імунітет) відповідних суб'єктів, лише збільшуватиметься.

Література

1. Вітальне слово директора Одеського НДІСЕ Кішка Д.І. до учасників конференції «Військова експертиза в умовах сьогодення: проблемні питання та шляхи їх вирішення», (25.04.2025). URL: https://ondise.minjust.gov.ua/pro-pochatok-roboti-vseukranskoï-naukovo-praktichnoï-konferenciï-vijskova-ekspertiza-v-umovax-sogodennya-problemni-pitannya-ta-shlyaxi-ïx-virishennya/.

2. Незалежне професійне обговорення на тему «Бойовий імунітет як механізм правового захисту військових», (01.05.2025). URL: https://unba.org.ua/news/10229-bojovij-imunitet-hto-i-yak-mae-ocinyuvati-rishennya-komandira.html.

УДК 004.738.5

БЛОКЧЕЙН ЯК ОСНОВА ДОСЛІДЖЕННЯ КРИПТОВАЛЮТИ В СУДОВІЙ КОМП'ЮТЕРНО-ТЕХНІЧНІЙ ЕКСПЕРТИЗІ

Андрій ДЕРЕЧА[1], e-mail: derechaandrej@gmail.com, ORCID: 0009-0004-4966-1974
Тарас АБРОСІМОВ[1], e-mail: taras.abrosimov@gmail.com, ORCID: 0009-0003-1270-9404

[1]Національний науковий центр «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України

Вступ. Активна інтеграція цифрових технологій у різні галузі діяльності – соціальну, економічну, управлінську та інші – викликала інтенсивний розвиток економічних відносин, що зумовило якісно новий вид злочинності, її перехід у віртуальний простір. При цьому, істотне розширення методів та засобів обробки цифрової інформації, а також поява новітніх фінансових інструментів, розвиток технології блокчейн, що є основою крипторинку, призвели до розвитку кримінальної технології скоєння злочинів із використанням сучасних інформаційних технологій.

Результати. Висновки експертів з проведення комп'ютерно-технічних експертиз та експертиз у сфері електронних комунікацій є одним із дійових засобів боротьби зі злочинністю у сфері сучасних інформаційних технологій. У деяких випадках криміналістично значущі обставини можуть бути встановлені лише шляхом призначення та проведення комплексної судової комп'ютерно-технічної та економічної експертизи.

При цьому, перед експертом можуть бути поставлені такі завдання: встановлення зв'язків між різними криптовалютними гаманцями, ідентифікація та встановлення потоку коштів, ідентифікація адреси, гаманця, мережі, асоційованих з користувачем щодо його участі у транзакціях, виявлення закономірностей та взаємозв'язок всередині блокчейну, виявлення на об'єктах ознак встановлення або використання криптогаманців, бірж чи DeFi-клієнтів (користувачів децентралізованих фінансів), встановлення транзакційної активності, дати, суми, контрагенти, призначення платежів тощо.

Удосконалення процесу експертного дослідження, достовірність та обґрунтованість та переконливість висновку експерта, є неможливим без розроблення новітніх методик проведення судових експертиз відповідно до установленого нормативно-правовими актами порядку. Методики проведення судових комп'ютерно-технічних експертиз на сьогодні перебувають на стадії активного розвитку відповідно до потреб судово-правоохоронної діяльності у сфері злочинів, пов'язаних, зокрема, з криптовалютами. Так, фахівцями Науково-дослідного центру судової експертизи у сфері інформаційних технологій та інтелектуальної власності та Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України розробляються методичні рекомендації з дослідження транзакцій в криптовалютних системах при проведенні комп'ютерно-технічних експертиз.

При дослідженні криптовалюти експерт має встановити: конкретний вид, основні характеристики криптовалюти, її кількість; наявність даного типу криптовалюти свого блокчейну, оскільки криптовалюта завжди ґрунтується на технології блокчейн; тип використаного електронного гаманця; IP-адреса, з якою він асоційований; чи використовувалася дана криптовалюта в раніше скоєних злочинах, при оплаті незаконних товарів та послуг; журнал операцій, пов'язаних із цим криптовалютним гаманцем; орієнтовна вартість криптовалют у фіатних валютах на момент аналізу;; адреси інших криптовалютних гаманців, що взаємодіяли з гаманцем власника; достовірну інформацію про особу, якій належить криптовалютний гаманець тощо.

Етапи проведення експертизи криптовалюти включають у себе: ознайомлення з документом про призначення судової експертизи та матеріалами справи, огляд пакування та фотографування об'єктів дослідження, визначення обсягу, методик проведення дослідження,

наявність програмного забезпечення, пов'язаного з використанням віртуальних валют, історія перегляду html-сторінок, пов'язаних із обігом віртуальних валют, встановлення факту використання онлайн-сервісів зберігання даних («хмарних сховищ») як джерела доказової інформації (наприклад, «Google Drive» зберігають резервні копії таких програм, як Whatsapp, Viber тощо), програмне забезпечення, що дозволяє зберігати інформацію про облікові записи та логіни користувача, журнал CoC, сторожові хеші для проміжних експортів, перевірити образи, реєстр хеш-значень, таблиці адреси, акаунтів, реєстр транзакцій, опис ознак privacy-технік тощо, оформлення висновку експерта.

Висновки. Таким чином, сучасні стратегії життя зумовлюють необхідність експертів бути адаптивними в умовах постійних змін, використовуючи методологію та новітні технології щодо внесення посильного вкладу у боротьбу з криптовалютними злочинами. Висновки експертів допомагають правоохоронним органам відстежувати підозрілі транзакції, виявляти закономірності та збирати докази незаконної діяльності.

З урахуванням важливості та значущості розвитку та вдосконалення судової експертизи, зокрема, з дослідження криптовалюти, пропонується вжити такі заходи: створювати новітні методики та методичні рекомендації з проведення судових експертиз; брати участь у науково-практичних конференціях і семінарах щодо розгляду процесуальних, організаційних та методичних аспектів проведення судових експертиз, організовувати стажування експертів, які спеціалізуються в галузі цифрових технологій, з метою підвищення їх кваліфікації; здійснення міжнародного співробітництва щодо транскордонного розслідування, пов'язаного з криптовалютами; посилити матеріально-технічне оснащення сучасним технічним обладнанням та програмним забезпеченням. Реалізація зазначених рекомендацій сприятиме подальшому розвитку судової експертизи, ефективного та оперативного розкриття злочинів, захисту прав, свобод і законних інтересів громадян України.

Література

1. Блокчейн для фінансів. Ліцензія: arXiv.org arXiv:2402.17219v1 [cs.CR], 27.02.2024. URL: https://arxiv.org/html/2402.17219v1?utm source=chatgpt.com (дата звернення 31.10.2025).

2. Сумісна кібербезпека з використанням Блокчейн. Ліцензія: arXiv:2403.04410v1 [cs.CR], 07.03.2024 URL: https://arxiv.org/html/2403.04410v1?utm source=chatgpt.com (дата звернення 31.10.2025).

УДК 343.98:61:619:665.6/.7

АКТУАЛЬНІСТЬ КОМПЛЕКСНОЇ СУДОВО-ВЕТЕРИНАРНОЇ ЕКСПЕРТИЗИ ТА ЕКСПЕРТИЗИ МАТЕРІАЛІВ, РЕЧОВИН ТА ВИРОБІВ У ВИЯВЛЕННІ ТА ДОСЛІДЖЕННІ СУЧАСНИХ СПОСОБІВ ТА ЗАСОБІВ ВЧИНЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Нінель КОЗАКОВА[1], e-mail: dgany30@gmail.com, ORCID: 0009-0000-6617-3228
Вікторія БУЛАВІНА[1], канд. вет. наук., доц., e-mail: viktoriyabulavina84@gmail.com, ORCID: 0000-0001-8746-9693
Ольга БУЙ[1], канд. хім. наук, e-mail: b.olga.d.75@gmail.com, ORCID: 0000-0003-2053-3122

[1]Національний науковий центр «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України

Вступ. У сучасних умовах збройного конфлікту кримінальна діяльність набуває нових форм і засобів, що значно ускладнює ідентифікацію, документування та доказування правопорушень. Особливою складністю вирізняються ситуації, пов'язані із жорстоким поводженням з тваринами, зокрема знущання над тваринами з подальшим їх підпалом із використанням спеціальних матеріалів, хімічних і побутових речовин. У такому контексті комплексна судово-ветеринарна експертиза в поєднанні з експертизою матеріалів, речовин та виробів стає критично важливою для встановлення фактів злочину, механізмів їх вчинення та оцінки правових наслідків [1].

Актуальність цього питання зумовлена поєднанням кількох факторів: зростанням випадків жорстокого поводження з тваринами із подальшим приховуванням злочину шляхом умисного підпалу трупів тварин, ускладненням експертної інтерпретації через деградацію об'єктів дослідження, а також необхідністю комплексного підходу, який об'єднує ветеринарну, хімічну науки та криміналістику. Практичні виклики включають правильну видову ідентифікацію обгорілих трупів тварин, правильну кваліфікацію заподіяних тілесних ушкоджень тварині, виявлення та ідентифікацію слідів нафтопродуктів, що є чинниками, які забезпечують розвиток пожежі, що в свою чергу вказує на умисний підпал, а також забезпечення належного ланцюга збереження доказів в умовах бойових дій [2].

Результати. Спираючись на особистий досвід проведення експертиз, слід окреслити необхідні складові комплексної судово-ветеринарної експертизи та експертизи матеріалів, речовин та виробів для встановлення факту жорстокого поводження із тваринами із подальшим приховуванням злочину шляхом умисного підпалу трупів тварин. В умовах війни, внаслідок масованих атак країни агресора, виникають чисельні пожежі у яких гинуть, як люди так і тварини. Такі згарища можуть використовуватися для приховування загибелі тварин унаслідок заподіяння їм тілесних ушкоджень, фізичного болю, страждань, мучення. У якості об'єктів дослідження були надані фрагментовані трупи тварин, що зазнали впливу високих температур. Деякі об'єкти зазнавши впливу полум'я зберегли морфологічні ознаки за якими видова ідентифікація не викликає складнощів у судово-ветеринарних експертів, інші були значно фрагментовані та обгорілі. У цьому випадку використання методу баркодінгу (метод таксономічної ідентифікації на основі ДНК) [3], де за кістковою тканиною, навіть тією, що зазнала впливу високих температур, є можливість безпомилково встановити видову належність обгорілих та значно фрагментованих решток тварин [4].

Важливою умовою отримання максимально точних результатів під час таких експертиз є забезпечення належного ланцюга збереження доказів, зокрема пакування об'єктів дослідження у герметичні полімерні пакети та збігання у замороженому стані. Такий спосіб пакування та зберігання дозволить зупинити гнилісні зміни об'єктів та збереже залишки легкозаймистих речовин, що можуть міститися на цих об'єктах, а також буде сприяти проведенню більш повного і всебічного дослідження.

В ході проведення вищезазначених комплексних експертиз, експертом-хіміком можливе застосування методів тонкошарової і газорідинної хроматографії для дослідження залишків нафтопродуктів в залежності від стану наданих об'єктів дослідження. Наявність великої кількості соекстрактивних речовин може значно ускладнювати процес дослідження та ідентифікації залишків речовин, що можуть забезпечувати розвиток горіння.

Висновки. Таким чином, даний приклад наглядно демонструє важливість комплексного підходу до вирішення поставлених питань. Використання класичних методів проведення судово-ветеринарної експертизи, зокрема зовнішній огляд об'єктів, судово-ветеринарний розтин трупів тварин, має бути доповнено більш сучасним методом баркодінгу, що розширить можливості видової ідентифікації значно розчленованих та обгорілих трупів тварин. У свою чергу залучення експерта-хіміка дозволяє підтвердити або спростувати наявність залишків речовин, що вказують на умисний підпал трупів тварин з метою приховування злочину. Використання широкого спектру методів дослідження з арсеналу експертів-криміналістів від зовнішнього огляду до газорідинної хроматографії з мас-детектуванням, дозволяють наблизитись до вирішення питань щодо обставин скоєння подібних злочинів.

Література

1. Ahmed Bakhsh, Ayoub, A., Laeeq, Z., & Afshan Maqbool. (2024). From ashes to evidence: Comprehensive analysis of forensic fire investigations. Forensic Insights and Health Sciences Bulletin, 2(2), 67–72. Retrieved from https://ammanif.com/journal/fi/index.php/home/article/view/118

2. Kazantsev, R. H. and Yatsenko, I. V. (2024) 'Forensic veterinary assessment of the expert informativeness of biotransformation patterns of dog and cat corpses in various states of decomposition', Journal for Veterinary Medicine, Biotechnology and Biosafety, 10(4), pp. 3–17. https://jvmbbs.kharkov.ua/archive/2024/volume10/issue4/article1.php?utm_source=chatgpt.com

3. Kelly A. Meiklejohn, Mary K. Burnham-Curtis, Dyan J. Straughan, Jenny Giles, M. Katherine Moore. (2021). Current methods, future directions and considerations of DNA-based taxonomic identification in wildlife forensics. Forensic Science International: Animals and Environments, Volume 1, 2021, 100030, https://doi.org/10.1016/j.fsiae.2021.100030.

4. Małgorzata Grela, Andrzej Jakubczak, Marek Kowalczyk, Piotr Listos, Magdalena Gryzińska. Effectiveness of various methods of DNA isolation from bones and teeth of animals exposed to high temperature. (2021). Journal of Forensic and Legal Medicine. Volume 78, 2021, 102131, https://doi.org/10.1016/j.jflm.2021.102131.

УДК 621.396

АКТУАЛЬНІ ПИТАННЯ ПРОВЕДЕННЯ НАУКОВО-ТЕХНІЧНИХ ТА СУДОВИХ ЕКСПЕРТИЗ ЩОДО ВИЯВЛЕННЯ І ДОСЛІДЖЕННЯ СУЧАСНИХ СПОСОБІВ І ЗАСОБІВ ВЧИНЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ В УМОВАХ ВІЙНИ

Сергій ШЕРЕМЕТОВ[1], e-mail: s.sheremetov60@gmail.com
Ростислав ГОЛОВАЧ[1], e-mail: vekvnnc@gmail.com

[1]Київський науково-дослідний інститут судових експертиз Міністерства юстиції України

Вступ. Пропонується розглянути актуальні напрями розвитку судово-військової експертизи в умовах широкомасштабної збройної агресії проти України, визначено сучасні способи та засоби вчинення кримінальних правопорушень у воєнний час, охарактеризовано виклики, що постають перед експертною діяльністю, та визначено пріоритети наукового і методичного забезпечення для підвищення ефективності досліджень.

Збройна агресія російської федерації проти України змінила характер кримінальної діяльності, технологічні підходи до її здійснення та ускладнила завдання щодо фіксації, дослідження й доказування кримінальних правопорушень. У сучасних умовах воєнних дій відбувається значне ускладнення способів і засобів здійснення кримінальних правопорушень, що потребує удосконалення підходів до їх виявлення, дослідження та документування. Необхідність оперативного реагування на нові форми злочинності, пов’язані з використанням сучасних військових технологій та гібридних методів протиправної діяльності, обумовлює розробку і впровадження нових методологічних рішень та експертних підходів. Судова військова експертиза виконує ключову роль у встановлених об'єктивних фактах злочинів, а також у визначених специфіках і методології розслідування в умовах війни. [1] [2]

Проблематика і актуальність. Зростання використання сучасних технологій у вчиненні злочинів (кіберзлочини, неправомірне використання безпілотних літальних апаратів, засобів радіоелектронної боротьби та протидії захисту, перехоплення зв’язку, навігаційних сигналів, втручання у роботу безпілотних систем, снайперська та диверсійна діяльність, застосування вибухових пристроїв сучасної конструкції). [3]

Потреба в оперативності дослідження при збереженні якості та достовірності.

Дефіцит первинних матеріалів дослідження через бойову обстановку, складність і специфіка збору та фіксації доказів у військових умовах: обмеження доступу до місця злочину та неможливість огляду місця події, загроза безпеці експертів, знищення доказів, обмеження в часі. [4]

Необхідність фіксації ушкоджень та бойових факторів з використанням сучасних цифрових технологій, геоінформаційних систем, супутникової розвідки.

Відсутність єдиних національних стандартів, адаптованих до воєнного стану, для проведення судових експертиз у таких умовах. [5]

Основні завдання судових військових експертиз в умовах війни.

Виявлення і документування слідів і характерних ознак використання сучасних засобів злочинного впливу – об’єктів військової експертизи. [6]

Визначення механізмів вчинення кримінальних правопорушень з урахуванням специфіки воєнного часу – дій (бездіяльності) посадових осіб. [7]

Оцінка правомірності військових рішень з урахуванням міжнародного гуманітарного права, стандартів НАТО, змін у тактиці і структурі бойових дій.

Оцінка доказової бази з огляду на вимоги судочинства та міжнародних стандартів. [8]

Розробка методичних рекомендацій щодо ефективного застосування новітніх технологій судово-експертної діяльності, оновлення науково-методичних підходів з урахуванням стандартів НАТО та міжнародного досвіду.

Нові підходи і методи дослідження. Використання цифрових технологій у фіксації та аналізі доказів (тривимірне моделювання, безпілотники, цифрова криміналістика). [8]

Інтеграція криміналістичних і технічних засобів дослідження (аналіз електронних пристроїв, радіолокаційних відомостей, біометричних даних).

Використання методів прогнозування та моделювання для визначення тенденцій у способах злочинного впливу в умовах бойових дій.

Виклики та перспективи підвищення ефективності експертиз. Обмежений доступ до необхідного сучасного обладнання та програмного забезпечення. [10]

Потреба у підготовці висококваліфікованих спеціалістів, ознайомлених із специфікою ведення експертизи під час війни.

Можливість налагодження міжвідомчої співпраці для комплексного розслідування та протидії новим кримінальним загрозам.

Впровадження єдиних методичних стандартів із урахуванням міжнародного досвіду.

Висновки. Судово-військова експертиза в умовах війни є ключовим елементом доказової діяльності та забезпечення національної безпеки. Нові технологічні та тактичні аспекти ведення бойових дій формують оновлене поле кримінальних правопорушень, що потребує адаптації науково-методичного інструментарію та підвищення вимог до компетентності експертів.

Комплексний міждисциплінарний підхід, впровадження сучасних аналітичних інструментів, цифрових технологій та міжнародних стандартів, а також розвиток кадрового потенціалу є запорукою підвищення ефективності експертної діяльності в умовах воєнного стану та післявоєнного правосуддя.

Рекомендації:

Визначити пріоритетні напрями науково-дослідних робіт з удосконалення судових експертиз у військових умовах.

Розробити та впровадити оновлені методичні рекомендації, методики дослідження та програми підготовки експертів, адаптовані до реалій сучасної війни.

Посилити співпрацю між науково-дослідними установами, судовими експертами, правоохоронними органами, сектором оборони та безпеки.

Забезпечити підвищення рівня технічного оснащення та цифрової інфраструктури для підвищення оперативності, точності та надійності експертних висновків.

Сприяти формуванню єдиної інформаційно-аналітичної платформи для обміну даними та уніфікації підходів до дослідження воєнних правопорушень.

Література

1. Яремчук В.О. Сучасні напрямки судової експертизи і криміналістики. Стаття. Серія ПРАВО. Випуск 80: частина 2. URL: https://doi.org/10.24144/2307-3322.2023.80.2.32. *208 с.*

2. Литвиненко Д.О., Шульженко А.В. Судова експертиза під час воєнного стану. Юридичний науковий електронний журнал. УДК 343.98. URL: https://doi.org/10.32782/2524-0374/2024-8/98.

3. Зайцев О., Присяжнюк М., Артюх С., Сидоренко С. та Максим Б. (2024). Застосування роботизованих систем в умовах збройної агресії Росії проти України. Соціальний розвиток і безпека , 14 (6), 53-60. https://doi.org/10.33445/sds.2024.14.6.6/

4. Шевчук В.М. Роль цифрової криміналістики у виявленні, фіксації та розслідуванні воєнних злочинів. Збірник-тез_Використання-цифрової-інформації_1212_2022.pdf. URL: https://doi.org/10.31359/978-966-998-460-9. *С 86.*

5. В. Ю. Шепітько. Розділ І Тенденції криміналістики в сучасних умовах технологізації науки. Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі. Монографія URL: https://ivpz.kh.ua/wp-content/uploads/2025/01/%D0%9C%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F-%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%D1%96%D1%81%D1%82%D1%96%D0%B2-2024.pdf. С. 20.

6. Антоніна Іванівна Черемнова. Цифрова криміналістика як складова криміналістичної техніки: сучасний стан та перспективи розвитку. URL: https://doi.org/10.32782/2522-9656/2024-16-6. *С. 61.*

7. Демидова Л.М. Воєнні злочини: проблеми визначення та кваліфікації. URL: https://notebooklm.google.com/notebook/3bf1cd70-679a-42df-902f-8a4413d35105#:~:text=%D0%A3%D0%94%D0%9A%20343.3/.7%20DOI%20https%3A//doi.org/10.24144/2307%2D3322.2024.84.3.42. *С. 278.*

8. Vyhivskyi, I., Martyniuk, O., Rossokxa, S., Shchupakivskyi, R., & Strunevych, O. Зленко Розслідування воєнних злочинів на деокупованих територіях: роль Національної поліції України. URL: https://doi.org/10.34069/AI/2024.78.06.5/

9. О.О., Котенко Б.В. Цифрова криміналістика: сьогодення та напрямки розвитку. URL: https://doi.org/10.32782/2524-0374/2022-10/155.

10. Використання цифрової інформації в розслідуванні кримінальних правопорушень. Матеріали міжнародного науково-практичного круглого столу, присвяченого Всеукраїнському тижню права м. Харків, 12 грудня 2022 року URL: https://doi.org/10.31359/978-966-998-460-9/ *С. 76-77.*

УДК 343.98:159.9.072.43

СИСТЕМНИЙ ПІДХІД ДО ДОСЛІДЖЕННЯ ОСОБИСТОСТІ В СУДОВО-ПСИХОЛОГІЧНІЙ ЕКСПЕРТИЗІ В УМОВАХ ВОЄННОГО СТАНУ

Євген ПІДЧАСОВ[1], канд. психол. наук, доц., e-mail: psyevgeniy@gmail.com, ORCID: 0000-0003-3023-4927
Надія ЧЕПЕЛЄВА[2], ст. викл., e-mail: chepn@ukr.net, ORCID: 0000-0003-2101-9571

[1]Харківський національний педагогічний університет імені Г.С. Сковороди
[2]Харківський національний університет внутрішніх справ

Вступ. Проведення експертного психологічного дослідження особистості є складним і багатоаспектним процесом, що супроводжується низкою методологічних і практичних труднощів. Основні з них зумовлені недоступністю психічних явищ для безпосереднього спостереження, багатофакторною детермінацією психічних механізмів, а також високою пластичністю й мінливістю психіки. Ускладнень додає і те, що судово-психологічна експертиза має специфічний, переважно ретроспективний характер, оскільки її об'єктом є події та стани, що вже відбулися. Просте перенесення актуальних на момент дослідження характеристик особистості на минулі обставини може призвести до методологічних помилок, адже психічні властивості змінюються під впливом життєвих подій, зокрема таких, що мають екстремальний характер.

У зв'язку з цим у процесі проведення експертного психологічного дослідження особлива увага має приділятися добору методів, здатних виявити стійкі, відносно стабільні риси особистості та відокремити їх від ситуативних або тимчасових проявів. Такий підхід забезпечує наукову обґрунтованість і достовірність висновків експерта, що особливо важливо в умовах сучасних соціальних трансформацій і воєнних викликів.

Результати. Зростання ролі системного знання у сучасній науці зумовлене як внутрішніми потребами розвитку психологічного пізнання, так і запитами практики. Поглиблення, диференціація та інтеграція наукового знання призвели до необхідності осмислення складних і багаторівневих структур людської психіки та поведінки, **особливо в умовах воєнного стану**, коли психологічні процеси набувають додаткової динаміки та напруження. У цьому контексті системний підхід став універсальним методологічним інструментом, що дозволяє розглядати об'єкти пізнання як цілісні утворення, в яких взаємозв'язки між елементами мають не менше значення, ніж самі елементи.

Сутність системного підходу полягає у вивченні явищ як динамічних систем, цілісність яких формується завдяки взаємодії складових частин. Ця цілісність є результатом інтеграції елементів, що забезпечує виникнення нових системних властивостей, не зведених до суми окремих характеристик. У науковому пізнанні кожна система може розглядатися як підсистема більшої системи, утворюючи багаторівневу ієрархічну структуру.

Поняття системного комплексу відображає ситуацію, коли декілька відносно самостійних, але взаємопов'язаних систем утворюють нове цілісне утворення. Так, у судово-психологічній експертизі особистість може виступати як окрема система, що включає когнітивні функції (увага, сприйняття, пам'ять, мислення), особистісні якості (характер, емоційні й мотиваційні процеси), поведінкові прояви, а також як елемент складнішого системного комплексу — наприклад «особистість – соціальне середовище – ситуаційні чинники». У межах таких комплексів об'єктом аналізу стають не лише індивідуально-психологічні особливості, а й характер взаємодії між учасниками події, соціальними умовами та емоційно-поведінковими реакціями, **що зазнають додаткових трансформацій під впливом воєнної ситуації** [1].

Принцип ієрархії систем у межах системного комплексу має особливе значення для судово-психологічної експертизи. Він дає змогу інтегрувати особистісні характеристики у ширший контекст міжособистісних і соціальних взаємодій, враховуючи вплив ситуаційних факторів, які можуть детермінувати як правомірну, так і девіантну поведінку. Система психічних явищ, у свою чергу, також має багаторівневу структуру, що включає когнітивну, регулятивну та

комунікативну підсистеми. Перша забезпечує процеси пізнання, друга — регуляцію діяльності та поведінки, а третя — реалізує соціальні форми взаємодії між людьми. Кожна з них взаємопов'язана і водночас може бути розділена на підсистеми нижчого рівня, що забезпечує динаміку і гнучкість психічного функціонування. Цілісність системи не є статичною — вона формується, трансформується або руйнується внаслідок дії внутрішніх і зовнішніх чинників. У контексті судово-психологічної експертизи це означає необхідність урахування динаміки особистісних змін, що відбуваються до, під час і після вчинку [1].

Об'єктом дослідження в судово-психологічній експертизі виступає особистість як учасник соціально-правових взаємодій і носій індивідуально-психологічних характеристик. Основним завданням експерта є виявлення закономірностей поведінки особистості в умовах певної категорії вчинку, а також побудова психологічного портрета підекспертної особи. Системний підхід у цьому контексті дозволяє простежити взаємозв'язки між соціальним середовищем, внутрішньою мотивацією, емоційним станом і конкретними формами поведінки [2].

Важливою перевагою системного підходу є можливість подолання лінійного детермінізму, який обмежує пояснення поведінки людини простим ланцюгом «причина – наслідок». Поведінка людини часто зумовлюється не однією причиною, а сукупністю взаємопов'язаних чинників, що діють на різних рівнях системи. Нелінійність системної детермінації дозволяє враховувати кумулятивний характер впливів (накопичення внутрішньої напруги, емоційних переживань, фрустрацій), які можуть призводити до афекту, стресу або дезадаптації [3].

В умовах воєнного стану психологічна система особистості зазнає додаткового навантаження, оскільки під впливом хронічного стресу, невизначеності, втрат і травматичних подій відбуваються глибокі зрушення у когнітивній, емоційній та мотиваційній сферах. Тривале перебування у стані напруги, небезпеки та соціальної нестабільності спричиняє порушення адаптаційних механізмів, що може проявлятися у дезорганізації поведінки, афективних вибухах або зміні системи цінностей і норм. Такі процеси ускладнюють роботу експерта, оскільки межа між ситуативною, травматично зумовленою реакцією та стійкими особистісними рисами стає розмитою. Тому аналіз психологічних особливостей у судово-психологічній експертизі в умовах війни потребує урахування посттравматичних змін, рівня емоційної стабільності та соціально-психологічної підтримки підекспертної особи.

Таким чином, для розкриття причинно-наслідкових зв'язків у поведінці особистості ключовим є поняття **системоутворювального чинника** — того елемента, який визначає організацію і спрямованість усієї системи. У межах судово-психологічного аналізу такими чинниками можуть бути мотиви, цілі, установки, емоційні стани або міжособистісні стосунки. Визначення системоутворювального чинника у полісистемі, до якої входять звинувачений, потерпілий, свідки та сам факт вчинку, дозволяє зрозуміти, яка саме взаємодія стала домінантною та зумовила поведінкові прояви учасників події.

Висновки. Отже, системний підхід у судово-психологічній експертизі забезпечує глибше розуміння закономірностей формування та прояву поведінки особистості у складних соціально-правових умовах. Він дозволяє розглядати індивіда не ізольовано, а як елемент цілісної, взаємопов'язаної структури, що охоплює внутрішні психологічні процеси, міжособистісні зв'язки та соціальне середовище. В умовах війни системний підхід набуває особливої значущості, адже дозволяє комплексно аналізувати трансформації психіки та поведінки людини під впливом екстремальних обставин, виявляючи як індивідуальні, так і соціальні механізми психологічної стійкості чи дезадаптації.

Література

1. Судово-психологічна експертиза : навч. посіб. / О. В. Землянська ; МВС України, Харків. нац. ун-т внутр. справ. – Х. : ХНУВС, 2012. – 300 с.

2. Землянська О. В. Особистість та методи її дослідження при проведенні судово-психологічної експертизи : моногр. / О. В. Землянська. – Х. : Титул, 2007. – 244 с.

3. Приходько Т. Фізіологічний афект – одна з підстав визнання особи обмежено осудною / Т. Приходько // Право України. – 2001. – № 1. – С. 53–55.

УДК 343.352(477)

АКТУАЛІЗАЦІЯ ПИТАНЬ НАУКОВО-МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ КОМПЛЕКСНОЇ СУДОВОЇ ВІЙСЬКОВОЇ ТА ВИБУХОТЕХНІЧНОЇ ЕКСПЕРТИЗИ У РОЗРІЗІ АГРЕСИВНИХ ДІЙ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ЩОДО СУВЕРЕНІТЕТУ УКРАЇНИ

Олександр КОЗЛОВ[1], e-mail: 1961.alex.kozlov@gmail.com, ORCID: 0009-0008-8893-7450
Роман МОМОТ[1], канд. техн. наук, ст. наук. співр., e-mail: mrmm@meta.ua, ORCID: 0000-0001-9483-2243
Олег КОЖУХАР[1], e-mail: olanko@ukr.net
Ігор ШЕБАЛКО[2], e-mail: shebalkov@ukr.net, ORCID: 0000-0002-8325-8327

[1]Київське відділення, Національний науковий центр
«Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України
[2]Науково-дослідний центр судової експертизи у сфері інформаційних технологій
та інтелектуальної власності Міністерства юстиції України

Вступ. Глобальне роззброєння та скорочення війська забезпечило російській федерації можливість переходу від політичного шантажу (1991 - 2013 роки) до дій у вигляді гібридної війни (2014 – 2022 роки), а в подальшому і до повномасштабної агресії щодо України (з 24.02.2022 і по цей час).

З початком повномасштабної військової агресії російської федерації (далі – рф) проти України, Указом Президента України було введено в країні правовий режим воєнного стану [1], що дозволило сконцентрувати всі зусилля нашої країни на протистоянні агресору. Активну участь у цьому приймають і науково-дослідні установи судових експертиз Міністерства юстиції України.

Слід зазначити, що проведення судових експертиз щодо наслідків військової агресії рф охоплює також ситуації загибелі і травмування військових та цивільних громадян України, руйнування об'єктів критичної та цивільної інфраструктури на території населених пунктів України. Враховуючи зазначене, уповноваженими органами призначаються комплексні судові військові та вибухотехнічні експертизи з метою дослідження дій збройних сил рф (військових посадових осіб) проти суверенітету та територіальної цілісності України з порушенням засобів і способів ведення бойових дій. Таким чином, проведення зазначених судових експертиз відбувається у тісній взаємодії експертів за спеціальностями 16.1 «Військові дослідження» та 5.2 «Дослідження вибухових пристроїв, слідів та обставин вибуху», що свідчить про актуальність розроблення експертної методики комплексних судових військових та вибухотехнічних експертиз.

Слід зазначити, що при організації проведення комплексних судових військових та вибухотехнічних експертиз, що пов’язані з дослідженнями дій збройних сил рф проти суверенітету та територіальної цілісності України з порушенням засобів та способів ведення бойових дій, утворюються унікальні для «Військової експертизи» об’єкт та предмет дослідження. Так, об’єктом судової військової експертизи можуть бути як матеріальні джерела інформації (зокрема, речові докази, наприклад: військове обладнання, зброя, сліди), документальні матеріали (карти, накази, відомості тощо), так і матеріалізовані джерела інформації – матеріали справи, фотоілюстрації, що мають значення для справи. Предметом судової військової експертизи є встановлення фактів за визначеними слідчим питаннями щодо ведення агресивної війни рф проти України такими засобами та способами, що не відповідають меті ведення бойових дій та нормативним актам (в тому числі національному законодавству рф) щодо обмеження засобів та методів ведення воєнних дій. Можливості вирішення окреслених завдань ускладнюються у зв’язку з відсутністю на сьогодні методик в Реєстрі методик проведення судових експертиз [2] щодо проведення комплексних судових військових та вибухотехнічних експертиз (досліджень) за військовими дослідженнями зі встановлення обставин застосування та дій збройних сил рф проти України як країни-агресора.

Відповідно до Науково-методичних рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень, затверджених наказом Мін'юсту України від 08.10.1998 р. № 53/5 [3], у VIII розділі «Військова експертиза», пункті 8.1. основним завданням військової експертизи на цей час є дослідження обставин застосування та дій військових формувань, які утворені у відповідності з законами України. В той же час у пункті 8.2 цього ж розділу відсутній орієнтовний перелік питань щодо дослідження обставин документального планування та підготовки ворога до ведення агресивної війни проти України із залученням військових формувань, а також встановлення причинно-наслідкових зв'язків щодо наслідків агресивної війни країни-агресора.

З огляду на викладену інформацію виникає необхідність щодо удосконалення нормативних актів, зокрема, внесення змін та доповнень до пунктів 8.1 та 8.2 зазначених Науково-методичних рекомендації.

Результати. З метою усунення прогалини у Національному науковому центрі «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України було ініційовано виконання науково-дослідної роботи за темою «Розробка методичних рекомендацій проведення судової військової експертизи щодо збройної агресії проти суверенітету та територіальної цілісності України», в якій запропоновано доповнити пункт 8.1 розділу VIII «Військова експертиза» Науково-методичних рекомендацій наступною інформацією:

«Основними завданнями судової військової експертизи при проведені дослідження щодо збройної агресії дій іноземних держав проти суверенітету та територіальної цілісності України є встановлення обставин застосування озброєння і військової техніки та дій військових службових осіб збройних сил агресора під час підготовки та ведення війни (бойових дій) проти суверенітету та територіальної цілісності України, що призвели до загибелі та поранення громадян, руйнування об'єктів критичної та цивільної інфраструктури».

Слід зауважити, що під час дослідження обставин застосування озброєння і військової техніки та дій військових службових осіб збройних сил агресора виникає необхідність проведення саме комплексних судових експертиз. В більшості випадків виконуються комплексні військові та вибухотехнічні дослідження. Це пов'язано із специфічними особливостями досліджуваних об'єктів та дослідженням їх наслідків чи встановленням причино-наслідкового зв'язку.

Водночас основними завданнями, що вирішуються при проведенні вибухотехнічних досліджень, є визначення виду вибухового пристрою чи боєприпасу, конструкції, призначення, принципу приведення в дію, способу виготовлення, а також бойових можливостей та розташування позицій зброї (озброєння) на місцевості, що використовує саме ці вибухові пристрої та боєприпаси.

Під час проведення експертом вибухотехнічного дослідження виникають певні труднощі. Останні полягають в тому, що огляд місця події, пов'язаного з вибухом, який стався у будівлі (або поруч) чи на відкритій ділянці місцевості, проводиться в умовах значного знищення та руйнування, спричиненого дією вибухового перетворення та ударною хвилею. А також можливий вплив на об'єкти інших чинників, таких як пожежа, забруднення чи зміна ландшафту.

У своїй практиці за даним видом дослідження експерт-вибухотехнік використовує наступні методи дослідження:

1. Візуальний огляд – оглядається уражений об'єкт та прилегла територія на наявність пошкоджень, уламків та залишків чи фрагментів ймовірного вибухового пристрою.

2. Інструментальний метод – з використанням спеціального обладнання оглядається уражена територія та об'єкт на предмет виявлення нерозірваних боєприпасів, фрагментів і уламків та проводиться оцінка стану конструкцій.

3. Лабораторний аналіз – здійснюється дослідження вилучених та наданих на дослідження об'єктів.

Враховуючи зазначене, авторами запропоновано типовий алгоритм (послідовність дій) використання судовими експертами за спеціальностями 16.1 та 5.2 нормативно-методичного забезпечення при проведені комплексної судової військової та вибухотехнічної експертизи (рис. 1).

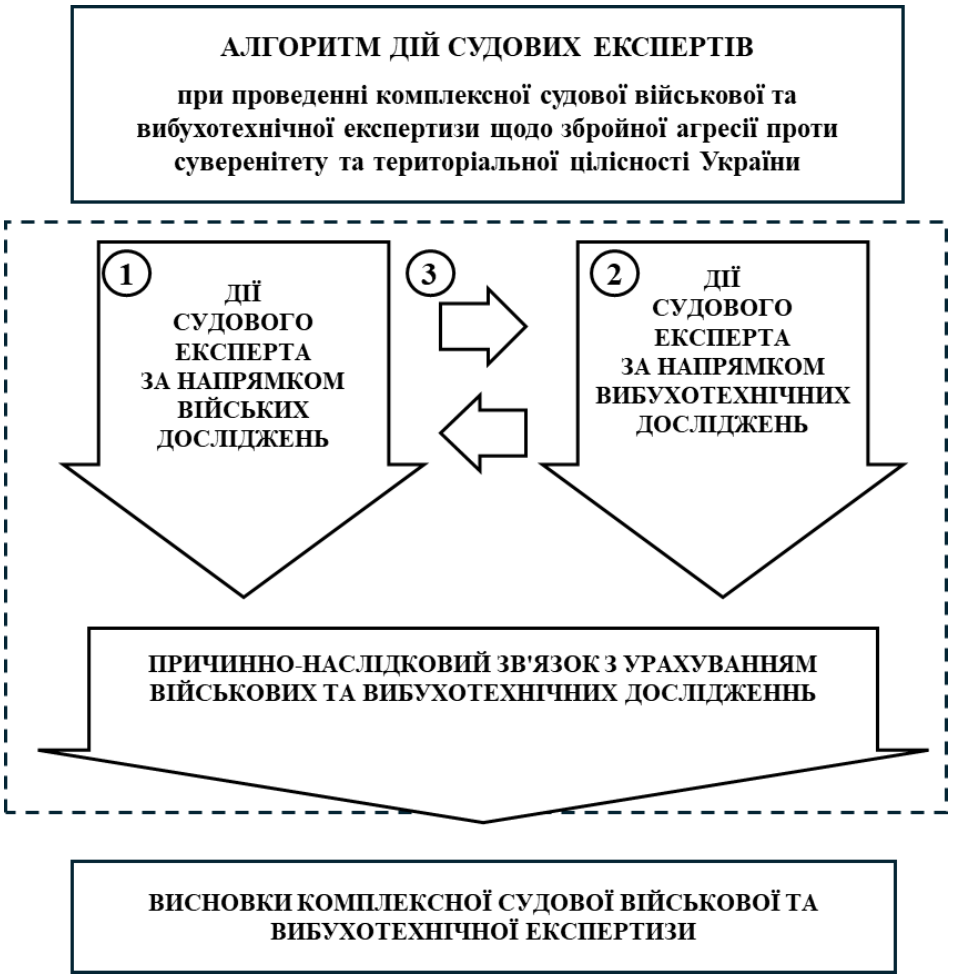
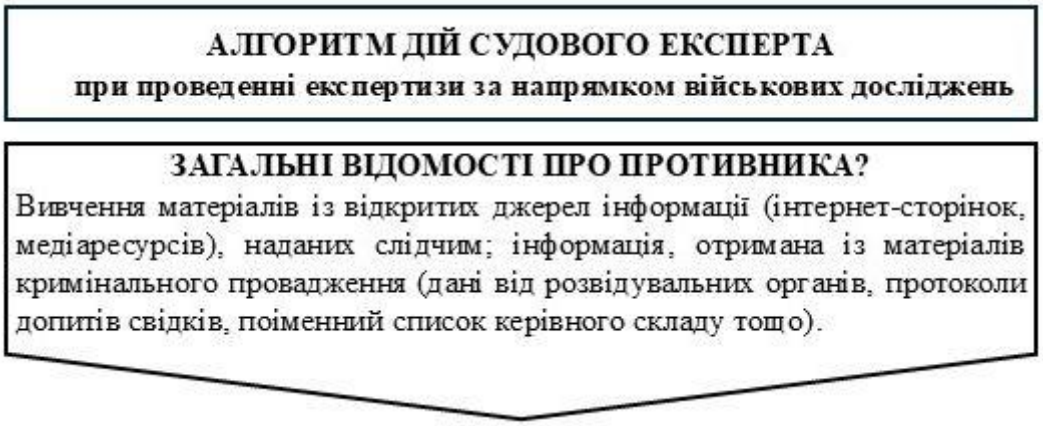


Рисунок 1 – Алгоритм дій судового експерта при проведенні комплексної судової військової та вибухотехнічної експертизи щодо збройної агресії проти суверенітету та територіальної цілісності України

Дії судового експерта за спеціальністю 16.1 при проведенні комплексної судової військової та вибухотехнічної експертизи щодо збройної агресії проти суверенітету та територіальної цілісності України за напрямом військового дослідження, висвітлено на рис. 2.



ЯК І ЯКІ САМЕ СЛУЖБОВІ І/АБО ПОСАДОВІ ОСОБИ КРАЇНИ АГРЕСОРА (ЯК ВІЙСЬКОВІ, ТАК І ЦИВІЛЬНІ) ЗДІЙСНЮВАЛИ ДОКУМЕНТАЛЬНЕ ПЛАНУВАННЯ ТА ПІДГОТОВКУ ДО ВЕДЕННЯ АГРЕСИВНОЇ ВІЙНИ ПРОТИ УКРАЇНИ?

Вивчення матеріалів кримінального провадження (дані від розвідувальних органів тощо); матеріали із відкритих джерел інформації (інтернет-сторінок, медіаресурсів), наданих слідчим; речові докази (мапи, інші документи планового, розпорядчого й керівного характеру.

ПІДТВЕРДЖЕННЯ ДОКУМЕНТАЛЬНОГО РОЗВ'ЯЗАННЯ ВОРОГОМ АГРЕСИВНОЇ ВІЙНИ ПРОТИ УКРАЇНИ?

Вивчення матеріалів кримінального провадження (дані від розвідувальних органів, бойові накази, розпорядження (шифротелеграми) частинам і підрозділам, рішення командирів частин, підрозділів щодо здійснення дій, мапи (робочі мапи, плани, схеми) рішень (маршрутів висування); протоколи допиту свідків тощо), матеріали із відкритих джерел інформації (інтернет-сторінок, медіаресурсів), наданих слідчим.

ЗА ЯКИХ ОБСТАВИН ТА ЯКІ САМЕ ВІЙСЬКОВІ ФОРМУВАННЯ (УГРУПУВАННЯ) КРАЇНИ АГРЕСОРА ВЧИНЯЛИ БОЙОВІ ДІЇ?

Матеріали кримінального провадження (дані від розвідувальних органів, бойові накази, розпорядження (шифротелеграми) частинам і підрозділам, рішення командирів частин, підрозділів щодо здійснення дій, мапи (робочі мапи, плани, схеми) рішень (маршрутів висування) тощо), матеріали із відкритих джерел інформації (інтернет-сторінок, медіаресурсів), наданих слідчим.

ЯКИЙ БУВ БОЙОВИЙ І ЧИСЕЛЬНИЙ СКЛАД ВІЙСЬКОВИХ ФОРМУВАНЬ КРАЇНИ АГРЕСОРА ТОЩО?

Матеріали кримінального провадження (дані від розвідувальних органів, списки (відомості) особового складу частини, підрозділу, журнал бойових дій частин, журнал обліку бойової підготовки, журнал обліку інструктажу особового складу, книга видачі зброї, план-завдання екіпажу (розрахунку, водію) машини, поіменний список інструктажу, список утрат особового складу (техніки), протоколи допиту свідків.

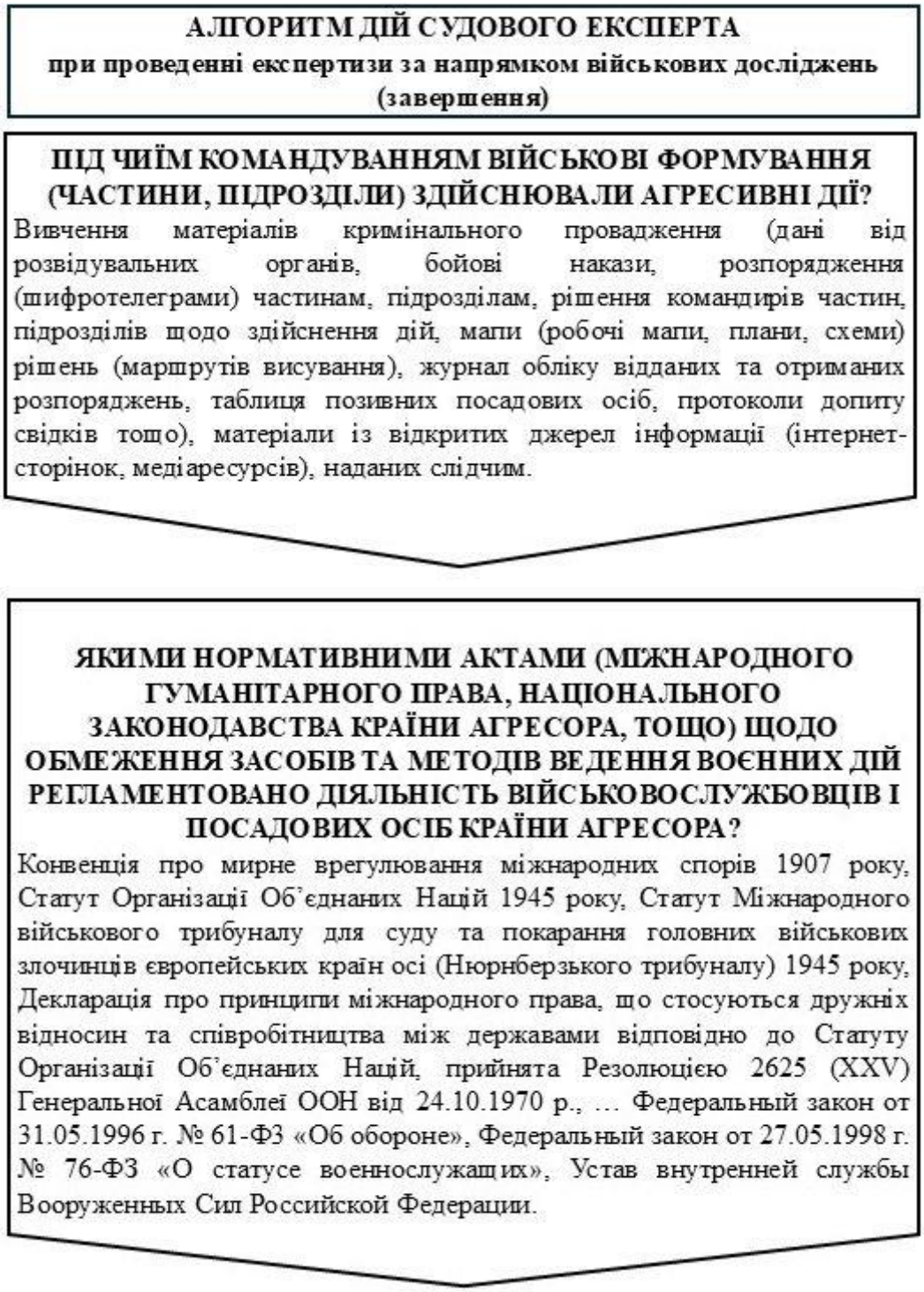


Рисунок 2 – Алгоритм дій судового експерта з вирішення орієнтовних питань під час проведення комплексної судової військової та вибухотехнічної експертизи щодо збройної агресії проти суверенітету та територіальної цілісності України за напрямком – військові дослідження

Дії судового експерта за спеціальністю 5.2 при проведенні комплексної судової військової та вибухотехнічної експертизи щодо збройної агресії проти суверенітету та територіальної цілісності України за напрямом вибухотехнічного дослідження, висвітлено на рис. 3.

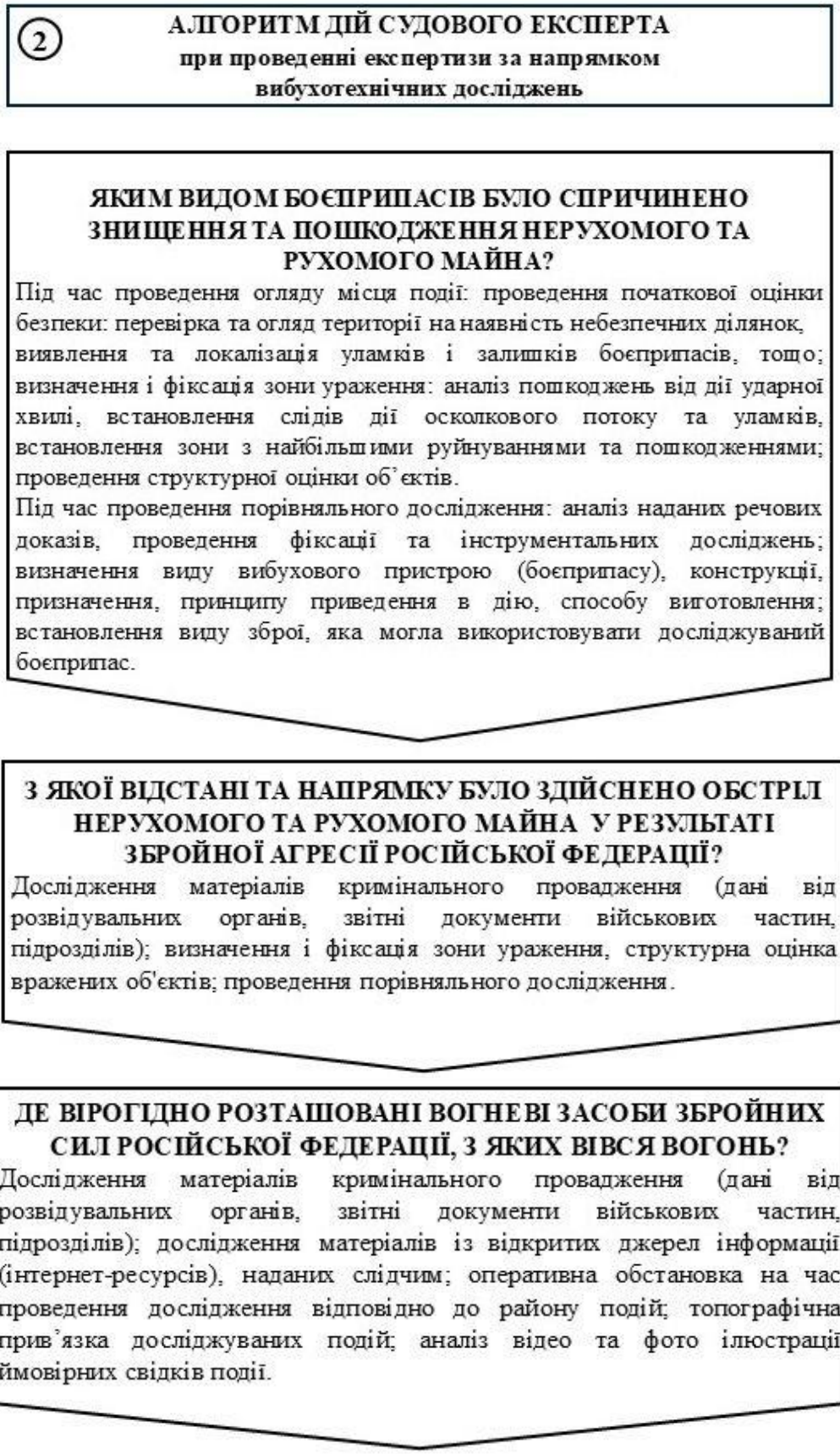


Рисунок 3 – Алгоритм дій судового експерта з вирішення орієнтовних питань під час проведення комплексної судової військової та вибухотехнічної експертизи щодо збройної агресії проти суверенітету та територіальної цілісності України за напрямком – вибухотехнічне дослідження

Якісна взаємодія між судовими експертами є запорукою своєчасного та ґрунтовного проведення комплексної судової військової та вибухотехнічної експертизи щодо збройної агресії проти суверенітету та територіальної цілісності України, враховуючи зазначене – авторами роботи запропоновано організаційні питання, якими доречно керуватись голові комісії при організації взаємодії між судовими експертами за спеціальностями 16.1 та 5.2 (рис. 4).

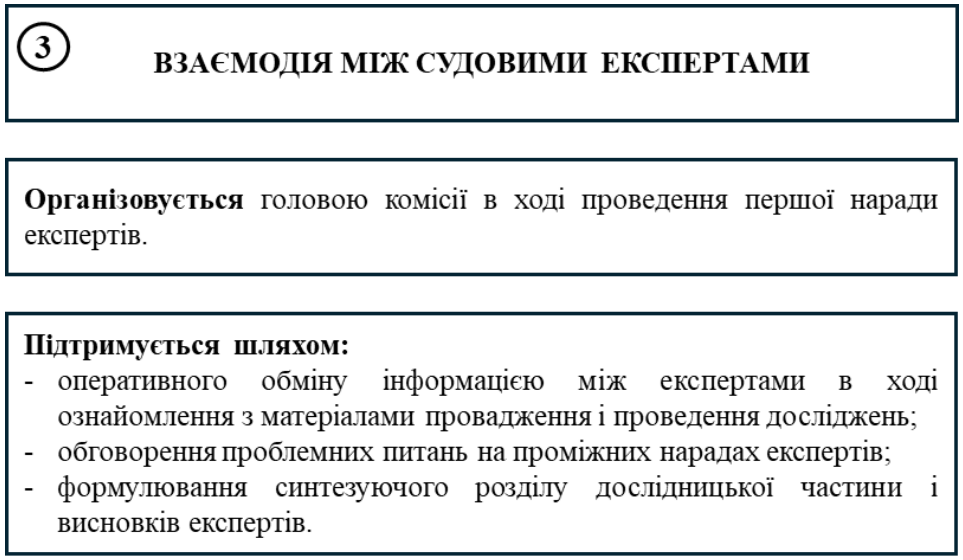


Рисунок 4 – Орієнтовні питання щодо якісної взаємодії між судовими експертами за спеціальностями 16.1 та 5.2

Зауважимо, що при проведенні комплексної експертизи керівник експертної установи доручає проведення досліджень відповідним підрозділам цієї установи, визначає, який з них є провідним. Керівник провідного підрозділу за погодженням з керівниками інших підрозділів – формує комісію експертів і призначає голову експертної комісії. Голова комісії виконує лише організаційні функції. Узагальнення та оцінка результатів окремих досліджень, які є підставою для формулювання висновків, повинні викладатися у синтезуючому розділі дослідницької частини висновку експерта.

Висновки. Таким чином, висвітлений алгоритм дій судових експертів при проведенні комплексної судової військової та вибухотехнічної експертизи щодо збройної агресії проти суверенітету та територіальної цілісності України (орієнтовні питання, нормативно-методичне забезпечення, а також питання взаємодії між експертами за спеціальностями 16.1 та 5.2) сприятиме судовим експертам у наданні повних та обґрунтованих відповідей на поставлені органами досудового розслідування питання та ефективному проведенню в подальшому інших процесуальних дій.

Література

1. Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 р. № 64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text (дата звернення 15.10.2025).

2. Реєстр методик проведення судових експертиз: вебсайт Міністерства юстиції України. URL: https://rmpse.minjust.gov.ua/search (дата звернення: 16.10.2025).

3. Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень: затв. наказ. Мін'юсту України від 08.10.1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 16.10.2025).

УДК 343.98

АКТУАЛЬНІ ПИТАННЯ ПРОВЕДЕННЯ СУДОВОЇ ЕКСПЕРТИЗИ З ОЦІНКИ МАЙНА І ТЕХНІКИ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ ТА ОЗБРОЄННЯ

Василь МАТВЕЇВ[1], e-mail: wwmatveevw@gmail.com

[1]Національний науковий центр «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України

Вступ. Одним з етапів при вирішенні завдань судової експертизи з оцінки військового майна (за експертною спеціальністю 12.5 «Оцінка майна і техніки військового призначення та озброєння») є ідентифікація об'єкта дослідження: встановлення типу, походження (країни виробника), технічних характеристик тощо, відповідно до класифікацій і стандартів в залежності від виду виробу.

Результати. Завдання, які ставлять перед експертом, це:

- визначення вартості наданих на дослідження об'єктів, які використовуються як військове майно;
- визначення типу та призначення наданих на дослідження об'єктів;
- визначення характеристик та властивостей наданих на дослідження об'єктів відповідно до Українського класифікатора товарів зовнішньоекономічної діяльності;
- визначення виробника, країни походження, року виготовлення (які вирішуються комплексно із залученням спеціалістів інших галузей знань, в тому числі з експертами трасологічних та балістичних видів досліджень);
- визначення змін показників якості наданих на дослідження об'єктів (які проводяться комплексно з відповідними фахівцями з експлуатації, ремонту та обслуговування майна військового призначення з метою надання Актів технічного стану, наприклад, із залученням фахівців з автомобільного, водного, авіаційного транспорту, інженерів військової техніки та озброєння та інших спеціалістів).

Судовими експертами оцінка військового майна проводиться на підставі Методики щодо визначення залишкової вартості майна Збройних Сил України та інших військових формувань (від 29.04.1998 №759), Методичних рекомендацій щодо визначення вартості військового майна, техніки та озброєння (КНДІСЕ, 2017 р.), Національного стандарту № 1 «Загальні засади оцінки майна і майнових прав» (від 10.09.2003 № 1440) та інших методик, нормативних актів, рекомендованих науково-технічних довідників та літератури.

Орієнтовний перелік питань, які вирішують судові експерти з оцінки військового майна, висвітлюється на сайтах експертних установ Міністерства юстиції України. Зокрема, до компетенції експертів-товарознавців відповідного напряму входять питання:

- яке найменування та призначення наданого на дослідження об'єкта?
- чи укомплектовано наданий на дослідження об'єкт відповідно до нормативно-технічної документації, а якщо ні, то в чому саме полягає неукомплектованість або невідповідність?
- який ступінь зносу наданого на дослідження об'єкта?
- яка залишкова вартість об'єкта дослідження (назва, марка, модель), що знаходився в експлуатації з (зазначається дата/період початку або строк експлуатації об'єкта дослідження, особливості об'єкта дослідження – витрати ресурсів, умови зберігання, категорії якісного/технічного стану, стан засобів тощо) станом на (зазначається дата оцінки)?
- яка ринкова вартість об'єкта станом на визначену дату (з урахуванням наданої експерту інформації щодо укладених угод купівлі-продажу аналогічних об'єктів на міжнародному ринку)?
- яка вартість ліквідації об'єкта станом на визначену дату?
- який розмір матеріальної шкоди, завданої у результаті пошкодження чи повного знищення об'єкта?

Вид озброєння та військової техніки, які є об'єктами дослідження експерта з оцінки військового майна, виокремлюються відповідно до їх цільового призначення за номенклатурою центральних органів забезпечення, а саме: ракетно-артилерійське озброєння, бронетанкове озброєння й техніка, автомобільна техніка, авіаційна техніка, техніка зв'язку та автоматизовані системи управління військами, засоби розвідки, повітряно-десантна техніка, засоби інженерного озброєння, озброєння та військова техніка і засоби радіаційного, хімічного та біологічного захисту, техніка радіоелектронної боротьби, технічні засоби вигорання, техніка тилу, медично-санітарна техніка, засоби наземного забезпечення польотів авіації, аеродромна техніка.

Слід зазначити, що перелік задач, які вирішують судові експерти зазначеного напряму, не є вичерпним, в кожному конкретному випадку слідством або судом можуть бути поставлені завдання, які мають більш вузьку направленість до військового майна, зокрема, щодо транспортних засобів: визначення ступеню зносу складової або виду ремонту, який необхідний для відновлення працездатності складової певного виду транспорту або виробу.

Під час проведення судової експертизи військового майна основними методичними підходами щодо визначення вартості є порівняльний і витратний. Оцінка товарів/виробів проводиться із застосуванням бази, що відповідає ринковій вартості або неринковим видам вартості. На даний час із 2022 року на проведення судових експертиз майна і техніки військового призначення та озброєння найчастіше органами досудового слідства ставляться завдання з визначення вартості матеріального збитку, завданого внаслідок пошкодження або повного знищення майна внаслідок військової агресії рф. При цьому експерти часто стикаються з проблемою відсутності будь-якої цінової інформації щодо об'єкта дослідження, яка необхідна для проведення товарознавчої експертизи з оцінки військового майна. Це обумовлюється, по-перше, відсутністю або обмеженою кількістю у загальнодоступних джерелах під час воєнного стану в країні цінової інформації про угоди купівлі-продажу різного роду військового майна та озброєння, по-друге, закритою інформацією щодо продажу або придбання Міністерством оборони України у профільних підприємств – спеціальних експортерів, які входять до складу Державного концерну «Укроборонпром». Водночас, враховуючи повномасштабне російське вторгнення в Україну, внаслідок потреби в озброєнні зріс попит на подібне майно, що впливає на співвідношення пропонування та попиту на ринку. Відповідно до цього під час проведення оцінки експертами враховуються ринкові коливання цін на подібне майно та інші фактори, що можуть призвести до змін у співвідношенні пропонування та попиту на подібне майно.

Важливим під час проведення оцінки військового майна є врахування істотних умов при проведенні досліджень по визначенню вартості будь-якого майна, визначення базових вихідних даних й проведення обов'язкових оціночних процедур, а саме:

- визначення мети, з якою проводиться оцінка;
- точна ідентифікація та класифікація майна;
- визначення виду вартості майна, яке оцінюється;
- визначення дати оцінки;
- окреслення методичних засад дослідження;
- обґрунтування застосованих припущень та обмежень;
- визначення фактору реального стану.

Вибір бази оцінки залежить від мети, з якою проводиться оцінка майна, його особливостей, а також нормативних вимог. Тобто, база оцінки – це комплекс методичних підходів, методів та оціночних процедур, що відповідають певному виду вартості майна. Для визначення бази оцінки враховуються мета оцінки та умови використання її результатів. Разом з цим слід зазначити, що визначення вартості майна та майнових прав регулюється Законом України «Про оцінку майна, майнових прав та професійну оціночну діяльність в Україні» (далі – Закон про оцінку) та здійснюється суб'єктами оціночної діяльності відповідно до нормативно-правових актів з оцінки майна: національних стандартів оцінки майна, що затверджуються Кабінетом Міністрів України, методик та інших нормативно-правових актів, які

розробляються з урахуванням вимог національних стандартів і затверджуються Кабінетом Міністрів України або Фондом державного майна України.

Діяльність судових експертів, пов'язана з оцінкою майна, здійснюється на підставах і в порядку, передбаченому Законом України «Про судову експертизу», з урахуванням особливостей, визначених Законом про оцінку щодо методичного регулювання оцінки майна. Таким чином судові експерти повинні дотримуватися положень національних стандартів оцінки майна під час здійснення експертних досліджень, суть яких полягає у визначенні вартості майна. Оцінка майна і майнових прав – це процес визначення їх вартості на дату оцінки за процедурою, яка встановлена нормативно-правовими актами, що регулюють питання вартості (ціни) майна та не повинна суперечити положенням (національним стандартам) з оцінки майна (стаття 9 Закону про оцінку).

Залишкова вартість майна Збройних Сил України, Служби безпеки України, Управління державної охорони, Національної гвардії України, Держприкордонслужби та інших утворених відповідно до законів військових формувань, Держспецзв'язку, а також майна МВС для цілей його відчуження, реалізації, утилізації, списання та оренди рухомого військового майна, визначається за методикою визначення залишкової вартості майна Збройних Сил України та інших військових формувань, затвердженою постановою Кабінету Міністрів України від 29 травня 1998 р. № 759. Для проведення визначення залишкової вартості військового майна у військових формуваннях утворюються комісії, до яких подаються документи, в яких міститься інформація про оцінюване військове майно, включаючи завірені належним чином копії формулярів, паспортів, актів технічного стану майна на дату оцінки, затверджених уповноваженими особами військових формувань, тощо.

Під час проведення судової експертизи військового майна основними методичними підходами щодо визначення вартості є порівняльний і витратний.

Оцінка товарів (виробів) проводиться із застосуванням бази, що відповідає ринковій вартості або неринковим видам вартості. Економічний (зовнішній) знос виробів зумовлений впливом соціально-економічних, екологічних та інших факторів на об'єкт оцінки. Визначення розміру матеріального збитку при знищенні об'єкту оцінки внаслідок підриву чи інших дій може бути здійснено шляхом розрахунку вартості ліквідації, яка може дорівнювати вартості металолому, кольорових металів або інших цінних матеріалів, які можна отримати у результаті переробки.

Із практики проведення судових експертиз та експертних досліджень з оцінки майна і техніки військового призначення та озброєння, експертам в більшості випадків недостатньо вихідних даних для ідентифікації об'єктів дослідження. Процес уточнення даних суттєво впливає на терміни виконання експертизи, оскільки експерту необхідно додатково направляти клопотання про надання додаткових матеріалів або уточнення вихідних даних з метою проведення об'єктивного та обґрунтованого товарознавчого дослідження. Тривалість експертизи з оцінки військового майна обумовлена також потребою вивчення і аналізу великої кількості наданих матеріалів. Наприклад, замовником експертизи зазначаються в питаннях та надаються документи про поставку боєприпасів без опису (назви) підривача, а саме: з повним зарядом боєприпасів чи зменшеним зарядом у комплекті із підривачем, з обмеженою чи збільшеною дальністю боєприпасів у комплекті з підривачем, типу заряду (розривний, метальний, піротехнічний, вишибний або їх поєднання). Водночас, до різного виду озброєння поставляються боєприпаси із різними підривачами залежно від їх призначення для ураження цілей, таких як: танків, гармат, гаубиць, мінометів, безвідкатних гармат, бойових машин, що суттєво впливає на вартість боєприпасів (рис. 1).

Загальний вигляд підривника					
Індекс підривника	**V-19-PF1**	**M211DS**	**КВ 9300**	**M12**	**M3-81**
Тип	ОФ	ОФ	О	ОФ	ОФ
До яких мін застосовується	MOD.63	M933D	М62П6	НЕ40М11	120-ЛМиСМ

Загальний вигляд підривника					
Індекс підривника	**AZ111A2**	**OFZ 1-15-9324**	**M/49/62**	**AF69**	**JVA 7575 is 72-23A**
Тип	ОФ	ОФ	ОФ	ОФ	ОФ
До яких мін застосовується	MORTAR SHELL HE	MMY03	M/50	HE120	JVA 1571

Загальний вигляд підривника					
Індекс підривника	**M783 PD/DLY**	**U2**	**PD M8100 (02-DM-19)**	**M51A5**	**PDB-332**
Тип	ОФ	ОФ	О	ОФ	О
До яких мін застосовується	M933A1	Nr.3	M530A1 (NT120 HE)	MOD 209	M-AE-85

Рисунок 1 – Різновиди підривників іноземного виробництва для 120-мм мін

Також, слід зазначити, що замовнику судової експертизи та судовому експерту необхідно звертати увагу у документах на інформацію (вихідні дані) в специфікаціях та додатках до договору про поставку боєприпасів і виробів, бо вони бувають, як складського зберігання так і поточного виробництва, що суттєво впливає на їхню вартість при укладанні договорів.

Зокрема: 1) складське зберігання боєприпасів (склад військової частини, який призначений для здійснення прийому, зберігання та забезпечення майном та технічними засобами номенклатури речового забезпечення підрозділів військової частини та особового складу); 2) поточне виробництво (спосіб організації виробництва, яке характеризується розчленуванням виробничого процесу на окремі, відносно короткі операції, що виконуються на спеціально обладнаних потокових лініях).

Висновки. Вихідні дані про комплектування боєприпасів різними підривачами залежно від їхнього призначення для ураження цілей до різного виду озброєння, умови складського зберігання або поточного виробництва боєприпасів – суттєво впливають на їхню вартість при наданні судовими експертами висновку. З метою повноти дослідження характеристик боєприпасів та інших виробів військового призначення, що дозволить провести найбільш точне визначення вартості майна, доцільним є залучення фахівців-інженерів, які спеціалізуються на питаннях сучасного військового озброєння, до проведення комплексних судових експертиз.

Література

1. Про затвердження Методики визначення залишкової вартості майна Збройних Сил України та інших військових формувань : Постанова Кабінету Міністрів України; Методика, Форма типового документа, Акт, Порядок від 29.05.1998 № 759. URL: https://zakon.rada.gov.ua/go/759-98-%D0%BF.

2. Про затвердження Національного стандарту № 1 "Загальні засади оцінки майна і майнових прав" : Постанова Кабінету Міністрів України; Стандарт від 10.09.2003 № 1440. URL: https://zakon.rada.gov.ua/go/1440-2003-%D0%BF.

3. Про оцінку майна, майнових прав та професійну оціночну діяльність в Україні : Закон України від 12.07.2001 № 2658-III. URL: https://zakon.rada.gov.ua/go/2658-14 .

4. Довідник щодо використання мінометних пострілів та мінометів різних виробників, наданих країнами-партнерами. СВП 07-(07)274. 2023. URL: https://ru.scribd.com/document/737264719/%D0%94%D0%BE%D0%B2%D1%96%D0%B4%D0%BD%D0%B8%D0%BA-%D0%B7-%D1%96%D0%BD%D0%BE%D0%B7%D0%B5%D0%BC%D0%BD%D0%B8%D1%85-%D0%BC%D1%96%D0%BD-%D0%A7%D0%B5%D1%82%D0%B2%D0%B5%D1%80%D1%82%D0%B0-%D0%A0%D0%B5%D0%B4%D0%B0%D0%BA%D1%86%D1%96%D1%8F

УДК 504.61:355.012(477)

ВПЛИВ ЗБРОЙНОЇ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ НА ЛІСОВІ РЕСУРСИ УКРАЇНИ

Ігор МАЛІК[1], науковий співробітник, судовий експерт, e-mail: IAM4@i.ua, ORCID: 0009-0009-3061-7048
Аліна МІМА[1], завідувач відділу, судовий експерт, e-mail: alina.chemistry17@gmail.com, ORCID: 0009-0008-1869-6516
Тетяна ПЕТРЕНКО[1], старший судовий експерт, e-mail: tpetrenko996@gmail.com, ORCID: 0009-0008-9128-0015

[1]Національний науковий центр «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України

Вступ. Повномасштабна збройна агресія російської федерації проти України, що триває з 2022 року, спричинила безпрецедентні екологічні наслідки для довкілля, зокрема — для лісових ресурсів. Ліси України виконують важливі екологічні, економічні та соціальні функції, однак унаслідок бойових дій вони зазнали значних втрат. Зруйновані екосистеми, пожежі, мінування територій, незаконні рубки та забруднення ґрунтів — усе це призводить до деградації лісових ландшафтів, втрати біорізноманіття та погіршення стану природного середовища в цілому.

У ході бойових дій лісові масиви зазнають безпосереднього механічного пошкодження. Обстріли, артилерійські снаряди та авіаційні бомби руйнують стовбури, гілля і кореневі системи дерев. Значні площі лісів були знищені внаслідок пожеж, які виникають під час обстрілів або вибухів. Проблема гасіння таких пожеж ускладнюється мінуванням територій та наявністю великої кількості вибухонебезпечних предметів, що унеможливлює оперативне втручання працівників ДСНС і лісової охорони.

Окремою проблемою є незаконні рубки на тимчасово окупованих територіях та вивезення деревини до російської федерації. Це не лише завдає прямих економічних збитків, але й сприяє порушенню природного відновлення лісів, ерозії ґрунтів та зміні гідрологічного режиму територій.

Крім того, бойові дії призводять до порушення екологічних функцій лісів — знижується здатність поглинати вуглекислий газ (CO_2), зменшується водоохоронна та ґрунтозахисна роль, а також деградують середовища існування диких тварин. Унаслідок знищення лісових екосистем втрачається біорізноманіття, гинуть популяції видів, занесених до Червоної книги України, та руйнуються природні ландшафти унікальних заповідних територій.

Відновлення пошкоджених лісів є тривалим і складним процесом, що потребує значних фінансових, технічних і людських ресурсів, а також безпечного доступу до територій. На сьогодні багато ділянок залишаються небезпечними через мінування, що унеможливлює проведення робіт із лісовідновлення. Це, своєю чергою, має соціально-економічні наслідки — зменшується ресурсна база лісового господарства, громади втрачають робочі місця та джерела доходів, погіршуються умови життя населення в прифронтових регіонах.

Результати. За даними Державної екологічної інспекції України, станом на середину жовтня 2025 року загальні збитки, завдані довкіллю внаслідок збройної агресії РФ, становлять 5 967 154 423 890 грн. Зокрема, збитки від лісових пожеж на площі 142,5 тис. га оцінюються у 777,5 млрд грн, забруднення ґрунтів — у 21,8 млрд грн, а пошкодження рослинного світу, включно з територіями природно-заповідного фонду, — у 273,4 млрд грн.

Для визначення шкоди та збитків, завданих лісовому фонду, діє Постанова Кабінету Міністрів України № 326 від 20.03.2022 р. «Про затвердження Порядку визначення шкоди та збитків, завданих Україні внаслідок збройної агресії російської федерації» [1]. Згідно з цим документом, втрати лісового фонду включають пошкодження та знищення лісів і лісових ділянок, обмеження прав користування земельними ділянками, втрати лісогосподарського виробництва та неодержані доходи від використання лісових ресурсів.

Крім того, Методика визначення шкоди та збитків, заподіяних лісовому фонду, затверджена наказом Міністерства захисту довкілля та природних ресурсів України від 05.10.2022 № 414 [2], конкретизує підходи до оцінювання шкоди. До складу втрат включаються:

– пошкодження лісових насаджень, розсадників, захисних смуг і мисливських угідь;

– втрати лісопродукції та доходів від рубок;

– збитки мисливського господарства (знищення біотехнічних споруд, загибель тварин);

– витрати на підготовку ґрунтів і створення лісових культур.

Фіксація фактів пошкодження та розрахунок збитків здійснюється комісіями, які створюються місцевими державними або військовими адміністраціями. До їхнього складу входять представники лісокористувачів, органів Держекоінспекції, ДСНС, Держгеокадастру, правоохоронних органів тощо. Такі комісії проводять обстеження територій, використовують дані дистанційного зондування Землі, висновки експертів, а також інформацію з офіційних джерел і повідомлення громадян.

Висновки. Таким чином, збройна агресія російської федерації завдала масштабної шкоди лісовим ресурсам України, наслідки якої матимуть довготривалий характер. Руйнування лісів, забруднення територій, втрата біорізноманіття та порушення екологічних функцій лісових екосистем становлять серйозну загрозу для національної екологічної безпеки.

Надзвичайно важливо забезпечити системне фіксування фактів пошкоджень, об’єктивне визначення розміру збитків та підготовку доказової бази для подальшого стягнення компенсацій з держави-агресора. Одночасно необхідно розробити довгострокові програми лісовідновлення, розмінування територій і підтримки постраждалих громад, що дозволить відновити екологічну рівновагу та сталий розвиток лісового господарства України.

Література

1. Про затвердження Порядку визначення шкоди та збитків, завданих Україні внаслідок збройної агресії російської федерації: Постанова Кабінету Міністрів України від 20.03.2022 № 326 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/326-2022-п (дата звернення: 23.10.2025).

2. Про затвердження Методики визначення шкоди та збитків, заподіяних лісовому фонду внаслідок збройної агресії російської федерації: Наказ Міндовкілля від 05.10.2022 № 414 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/z1308-22 (дата звернення: 23.10.2025).

УДК 343.98

СПОРИ ЩОДО ВИЗНАЧЕННЯ МІСЦЯ ПРОЖИВАННЯ ДІТЕЙ ПРИ РОЗЛУЧЕННІ БАТЬКІВ: РОЛЬ ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ПСИХОЛОГІЧНИХ ЗНАНЬ

Наталія ТОКАР[1], канд. юрид. наук, e-mail: tnv.poshta@gmail.com

[1]Суддя Чечелівського районного суду міста Дніпра

Вступ. Одним з негативних наслідків війни є збільшення числа розлучень, умовами яких стають тривале окреме проживання подружжя внаслідок переїзду дружини з дітьми за межі України та неможливість батька навіщати родину в іншій країні, наявність додаткових побутових, фінансових проблем та емоційне виснаження тощо. Суд є тією інстанцією та останнім інструментом, який допомагає вирішити той чи інший сімейний спір, який сторони не можуть розв'язати самостійно. Процес розлучення між батьками суттєво зачіпає інтереси дітей та має відбутися таким чином, щоб після ухвалення рішення суду у справах про розірвання шлюбу батько і матір продовжували виконувати свої батьківські обов'язки і співпрацювали один з одним не на шкоду дитині.

Багато з батьків помилково вважають, що після розлучення дитині буде достатньо лише їхньої участі у вихованні, а участь іншого з батьків є не важливою, або що саме вони є кращими, більше розуміють потреби дитини, мають більше досвіду у вихованні, часу для дитини тощо. Але такі уявлення не завжди є об'єктивними і обґрунтованими, не враховують потреби, інтереси та почуття дитини. Нерідкими є і випадки використання батьками своїх дітей як інструменту помсти, або досягнення корисливих цілей. А під час війни прагнення одного з батьків залишити проживати із собою дитину за рішенням суду може бути викликано намаганням уникнути мобілізації.

Таким чином, ухваленню рішення має передувати ретельний аналіз обставин життя дитини і її батьків. А особливість судових проваджень у справах про розлучення батьків полягає в тому, що не зважаючи на змагальність і суперництво сторін (позивача і відповідача), вони мають об'єднати свої дії, щоб сприяти виваженому судовому рішенню, яке, в першу чергу, буде будуватися не на амбіціях, а виходити з інтересів їх дітей.

Результати. Під час розгляду такої категорії справ як сімейні спори кожен суддя намагається зосередити увагу сторін, батька і матері, на важливих питаннях правового та неправового характеру, та спрямувати їх до конструктивного вирішення спільних питань щодо подальшої участі у вихованні дітей.

Адвокати, які спеціалізуються на розгляді сімейних справ, в свою чергу, також відіграють надзвичайно важливу роль у вирішенні сімейних спорів, намагаючись підтримувати сторони в прийнятті розумних рішень на всіх стадіях розгляду справи. Сімейний адвокат навіть може допомогти сторонам уникнути звернення до суду, залученню дитини до перебігу судового процесу та досягти гармонійного результату, який буде задовольняти кожну сторону, зокрема, й щодо порядку участі у вихованні спільних дітей. Одним із шляхів досудового вирішення питання розлучення є закріплення домовленостей щодо розв'язання сімейного спору у нотаріуса, який в межах своєї компетенції має право на посвідчення тих чи інших правочинів.

Щодо судової практики, Верховний Суд постійно наголошує на тому, що згідно із законом на суд покладений обов'язок при вирішенні спорів щодо участі одного з батьків у вихованні дитини, визначення місця проживання дитини, відібрання дитини, позбавлення та поновлення батьківських прав, побачення з дитиною матері, батька дитини, які позбавлені батьківських прав, відібрання дитини від особи, яка тримає її у себе не на законних підставах або не на основі рішення суду, враховувати факти вчинення домашнього насильства як стосовно дитини, так і у присутності дитини. Тобто, в разі посилання учасників сімейного спору на факти вчинення одним із подружжя домашнього насильства обов'язково слід перевіряти інформацію, чи відбувалося домашнє насильство щодо дитини або у її присутності, які умови та обставини передували цьому, які наслідки мали місце та ін.

Так само і Європейський Суд з прав людини звертає увагу на те, що при ухваленні рішень щодо обмеження права батьків на спілкування з дитиною національні органи влади зобов'язані враховувати встановлену історію домашнього насильства як відповідний і обов'язковий фактор, який повинен бути зважений під час оцінки.

Необхідним доказом у відповідній категорії справ стає висновок судового експерта-психолога, завданням якого є з'ясування психічного стану дитини, її властивостей, інтересів та характеру взаємовідносин з кожним з батьків, а також інших обставин в родині та їх впливу на дитину, її розвиток та психічний стан.

Так, у справі № 755/5133/20 від 02.07.2025 Верховний суд встановив наступне. Сторони перебували у шлюбі, який було розірвано рішенням суду. Від шлюбу сторони мають двох дітей. За домовленістю сторін після розірвання шлюбу одна дитина вирішила проживати разом з батьком, інша – з матір'ю. Також сторони домовилися, що батько буде проводити з сином, який проживав з матір'ю, певний час кожної неділі. Одного разу батько взяв сина для проведення з ним відведеного за усною домовленістю часу, проте останній повертатися до місця свого проживання до матері відмовився. З висновку судово-психіатричної та психологічної експертизи суди встановили, що психічний розвиток дитини не відповідає віковій нормі. Таке уповільнення психічного розвитку вказує на педагогічну занедбаність. На момент дослідження у дитини наявні важкі для неї переживання, з якими вона не може впоратися через вікову незрілість психіки, інтенсивність психотравмуючих подій. Аналіз усієї сукупності даних, виявлених у ході психологічного дослідження, дозволяє стверджувати, що мати не несла відповідальності і не задовольняла основні потреби свого сина: у повазі до нього, в емоційному контакті, спілкуванні з ним, достатньому інформаційному і сенсорному просторі для пізнавального розвитку, не турбувалася про психологічну безпеку і переживання суб'єктивного благополуччя своєї власної дитини. Своїх батьків дитина не сприймає як подружню пару, виявляє надійну прихильність до свого батька, якість турботи якого забезпечила у дитини почуття безпеки та стабільності. При спільному проживанні з батьком дитина знаходиться у сприятливих для нього умовах проживання і виховання. У взаємодії з матір'ю дитина знаходиться у стані емоційної напруги, стресу, що перешкоджає відчуттю безпеки і благополуччя і не може бути сприятливим для неї та її особистісного розвитку. На час проведення дослідження спостерігаються виражені негативні зміни психоемоційного стану (нестійкість настрою, емоційна лабільність, виражена ситуативна тривожність, негативізм), які є проявом психотравмуючого впливу виховної поведінки матері та обраного нею способу вирішення сімейного конфлікту.

Орган опіки та піклування надав висновок про доцільність визначення місця проживання малолітньої дитини разом з батьком.

Під час розгляду справи дитина висловила бажання проживати з батьком та братом, з яким у нього гарні відносини. Щодо матері – вважав її недоброзичливою.

Ухвалюючи рішення у цій справі, суд керувався інтересами самої дитини, враховуючи, у тому числі, сталі соціальні зв'язки дитини, теплі стосунки зі старшим братом, його психологічний стан, зокрема, прихильність до батька, тривале проживання з ним, відносини між батьком та дитиною, зокрема, сумлінне ставлення батька до виконання батьківських обов'язків, виховання дитини в атмосфері турботи і любові, те, що дитина вже має своє оточення, забезпечена всім необхідним та має належні умови проживання, на підставі чого дійшов висновку про те, що саме батько забезпечить кращі інтереси сина з метою реалізації його прав на освіту, всебічний розвиток, здоров'я, виховання в оточенні любові і поваги [1].

За наведених умов таке рішення відповідає якнайкращим інтересам дитини, які мають першочергове значення для вирішення спору, тому визначення місця проживання сина з батьком за обставин цієї справи є пропорційним меті забезпечення зазначених інтересів дитини.

При цьому судом враховано, що мати дитини, безсумнівно, відіграє важливу роль у житті та розвитку дитини, має право та обов'язок піклуватися про здоров'я дитини, стан її розвитку, незалежно від того, з ким дитина буде проживати, однак при розгляді цієї справи не

встановлено обставин, які б давали підстави для висновку щодо доцільності проживання дитини з матір'ю, яке фактично призведе до зміни місця її проживання у звичному для дитини середовищі, і не буде мати більш позитивний вплив на дитину. Водночас, у разі зміни обставин у відносинах сторін спору визначене у справі місце проживання дитини може бути змінене як за згодою батьків, так і в судовому порядку.

Висновки. Кожна ситуація під час розгляду судових спорів щодо розлучення батьків і визначення місця проживання дитини й участі батьків у її вихованні повинна ґрунтуватися на всебічному аналізі як особистості сторін спору і дитини, так і характеру стосунків між ними, для з'ясування яких має бути призначена судова психологічна або комплексна судова психіатрична та психологічна експертиза, висновки яких мають бути оцінені в сукупності з іншими доказами у справі (показаннями сторін, свідків, документів тощо).

Література

1. Постанова Касаційного цивільного суду Верховного суду від 02.07.2025 у справі № 755/5133/20. Єдиний державний реєстр судових рішень: електронна платформа. [Електронний ресурс]. – Режим доступу: https://reyestr.court.gov.ua/Review/128685571 (дата звернення: 12.10.2025).

УДК 343.98

ПРОБЛЕМНІ ПИТАННЯ ОРГАНІЗАЦІЇ ПРОВЕДЕННЯ ДОДАТКОВИХ, ПОВТОРНИХ, КОМІСІЙНИХ ТА КОМПЛЕКСНИХ СУДОВИХ ЕКСПЕРТИЗ В КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Євген ЯРЕМЕНКО[1], e-mail: donetsk_ndekc@ukr.net
Вікторія АЛЄКСЄЙЧУК[1], канд. юрид. наук, доцент, e-mail: alexeychukviktoriya@gmail.com, ORCID: 0000-0001-7579-3322
Євгенія ДЕМИДОВА[1], канд. юрид. наук, доцент, e-mail: d.e.e@ukr.net, ORCID: 0000-0002-5049-7946

[1]Київське відділення, Національний науковий центр
«Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України

Вступ. Законодавство, яким керуються замовники судових експертиз та судові експерти складається із процесуальних норм (процесуальні кодекси), Закону України «Про судову експертизу» та відомчих інструкцій, які визначають порядок призначення і проведення судових експертиз. При цьому одні й ті самі питання в кожному із зазначених нормативно-правових актів розглянуті по-різному, або не врегульовані взагалі, що призводить до неоднозначної практики їх застосування, а в суді може бути розцінене як порушення процесуального характеру під час організації і проведення експертизи, що може призводити до негативних наслідків – визнання висновку експерта недопустимим доказом.

Результати. Одним з таких проблемних питань на сьогодні є можливість проведення додаткових, повторних, комісійних та комплексних експертиз в кримінальному провадженні. Так, в Законі України «Про судову експертизу» взагалі відсутнє визначення поняття, процедури призначення і проведення відповідних видів експертиз, водночас у статті 4 згаданого Закону серед гарантій незалежності судового експерта та правильності його висновку зазначено «можливість призначення повторної експертизи». Кримінальний процесуальний кодекс України (далі – КПК України) також не містить відповідних положень про такі види експертиз, а обмежується лише загальними підставами призначення судової експертизи у кримінальному провадженні: на стадії досудового розслідування (ст. 242 КПК України «Підстави проведення експертизи») та стадії судового розгляду (ст. 332 КПК України «Проведення експертизи за ухвалою суду») [1]. В цій частині в інших видах судових проваджень детально регламентовано особливості призначення та проведення додаткових, комісійних, повторних та комплексних експертиз (Цивільний процесуальний кодекс України – статті 111 – 113, Господарський процесуальний кодекс України – статті 105 – 107, Кодекс адміністративного судочинства України – статті 109 – 111).

Відомчі підзаконні нормативно-правові акти, видані державними органами, якими утворені спеціалізовані експертні установи, розглядають поняття, підстави і порядок проведення первинних, додаткових, повторних, комісійних та комплексних експертиз, не обмежуючи їх якимись окремими видами судових проваджень. Такі норми, зокрема, містяться в Інструкції про призначення та проведення судових експертиз та експертних досліджень, затвердженої наказом Міністерства юстиції України № 53/5 від 08.10.1998 р. (далі – Інструкція № 53/5), у пунктах: 1.2.13, 3.6 – 3.8, 4.4 – 4.9, 4.12, 4.13, 4.16, 4.17 [2]. У зв'язку із вказаними розбіжностями законодавства деякі судові експерти та керівники експертних установ вважають, що у кримінальному провадженні не можна виокремлювати повторні, додаткові, комісійні та комплексні експертизи, при цьому фактично допускають проведення експертиз, до яких залучаються декілька експертів, у тому числі різних галузей знань (експертних спеціальностей), а також експертиз із вирішення додаткових питань або дослідження додаткових об'єктів (або вирішення тих самих питань за тими самими об'єктами) за раніше проведеними експертизами, без зазначення у найменуванні відповідного виду (категорії) експертизи. В подальшому такі висновки експертів неоднозначно сприймаються сторонами,

судом, а також дисциплінарною комісією (дисциплінарна палата Центральної експертно-кваліфікаційної комісії, що діє при Міністерстві юстиції України).

Другим проблемним питанням є неоднозначність підходів щодо права керівника експертної установи (або експерта) самостійно змінити вказаний замовником вид експертизи, який визначений неправильно. Наприклад: а) експертизу призначено як повторну, але при цьому формулювання поставлених питань має відмінності в порівнянні з тими, які вирішувались під час первинної експертизи, або на дослідження надано додатковий документ, чи не надано висновок первинної експертизи; б) експертизу призначено як додаткову, але завданням є проведення повноцінного дослідження інших об'єктів у справі, яке не пов'язане із попереднім дослідженням; в) експертизу призначено як комплексну, але експертне завдання не має інтеграційного характеру, а може бути вирішено шляхом послідовного проведення експертиз різних напрямів (товарознавчої, а далі – економічної, будівельно-технічної, а на її підставі – економічної тощо).

Особливої актуальності питання зміни виду експертизи набуло з часу внесенням змін до Інструкції № 53/5 наказом Міністерства юстиції України від 20.01.2021 № 243/5 «Про затвердження Змін до деяких нормативно-правових актів з питань судово-експертної діяльності». Так відповідними змінами із Інструкції № 53/5 було виключено пункт 4.2, яким передбачалося, що: «У разі, коли призначена первинна, додаткова, повторна або комплексна експертиза за процесом дослідження чи наданими об'єктами не є такою по суті, керівник експертної установи організовує проведення відповідної експертизи, а у вступній частині висновку зазначаються мотиви зміни її процесуального визначення до законодавства» [3]. Тобто до 02.02.2021 року (дата набуття чинності змінами) керівник експертної установи мав право організовувати проведення додаткових, повторних, комісійних та комплексних судових експертиз самостійно, виходячи зі змісту поставленого експерту завдання (питання), особливостей процесу дослідження та наданих об'єктів. На сьогодні такі повноваження у керівника експертної установи та експерта відсутні.

За таких умов судові експерти після ознайомлення з документом про призначення експертизи та наданими на дослідження матеріалами кримінальних проваджень змушені заявляти клопотання про зміну категорії судової експертизи (уточнення змісту експертного завдання), що в свою чергу передбачає внесення змін до постанов, ухвал та заяв про призначення (доручення проведення) судової експертизи. Варто зауважити, що практика розгляду таких клопотань не є однозначною. Зокрема, мають місце випадки відмови здебільшого судів щодо винесення ухвал у зміненій редакції (скасування попередньої ухвали та прийняття нової), з підстав відсутності глибоких знань щодо особливостей проведення різних видів експертиз. Крім цього, процедура направлення і розгляду клопотань призводить до затягування строків проведення судових експертиз та неможливості своєчасного захисту особи, суспільства та держави від кримінальних правопорушень, порушених прав, свобод та законних інтересів учасників кримінального провадження.

Тобто між нормами КПК України та Інструкції 53/5 є неузгодженість, яка суттєво ускладнює визначення і зміну категорії судової експертизи як судовими експертами, так і замовниками експертиз, що призводить до неоднакової практики в оформленні висновків експертів, постанов, ухвал про призначення та заяв про проведення судових експертиз.

Неузгодженість між чинними нормативно-правовими актами з одного й того самого питання створює ситуацію вибору, на яку поширюються загальні правила:

1. У разі існування неузгодженості між нормами, виданими одним і тим самим нормотворчим органом, застосовується акт, виданий пізніше, навіть якщо прийнятий раніше акт не втратив своєї чинності.

2. У разі існування суперечності між актами, прийнятими різними за місцем в ієрархічній структурі органами – вищим та нижчим, застосовується акт, прийнятий вищим органом, як такий, що має більшу юридичну силу (наприклад, застосовується норма закону, якщо вона суперечить або не співпадає з нормою наказу органу виконавчої влади).

3. При розбіжності між загальним і спеціальним нормативно-правовим актом перевага надається спеціальному, якщо він не скасований виданим пізніше загальним актом [4].

Відповідно до статті 66 Закону України «Про правотворчу діяльність» колізія норм права може полягати у протиріччі або невідповідності між нормами права у нормативно-правових актах, що регулюють одні й ті самі суспільні відносини. Протиріччя між нормами права у нормативно-правових актах – це колізія норм права в нормативно-правових актах рівної юридичної сили. Невідповідність між нормами права у нормативно-правових актах – це колізія норм права в нормативно-правових актах різної юридичної сили.

У разі виявлення колізії між нормативно-правовими актами різної юридичної сили пріоритет у застосуванні мають норми, що містяться у нормативно-правовому акті вищої юридичної сили [5]. Але акт вищої юридичної сили в розглянутій ситуації – КПК України взагалі не містить норм щодо призначення додаткових, комісійних, повторних, комплексних судових експертиз, на відміну від підзаконного нормативно-правового акту – Інструкції № 53/5, яка передбачає їх проведення.

Висновки. З метою усунення умов (невідповідностей у законодавстві), які ускладнюють процес належного проведення судових експертиз та уникнення експертних проступків та помилок доцільним вбачається:

1. Застосувати уніфікований підхід щодо визначення видів (категорій) експертиз, порядку їх призначення та проведення, який буде однаковим для експертних установ (експертів) різної відомчої підпорядкованості та в різних видах проваджень (кримінальному, цивільному, господарському, адміністративному). Вказане можливо забезпечити шляхом доповнення базового Закону України «Про судову експертизу» додатковими статтями відповідного змісту: «Додаткова експертиза», «Повторна експертиза», «Комісійна експертиза», «Комплексна експертиза», в яких викласти поняття відповідних видів (категорій) експертиз, підстави призначення та порядок проведення.

2. Водночас, з метою усунення розбіжностей з процесуальними кодексами – встановити в кожному процесуальному кодексі відсилочну норму до Закону України «Про судову експертизу»: «Під час провадження можуть бути проведені додаткові, повторні, комісійні та комплексні експертизи на підставах і в порядку, визначених Законом України «Про судову експертизу»».

3. Передбачити в Законі України «Про судову експертизу» право керівника експертної установи організовувати проведення експертизи, виходячи з поставленого експертного завдання (питань), в тому числі: змінювати категорію експертизи, якщо вона не відповідає поставленому експертному завданню. А також встановити обов’язок експерта зазначати обставини і підстави організації проведення експертизи в іншому порядку (як іншого виду (категорії)) у вступній частині висновку.

Література

1. Кримінальний процесуальний кодекс України: Кодекс України, Закон, Кодекс № 4651-VI від 13.04.2013. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 22.10.2025).

2. Інструкція про призначення та проведення судових експертиз та експертних досліджень: наказ Міністерства юстиції України № 53/5 від 08.10.1998 р. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 22.10.2025).

3. Про затвердження Змін до деяких нормативно-правових актів з питань судово-експертної діяльності: наказ Міністерства юстиції України № 243/5 від 20.01.2021. URL: https://zakon.rada.gov.ua/laws/show/z0089-21#Text (дата звернення: 22.10.2025).

4. Щодо практики застосування норм права у випадку колізії: лист Міністерства юстиції України від 26.12.2008 № 758-0-2-08-19. URL: https://zakon.rada.gov.ua/laws/show/v0758323-08#Text (дата звернення: 22.10.2025).

5. Про правотворчу діяльність: Закон України № 3354-IX від 24.08.2023. URL: https://zakon.rada.gov.ua/laws/show/3354-20#Text (дата звернення: 22.10.2025).

УДК 343.98

ВИКОРИСТАННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З МЕТОЮ ВЧИНЕННЯ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ ВИБУХОВИХ ПРИСТРОЇВ

Олександр ШМЕРЕГО[1], e-mail: a.shmerego@gmail.com, ORCID: 0009-0006-2870-700X

[1]Національний науковий центр «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України

Вступ. Перехід індустріального суспільства до інформаційного проявився в стрімкому розвитку комп'ютерних технологій, широкому впровадженні засобів комп'ютерної техніки до виробництва, торгівлі, а також до життя і побуту людей. Комп'ютерні технології стали найголовнішим засобом обміну інформацією, які значно полегшили як життя, так і роботу людей. Але разом із значними перевагами дані технології створюють реальні загрози як для правопорядку в кожній окремій країни, так і світового правопорядку, в першу чергу – безпеки громадян, оскільки з'явилися нові можливості для вчинення кримінальних правопорушень, які мають свої особливості.

Взагалі, комп'ютерна злочинність – це особливий вид кримінальних правопорушень, пов'язаних із незаконним використанням сучасних інформаційних технологій і засобів комп'ютерної техніки [Див: 1]. В їх основі можуть бути політичні, хуліганські, корисливі й інші мотиви. Згідно із чинним законодавством України, кримінальну відповідальність за злочини у сфері використання електронних обчислювальних машин (ЕОМ), комп'ютерних мереж і мереж електрозв'язку передбачено у Розділі XVI Кримінального кодексу України.

На сьогодні реалізація злочинних задумів набула нових способів реалізації. Наприклад, приведення в дію вибухового або запалювального пристрою, який заздалегідь встановлений особою у «потрібному» місці, можливо здійснити з будь-якого місця на планеті, для чого у нагоді стають різні телекомунікаційні ресурси й сучасні цифрові технології.

Результати. В більшості випадків такі пристрої містять вибухову або горючу речовину і відповідно засоби ініціювання таких пристроїв. Але на сьогодні відомі випадки вчинення терористичних актів, коли знаряддя вчинення злочинів не містять нічого з перелічених складників.

17 вересня 2024 року у Лівані близько 15:30 за місцевим часом у руках, кишенях піджаків та штанів, сумках тисяч членів терористичного проіранського угрупування «Хезболла» почали детонувати пейджери. Тривало це протягом години. Наслідок – вибиті очі, обпалені обличчя, рвані рани в області живота та стегон, поранені кисті аж до подальшої ампутації. Пейджери видавали звуковий сигнал протягом 10 секунд, перш ніж здетонувати. Багато людей через це піднесли пристрої до очей і обличчя, щоб прочитати повідомлення, яке надійшло на пейджер, і через це отримали відповідні травми («New York Times») [2]. Залишки одного з вказаних пейджерів, в якому джерелом живлення слугували літій-іонні акумулятори (рис. 1).

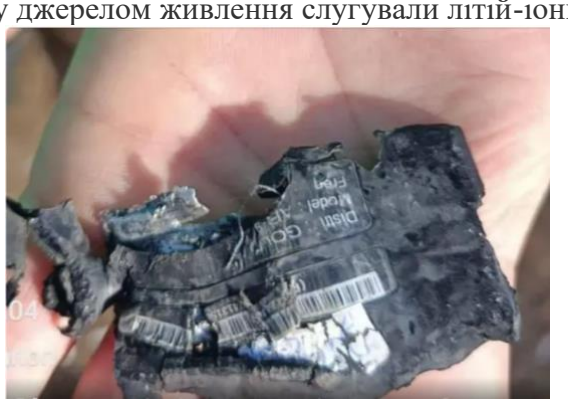


Рисунок 1 – Залишки пейджера, власник якого є член «Хезболли», після вибуху його елементів живлення (літій-іонних акумуляторів)

Літій-іонні акумулятори складаються з анода та катода, які розділені пористим полімерним сепаратором. Найчастіше активним матеріалом катода є оксиди перехідних металів з інтегрованими в кристал іонами літію. В аноді використовується графіт. Електроліт, являє собою органічний розчин солей літію. При першій зарядці, при вбудовуванні літію в анод на електродах (особливо на аноді) утворюється захисний іон-провідний шар (SEI), що складається з електроліту, який розклався. Цей шар захищає електроди від паразитичних реакцій із електролітом (рис. 2).

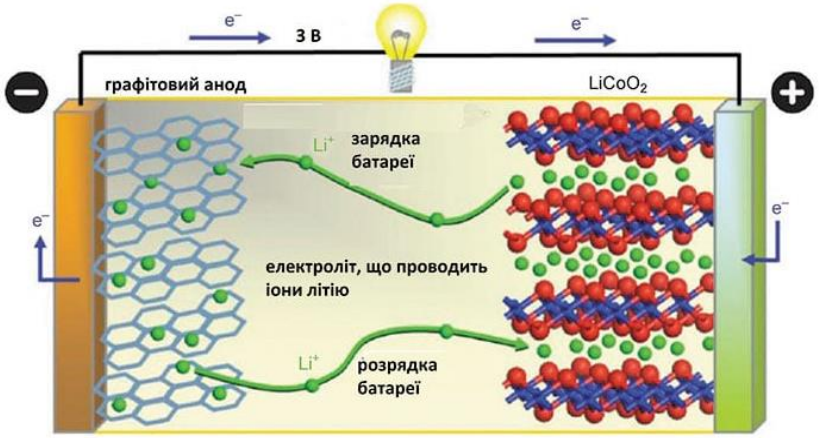


Рисунок 2 – Принципова схема конструкції та роботи літій-іонного акумулятора [3]

Найчастіше причиною займання таких акумуляторів є виникнення аварійного процесу, пов’язаного з настанням короткого замикання всередині електрохімічного осередку. Вчені досліджували різні причини самозаймання високовольтних акумуляторних батарей. Ці основні причини: внутрішнє коротке замикання, перегрів акумулятора, перевищення максимально допустимої напруги, зарядка високими струмами, занадто глибокий розряд. Всі ці причини призводять до одного результату – теплового розгону та розкладання електроліту при взаємодії з електродами з різницею лише у швидкості реакції. Коротке замикання всередині може бути викликане великою кількістю факторів, які можуть залежати від наступних причин: механічне пошкодження елемента, порушення технології виробництва, наявність або потрапляння металевих частинок між анодом і катодом, утворення ланцюжків дендритів літію (металевий літій). Утворення дендритів літію відбувається, якщо іони літію не встигають інтегруватися в кристал анода при низьких температурах або високих швидкостях зарядки, а також за умови, що ємність активного матеріалу катода вища, ніж у анода. Наслідком цього є поява відкладень на поверхні анода, які з часом зростають (рис. 3).

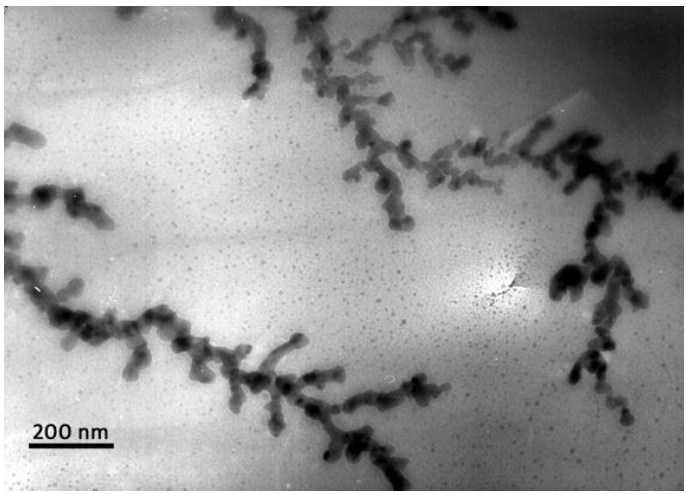


Рисунок 3 – Зображення ланцюжків проростання металевого літію (дендрит) через сепаратор

Літієві накопичувачі енергії, крім високої напруги, у разі порушення умов експлуатації можуть бути джерелом високих температур та пожежі, а також їдкого густого диму. Також, при пошкодженні літій-іонних акумуляторів, може виділятися плавикова кислота. Відомо, що виділення газу назовні, при взаємодії з киснем, призводить до пожежі. Таким чином, навіть за наявності захисних систем та механізмів, при зовнішньому механічному впливі на акумулятор існує високий ризик виникнення пожежі. Подібні випадки неодноразово фіксувалися в дорожньо-транспортних пригодах за участю електромобілів.

Слід зазначити, що акумуляторна батарея, яка використовується не лише в електромобілях, складається з окремих літій іонних акумуляторів і в процесі розвитку аварійного (анормального) процесу в одному з акумуляторів, внаслідок підвищення температури, анормальні аналогічні описаному вище процеси набувають розвитку в інших акумуляторах. Це призводить до накопичення в герметичному корпусі акумуляторної батареї етану, метану, етилену та інших газів, які утворюють надлишковий тиск в середині її корпусу. Коли тиск в середині корпусу акумуляторної батареї перевищує межу міцності оболонки цього корпусу відбувається її розгерметизація, при цьому в навколишнє середовище викидається зазначена суміш горючих газів, які в суміші з киснем повітря здатні утворювати вибухове середовище.

Оскільки, в подальшому, після розгерметизації корпусу акумуляторної батареї, аварійний процес руйнування в описаний вище спосіб продовжується в інших акумуляторах, то внаслідок розвитку в них аварійних процесів утворюються іскри електричного походження, а навколо них на той час вже наявна вибухова концентрація зазначених газів в суміші з киснем повітря. Коли потужність іскри (іскор) виявляється достатньою для запалення наявного вибухового середовища, відбувається запалення вибухової газоповітряної суміші, а фронт стискання вибухової хвилі, що поширюється від місця, де відбулося займання внаслідок об’ємного вибуху, руйнує навколишні об’єкти, що власне і відбувалось 17 вересня 2024 у Лівані.

Власне, хімічні та електрохімічні процеси, що відбуваються у таких акумуляторах можуть спричинити неконтрольовану екзотермічну реакцію. Такі реакції призводять до викиду шкідливих і небезпечних газів [4, 5], займань, вибухів та завдають не лише матеріальних збитків, але й людських жертв [6 – 8].

Висновки. Детальне дослідження та опис механізмів вибуху і пожежі, а також слідів та їх наслідків в умовах використання літій-іонних акумуляторів може виступати основою для формування експертної методики комплексної електротехнічної та пожежотехнічної експертизи з метою визначення причин та умов виникнення вибухів та пожеж, способів і засобів, які використовувались з метою вчинення умисного підпалу або вибуху, або необережне використання яких призвело до настання вибуху/пожежі, а також формулювання рекомендацій щодо фіксації необхідної інформації під час проведення огляду місця події.

Література

1. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), автоматизованих систем та комп’ютерних мереж і мереж електрозв’язку. Вісник Верховного Суду України. 2010. № 2. С. 29-34. [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/UJRN/vvsu_2010_2_7 (дата звернення: 30.10.2025).

2. Як Ізраїль провів унікальну операцію проти «Хезболли». УКРІНФОРМ від 18.09.2024 [Електронний ресурс]. – Режим доступу: https://www.ukrinform.ua/rubric-ato/3907132-ak-izrail-proviv-unikalnu-operaciu-proti-hezbolli.html (дата звернення: 30.10.2025).

3. Фея О. Літієва доба. Український тиждень. № 42 (622) від 20.10.2019 [Електронний ресурс]. – Режим доступу: https:// tyzhden.ua/ litiieva-doba/

4. Гаврилюк А.Ф. & Кушнір А.П. (2022). Аналіз пожежної небезпеки електромобілів за термічною стабільністю силової літієвої акумуляторної батареї. Пожежна безпека, 40, 31-39. https://doi.org/https://doi.org/10.32447/20786662.40.2022.04.

5. Willstrand, O., Bisschop, R., Blomqvist, P., Temple, A., & Anderson, J. (2020). Toxic Gases from Fire in Electric Vehicles. 240 p. [Електронний ресурс]. – Режим доступу: https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1522149&dswid=3634 (дата звернення: 30.10.2025).

6. Zhang, Z. J., Ramadass, P., & Fang, W. (2014). Safety of lithium-ion batteries. In Lithium-ion batteries (pp. 409-435). https://doi.org/10.1016/B978-0-444-59513-3.00018-2

7. Gavryliuk, A., Yakovchuk, R., Ballo, Y., and Rudyk, Y. Thermal Modeling of the Electric Vehicle Fire Hazard Effects on Parking Building, SAE Int. J. Trans. Safety 11(3):2023, p. 1-14. doi:10.4271/09-11-03-0013

8. N. Goto, Aircraft serious incident investigation report: all Nippon airways Co. Ltd. JA804A. Japan Transport Safety Board, Tokyo, Japan, Rep. No. AI2014-4, Sep. 25, 2014. 115 p. [Електронний ресурс]. – Режим доступу: https://jtsb.mlit.go.jp/eng-air report/JA804A.pdf (дата звернення: 30.10.2025).

Державний науково-дослідний інститут
технологій кібербезпеки та захисту інформації
Державної служби спеціального зв'язку
та захисту інформації України

Національний науковий центр
«Інститут судових експертиз
ім. Засл. проф. М. С. Бокаріуса»
Міністерства юстиції України

Центральний науково-дослідний інститут озброєння
та військової техніки Збройних Сил України
Міністерства оборони України

Київський науково-дослідний інститут
судових експертиз
Міністерства юстиції України