по його парності роблять висновок, який саме біт (0 чи 1) було приховано у даному блоці.

Проведені експерименти показали високу візуальну якість стегоконтейнера (PSNR > 35 dB) та високу стійкість до шумів: гаусівського (при σ = 5 – відсоток відновлення повідомлення до 100%; σ = 15 – середній рівень шуму, відновлення до 80%); мультиплікативного (при низькому рівні імпульсного шуму P < 0,5 %) точність відновлення майже 100 %. Стійкість до компресії JPEG (Q=70, Q=50), завдяки варіативному вибору параметра α, одержували PSNR 45-40дБ.

1. Кобозєва А.А., Хорошко В.О. Аналіз захищеності інформаційних систем. К.: Вид. ДУІКТ, 2010. 309 с.

Вимоги до простежуваності та обґрунтованості результатів вимірювання критичності кіберінцидентів

УДК 004.056:006.91

Ярослав Тарасенко[1], Роман Орлов[2]

[1]Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки, yaroslav.tarasenko93@gmail.com,
[2]Державний університет інформаційно-комунікаційних технологій, romanorlov0110@gmail.com

У сучасних інформаційно-комунікаційних системах важливою умовою обґрунтованого реагування та вибору пріоритетів подальших дій є визначення критичності кіберінцидентів. У задачах реагування на кіберінциденти результат вимірювання критичності є основою для прийняття рішень. У роботі [1] автоматизована класифікація кіберінцидентів за рівнями тяжкості ґрунтується на наборі ознак і моделей їх інтерпретації. Підсумкова оцінка критичності повинна бути простежувана та спиратися на цифрові спостереження.

Перша вимога полягає у простежуваності результату до вихідних даних. Кожна оцінка повинна бути відновлювана на основі журналів подій, телеметрії, засобів виявлення та інших відомостей, використаних для її формування. Друга вимога простежуваності відноситься до обробки інформації та полягає у фіксації послідовності обробки даних і формуванні правил переходу від спостережень до підсумкової оцінки. Такий підхід ґрунтується на охопленні сутності, процесів та користувачів, пов’язаних з історією даних, що представлено у роботі [2]. До третьої вимоги варто віднести структурну обґрунтованість результату. Під структурною обґрунтованістю мається на увазі потребу у врахуванні впливу сукупності змістовних компонентів та контексту події на оцінку критичності. Четверта вимога, пов’язана з пояснюваністю, націлена на можливість демонстрації шляхів формування підсумкового результату критичності за рахунок ознак, вагових коефіцієнтів та порогових значень. Доцільність такої вимоги пояснена у роботі [3], де непрозорість моделей виступає чинником зниження довіри до кібербезпекових рішень, зокрема з використанням штучного інтелекту. П’ятою вимогою є відтворюваність результату. Отже, простежуваність даних і перетворень,

структурна обґрунтованість, пояснюваність та відтворюваність розглядаються як базові вимоги до результатів вимірювання критичності кіберінцидентів.

1. DeCastro-Garcia N., Munoz Castaneda A.L., Fernandez-Rodriguez M. Machine learning for automatic assignment of the severity of cybersecurity events. Computational and Mathematical Methods. 2020. Vol. 2, № 1. URL: https://doi.org/10.1002/cmm4.1072 (дата звернення: 02.05.2026)
2. Pan B., Stakhanova N., Ray S. Data provenance in security and privacy. ACM Computing Surveys. 2023. Vol. 55, Issue 14s. URL: https://doi.org/10.1145/3593294 (дата звернення: 03.05.2026).
3. A survey on explainable artificial intelligence for cybersecurity / G. Rjoub et al. IEEE transactions on network and service management. 2023. Vol. 20, № 4. P.5115-5140.

Відповідальність під час використання штучного інтелекту в судочинстві: теоретичні засади, правові виклики

УДК 347.9:004.8

Віталій Вітів

Тернопільський національний технічний університет імені Івана Пулюя

У сучасному світі стрімке впровадження штучного інтелекту в усі сфери суспільного життя створює значні виклики для судової системи та юриспруденції, зокрема щодо розподілу відповідальності [1, 2].

Алгоритми, що використовуються для аналізу даних, підготовки процесуальних документів, прогнозування судових рішень та автоматизації адміністративних процедур, здатні суттєво підвищити ефективність правосуддя, зменшити навантаження на суддів і сприяти більшій доступності справедливості. Водночас постає фундаментальне питання: хто повинен нести юридичну та моральну відповідальність за помилки, алгоритмічну упередженість, «галюцинації» чи порушення прав учасників процесу, спричинені діями штучного інтелекту. Додатковим ризиком є розголошення конфіденційної інформації та професійної таємниці через завантаження матеріалів до систем штучного інтелекту.

Українська правова система активно розвивається в напрямку цифровізації, однак комплексне регулювання використання штучного інтелекту в судочинстві ще не сформоване. Правові позиції в Україні щодо цієї технології є обережними. Зокрема, стаття 16 Кодексу суддівської етики передбачає, що використання суддею технологій штучного інтелекту є допустимим лише за умови, якщо воно не впливає на незалежність та неупередженість судді, не стосується оцінки доказів, процесу ухвалення рішень і не порушує вимог законодавства [5]. Аналогічний підхід закріплено в Законі України «Про адміністративну процедуру»: адміністративний орган несе відповідальність за акти, прийняті в автоматичному режимі (статті 62–69) [4].