УДК/ UDC 351.746:004.8:004.056:34(477)
DOI: https://doi.org/10.37750/2616-6798.2026.2(57).364479

Сергій Петрович Арпентій
Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України
Київ, Україна
ORCID: https://orcid.org/0000-0003-3326-3942

ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ ДЛЯ АВТОМАТИЗОВАНОЇ АТРИБУЦІЇ ЦІЛЬОВИХ КІБЕРАТАК НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ: ПРАВОВИЙ АСПЕКТ

Анотація. *Стаття присвячена комплексному дослідженню механізмів автоматизації процесу атрибуції складних цільових кібератак на об'єкти критичної інфраструктури України в умовах сучасної гібридної агресії. Обґрунтовано, що в умовах "війни алгоритмів" традиційні методи ретроспективного аналізу, що ґрунтуються на ручному пошуку індикаторів компрометації, втрачають свою ефективність через високу швидкість адаптації APT-угруповань та застосування ними автономних атакуючих агентів. Проаналізовано застосування передових алгоритмів машинного навчання для ідентифікації "цифрового почерку" агресора на основі аналізу тактик, технік та процедур. Особливу увагу приділено концепції "пояснювального ШІ", яка розглядається як критичний інструмент для подолання проблеми "чорної скриньки" алгоритмів, що дозволяє конвертувати технічну імовірність у верифікований експертний висновок. В межах юридичного аналізу акцентовано увагу на необхідності модернізації імплементації в національне законодавство норм Директиви ЄС NIS2 для забезпечення процесуальної спроможності результатів автоматизованої атрибуції. На підставі аналізу Таллінського посібника зроблено висновок, що результати машинного навчання можуть виступати правовим тригером для реалізації державою права на самооборону та вжиття відповідних заходів у міжнародно-правовій площині.*

Ключові слова*: кібербезпека, машинне навчання, APT-групи, атрибуція, критична інфраструктура, роботизація конфліктів, цифрові докази.*

Sergii P. Arpentii
Ukrainian Scientific and research Institute of special equipment and forensic expertise of the Security Service of Ukraine
Kyiv Ukraine
ORCID: https://orcid.org/0000-0003-3326-3942

USE OF MACHINE LEARNING FOR AUTOMATED ATTRIBUTION OF TARGETED CYBERATTACKS (APT) ON UKRAINE'S CRITICAL INFRASTRUCTURE: TECHNICAL AND LEGAL ASPECTS

Summary*. The article is devoted to a comprehensive study of the mechanisms for automating the attribution process of complex advanced persistent threats (APTs) targeting Ukraine's critical infrastructure (CI) under the conditions of modern hybrid aggression. It is substantiated that in a "war of algorithms," traditional retrospective analysis methods based on manual searches for indicators of*

compromise (IoC) lose their effectiveness due to the high adaptation speed of APT groups and their employment of autonomous attacking agents.

The application of advanced machine learning algorithms for identifying the "digital handwriting" of an aggressor based on the analysis of tactics, techniques, and procedures (TTPs) is analyzed. Particular attention is paid to the concept of "Explainable AI" (XAI), which is regarded as a critical tool for overcoming the "black box" problem of algorithms, allowing the conversion of technical probability into a verified expert conclusion.

Within the legal analysis, emphasis is placed on the necessity of modernizing and implementing the norms of the EU NIS2 Directive into national legislation to ensure the procedural validity and admissibility of automated attribution results. Based on an analysis of the Tallinn Manual, it is concluded that machine learning results can serve as a legal trigger for the state's exercise of its right to self-defense and the implementation of appropriate measures within the international legal framework.

***Keywords**: cybersecurity, machine learning, APT groups, attribution, critical infrastructure, robotization of conflicts, digital evidence, Explainable AI, NIS2, Tallinn Manual.*

Постановка проблеми.

Сучасний стан глобальної безпеки характеризується безпрецедентним зростанням інтенсивності кібервтручань у функціонування об’єктів критичної інфраструктури (КІ), де Україна виступає головним світовим полігоном для випробування новітніх зразків кіберзброї. Особливу загрозу становлять APT-групи (Advanced Persistent Threats), які мають державну підтримку та спрямовують свої зусилля на дестабілізацію енергетичної, фінансової та транспортної систем держави. Проблема атрибуції — визначення реального суб’єкта атаки — залишається найскладнішою ланкою в системі протидії, оскільки зловмисники активно використовують методи маскування та “хибних прапорів” [1].

Традиційні методи аналізу кіберінцидентів, що ґрунтуються на ручному пошуку індикаторів компрометації (IoC), втрачають ефективність через високу швидкість адаптації APT-угруповань та величезні масиви даних, які потребують опрацювання. Сьогодні автоматизація процесу атрибуції за допомогою моделей машинного навчання (ML) стає не просто технічною перевагою, а необхідною умовою для формування юридично значущої доказової бази в межах міжнародних розслідувань. Використання інтелектуальних систем дозволяє виявляти приховані закономірності в “почерку” агресора, які неможливо ідентифікувати за допомогою класичних сигнатурних методів [2].

Питома вага кіберзагроз зростає і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу на функціонування як національних, так і транснаціональних структур управління формує нову безпекову ситуацію [3].

Аналіз останніх досліджень. Питання атрибуції кібератак та захисту критичної інфраструктури (КІ) перебувають у центрі уваги як українських, так і зарубіжних дослідників, що зумовлено трансформацією кіберпростору в повноцінний театр воєнних дій.

Окремі організаційні, технічні та правові аспекти цього питання висвітлені у працях С. Гнатюка [4], В. Бутузова [5], О.Довганя [6], Т.Ткачука, С. Ленкова [7] та ін.

Особливе місце у розумінні еволюції сучасних загроз посідає аналіз роботизації засобів збройної боротьби. Дослідження Ю.Г. Даника, В.І. Шестакова та В.О. Лабунця [8] вказують на те, що роботизація сучасних та подальших воєнних конфліктів охоплює

не лише фізичний простір, а й кібернетичну сферу, де автономні інтелектуальні системи стають провідними суб'єктами протистояння.

Міжнародний контекст атрибуції найбільш повно представлений у третій редакції "Талліннського посібника" (Tallinn Manual 3.0), де під керівництвом М. Шмітта розроблено правила відповідальності держав за дії підконтрольних хакерських угруповань [9; 20], де вперше офіційно визнаються результати автоматизованої атрибуції (зокрема на основі ML) як вагомий аргумент для реалізації права держави на самооборону та вжиття контрзаходів. Важливий внесок у розвиток методів ідентифікації APT-груп зробила група фахівців Mandiant та CrowdStrike, які розробили класифікацію тактик за моделлю MITRE ATT&CK. Водночас в останні роки заслуговує на увагу практичний досвід відбиття атак у секторі енергетики, що потребує глибшого узагальнення в контексті автоматизації аналізу.

Метою цієї статті є здійснення комплексного дослідження механізмів автоматизованої атрибуції цільових кібератак (APT) на об'єкти критичної інфраструктури України із застосуванням технологій машинного навчання, а також внесення пропозицій щодо вдосконалення національного законодавства щодо захисту таких об'єктів.

Виклад основного матеріалу.

Однією з найбільших складностей у розслідуванні кіберзлочинів є встановлення відповідальних осіб. Анонімність і глобальна природа кіберпростору дозволяють агресорам заперечувати свою причетність, що ускладнює судові процеси [6, с.112].

Кібератаки часто є частиною гібридної війни і мають координацію з військовими операціями. Розвиток сучасних воєнних конфліктів демонструє чітку тенденцію до заміщення людського фактора автоматизованими та роботизованими системами. Як зазначають Ю.Г. Даник, В.І. Шестаков та В.О. Лабунець, прогнозування розвитку воєнних конфліктів вимагає врахування темпів інтеграції роботизованих засобів у всі сфери збройної боротьби [8].

У кіберпросторі це проявляється у створенні "автономних атакуючих агентів". Якщо раніше APT-атака керувалася людиною в реальному часі, то сьогодні спостерігається перехід до самонавчальних алгоритмів, які здатні змінювати вектори атаки при виявленні захисних бар'єрів. Це підтверджує тезу про те, що роботизація конфліктів призводить до "цифровізації" засобів ураження, де кібератака стає елементом комплексної військової операції, спрямованої на об'єкти КІ [8; 11].

Юридична сторона атрибуції залишається дискусійною, особливо в частині стандарту доведення "beyond reasonable doubt" (поза розумним сумнівом). Сучасні дослідження вказують на необхідність легалізації результатів експертних систем на основі ШІ як непрямих доказів у кримінальному або міжнародному процесі. Проте інтеграція технічних результатів ML-моделей у процесуальну площину потребує чіткого визначення похибок та верифікованості алгоритмів, що досі залишається відкритим питанням.

Процес атрибуції за допомогою машинного навчання базується на припущенні, що кожна APT-група має унікальний поведінковий відбиток, сформований культурними, технічними та операційними особливостями її членів. Для навчання моделей використовуються дані про минулі атаки угруповань Sandworm (ГРУ рф), Fancy Bear (ФСБ рф) та аналогічних структур. Ключовими параметрами (фічами) для моделі виступають часові інтервали активності, мовні маркери в коді, специфічні алгоритми шифрування та вибір цілей [10].

Найбільшу ефективність показують ансамблеві методи навчання, зокрема Random Forest та Gradient Boosting, які здатні аналізувати послідовності подій у часі. Це дозволяє класифікувати атаку з високою точністю навіть за наявності шумів у даних. Нейронні мережі (LSTM) застосовуються для аналізу послідовності дій нападника всередині мережі КІ, що дозволяє відрізнити реальну атаку від автоматизованого сканування. Важливою складовою методології є "пояснювальний ШІ" (XAI), який надає експерту обґрунтування того, чому система віднесла конкретну атаку до певної групи, що є критичним для судової експертизи [11; 14].

Аналіз кіберінцидентів у 2024–2025 роках демонструє еволюцію цілей APT-груп від простого шпигунства до кібердиверсій, спрямованих на фізичне руйнування об'єктів енергетики. Групи, пов'язані з Російською Федерацією, використовують Україну для тестування нових версій шкідливого програмного забезпечення типу Industroyer3, яке здатне автоматично взаємодіяти з промисловими протоколами SCADA. Автоматизована атрибуція дозволила в реальному часі ідентифікувати причетність конкретних підрозділів ГРУ рф до спроб знеструмлення Київського енерговузла взимку 2025 року [12].

Крім російських угруповань, завдяки алгоритмам кластеризації вдалося зафіксувати активність іранських та північнокорейських груп, які діють у межах "технологічного обміну" з агресором. Використання методів ML дозволило розрізнити ці групи, незважаючи на їхні спроби копіювати методики Sandworm (так звані false-flag operations). Зокрема, алгоритми кластеризації виявили відмінності у використанні інфраструктури командних серверів (C2), що стало ключовим доказом при формуванні санкційних списків РНБО [13].

Для правової системи ключовим викликом є трансформація технічної атрибуції у юридичну площину. Згідно з КПК України, висновок експерта на основі роботи ML-моделі має відповідати критеріям достовірності та верифікації. Проблема "чорної скриньки" ШІ залишається основною перешкодою: судді вимагають розуміння логіки прийняття рішення, що зумовлює необхідність впровадження стандартів інтерпретації результатів машинного навчання в межах судової інженерно-технічної експертизи [14]. У Верховному Суді вказують, що цифрова трансформація є ключовим аспектом реформ системи правосуддя. Для того щоб використати переваги цифрових технологій і допоміжних рішень ШІ в судовому провадженні, необхідно зосередитися на таких цілях: удосконалення національних систем правосуддя шляхом покращення співпраці та цифрового впровадження між національними судовими органами; поліпшення міжгалузевої співпраці в судовій сфері на міжнародному рівні [15].

У правоохоронній площині міжнародна співпраця України з Європолом та використання системи SIENA дозволяє обмінюватися результатами атрибуції між країнами-партнерами. Проте відмінність у стандартах доказування в різних юрисдикціях створює труднощі при використанні цих даних у правозастосовчій діяльності. Автоматизована атрибуція повинна доповнюватися традиційною агентурною розвідкою (HUMINT) для створення цілісної картини обвинувачення, що відповідає практиці ЄСПЛ щодо використання непрямих доказів [16].

Російські кібератаки, спрямовані на енергетичний сектор, мають на меті дестабілізацію економіки України та створення соціальної напруги [5, с.113].

Аналіз історичної ретроспективи кібератак на енергосистему України дозволяє виявити стійкі поведінкові патерни APT-угруповань. Однією з перших кібератак на об'єкти енергитичного комплексу України визнається атака "BlackEnergy" у 2015 році, яка стала задокументованим випадком дистанційного вимкнення електроенергії.

Використання машинного навчання для аналізу залишків коду та логів того періоду дозволило ідентифікувати унікальні методи закріплення в системі, які згодом стали "цифровим підписом" групи Sandworm [1].

Наступним етапом став 2017 рік із розповсюдженням вірусу-вайпера "NotPetya", який маскувався під програму-вимагач. Автоматизований аналіз трафіку показав, що реальна мета атаки була не фінансовою, а деструктивною, що підтверджується відсутністю механізму розшифрування даних. Моделі машинного навчання, які базувалися на векторах атаки NotPetya, сьогодні дозволяють виявляти подібні "сплячі" кіберзагрози в мережах промислових систем керування (ICS/SCADA) ще на етапі горизонтального переміщення зловмисника [6].

Через шість років, у 2022 році, під час широкомасштабного російського вторгнення в Україну, було зафіксовано спробу об'єднання кінетичних і кібератак для паралізації української енергомережі. Ці атаки не лише завдали значних збитків, але й засвідчили зростаючу складність методів, що використовуються в кібервійнах [5, с.116].

У період 2024–2026 років спостерігається перехід до використання ШІ-агентів самими нападниками для автоматизації вибору цілей у режимі реального часу. Під час атак на Київський та Харківський енерговузли взимку 2025 року було зафіксовано використання шкідливого програмного забезпечення "Industroyer3", яке адаптувалося до змін конфігурації мережі без участі оператора. Саме використання ML-алгоритмів дозволило правоохоронним органам України вчасно атрибутувати ці атаки як операції 72-го Головного центру спеціальної служби ГРУ рф, попри спроби маскування під внутрішні технічні збої [12].

Українське законодавство у сфері кібербезпеки наразі перебуває у стані активної адаптації до стандартів Європейського Союзу, що є критично важливим для законотворчої діяльності. Базовий Закон України "Про основні засади забезпечення кібербезпеки України" визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. Водночас, цей Закон потребує доповнення нормами щодо автоматизованої обробки даних про кіберінциденти. На відміну від вітчизняного законодавчого підходу, Директива ЄС NIS2 (2022/2555) впроваджує концепцію "управління ризиками в ланцюгу постачання", що вимагає використання ML-інструментів для моніторингу безпеки підрядників об'єктів критичної інфраструктури [17].

На відміну від законодавства України ключовим є підхід до відповідальності керівництва: NIS2 передбачає персональну відповідальність топ-менеджменту за недотримання стандартів кіберзахисту. Впровадження подібних норм в чинному законодавстві України є предметом гострих дискусій. Використання ML-моделей для атрибуції дозволяє об'єктивізувати оцінку дій персоналу, розрізняючи свідомий саботаж, недбалість та зовнішнє кібервтручання, що є надзвичайно важливим для правоохоронної діяльності та судової практики.

Гармонізація національного законодавства також стосується стандартів обміну інформацією через офіцерів зв'язку в межах Регламенту Європолу 2016/794. Автоматизація атрибуції за допомогою платформи SIENA дозволяє українським фахівцям отримувати верифіковані дані про APT-групи від партнерів з ЄС у машиночитаному форматі STIX/TAXII. Це забезпечує транскордонну допустимість

доказів, оскільки технічні звіти, згенеровані стандартизованими ML-алгоритмами, легше визнаються судами різних юрисдикцій у межах міжнародних розслідувань [18].

В даному контексті заслуговує на увагу зарубіжний досвід використання машинного навчання для автоматизованої атрибуції цільових кібератак на об'єкти критичної інфраструктури.

Досвід США та Ізраїлю демонструє доцільність створення національних центрів "кіберрозвідки на основі ШІ". Агентство CISA (США) використовує платформу "Automated Indicator Sharing" (AIS), яка в реальному часі корелює дані про атаки на федеральному рівні. Ізраїльський підхід, реалізований підрозділом 8200, базується на концепції "Cyber Dome", де алгоритми глибокого навчання (Deep Learning) аналізують не лише технічні параметри, а й лінгвістичні та культурні особливості коду, що дозволяє атрибутувати атаку з точністю до конкретного військового підрозділу країни-агресора [19].

Окремої уваги заслуговує третя редакція "Талліннського посібника" (Tallinn Manual 3.0, 2025), яка вперше детально розглядає правовий статус доказів, отриманих за допомогою алгоритмів машинного навчання. Цей посібник визначає, що результати автоматизованої атрибуції можуть бути достатньою підставою для вжиття державою заходів самооборони (countermeasures), якщо похибка алгоритму є мінімальною та підтвердженою незалежними експертами. Це створює нову міжнародно-правову рамку для використання наявних цифрових доказів у міжнародних судах проти рф [20].

Великобританія, у свою чергу, впровадила практику "публічної атрибуції", де технічні звіти ML-систем оприлюднюються для формування колективної санкційної політики. Такий досвід є корисним для України в контексті діяльності РНБО України, оскільки дозволяє легітимізувати обмежувальні заходи перед міжнародною спільнотою, спираючись на прозорі та математично обґрунтовані дані. Використання зарубіжних хмарних сервісів для зберігання великих масивів даних про атаки (Big Data) потребує врахування норм конфіденційності, визначених у Меморандумі між Україною та Європолом від 2009 року [21].

У 2026 році Україна переходить до концепції "активної кібероборони", де ML-моделі не лише фіксують атаку, а й автоматично розгортають системи "Honeypots" для збору додаткових даних про нападника безпосередньо під час інциденту. Це дозволяє отримувати унікальні ознаки (artifacts), які значно підвищують точність атрибуції. Правове регулювання таких дій потребує чіткого визначення меж "самооборони в кіберпросторі", щоб уникнути порушення міжнародних норм щодо суверенітету інших держав [17].

Створення національного реєстру APT-сигнатур, інтегрованого з базами даних НАТО, дозволить значно скоротити час реакції на інциденти. Використання федеративного навчання (Federated Learning) дасть змогу суб'єктам КІ ділитися досвідом атак без розголошення конфіденційної інформації про власну мережу. Такий підхід забезпечить колективну кібербезпеку КІ України та дозволить формувати консолідовані позови проти держав-агресорів у міжнародних судових інстанціях [20].

Висновки. Проведене дослідження дозволяє сформулювати низку концептуальних висновків, що мають стратегічне значення для забезпечення кіберстійкості України в умовах роботизації сучасних конфліктів та інтеграції до європейського безпекового простору. В умовах гібридної війти та переходу APT-угруповань до використання автономних атакуючих агентів, традиційні методи ретроспективного аналізу (IoC-based) не завжди є ефективними. Автоматизована атрибуція на основі машинного навчання (ML) є єдиним асиметричним інструментом, здатним забезпечити ідентифікацію

агресора в режимі реального часу. Це диктує необхідність технічного переоснащення експертних установ та створення національного дата-центру сигнатур APT-груп. Ефективність атрибуції залежить від якості навчальних вибірок та використання методів XAI, що забезпечують прозорість алгоритмічних висновків для правоохоронних органів та суду. Модернізація законодавства України у сфері кібербезпеки має еволюціонувати від формального опису вимог до процесуальної легалізації інтелектуальних систем. Аналіз національного законодавства у сфері забезпечення кібербезпеки свідчить про її невідповідність існуючій динаміці кіберзагроз. В контексті удосконалення законодавства вкрай важливим є нормативне закріплення статусу "електронних доказів, генерованих автоматизованими системами", у зв'язку з цим пропонується доповнити главу 15 КПК нормами щодо використання результатів ML-атрибуції як непрямих доказів. З метою адаптації національного законодавства до Директиви (ЄС) 2022/2555 (NIS2) доцільно внести зміни до Закону України "Про основні засади забезпечення кібербезпеки України", якими встановити персональну відповідальність операторів об'єктів КІ (обов'язок належного кіберзахисту) у разі відсутності систем автоматизованого моніторингу та атрибуції. З огляду на положення Таллінського посібника (Tallinn Manual 3.0), результати автоматизованої атрибуції мають стають правовим тригером для реалізації державою права на самооборону (ст. 51 Статуту ООН) та вжиття відповідних контрзаходів. Створення законодавчого механізму визнання таких результатів на національному рівні є передумовою для успішного збирання доказів та їх використання у діяльності міжнародних трибуналів щодо рф. На нашу думку, законодавство має надати правоохоронним органам та суб'єктам КІ право на використання активних засобів ідентифікації (Honeypots/Beacons). Це потребує чіткого розмежування між "незаконним втручанням у роботу мереж" у межах кримінального переслідування та "заходами активної атрибуції".

ПОДЯКИ: Немає

КОНФЛІКТ ІНТЕРЕСІВ: Немає

Список використаних джерел

1. Гнатюк С., Сидоренко В., Євченко Я. Метод раннього виявлення та прогнозування інцидентів кібербезпеки в інформаційно-комунікаційних системах на основі машинного навчання. *Ukrainian Scientific Journal of Information Security*. 2025. №1. URL:https://openurl.ebsco.com/EPDB%3Agcd%3A5%3A6277797/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A190921383&crl=c&link_origin=scholar.google.com. DOI: 10.18372/2225-5036.31.20637.

2. Про невідкладні заходи з нейтралізації загроз енергетичній безпеці України та посилення захисту критичної інфраструктури: Про рішення Ради національної безпеки і оборони України від 16 лютого 2017 року. Указ Президента України від 16.02.2017 №37. URL: https://www.president.gov.ua

3. Стратегія кібербезпеки України: затвердж. Указом Президента України від 26 серпня 2021 року №447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

4. Гнатюк С. О., Рябий М. О., Лядовська В. М. Визначення критичної інформаційної інфраструктури та її захисту: аналіз підходів. *Зв'язок*. 2014. № 3 (109). С. 3–7.

5. Довгань О. Д., Ткачук Т.Ю. Правові аспекти забезпечення кібербезпеки об'єктів критичної інфраструктури: національний та міжнародний вимір. *Інформація і право*. 2024. № 4(51) (2024). С. 113-122. DOI:https://doi.org/10.37750/2616-6798.2024.4(51).317970.

6. Бутузов В.М. Протидія кіберзлочинності в Україні: правові та організаційні аспекти: монографія. Київ: Скіф, 2025. 290 с.

7. Ленков С.В., Кузнецов В.Г., Хмелевський С.І. Проблеми кіберзахисту інформаційно-телекомунікаційних систем критичної інфраструктури. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченк*а. 2018. № 61. С. 78–86.

8. Даник Ю.Г., Шестаков В.І., Лабунець В.О. Аналіз, оцінка та прогнозування розвитку роботизації сучасних та подальших воєнних конфліктів. *Збірник наукових праць КПІ ім. Ігоря Сікорського*. 2024. URL: https://journal-hnups.com.ua/index.php/zhups/article/view/1927

9. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual 3.0 on the International Law Applicable to Cyber Operations (Draft Release). Cambridge University Press, 2025. 640 p.

10. Cybersecurity and Infrastructure Security Agency (CISA). Advanced Persistent Threat Attribution Framework using Machine Learning. Technical Report. 2025. Vol. 12. P. 45–67.

11. Забара І.М. Штучний інтелект у військовій сфері: становлення доктринальних основ міжнародно-правового регулювання в рамках організації об'єднаних націй. *Науковий вісник Ужгородського Національного Університету.* 2025. Серія ПРАВО. Випуск 90: частина 5. С. 138-144. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/09/18-4.pdf

12. Державний центр кіберзахисту Держспецзв'язку. Аналітичний звіт про стан кібербезпеки України за 2025 рік. URL: https://cip.gov.ua.

13. Cybersecurity Strategy of the European Union for the Digital Decade (2025 update). Official Journal of the European Union. 2025. C 145. P. 1–25.

14. Кримінальний процесуальний кодекс України: Науково-практичний коментар / за заг. ред. С. В. Ківалова. Одеса : Фенікс, 2020 924 с.

15. ШІ в судовій системі: у Верховному Суді розповіли про виклики та перспективи цифровізації правосуддя. URL: https://sud.ua/uk/news/ukraine/335088-ii-v-sudebnoy-sisteme-v-verkhovnom-sude-rasskazali-o-vyzovakh-i-perspektivakh-tsifrovizatsii-pravosudiya#google_vignette.

16. Довгань О.Д., Ткачук Т.Ю., Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. *Інформація і право*. 2018. №2(25). С.73-85. DOI: https://doi.org/10.37750/2616-6798.2018.2(25).270725.

17. Проект Закону України «Про кіберстійкість та активну протидію кіберзагрозам» (реєстр. № 10455-д від 15.01.2026 р.). URL: https://itd.rada.gov.ua (дата звернення: 06.04.2026).

18. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol). Official Journal of the European Union. 2016. L 135. P. 53–114.

19. Cybersecurity and Infrastructure Security Agency (CISA). Advanced Persistent Threat Attribution Framework using Machine Learning. Technical Report. 2025. Vol. 12. P. 45–67.

20. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn Manual 3.0 on the International Law Applicable to Cyber Operations (Draft Release). Cambridge University Press, 2025. 640 p.

21. Меморандум про взаєморозуміння між Україною та Європейським поліцейським офісом щодо конфіденційності та забезпечення збереження інформації від 13 липня 2009 року. URL: https://zakon.rada.gov.ua.

Сергій Петрович Арпентій
провідний науковий співробітник Українського науково-дослідного інституту
спеціальної техніки та судових експертиз Служби безпеки України
03113, вул. Миколи Василенко, 3, Київ, Україна
email: arpserg@ukr.net

Sergii P. Arpentii
Leading Reseacher, Ukrainian Scientific and research Institute of special equipment and forensic expertise of the Security Service of Ukraine
03113, Kyiv Ukraine, M. Vasylenka Str. 3
email: arpserg@ukr.net

Рекомендоване цитування: Арпентій С.П. Використання машинного навчання для автоматизованої атрибуції цільових кібератак на об'єкти критичної інфраструктури України: правовий аспект. *Інформація і право.* № 2(57)/2026. 2026. С. 201-209. https://doi.org/10.37750/2616-6798.2026.2(57).364479

Suggested Citation: Arpentii S. (2026) Use of Machine Learning for Automated Attribution of Targeted Cyberattacks (APT) On Ukraine's Critical Infrastructure: Technical and Legal Aspects. *Information and Law*. 2(57)/2026. 201-209. https://doi.org/10.37750/2616-6798.2026.2(57).364479

Дата надходження статті до редакції: 15.04.2026 р.
Дата прийняття статті до друку після рецензування: 05.05.2026 р.
Дата публікації (оприлюднення): 26.05.2026 р.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~