

Проте впровадження систем штучного інтелекту в правоохоронній та безпековій діяльності має супроводжуватися урахуванням специфічних ризиків. По-перше, існує проблема "отруєння даних", коли зломисники можуть навмисно модифікувати навчальні вибірки для того, щоб модель ігнорувала певні типи вразливостей. По-друге, моделі ШІ самі по собі можуть бути вразливими до атак (Adversarial attacks) [3].

Висновки. Використання можливостей систем штучного інтелекту для аналізу вразливостей програмного забезпечення є перспективним напрямком, що дозволяє суттєво підвищити рівень кібербезпеки. Вони автоматизують рутинні процеси тестування, знижують навантаження на інженерів з безпеки та дозволяють виявляти складні логічні помилки. Однак для успішного використання таких систем у правоохоронній діяльності необхідно забезпечити прозорість алгоритмів прийняття рішень та створити надійні механізми захисту.

Список використаних джерел

1. Карпенко О. В. Штучний інтелект у кібербезпеці: сучасний стан та перспективи розвитку. *Інформаційні технології та захист інформації*. 2023. № 2. С. 45–52.
2. Buczak A. L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*. 2016. Vol. 18, no. 2. P. 1153–1176.
3. Мельник В. А. Використання нейронних мереж для статичного аналізу коду. *Науковий вісник кібербезпеки*. 2024. Вип. 1. С. 112–119.

Антон ЛИСЕНКО, курсант ННІ 2-25-104
Пд, Харківський національний університет
внутрішніх справ, рядовий поліції.

Науковий керівник:

Олександр СКЛЯР, старший викладач
кафедри тактико-спеціальної підготовки,
Харківський національний університет
внутрішніх справ, капітан поліції, доктор
філософії

ШТУЧНИЙ ІНТЕЛЕКТ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ: МОЖЛИВОСТІ ТА РИЗИКИ ЗАСТОСУВАННЯ

Використання штучного інтелекту в правоохоронній діяльності є одним із найбільш перспективних і водночас ризикованих напрямів цифрової трансформації держави. У правоохоронній діяльності штучний інтелект (далі ШІ) використовують для швидкої обробки великої кількості інформації, пошуку закономірностей, аналізу даних і допомоги працівникам поліції під час ухвалення рішень. У сучасних умовах ШІ може застосовуватися не як заміна слідчого, оперативного працівника, прокурора чи суду, а як допоміжний інструмент. Він підвищує швидкість аналізу інформації, покращує координацію підрозділів і дає змогу ефективніше реагувати на злочинність. При цьому використання ШІ повинно відповідати вимогам законодавства, не порушувати права людини та перебувати під контролем уповноважених органів.

Одним із найбільш практичних напрямів застосування ШІ в правоохоронній діяльності є аналітична обробка даних. Щодня правоохоронні органи опрацьовують велику кількість інформації: матеріали справ, відео, бази даних, повідомлення в соціальних мережах та інші джерела. ШІ може допомагати швидше аналізувати ці дані та знаходити зв'язки між подіями

й особами. Наприклад, алгоритми можуть допомагати у виявленні серійних правопорушень, шахрайських схем, кіберзлочинів, незаконних фінансових операцій, підроблених документів або повторюваних моделей поведінки правопорушників. INTERPOL також наголошує, що використання ІІІ в поліції повинно відповідати правам людини та етичним принципам [1, с. 91].

Одним із поширених напрямів використання ІІІ є відеоспостереження та розпізнавання об'єктів. Системи комп'ютерного зору можуть аналізувати відео з камер спостереження, розпізнавати номерні знаки транспортних засобів, фіксувати підозрілі предмети, виявляти залишені речі в громадських місцях, допомагати у пошуку зниклих осіб або встановленні маршруту руху певного транспортного засобу.

Однак найбільш дискусійним є використання технологій розпізнавання облич. З одного боку, вони можуть прискорити розшук осіб, ідентифікацію підозрюваних або потерпілих, а також допомогти в умовах масових подій чи надзвичайних ситуацій. Проте такі технології можуть помилятися та порушувати право людини на приватність, гарантоване Конституцією України. Саме тому в Європейському Союзі використання систем дистанційної біометричної ідентифікації в режимі реального часу у публічних місцях для правоохоронних цілей розглядається як особливо чутливе й допускається лише за суворих умов, зокрема за наявності спеціального дозволу та з урахуванням принципів необхідності й пропорційності [2, с. 261].

Окремий напрям становить прогнозна аналітика злочинності, тобто використання алгоритмів для визначення територій, часу або ситуацій із підвищеним ризиком вчинення правопорушень. Наприклад, система може аналізувати статистику попередніх правопорушень, соціально-економічні фактори, повторюваність подій, сезонність, транспортну активність і на основі цього пропонувати посилення патрулювання в певному районі. Проте такий підхід має суттєві ризики. Якщо система штучного інтелекту навчається на неповних, неточних або упереджених даних, вона може повторювати помилки, які вже існують у правоохоронній системі. У результаті поліція може частіше звертати увагу на окремі райони, соціальні групи чи певні категорії осіб навіть без достатніх підстав. Це створює ризик несправедливого ставлення та порушення прав людини. Тому рішення не повинні прийматися лише на основі прогнозів системи. Вона може бути лише інструментом планування ресурсів, але не самостійною підставою для обмеження прав особи, проведення обшуку, затримання або повідомлення про підозру [3, с. 46]. У кримінальному процесі ІІІ може застосовуватися для систематизації матеріалів провадження, пошуку релевантних документів, аналізу великих масивів електронних доказів, розшифрування аудіо- та відеозаписів, виявлення збігів у показаннях, підготовки аналітичних довідок.

Це особливо важливо у складних кримінальних провадженнях, пов'язаних з організованою злочинністю, корупцією, кіберзлочинами, фінансовими махінаціями або воєнними злочинами, де обсяг доказової інформації може бути надзвичайно великим. Водночас ІІІ не може самостійно визнавати особу винною, оцінювати докази замість суду чи підміняти процесуальну діяльність слідчого. Відповідно до принципів кримінального процесу, доказ має оцінюватися людиною – уповноваженою службовою особою або судом – з урахуванням належності, допустимості, достовірності та достатності. ІІІ може допомагати в аналізі даних, але остаточне рішення повинна приймати людина.

Особливу увагу потрібно приділити захисту персональних даних. Правоохоронна діяльність часто передбачає обробку чутливої інформації: біометричних даних, даних про місце перебування, комунікації, фінансові операції, соціальні зв'язки, судимість, стан здоров'я або інші персональні відомості. Використання ІІІ також створює ризик витоку даних або їх неправильного використання. Тому використання ІІІ в правоохоронних органах повинно чітко регулюватися законом і застосовуватися лише в межах визначених повноважень. У цьому контексті важливим є підхід Ради Європи, яка у Рамковій конвенції про штучний інтелект наголошує на тому, що системи ІІІ повинні використовуватися з дотриманням прав людини та вимог законодавства [4, с. 180].

Для України питання використання ІІІ в правоохоронній діяльності має особливе значення через умови воєнного стану, зростання кіберзагроз, необхідність документування

воєнних злочинів, протидію колабораційній діяльності, шахрайству, незаконному обігу зброї, дезінформації та іншим загрозам безпеці. ШІ може використовуватися для фіксації доказів, обробки супутникових знімків і пошуку інформації у відкритих джерелах. Також він допомагає виявляти інформаційні операції, аналізувати повідомлення громадян та встановлювати зв'язок між різними подіями. Однак саме в умовах війни ризик надмірного втручання держави в права людини є особливо високим, тому застосування таких технологій має супроводжуватися парламентським, судовим, прокурорським, відомчим і громадським контролем. Україна вже рухається до формування правового регулювання ШІ: Міністерство цифрової трансформації презентувало дорожню карту регулювання штучного інтелекту, яка передбачає поступову підготовку до майбутнього законодавства, наближеного до європейського AI Act.

Серед основних проблем використання ШІ можна виділити помилки систем, неточне розпізнавання людей і можливе порушення прав людини. Наприклад, якщо система помилково вказує на особу як на ймовірного правопорушника, виникає питання: хто відповідатиме за наслідки – розробник програми, орган, який її закупив, оператор системи чи посадова особа, яка використала результат? Тому остаточне рішення завжди повинна приймати людина. Кінцевий висновок про застосування примусових заходів, повідомлення про підозру, затримання, проведення слідчої дії або передачу справи до суду не може ухвалюватися виключно алгоритмом. ШІ має надавати допоміжну інформацію, а не створювати автоматизовану форму кримінального переслідування.

Отже, використання штучного інтелекту в правоохоронній діяльності має подвійний характер. З одного боку, ШІ здатний істотно підвищити ефективність боротьби зі злочинністю, пришвидшити аналіз доказів, оптимізувати розподіл ресурсів, покращити розшук осіб, посилити кібербезпеку та допомогти у документуванні складних правопорушень. З іншого боку, без належного правового регулювання він може стати інструментом необґрунтованого контролю, дискримінації, масового стеження та порушення основоположних прав людини. Тому використання ШІ у правоохоронній сфері має бути не лише ефективним, а й законним та безпечним для прав людини.

Список використаних джерел

1. Муравська Ю. Перспективи використання технологій штучного інтелекту у юриспруденції та правоохоронній діяльності. *Актуальні проблеми правознавства*. 2024. С. 90-97. URL: <https://appj.wunu.edu.ua/index.php/appj/article/view/1890/1939> (дата звернення 11.05.2026)
2. Вікторчук М. В., А. С. Багатко. Вітчизняний та міжнародний досвід використання технологій штучного інтелекту в правоохоронній діяльності. *Науковий вісник Ужгородського національного університету*. Серія: Право. № 86. 2024. С. 257-263. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/01/41-2.pdf> (дата звернення 11.05.2026).
3. Величко Д. В., В. Ю. Калугін. Перспективи використання штучного інтелекту в правоохоронній діяльності. Рекомендовано до друку та поширення через мережу Інтернет Вченою радою Львівського державного університету внутрішніх справ (протокол № 14 від 25 березня 2025 року). 2025. С. 46. URL: https://if.uu.edu.ua/wp-content/uploads/2025/05/14_03_2025.pdf (дата звернення 13.05.2026).
4. Троцький О. О. Правове регулювання та потенційні ризики застосування штучного інтелекту в правоохоронній діяльності. Штучний інтелект у правовій практиці: межі. 2024. С. 180. URL: https://www.lvduvs.edu.ua/uk/karta-dokumentiv/category/391-conference-2024-magazine.html?download=5479%3Ashtuchnyi-intelekt-u-pravovii-praktytsi-mezhi-ta-mozhlyvosti-materialy-kruhloho-stolu-15-bereznia-2024-roku&utm_source=chatgpt.com (дата звернення 17.05.2026).