https://doi.org/10.26565/2075-1834-2026-41-30
УДК 341.1:004.056

КОРИСТІН О.Є.
доктор юридичних наук, професор,
заслужений діяч науки і техніки України
E-mail: alex@korystin.pro ORCID: https://orcid.org/0000-0001-9056-5475
Департамент кіберполіції Національної поліції України
м. Київ, 02093, вул. Бориспільська,19
Інститут дослідження кібервійни
м.Київ, 01024, вул. Шовковична, б.16б

ДЕМЕДЮК С.В.
кандидат юридичних наук, доцент
E-mail: cyberdemediuk@protonmail.com ORCID: https://orcid.org/0009-0008-1359-5265
Національна академія Служби безпеки України
м. Київ, 03066, вул. М. Максимовича, 22
Інститут дослідження кібервійни
м.Київ, 01024, вул. Шовковична, б.16

ПРАВОВІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ ІМПЛЕМЕНТАЦІЇ ЄВРОПЕЙСЬКИХ СТАНДАРТІВ ІОСТА У СИСТЕМУ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ БЕЗПЕКИ УКРАЇНИ: ГУМАНІТАРНИЙ АСПЕКТ

АНОТАЦІЯ. *Вступ.* У статті здійснено комплексний науково-теоретичний аналіз правових та методологічних засад імплементації європейської методології аналізу загроз організованої злочинності в Інтернеті (ІОСТА) у національну систему цифрової безпеки. Актуальність дослідження зумовлена необхідністю трансформації техноцентричних підходів до кібербезпеки в умовах воєнного стану та переходу до антропоцентричної моделі захисту конституційних прав громадян. Постановка проблеми полягає у виявленні ризиків «інституційного ізоморфізму» та явища «декаплінгу» при формальному запозиченні західних моделей без їх належної реконтекстуалізації. Методологічну основу дослідження становлять концепції соціологічного інституціоналізму Стенфордської школи, системно-структурний метод та методи предиктивного моделювання ризиків. Метою статті є обґрунтування гуманітарного вектора цифрової безпеки як фундаменту інституційної стійкості України.

Короткий зміст основних результатів дослідження. Доведено, що цифрова безпека в сучасних умовах є не лише технічною функцією, а критичним гуманітарним завданням, спрямованим на захист гідності та свободи особистості. Авторами проведено критичний аналіз попереднього досвіду імплементації методології SOCTA в Україні, який виявив втрату проактивності аналітики та неспроможність прогнозного використання результатів через формальний підхід до запозичення стандартів. Обґрунтовано перехід від «аналітики контролю» до «аналітики довіри», де ключовим показником є зміцнення суспільної стійкості. У статті деталізовано регламент стратегічного аналітичного циклу, що включає безперервний OSINT-моніторинг, експертну валідацію через глибинні інтерв'ю та комплексний Форсайт-аналіз за пріоритетними векторами діяльності. Особливу увагу приділено етичній складовій аналітичного процесу, де аналітик постає як комунікатор стратегічних сенсів та етичний медіатор. Запропоновано створення української школи аналітики для формування нових інституційних компетентностей правоохоронних органів.

Висновки. Сформульовано нову парадигму цифрової безпеки, яка базується на предиктивному управлінні ризиками та інституційній спроможності адаптувати міжнародні стандарти до специфічного соціоправового контексту. Констатовано, що успіх імплементації ІОСТА залежить від здатності аналітичної системи виявляти «слабкі сигнали» технологічних загроз, підпорядковуючи їх захисту людської гідності та зміцненню демократичного ладу. Визначено, що побудова культури предиктивної аналітики є ключовим кроком до подолання системних уразливостей та забезпечення сталого розвитку України в умовах глобальної цифровізації.

КЛЮЧОВІ СЛОВА*: цифрова безпека, ІОСТА, гуманітарний аспект, аналітика довіри, декаплінг, стратегічний аналітичний цикл*

Як цитувати: Користін О.Є., Демедюк С.В. Правові та методологічні засади імплементації європейських стандартів іосta у систему забезпечення цифрової безпеки України: гуманітарний аспект *Вісник Харківського національного університету імені В. Н. Каразіна, серія «Право».* 2026. Вип. 41. С. 322-330. https://doi.org/10.26565/2075-1834-2025-40-31

In cites: . O. Y. Korystin, S. V. Demediuk (2026) Legal and methodological foundations for the implementation of european iocta standards in the digital security system of Ukraine: a humanitarian aspect. *The Journal of V.N. Karazin Kharkiv National University, Series "Law"*, (41), P. 322-330.. https://doi.org/10.26565/2075-1834-2025-40-31 (in Ukrainian)

© Користін О.Є., Демедюк С.В., 2026
This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0

Вступ. Цифрова безпека в сучасному правовому дискурсі стрімко трансформується з вузькоспеціалізованої технічної функції у фундаментальне гуманітарне завдання. В умовах повномасштабної збройної агресії проти України та інтенсифікації гібридних загроз, цифровізація суспільних відносин потребує не лише технологічного захисту, а й глибокого соціоправового осмислення. Онлайн-середовище стає простором реалізації та захисту конституційних прав людини, її гідності та свободи, що вимагає впровадження ефективних методологій аналізу та протидії загрозам. Одним із таких інструментів є європейська методологія аналізу загроз організованої злочинності в Інтернеті (Internet Organised Crime Threat Assessment – IOCTA), розроблена Європолом. Проте її успішна імплементація в національну систему права залежить не лише від технічної інтеграції, а й від здатності держави адаптувати ці інструменти до специфічних умов вітчизняного правового поля.

Актуальність дослідження зумовлена необхідністю подолання техноцентричного підходу в діяльності правоохоронних органів та переходу до антропоцентричної моделі безпеки. Закон України «Про основні засади забезпечення кібербезпеки України» закладає правовий фундамент для захисту інтересів суспільства [1], однак практична реалізація превентивних заходів часто стикається з браком методологічної гнучкості.

Сучасний стан наукової розробки питань протидії кіберзлочинності характеризується міждисциплінарним підходом, що охоплює технологічні, методологічні та правові аспекти, які в сукупності формують цілісну стратегію цифрової безпеки. Ключовим напрямом є цифрова форензика, де науковці детально аналізують інструментарій комп'ютерних, мобільних та мережевих розслідувань, виокремлюючи проблеми шифрування, юрисдикційної невизначеності та використання технологій штучного інтелекту для виявлення цифрових артефактів [2-5]. Центральним об'єктом дослідження у сучасній цифровій форензиці є інтеграція штучного інтелекту та машинного навчання, що зумовлює перехід від ручного аналізу до автоматизованих систем. Як зазначають Д. Дансін (Dunsin D.) та співавтори, такий підхід дозволяє ефективно обробляти масиви Big Data під час розслідування інцидентів та забезпечувати предиктивне виявлення загроз [3]. Питання комплексного виявлення кіберзлочинів та аналізу технік атак детально розкриті у працях У. Аль-Кхатер (Al-Khater W.) та ін., де наголошується на критичній важливості скорочення часу реагування [6]. Значна увага приділяється вивченню еволюції тактики вчинення кіберзлочинів та розбудові систем кіберрозвідки для моніторингу ландшафту загроз, зокрема в Deep та Dark Web [7]. Зокрема, дослідження М. Саід (Saeed M.) та ін. спрямовані на систематизацію знань про сучасні тренди та шаблони атак для формування ефективних контрзаходів у межах організацій [8].

Особлива увага приділяється оцінці ефективності розслідувань, ідентифікації зловмисників та необхідності створення спеціалізованих центрів експертизи [9]. Водночас науковцями пропонуються моделі співпраці та стандартизації процесів, зокрема спеціалізовані моделі розслідування для правоохоронних органів [10]. В українському сегменті досліджень акцент зміщується на роль цифрових доказів у сфері е-комерції та аналіз правового статусу суб'єктів, що здійснюють протидію кіберзагрозам [11].

Публікації останніх років фокусуються на критичній оцінці спроможності правоохоронних органів протидіяти злочинності. Так, Ф. Аскар (Askar F.) та ін. пропонують методологію оцінки реальної ефективності цифрових розслідувань, виявляючи прогалини у поточних підходах до боротьби з кіберзлочинністю [12]. А. Кесіді (Cassidy A.A.T.J.) та співавтори аналізують нові виклики цифрового злочинного світу, акцентуючи увагу на тактиках кіберзлочинців та необхідності постійної модернізації засобів протидії [13]. Окремий масив досліджень присвячений розриву між стрімким розвитком технологій та консервативною правовою рамкою. Зокрема, Н. Ракха (Rakha N.A.) досліджує виклики, які цифрова форензика ставить перед кримінальним процесуальним правом, обґрунтовуючи потребу в уніфікації процедур обігу цифрових доказів та нових інституційних структурах, здатних оперувати сучасними аналітичними інструментами [14].

Таким чином, зарубіжна наукова думка демонструє чіткий тренд до інтелектуалізації та проактивності аналітичних процесів. Основний акцент зміщується з ретроспективного опису вчинених злочинів на предиктивне моделювання загроз за допомогою штучного інтелекту та побудову стратегічних систем кіберрозвідки, що вимагає одночасного оновлення нормативно-правової бази.

Водночас, юридичний та інституційний виміри протидії кіберзлочинності базуються на поведінковому аналізі злочинів, типології інцидентів та розробці моделей публічно-приватної співпраці [15]. Науковці констатують відсутність єдиного глобального визна-

чення кібербезпеки та вказують на гостру потребу в скоординованій міжнародній політиці та підготовці кадрів [16]. Значним викликом для сучасної юриспруденції залишається відсутність уніфікованих процедур обігу цифрових доказів та потреба в чітких правових рамках для цифрової форензики в межах кримінальних розслідувань [17].

В контексті вітчизняного законодавства обґрунтовується трансформація адміністративно-правового статусу суб'єктів протидії кіберзлочинності, що включає пропозиції щодо створення спеціалізованих підрозділів розслідування. Теоретико-правові засади формування національної системи кібербезпеки в контексті євроінтеграції ґрунтовно досліджені у працях В. Євдокимова, Д. Грицишена [18], які акцентують увагу на необхідності гармонізації українського законодавства з європейською системою протидії кібезлочинності. Особливості запобігання та методики розслідування цієї категорії кримінальних правопорушень розглядали О. Денькович, В. Луцик, Д. Цехан [19] К. Чаплинський [20]. При цьому міжнародно-правове співробітництво та імплементація положень Будапештської конвенції залишаються невід'ємним підґрунтям для формування національних стратегій цифрової безпеки. Кримінологічна характеристика сучасної кіберзлочинності та стратегії превенції стали предметом дослідження у низці авторських публікацій [21-27]. Водночас гуманітарний аспект імплементації саме IOCTA залишається недостатньо висвітленим, що створює розрив між технологічними спроможностями та рівнем суспільної довіри.

Для врахування цієї специфічної особливості розвитку вітчизняного науково-практичного дискурсу, запропоновано використання відповідної методологічної бази із врахуванням положень концепції соціологічного інституціоналізму, зокрема праць представників Стенфордської школи.

У дослідженнях Дж. Мейєра (Meyer J.) та Б. Роуена (Rowan B.), обґрунтовано концепцію «декаплінгу» (decoupling), яка пояснює ризики формального впровадження іноземних моделей без їх реальної інтеграції у внутрішні процеси організації чи держави [28]. Водночас, У. Скотт (Scott W.) розглядає інституційну спроможність як результат гармонізації регуляторних, нормативних та культурно-когнітивних елементів [29]. У межах цієї логіки успіх запозиченої методології IOCTA залежить не від її внутрішньої якості як технічного продукту Європолу, а від глибини її «перекладу» в місцевий правовий та соціальний контекст. Саме «реконтекстуалізація» міжнародних стандартів через призму гуманітарного завдання є запобіжником від інституційного ізоморфізму, що веде до неефективності [30].

Метою статті є обґрунтування гуманітарного вектора та процесуального змісту імплементації методології IOCTA в Україні як засобу зміцнення інституційної стійкості та формування культури прогностичної аналітики.

Основні результати дослідження.

Гуманітарний вимір цифрової безпеки в умовах збройної агресії: правова природа та новітні уразливості

У сучасній юридичній науці цифрова безпека все частіше постає не лише як технічна або правозастосовна функція, а як комплексне гуманітарне завдання, що безпосередньо впливає на життя людей, стабільність державних інституцій та рівень довіри у суспільстві. З розвитком цифрової інфраструктури, особливо в умовах воєнного стану та гібридних загроз, потреба у системному осмисленні безпеки онлайн-середовища вийшла за межі вузькопрофільних технічних рішень. Вона перетворилася на міждисциплінарний виклик, де об'єднуються технології, право, етика, соціальна відповідальність та публічна політика.

Україна, долаючи наслідки повномасштабної агресії, стала ареною для тестування новітніх форм цифрової уразливості: від масових кампаній дезінформації та цілеспрямованих кібератак на критичну інфраструктуру до поширення онлайн-насильства та фішингових схем. У таких обставинах цифрова безпека переходить у площину захисту фундаментальних прав – гідності, свободи і життєвої стабільності особи. Як зазначає М. Макгвайр (McGuire M.), у цифрову епоху право на безпеку має тлумачитися розширено, включаючи захист від маніпулятивного контенту, спрямованого проти вразливих груп населення [31].

У цьому контексті європейська методологія IOCTA (Internet Organised Crime Threat Assessment), розроблена Європолом, постає як важливий орієнтир для системного аналізу цифрових загроз та координації міжвідомчих дій [32; 33]. Проте, враховуючи напрацювання Стенфордської школи щодо ризиків «декаплінгу», пряме перенесення IOCTA до українського контексту вимагає глибокої адаптації [28; 29]. Це зумовлено не лише специфікою війни та вітчизняною правовою базою, а й необхідністю врахування гуманітарного виміру: цифрова безпека має не лише виявляти ризики, а й пропонувати сценарії розвитку, які захищають людей у техносфері.

Методологічна трансформація: від «аналітики контролю» до «аналітики довіри»

Методологічна еволюція цифрової аналітики в Україні відображає зміну парадигми мислення щодо природи цифрових загроз та ролі правоохоронних органів. Стратегічний аналіз на основі методології ІОСТА базується на централізованому зборі правоохоронних даних, аналізі транзакцій та криптовалютних потоків. Її інституційна логіка орієнтована на запобігання організованій злочинності через мережеву розвідку та криміналістику.

Натомість українська правова та аналітична рамка, що формується в умовах гібридної війни, спирається на ширше поле джерел: відкриті дані (OSINT), гуманітарні спостереження, аналіз соціальних медіа та сигнали від територіальних громад. Це дозволяє ідентифікувати не лише склад злочину, а й осмислити його вплив на рівень довіри до державних інституцій.

Важливим нововведенням є поява критеріїв аналітичної валідності, таких як соціальна релевантність та наративна глибина. Як підкреслює П. Грабоський (Grabosky P.), в умовах постконфліктного відновлення факти втрачають силу, якщо вони не пояснюють вплив інформації на поведінку спільнот [34].

У межах цієї еволюції формується концепція «аналітики довіри», яка протистоїть класичній «аналітиці контролю». Якщо ІОСТА історично орієнтована на забезпечення інституційного реагування, то українська модель прагне до побудови міжсекторальної співпраці, де аналітика стає платформою діалогу. Аналітика довіри базується на принципах відкритості та етичності; вона не просто повідомляє про загрозу, а інформує про наслідки та мобілізує до спільного реагування.

Системні ризики «декаплінгу» в правоохоронній діяльності: критичний аналіз імплементації методології SOCTA в Україні.

Дослідження процесів інституційної трансформації правоохоронних органів України неможливе без критичного аналізу досвіду імплементації методології SOCTA (Serious and Organised Crime Threat Assessment) [35; 36]. Попри задекларовану інтеграцію європейських стандартів стратегічного аналізу, практична реалізація цієї моделі часто демонструє ознаки «декаплінгу» – явища, описаного представниками Стенфордської школи соціологічного інституціоналізму (Дж. Мейєр, Б. Роуен), як стан формальної відповідності структурі за відсутності реальної зміни змісту аналітичної діяльності. Основним викликом став розрив між теоретичною рамкою ризик-орієнтованого підходу та існуючою процесуальною парадигмою досудового розслідування [37].

Аналіз вітчизняної практики свідчить про поступову втрату проактивності аналітики. Замість предиктивного моделювання загроз, як того вимагають стандарти ЄС щодо Intelligence-led Policing [38], аналітичні продукти часто зводяться до узагальнення статистичних даних щодо вже вчинених правопорушень. Це призводить до відсутності реальної оцінки ризиків як динамічного процесу виявлення системних уразливостей. У результаті, стратегічні звіти втрачають свою управлінську цінність, перетворюючись на формальні реляції, які не здатні впливати на пріоритезацію ресурсів чи зміну оперативних тактик.

Ключовою проблемою залишається неспроможність прогнозного використання результатів. У межах соціологічного інституціоналізму це пояснюється опором існуючої правової культури, де показником ефективності залишається кількість зареєстрованих проваджень, а не рівень зниження ризиків вчинення злочинів та ризиків вразливості безпекового середовища. Неспроможність імплементації методології у площину прикладних правових рішень призвела до того, що інструмент, створений для випередження організованої злочинності, в українських реаліях часто працює в режимі «ретроспективного опису».

Такий невдалий приклад імплементації SOCTA слугує застереженням для процесу впровадження ІОСТА. Нерозуміння того, що успіх запозиченої методології залежить від її глибокої реконтекстуалізації та формування нових інституційних компетентностей, може призвести до повторення помилок: створення «карго-культу» цифрової безпеки, де за європейською фасадною структурою ховатиметься неспроможність адекватно оцінювати та прогнозувати загрози у кіберпросторі.

Аналітична етика як запобіжник інституційної деградації: гуманітарний вимір.

Аналітична етика в межах нової гуманітарної парадигми в Україні постає як фундаментальний правовий та професійний запобіжник, оскільки в умовах постконфліктної реальності дані перестають бути нейтральними об’єктами. Вони безпосередньо впливають на стан суспільної стійкості, довіри та правопорядку. У цьому контексті цифрова аналітика трансформується у форму сучасного гуманізму, здатну захищати людську гідність, забезпечувати свободу вибору та посилювати психологічну витривалість громад.

Принципи дії – гідність, свобода, стійкість та співпраця – формують ціннісний кар-

кас аналітичної практики. Вони визначають стратегічні орієнтири: об'єкт аналізу, цільову аудиторію та тональність аналітичного продукту. Як зазначає М. Макгвайр, етична зорієнтованість є критичною при роботі з вразливими групами [31]. Впровадження цих принципів на всіх етапах, від збору даних до презентації висновків, дозволяє мобілізувати суспільство до спільної дії, уникаючи продукування страху чи соціального розколу. Особливого значення набуває інтеграція емоційного інтелекту та соціальної емпатії у методологію, що дозволяє аналітику ідентифікувати невербальні сигнали тривоги чи запити на допомогу в публічному цифровому просторі.

Мультисекторальність та комунікативний дизайн: від звітів до стратегічних смислів.

Мультисекторальний підхід трансформує цифрову аналітику з вузькопрофесійної галузі у публічний стратегічний інструмент. Така еволюція зумовлена необхідністю не лише оперативного реагування на кіберризики, а й комунікації цих загроз у спосіб, що підтримує демократичні процеси та соціальну згуртованість. Це вимагає зміни характеру аналітичних продуктів: перехід від суто технічних звітів до стратегічних записок, мультимедійних кейсів та освітніх матеріалів, адаптованих до потреб різних аудиторій.

У цьому контексті суттєво змінюється роль аналітика: він перестає бути лише «генератором даних» і стає комунікатором сенсів та модератором суспільного діалогу. Здатність аналітика передавати складну юридичну та технічну інформацію у доступній та етичній формі стає критично важливою для зміцнення довіри до державних інституцій. Мультисекторальність у поєднанні з комунікативним дизайном виступає механізмом побудови інклюзивного інформаційного середовища, де аналітика є джерелом не лише рішень, а й інституційного натхнення.

Практичне застосування та системні виклики: шлях до української школи аналітики.

Практична імплементація гуманітарної аналітики в Україні охоплює забезпечення цифрової безпеки територіальних громад, протидію дезінформації та підтримку процесів регіональної реконструкції. Проте застосування цієї моделі стикається з низкою системних бар'єрів:

низький рівень довіри до правоохоронних та державних інституцій;

фрагментованість міжсекторальної комунікації;

недостатній рівень компетентності фахівців у сфері етичного аналізу.

Для подолання цих викликів пропонується створення української школи аналітики, яка поєднуватиме технічне навчання з розвитком стратегічного мислення та закріпленням суспільної ролі аналітика як етичного медіатора. Така школа має базуватися на мультидисциплінарному підході, де аналітичні навички доповнюються знаннями гуманітарних принципів та практиками соціального моніторингу. Це дозволить перетворити аналітика на рушія соціального оновлення та архітектора довіри в цифровому середовищі. Стратегічний аналітичний цикл: регламентна та ресурсна модель управління ризиками.

Ефективна імплементація методології IOCTA в Україні вимагає переходу до безперервного операційного циклу, що органічно поєднує кількісні технологічні методи із якісними гуманітарними дослідженнями. Запропонована модель стратегічного аналізу розглядається як безперервна діяльність, де процес трансформації первинних даних у стратегічні рішення починається з постійного моніторингу цифрового середовища (OSINT-горизонт). На цьому щомісячному етапі здійснюється системний збір інформації з відкритих джерел, технічних форумів та мереж Dark Web, що дозволяє не лише фіксувати тактики і методи зловмисників , а й здійснювати гуманітарну ідентифікацію категорій потерпілих, оцінюючи еволюцію інструментарію маніпулятивного впливу на свідомість громадян. Отримана інформація проходить обов'язкову стадію верифікації та очищення від «інформаційного шуму», що гарантує формування об'єктивної картини поточних загроз.

Для подолання ризиків інституційного формалізму та «декаплінгу» впроваджується рівень експертної валідації через масові опитування та глибинні інтерв'ю. Щорічне опитування фахівців дозволяє здійснити аналітичне опрацювання ризиків та оцінити власну інституційну кіберстійкість держави, тоді як щоквартальні інтерв'ю зі спеціалістами забезпечують отримання інсайдерських даних про організаційні прогалини в захисті. Наступним критично важливим етапом є комплексний Форсайт, спрямований на предиктивне моделювання майбутнього за ключовими векторами діяльності. Застосування методів сценарного планування дозволяє виявляти «слабкі сигнали» та нові технології, такі як агентний штучний інтелект, що можуть стати критичними інструментами порушення прав людини у майбутньому.

Завершальна стадія циклу передбачає підготовку стратегічного звіту за зразком

IOCTA, який, на відміну від ретроспективної статистики, містить адресні рекомендації щодо модернізації нормативної бази та перерозподілу ресурсів на користь захисту вразливих сегментів суспільства. Процес замикається етапом адаптації та навчання, де висновки з подоланих інцидентів інтегруються у нові предиктивні алгоритми, а аналітичні навички фахівців доповнюються знаннями гуманітарних принципів у межах стратегічної експертизи. Обов'язковим елементом цього етапу є впровадження стандартизованих інструментів оцінки результатів: системного аудиту ефективності вжитих заходів протидії та вимірювання реального впливу реалізованих стратегій на стан захищеності цифрового середовища. Такий підхід дозволяє верифікувати дієвість інструментарію не за кількістю формальних звітів, а за показниками фактичного зниження рівня вразливості та підвищення якості реагування. Таким чином, регламентована модель перетворює аналітичний процес на динамічну систему захисту національного цифрового суверенітету, де технологічна досконалість виступає інструментом забезпечення людської гідності та зміцнення суспільної довіри

Висновки. У результаті проведеного дослідження обґрунтовано, що імплементація європейської методології IOCTA в Україні має відбуватися не шляхом формального запозичення технічних інструментів, а через парадигмальний зсув у бік гуманітарного виміру цифрової безпеки. На основі аналізу соціолого-інституційних ризиків «декаплінгу» та врахування досвіду впровадження SOCTA доведено, що успіх міжнародних стандартів прямо залежить від глибини їх «реконтекстуалізації» в національне соціоправове поле.

Основними науковими та практичними результатами проведеного дослідження є теоретичне обґрунтування та розробка концепції «аналітики довіри», яка, на відміну від класичної «аналітики контролю», фокусується на зміцненні суспільної стійкості та забезпеченні захисту конституційних прав людини в онлайн-середовищі. В умовах гібридної агресії така парадигма стає критично важливою, оскільки вона зміщує акцент з механічного моніторингу на превентивний захист інтересів громадян. У межах цієї концепції визначено, що стратегічний аналітичний цикл за методологією IOCTA повинен функціонувати як безперервна операційна система, що інтегрує OSINT-моніторинг, предиктивне сценарне моделювання та багаторівневу етичну валідацію даних через експертні інтерв’ю та форсайт-дослідження.

Логічним завершенням запропонованої моделі є обґрунтування необхідності розбудови української школи аналітики на основі розвитку міждисциплінарного інституту підготовки фахівців нового типу. Такі фахівці мають володіти здатністю поєднувати глибоку цифрову експертизу з високою етичною відповідальністю та соціальною емпатією, що дозволить перетворити аналітичний процес на дієвий інструмент зміцнення суспільної згуртованості та національної стійкості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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

2. Shukla, G. (2023). Cyber crime investigation and digital forensics. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4616519.

3. Dunsin, D., Ghanem, M., Ouazzane, K., & Vassilev, V. (2023). A Comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response. Forensic Sci. Int. Digit. Investig., 48, 301675. https://doi.org/10.1016/j.fsidi.2023.301675.

4. Khan, H., Atif, S., & Mustufa, A. (2025). The Role of Digital Forensics in Cybercrime Investigations. NUML International Journal of Engineering and Computing. https://doi.org/10.52015/nijec.v3i2.85.

5. Narasimhan, P., & Kala, N. (2025). Emerging Trends in Digital Forensics : Investigating Cybercrime. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. https://doi.org/10.32628/cseit251451.

6. Al Khater W. та ін. Comprehensive Review of Cybercrime Detection Techniques. IEEE Access. 2020. DOI: 10.1109/ACCESS.2020.3011259

7.Cascavilla G., Tamburri D., Heuvel W. Cybercrime Threat Intelligence: A Systematic Multi Vocal Literature Review. Computers & Security. 2021. DOI: 10.1016/j.cose.2021.102258

8.Saeed M., Alshahrani Z., Mahmoud A.I., Ramadan. Cyber Attacks – Trends, Patterns, and Security Countermeasures. 2020.

9. Didenko, O. (2025). Digital forensics and international counteraction to cybercrime (based on the example of e-commerce). Analytical and Comparative Jurisprudence. https://doi.org/10.24144/2788-6018.2025.04.3.26.

10. Al-Husaini, Y., Al-Khateeb, H., Warren, M., Pan, L., & Epiphaniou, G. (2020). Collaborative Digital Forensic Investigations Model for Law Enforcement. Security and Organization within IoT and Smart Cities. https://doi.org/10.1201/9781003018636-9.

11. Korzun, S. (2024). Transformation of the administrative and legal status of cybercrime countermeasures entities. Public Policy and Accounting. https://doi.org/10.26642/ppa-2024-2(10)-53-62

12.Askar, F.A. et al. trans. 2025. Evaluating the Effectiveness of Digital Forensic Investigations in Combating Cybercrime. Journal of Science and Technology. 30, 10 (Sep. 2025). DOI:https://doi.org/10.20428/jst.v30i10.2911..

13.Cassidy A.A.T.J., Fuad A., As Shofy M.U.A. Emerging Trends and Challenges in Digital Crime: Cyber Criminal Tactics and Countermeasures. TechComp Innovations. 2024. DOI: 10.70063/techcompinnovations.v1i1.25

14. Rakha N.A. Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. Mexican Law Review. 2024. DOI: 10.22201/iij.24485306e.2024.2.18892.

15. Sarkar, G., & Shukla, S. (2023). Behavioral Analysis of Cybercrime: Paving the Way for Effective Policing Strategies. Journal of Economic Criminology. https://doi.org/10.1016/j.jeconc.2023.100034.

16. Mphatheni, M., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime. International Journal of Research in Business and Social Science (2147- 4478). https://doi.org/10.20525/ijrbs.v11i4.1714.

17. Surakanti, S., Goundar, S., & Dwight, J. (2025). Countering anti-forensic tactics in cybercrime investigations – a systematic literature review. International Journal of Information Security, 24. https://doi.org/10.1007/s10207-025-01131-y.

18. Стратегія інтеграції державної політики протидії кіберзлочинності в європейську систему кібербезпеки : монографія / За загальною редакцією В. В. Євдокимова, Д. О. Грицишена. – Житомир : Вид. О. О. Євенок, 2024. –300с.

19. Кіберзлочинність та електронні докази : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. Юрид. Наук, доц. Ольги Денькович, д-ра права, проф. Габріеле Шмельцер. – Електрон. Вид. – Львів : ЛНУ імю Івана Франка, 2022. – 298 с.

20. Методика розслідування шахрайства в інтернет-комерції: теорія та практика : монографія / К. О. Чаплинський, А. В. Рейнгольд, Н. В. Павлова. — Одеса : Видавництво «Юридика», 2024. — 242 с.

21.Korystin O., Korchenko O., Kazmirchuk S., Demediuk S., Korystin O. Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Sets Theory. International Journal of Computer Network and Information Security. 2024. Vol. 16. №. 1. P. 24-34. DOI: https://doi.org/10.5815/ijcnis.2024.01.02. SCOPUS Q3

22.Korystin O., Demediuk S., Likhovitskyy Y., Kardashevskyy Y., Mitina O. Priorities for the Strategic Development of Ukraine's Cybersecurity Based on the Analysis of Expert Sampling Patterns, International Journal of Information Technology and Computer Science. 2025. Vol. 17. No. 2. P. 24-35. DOI: https://doi.org/10.5815/ijitcs.2025.02.03 (SCOPUS Q3)

23.Korchenko O., Korystin O., Shulha V., Kazmirchuk S., Demediuk S., Zybin S. Sustainable Development of Smart Regions via Cybersecurity of National Infrastructure: A Fuzzy Risk Assessment Approach. Sustainability. (2025). Vol. 17. Is. 19. P. 8757. https://doi.org/10.3390/su17198757

24. Користін О.Є., Демедюк С.В., Панченко Є.В., Користін О.О. Національні реалії аналізу кіберзлочинності за методологією Європолу IOCTA. Південноукраїнський правничий часопис. 2023. № 3. С.53-59. DOI https://doi.org/10.32850/sulj.2023.3.10

25. Демедюк С.В., Користін О.Є. Тенденції та характерні особливості on-line шахрайства в Україні. Наука і правоохорона. 2024. Том 3-4. № 65-66. С. 142-154. DOI: https://doi.org/10.36486/np.2024.3(65).12

26. Демедюк С.В. Сучасні тенденції on-line шахрайства в Україні. Право і суспільство. 2025. №4. Т. 2. С. 186-194. DOI: https://doi.org/10.32842/2078-3736/2025.4.2.28

27. Демедюк С.В. Темна сторона комп'ютерних мереж: злочини та незаконна діяльність он-лайн. Правові новели. 2025. № 26. 157-166. DOI: https://doi.org/10.32782/ln.2025.26.18

28.Meyer J. W., Rowan B. Institutionalized Organizations: Formal Structure as Myth and Ceremony. American Journal of Sociology. 1977. Vol. 83, No. 2. P. 340–363. http://dx.doi.org/10.1086/226550

29.Scott W. R. Institutions and Organizations: Ideas, Interests, and Identities. 4th ed. SAGE Publications, 2013. 360 p.

30.Brenner, Susan W, Cyber Threats: The Emerging Fault Lines of the Nation State (New York, 2009; online edn, Oxford Academic, 1 Sept. 2009), https://doi.org/10.1093/acprof:oso/9780195385014.001.0001.

31.McGuire M. Hypercrime: The New Geometry of Harm. Routledge, 2007. 400 p.

32.Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024. URL: https://www.europol.europa.eu/publications-events/main-reports/iocta-2024.

33.Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf

34.Grabosky P. Cybercrime. Cambridge University Press, 2016. 168 p.

35.EU-SOCTA 2025. EUROPEAN UNION SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT. https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA%202025%20-%20Executive%20Summary.pdf

36.Постанова КМУ від 26 січня 2022 р. №59. Деякі питання запровадження в діяльність центральних органів виконавчої влади системи оцінки SOCTA Україна. https://zakon.rada.gov.ua/laws/show/en/59-2022-%D0%BF/ed20220126#n64

37.Korystin O., Svyrydiuk N. NATIONAL REALITIES OF IMPLEMENTATION OF EUROPOL METHODOLOGY "SOCTA". South Ukrainian Law Journal. January 2022. DOI: 10.32850/sulj.2022.1-2.20.

38.Ratcliffe, J. H. (2016). Intelligence-Led Policing. Australian Institute of Criminology. https://doi.org/10.4324/9781315717579

Внесок авторів: всі автори зробили рівний внесок у цю роботу
Конфлікт інтересів: автори повідомляють про відсутність конфлікту інтересів

Стаття надійшла до редакції 11.03.2026 Переглянуто 15.04.2026
Стаття рекомендована до друку 24.05.2026 Опубліковано 30.05.2026

O.Y. KORYSTIN
DSc (Law), Professor, Honored Worker of Science and Technology of Ukraine
E-mail: alex@korystin.pro ORCID: https://orcid.org/0000-0001-9056-5475
Cyber Police Department of the National Police of Ukraine
19 Boryspilska St., Kyiv, 02093
Institute of Cyber Warfare Research
16b Shovkovychna St., Kyiv, 01024

S.V. DEMEDIUK
PhD in Law, Associate Professor
E-mail: cyberdemediuk@protonmail.com ORCID: https://orcid.org/0009-0008-1359-5265
National Academy of the Security Service of Ukraine
22 M. Maksymovycha St., Kyiv, 03066
Institute of Cyber Warfare Research
16b Shovkovychna St., Kyiv, 01024

LEGAL AND METHODOLOGICAL FOUNDATIONS FOR THE IMPLEMENTATION OF EUROPEAN IOCTA STANDARDS IN THE DIGITAL SECURITY SYSTEM OF UKRAINE: A HUMANITARIAN ASPECT

ANNOTATION. *Introduction.* The article provides a comprehensive theoretical and legal analysis of the implementation of the European methodology for the Internet Organised Crime Threat Assessment (IOCTA) into the national digital security system. The relevance of the study is driven by the necessity to transform techno-centric approaches to cybersecurity under martial law and transition toward an anthropocentric model for protecting citizens' constitutional rights. The problem statement identifies the risks of "institutional isomorphism" and the phenomenon of "decoupling" in the formal adoption of Western models without proper recontextualization. The methodological framework of the study is based on the concepts of sociological institutionalism from the Stanford School, the system-structural method, and methods of predictive risk modeling. The aim of the article is to justify the humanitarian vector of digital security as a foundation for Ukraine's institutional resilience.

Summary of the main research results. It is proven that digital security in modern conditions is not merely a technical function but a critical humanitarian task aimed at protecting human dignity and freedom. The author conducts a critical analysis of previous experience with implementing the SOCTA methodology in Ukraine, which revealed a loss of proactive analytics and an inability to use results predictively due to a formalistic approach to standard adoption. The transition from "analytics of control" to "analytics of trust" is justified, where the key indicator is the strengthening of social resilience. The article details the regulations of the strategic analytical cycle, including continuous OSINT monitoring, expert validation through in-depth interviews, and comprehensive Foresight analysis across priority sectors. Particular attention is paid to the ethical component of the analytical process, where the analyst emerges as a communicator of strategic meanings and an ethical mediator. The creation of a "ukrainian school of analytics" is proposed to develop new institutional competencies for law enforcement agencies.

Conclusions. A new paradigm for digital security is formulated, based on predictive risk management and institutional capacity to adapt international standards to a specific socio-legal context. It is concluded that the success of IOCTA implementation depends on the analytical system's ability to detect "weak signals" of technological threats while subordinating them to the protection of human dignity and the strengthening of the democratic order. Building a culture of predictive analytics is identified as a key step toward overcoming systemic vulnerabilities and ensuring Ukraine's sustainable development in the era of global digitalization.

KEY WORDS: *digital security, IOCTA, humanitarian aspect, analytics of trust, decoupling, strategic analytical cycle.*

REFERENCES

1.Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (in Ukrainian)

2. Shukla, G. (2023). Cyber crime investigation and digital forensics. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4616519.

3. Dunsin, D., Ghanem, M., Ouazzane, K., & Vassilev, V. (2023). A Comprehensive Analysis of the Role of Artificial Intelligence and Machine Learning in Modern Digital Forensics and Incident Response. Forensic Sci. Int. Digit. Investig., 48, 301675. https://doi.org/10.1016/j.fsidi.2023.301675.

4. Khan, H., Atif, S., & Mustufa, A. (2025). The Role of Digital Forensics in Cybercrime Investigations. NUML International Journal of Engineering and Computing. https://doi.org/10.52015/nijec.v3i2.85.

5. Narasimhan, P., & Kala, N. (2025). Emerging Trends in Digital Forensics : Investigating Cybercrime. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. https://doi.org/10.32628/cseit251451.

6. Al Khater W. та ін. Comprehensive Review of Cybercrime Detection Techniques. IEEE Access. 2020. DOI: 10.1109/ACCESS.2020.3011259

7.Cascavilla G., Tamburri D., Heuvel W. Cybercrime Threat Intelligence: A Systematic Multi Vocal Literature Review. Computers & Security. 2021. DOI: 10.1016/j.cose.2021.102258

8.Saeed M., Alshahrani Z., Mahmoud A.I., Ramadan. Cyber Attacks – Trends, Patterns, and Security Countermeasures. 2020.

9. Didenko, O. (2025). Digital forensics and international counteraction to cybercrime (based on the example of e-commerce). Analytical and Comparative Jurisprudence. https://doi.org/10.24144/2788-6018.2025.04.3.26.

10. Al-Husaini, Y., Al-Khateeb, H., Warren, M., Pan, L., & Epiphaniou, G. (2020). Collaborative Digital Forensic Investigations Model for Law Enforcement. Security and Organization within IoT and Smart Cities. https://doi.org/10.1201/9781003018636-9.

11. Korzun, S. (2024). Transformation of the administrative and legal status of cybercrime countermeasures entities. Public Policy and Accounting. https://doi.org/10.26642/ppa-2024-2(10)-53-62

12.Askar, F.A. et al. trans. 2025. Evaluating the Effectiveness of Digital Forensic Investigations in Combating Cybercrime. Journal of Science and Technology. 30, 10 (Sep. 2025). DOI: https://doi.org/10.20428/jst.v30i10.2911.

13.Cassidy A.A.T.J., Fuad A., As Shofy M.U.A. Emerging Trends and Challenges in Digital Crime: Cyber Criminal Tactics and Countermeasures. TechComp Innovations. 2024. DOI: 10.70063/techcompinnovations.v1i1.25

14.Rakha N.A. Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. Mexican Law Review. 2024. DOI: 10.22201/iij.24485306e.2024.2.18892.

15. Sarkar, G., & Shukla, S. (2023). Behavioral Analysis of Cybercrime: Paving the Way for Effective Policing Strategies. Journal of Economic Criminology. https://doi.org/10.1016/j.jeconc.2023.100034.

16. Mphatheni, M., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime. International Journal of Research in Business and Social Science (2147- 4478). https://doi.org/10.20525/ijrbs.v11i4.1714.

17. Surakanti, S., Goundar, S., & Dwight, J. (2025). Countering anti-forensic tactics in cybercrime investigations – a systematic literature review. International Journal of Information Security, 24. https://doi.org/10.1007/s10207-025-01131-y.

18. Stratehiia intehratsii derzhavnoi polityky protydii kiberzlochynnosti v yevropeisku systemu kiberbezpeky : monohrafiia / Za zahalnoiu redaktsiieiu V. V. Yevdokymova, D. O. Hrytsyshena. – Zhytomyr : Vyd. O. O. Yevenok, 2024. –300c. (in Ukrainian)

19. Kiberzlochynnist ta elektronni dokazy : navch. posibnyk / [B. M. Holovkin, O. I. Denkovych, V. V. Lutsyk, D. M. Tsekhan] ; za red. kand. Yuryd. Nauk, dots. Olhy Denkovych, d-ra prava, prof. Habriele Shmeltser. – Elektron. Vyd. – Lviv : LNU imiu Ivana Franka, 2022. – 298 c. (in Ukrainian)

20. Metodyka rozsliduvannia shakhraistva v internet-komertsii: teoriia ta praktyka : monohrafiia / K. O. Chaplynskyi, A. V. Reinhold, N. V. Pavlova. — Odesa : Vydavnytstvo «Yurydyka», 2024. — 242 c. (in Ukrainian)

21.Korystin O., Korchenko O., Kazmirchuk S., Demediuk S., Korystin O. Comparative Risk Assessment of Cyber Threats Based on Average and Fuzzy Sets Theory. International Journal of Computer Network and Information Security. 2024. Vol. 16. №. 1. P. 24-34. DOI: https://doi.org/10.5815/ijcnis.2024.01.02. SCOPUS Q3

22.Korystin O., Demediuk S., Likhovitskyy Y., Kardashevskyy Y., Mitina O. Priorities for the Strategic Development of Ukraine's Cybersecurity Based on the Analysis of Expert Sampling Patterns, International Journal of Information Technology and Computer Science. 2025. Vol. 17. No. 2. P. 24-35. DOI: https://doi.org/10.5815/ijitcs.2025.02.03 (SCOPUS Q3)

23.Korchenko O., Korystin O., Shulha V., Kazmirchuk S., Demediuk S., Zybin S. Sustainable Development of Smart Regions via Cybersecurity of National Infrastructure: A Fuzzy Risk Assessment Approach. Sustainability. (2025). Vol. 17. Is. 19. P. 8757. https://doi.org/10.3390/su17198757

24. Korystin O.Ye., Demediuk S.V., Panchenko Ye.V., Korystin O.O. Natsionalni realii analizu kiberzlochynnosti za metodolohiieiu Yevropolu IOSTA. Pivdennoukrainskyi pravnychyi chasopys. 2023. № 3. S.53-59. DOI https://doi.org/10.32850/sulj.2023.3.10(in Ukrainian)

25. Demediuk S.V., Korystin O.Ye. Tendentsii ta kharakterni osoblyvosti on-line shakhraistva v Ukraini. Nauka i pravookhorona. 2024. Tom 3-4. № 65-66. S. 142-154. DOI: https://doi.org/10.36486/np.2024.3(65).12 (in Ukrainian)

26. Demediuk S.V. Suchasni tendentsii on-line shakhraistva v Ukraini. Pravo i suspilstvo. 2025. №4. T. 2. S. 186-194. DOI: https://doi.org/10.32842/2078-3736/2025.4.2.28(in Ukrainian)

27. Demediuk S.V. Temna storona kompiuternykh merezh: zlochyny ta nezakonna diialnist on-lain. Pravovi novely. 2025. № 26. 157-166. DOI: https://doi.org/10.32782/ln.2025.26.18(in Ukrainian)

28. Meyer J. W., Rowan B. Institutionalized Organizations: Formal Structure as Myth and Ceremony. American Journal of Sociology. 1977. Vol. 83, No. 2. P. 340–363. http://dx.doi.org/10.1086/226550

29.Scott W. R. Institutions and Organizations: Ideas, Interests, and Identities. 4th ed. SAGE Publications, 2013. 360 p.

30.Brenner, Susan W, Cyber Threats: The Emerging Fault Lines of the Nation State (New York, 2009; online edn, Oxford Academic, 1 Sept. 2009), https://doi.org/10.1093/acprof:oso/9780195385014.001.0001.

31.McGuire M. Hypercrime: The New Geometry of Harm. Routledge, 2007. 400 p.

32.Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024. URL: https://www.europol.europa.eu/publications-events/main-reports/iocta-2024.

33.Europol. Internet Organised Crime Threat Assessment (IOCTA) 2024. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf

34.Grabosky P. Cybercrime. Cambridge University Press, 2016. 168 p.

35.EU-SOCTA 2025. EUROPEAN UNION SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT. https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA%202025%20-%20Executive%20Summary.pdf

36.Postanova KMU vid 26 sichnia 2022 r. №59. Deiaki pytannia zaprovadzhennia v diialnist tsentralnykh orhaniv vykonavchoi vlady systemy otsinky SOCTA Ukraina. https://zakon.rada.gov.ua/laws/show/en/59-2022-%D0%BF/ed20220126#n64(in Ukrainian)

37.Korystin O., Svyrydiuk N. NATIONAL REALITIES OF IMPLEMENTATION OF EUROPOL METHODOLOGY "SOCTA". South Ukrainian Law Journal/ January 2022. DOI: 10.32850/sulj.2022.1-2.20.

38.Ratcliffe, J. H. (2016). Intelligence-Led Policing. Australian Institute of Criminology. https://doi.org/10.4324/9781315717579

Authors Contribution: All authors have contributed equally to this work
Conflict of Interest: The authors declare no conflict of interest

The article was received by the editors 11.03.2026 The article was revised 15.04.2026
The article is recommended for printing 24.05.2026 This article published 30.05.2026