

УДК 342.951

МАСТНИЙ М.І., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: <https://orcid.org/0000-0001-9123-0706>.

ШТУЧНІ НЕЙРОННІ МЕРЕЖІ: ПЕРСПЕКТИВИ ВИКОРИСТАННЯ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Анотація. Проаналізовано окремі заходи у рамках виконання зарубіжного законодавства, присвячені питанням використання штучних нейронних мереж. Обґрунтовано результативні показники впровадження штучних нейронних мереж у правоохоронну діяльність. Розглянуто здобутки, отримані за результатами використання штучних нейронних мереж у правоохоронну діяльність. Окреслені загальносвітові тенденції розвитку та використання штучних нейронних мереж для потреб правоохоронної діяльності.

Ключові слова: інформаційне забезпечення, штучні нейронні мережі, штучний інтелект, цифрові технології, злочинність, система безпеки, кримінальна статистика.

Summary. Some measures within the framework of foreign legislation on the use of artificial neural networks are analyzed. The effective indicators of introduction of artificial neural networks in law enforcement activity are substantiated. The achievements obtained as a result of the use of artificial neural networks in law enforcement are considered. The general tendencies of development and using of artificial neural networks for the needs of law enforcement activity are outlined.

Keywords: information support, artificial neural networks, artificial intelligence, digital technologies, crime, security system, criminal statistics.

Аннотация. Проанализированы отдельные мероприятия в рамках исполнения зарубежного законодательства, посвященного вопросам использования искусственных нейронных сетей. Обоснованы результативные показатели внедрения искусственных нейронных сетей в правоохранительную деятельность. Рассмотрены достижения, полученные в результате использования искусственных нейронных сетей в правоохранительной деятельности. Очерчены общемировые тенденции развития и использования искусственных нейронных сетей для потребностей правоохранительной деятельности.

Ключевые слова: информационное обеспечение, искусственные нейронные сети, искусственный интеллект, цифровые технологии, преступность, система безопасности, уголовная статистика.

Постановка проблеми. В сучасних умовах інформаційно-комунікаційні технології стали невід'ємною частиною сучасних управлінських систем у всіх галузях економіки, сферах державного управління, оборони, безпеки держави та забезпечення правопорядку, протидії злочинності. Разом з тим застосування сучасних цифрових технологій та штучного інтелекту формують нові платформи побудови взаємовідносин між громадянами, державними інституціями, громадянським суспільством, Інтернет речей тощо. Використовуючи розширені можливості комунікацій та відповідні онлайн-платформи, держава намагається контролювати цифрову інфраструктуру, відстежувати та здійснювати моніторинг переконань та уподобань тих чи інших соціальних груп населення. Проте міжнародно-правові механізми, які дозволяють відстоювати суверенне право держав на регулювання інформаційного простору, у тому числі, у національному сегменті мережі Інтернет, остаточно не встановлені. Більшість країн світу вимушені

“на ходу” адаптувати своє законодавство та впроваджувати державне регулювання сфери інформаційних технологій, у тому числі й цифрових.

Зусилля переважної більшості держав світу спрямовані на пріоритетний розвиток національної інформаційної сфери та її складових. Популярність цифрової економіки як принципово нової моделі розвитку глобальної економічної системи постійно зростає. У зв'язку із постійним збільшенням чисельності населення планети, цифровізації суспільства, активізації формату споживання різноманітних ресурсів, електронна економіка здатна вплинути на кожний аспект життєдіяльності людини у сучасному світі, зокрема у таких кластерах, як: промисловість, охорона здоров'я, освіта, соціальна політика, сільське господарство, культура. Збільшуються темпи зростання сучасних технологій, створених на основі передових знань (нано- та біотехнології, штучний інтелект, альтернативні джерела енергії). Створення, обробка та поширення інформації значно перевищили можливості більшості людей в опануванні та застосуванні знань, що призвело до появи нової моделі сприйняття великих масивів інформації, яка значно спрощує масштабне поширення та використання інформаційно-цифрових технологій та штучного інтелекту у повсякденному житті пересічних громадян та у питаннях державного управління, правоохоронної діяльності тощо.

Інформація являє собою велику цінність, а розвиток технологій її передачі та обробки визначив подальший розвиток широкого спектру злочинної діяльності, пов'язаної з незаконним доступом до інформації та її подальшого протиправного використання. Таким чином, формування сегменту сучасних економічних відносин у поєднанні з передовими технічними досягненнями, глобальною мережею та інформаційними системами являє собою цифрову економіку, а головним фактором її ефективного забезпечення стає впровадження технологій обробки даних, що дає змогу значно зменшити витрати під час виробництва товарів та надання послуг. За таких умов саме новітні цифрові технології та штучний інтелект визначатимуть майбутнє та сприятимуть динамічним змінам різноманітних соціальних регуляторів у світовому вимірі.

В сучасних умовах існує чимало технологічних рішень, які застосовуються з метою централізованого моніторингу і спостереження за кримінальною обстановкою у “розумних” містах. У світових масштабах сучасні реалії мегаполісів і більш дрібних міст такі, що під наглядом повинна знаходитися якомога більша кількість вулиць, кварталів, житлових і промислових об'єктів тощо. Інтелектуальні системи безпеки, які керовані командними центрами у поєднанні з системами відеоспостереження, дійсно ефективні у питаннях спостереження, запобігання терористичним атакам, диверсіям та іншим злочинам. В розбудові інфраструктури смарт-міст процесам забезпечення безпеки відводиться одна з ключових ролей. На цьому фоні тематика розвитку штучних нейронних мереж та цифрових технологій та їх використання у масштабах правоохоронної діяльності набуває неабиякої актуальності.

Результати аналізу наукових публікацій. Технології штучного інтелекту та їх вплив на стан забезпечення кібербезпеки певною мірою досліджували у своїх працях такі науковці: В. Брижко [1], О. Бусол [2], В. Савченко [3] тощо. Питання правового врегулювання засад розвитку штучного інтелекту розглядали: О. Баранов [4], А. Бежевець [5], О. Косілова [6], О. Кривецький [7], О. Радутний [8] тощо. Проте вбачаються недостатньо висвітленими питання використання штучних нейронних мереж у правоохоронній діяльності, у зв'язку із чим потребують детального розгляду зарубіжні ініціативи, які впроваджуються останнім часом у цій площині.

Метою статті є узагальнення кращих практик зарубіжного досвіду використання штучних нейронних мереж та на підставі їх аналізу визначення дієвих шляхів удосконалення з покращення результативності правоохоронної діяльності.

Виклад основного матеріалу. Сучасні штучні нейронні мережі складаються з великої кількості простих процесорних елементів з деякою кількістю локальної пам'яті (нейронів), об'єднаних за допомогою дискретних або неперервних комунікаційних каналів. Задачі, що вони розв'язують, підлягають декомпозиції на множину локальних завдань, кожне з яких може бути розв'язане за допомогою окремого нейрону шляхом реалізації певного алгоритму обробки локальних даних. Вірогідно, що у сучасних умовах для більшості передових держав світу штучний інтелект та новітні цифрові технології як важливі складові цифрової економіки мають вирішувати не тільки звичайні повсякденні завдання, а також стати ефективним інструментом у боротьбі з організованою злочинністю та корупцією.

Так у КНР вирішили подолати корупцію за допомогою саме штучних нейронних мереж та їх активного впровадження. Китай, безумовно, є однією з найбільш високотехнологічних держав у світі, яка потужно розвиває штучний інтелект та цифрові технології вже застосовує удосконалені системи у сфері державного менеджменту. Так, наприклад, в деяких регіонах КНР з 2012 року працює національна система безпеки, що відстежує громадян за допомогою системи розпізнавання обличчя та ідентифікації особи. Інші ж цифрові технології успішно допомагають контролювати роботу правоохоронних органів та навіть захищають державні бази даних від стороннього несанкціонованого втручання.

У 2012 році в КНР розпочала функціонування система “Zero Trust” (нульова довіра) на основі штучного інтелекту. Розроблена Китайською академією наук для “внутрішнього контролю, оцінки або втручання в роботу і особисте життя державних службовців”, наразі “Zero Trust” працює тільки у 30 регіонах та містах, – понад 1 % від адміністративних територій КНР у форматі пілотного проекту. Повномасштабне запровадження цієї системи у КНР очікується у найближчій перспективі, оскільки існує формат “недовіри” політиків до сучасних цифрових технологій. Система “Zero Trust” має доступ до 150 захищених баз даних, може створити аналітику поведінки державних службовців, виявляти підозрілі операції відчуження чи набуття власності, факти незаконного будівництва, придбання землі або знесення будинків, незаконного збагачення з використанням тіншових схем.

Операційно система також передбачає постійний аналіз великого масиву даних, що зумовлює використання інформації з абсолютно різних джерел. Наприклад, можливо залучення супутників для того, щоб відстежити, що гроші на будівництво сільської дороги дійсно були витрачені за цільовим призначенням, чи провести аналіз інформації з банківських рахунків, на випадок, якщо помічено підозріле збагачення або покупка на велику суму. За переконанням розробників, головною проблемою системи “Zero Trust” став той факт, що штучний інтелект допомагав декларувати потенційну корупційну активність, але не завжди надавав пояснення, яким саме чином системні алгоритми це вираховували. Враховуючи такий стан справ, ця технологія залишається тільки допоміжним інструментом, а кінцеве рішення повинні приймати правоохоронні органи, які здійснюють боротьбу з корупційними злочинами.

Проте, навіть функціонування китайської системи “Zero Trust” у тестовому режимі за шість років з 2012 по 2018 роки, надала змогу викрити або попередити незаконні дії майже 9000 державних службовців, більшість з яких зберегли свої посади, але отримали попередження або мінімальні покарання. Лише деякі з них були засуджені до реальних

строків тюремного ув'язнення. За стратегічним задумом метою діяльності системи “Zero Trust” мало стати попередження корупційних ризиків, адже до політиків, вина яких була доведена, замість дисциплінарних заходів, застосовувалися занадто жорсткі покарання, що, певним чином, стурбувало співробітників державного апарату. Щодо подальшої долі системи штучного інтелекту технології “Zero Trust” поки невідомо, але деякі китайські політики вже виносять на обговорення питання про її законність, оскільки доступ комп'ютерних або роботизованих систем до закритих баз даних законодавчо жодним чином не регламентовано на території КНР. Деякі експерти прогнозують, що вона швидше за все буде працювати на загальнонаціональному рівні лише вибірково. Враховуючи такий стан справ, Китай вирішив відмовитися від впровадження такої антикорупційної системи, враховуючи її високу ефективність. Також політична влада КНР ще у липні 2017 року анонсувала, що до 2030 року планує побудувати індустрію штучного інтелекту з обігом \$150 млрд. США. При цьому саме протидія злочинності має стати основною функцією штучного інтелекту. Однією із найбільш амбіційних розробок Китаю у цій сфері має стати система “Поліцейська хмара”, яка, за задумом, повинна збирати інформацію з історій покупок у торгівельній мережі, замовлень доставок їжі, відвідувань лікарень, під час яких збираються зразки ДНК та з інших джерел. Система схожа до методів збору даних для визначення соціального рейтингу громадян та інтегрує масиви даних, починаючи від ір-адреси, аккаунтів, телефонних номерів, вхідних та вихідних дзвінків і закінчуючи придбанням даних про користувачів у приватних компаній, отримуючи при цьому доступ до *mac*-адрес персональних комп'ютерів та інформації з їх роутерів.

Слід також зазначити, що штучні нейронні мережі активно використовуються поліцейськими США з метою профілактики та попередження злочинності. Ще у 2009 році приватна американська компанія “Palantir Technologies” розробила сучасне програмне забезпечення під кодовою назвою “Palantir” з метою прогнозування поширення злочинності [9]. Ця компанія відома співпрацею із спецслужбами та урядовими установами, кілька років тому потайки запровадила у одному з міст США поліцейську технологію з метою прогнозування правопорушень. Секретна програма виявляла та відстежувала зв'язки членів банд. Вона аналізувала соцмережі та передбачала ймовірність того, що ті чи інші особи вчинять злочин або стануть жертвами. Співпраця стартапу з владою Нового Орлеану активно розпочалася у 2012 році. Тоді “Palantir Technologies”, одним із постійних замовників якого було Центральне розвідувальне управління, надав своє ПЗ у вигляді неофіційної благодійної допомоги. Більшість урядовців Нового Орлеану – окрім вузького кола на чолі з мером Мітчем Ландре – не знали про цей проект.

Основний операційний функціонал цієї програми спрямований на візуалізацію великих масивів інформації, що допомагає працівникам правоохоронних органів встановлювати причинно-наслідковий зв'язок між поведінкою осіб та скоєними ними правопорушеннями. Після тривалого використання поліцейськими Нового Орлеану та спецслужбами США “Palantir Technologies” запатентував свою систему прогнозування злочинності, зокрема терористичної діяльності. Використання поліцією алгоритмів полягає у прогнозуванні злочинної поведінки. Наприклад, один із інструментів програми зазначеної компанії “HunchLab” об'єднує статистику злочинності із соціально-економічними даними, іншою оприлюдненою інформацією з метою визначення найбільшої вірогідності скоєння правопорушення. Практичне використання цієї системи поліцейськими Чикаго дозволило завдяки новітнім технологіям суттєво знизити рівень злочинності. Інша програма – “Готем” використовується поліцейськими для

розпізнавання та затримання майбутніх злочинців. Інформація з протоколів затримань, матеріалів кримінальних справ завантажується в єдину базу, яка формує відповідний список осіб, які мають відношення до криміналітету. У США програми прогнозування злочинності досить часто мають непублічний характер, у зв'язку з чим громадян не попереджають про використання таких систем, оскільки актуальним питанням у США стала легітимність підстав для обміну даними та конфіденційність такої інформації. Саме тому деякі міста (Сієтл, Окленд) схвалили відповідні місцеві закони, а інші мегаполіси на рівні муніципалітетів ще й досі обговорюють питання забезпечення конфіденційності інформації в епоху цифрових технологій. Протягом двох років функціонування програми аналізу компанії “Palantir Technologies” відбулося різке зменшення кількості вбивств та актів насильства з використанням зброї, проте згодом результати практичного застосування продемонстрували зменшення її ефективності. Інші розроблені інструменти під назвою “Strategic Subject’s List” та “ShotSpotter” визначають вірогідність місць вчинення злочинів на основі активності вуличних банд та продавців наркотиків. У 2017 році в Каліфорнії відкрили “Кримінологічний центр режиму реального часу”, який займається прогнозуванням можливостей скоєння злочинів та визначає “потенційний ступінь загрози” з боку окремих категорій громадян.

За переконанням вчених та поліцейських штучний інтелект не є панацеєю, оскільки він не може впливати на причини та передумови, які породжують злочинність, наприклад такі як недоступність освіти або відсутність економічних можливостей у певної особи. Проте позитивним моментом впровадження штучного інтелекту у правоохоронну діяльність стало розширення можливостей прогнозування, оскільки воно стає швидшим, дешевшим і якіснішим. Цей інструмент має тенденцію до більш широкого використання. Для використання штучного інтелекту потрібно обов'язково додати камери та пристрої радіолокації й лазерної локації (LIDAR), за допомогою яких він отримуватиме дані та намагатиметься передбачити, які можуть бути подальші дії злочинця. Про намір залучити роботів до служби в поліції повідомили в прес-службі поліцейського управління Дубаї. Спочатку заплановано використовувати їх для проставлення штампів на документах, нагадування про справи та важливі робочі моменти, фіксації різного роду порушень роботи, а прикордонники мають намір обладнати аеропорти системою розпізнавання не задекларованих речей.

У Великобританії створена власна система профілактичних заходів з метою запобігання використанню мобільних телефонів під час руху за кермом. Щоб зрозуміти, чому дорожній безпеці приділяється так багато уваги в усьому світі, звернемося до офіційних даних: наприклад, у США мобільні телефони стають причиною 70 тисяч ДТП на рік, а у Великобританії розмова по телефону за кермом призводить до одного летального випадку кожні 10 днів.

Профілактика ДТП приносить свої результати і велике значення тут мають сучасні технології, а саме системи штучного інтелекту. В Австралії, наприклад, поліція впроваджує нові дорожні камери, призначені для відстеження водіїв, які розмовляють по телефону під час руху. Після успішного тестового періоду, що завершився у жовтні 2018 року, штрафи отримали понад 11 тисяч водіїв. Працює така технологія на основі сенсорних радарних систем, що роблять фотографії водіїв через вітрове скло. Потім зроблені фото передаються до нейронної мережі, яка аналізує знімок людини на предмет наявності мобільного телефону. Неправомірність дій водія можна легко довести на підставі фотографії. З появою платформи iOS 11 користувачам iPhone стала доступною нова вбудована функція “Не турбувати під час водіння”. У цьому режимі блокуються вхідні дзвінки і будь-які повідомлення. Ця технологія також доступна на смартфонах з

ОС Android. Сучасні глобальні системи безпеки реагують на погодні умови, тремтіння камери, тіні і навіть ворухіння листя, використовують технологію розпізнавання облич. Сейсмічні датчики вміють розрізнити транспортні засоби або людей.

Для запобігання масовим заворушенням, терактам, забезпечення безпеки на концертах або інших масових зкупченнях людей теж розробляються спеціальні технологічні рішення. Наприклад, компанія “Evolv Technology” розробила машину безпеки на базі штучного інтелекту, що працює через додаток “Evolv Pinpoint” і використовує функцію розпізнавання облич. Конструкцію можна встановити на вході у комерційні установи, школи, торгові центри, аеропорти, нічні клуби, ресторани і т.д. Для перевірки людині досить пройти через конструкцію як через звичайний металощукач. Пропускна можливість такого детектора становить 600-900 осіб на годину. Перевірка проводиться вбудованою камерою, алгоритми “Evolv Pinpoint” зіставляють особи відвідувачів з особами в списку спостереження, завантаженому у базу даних системи. Якщо з’ясується, що відвідувач представляє інтерес для поліції або інших служб, його зображення і особисті дані відображаються на планшеті співробітника служби безпеки, що підсвічуються червоним кольором. Жовте підсвічування говорить про неперевірену загрозу. Тоді профіль перевіряється у реальному часі протягом декількох секунд.

Проте штучні нейронні мережі не позбавлені недоліків. Оскільки штучний інтелект базується лише на даних, які відомі, він може працювати некоректно у деяких випадках. Так, якщо злочинець раніше не стикався з правоохоронними органами і не був засуджений, про нього не буде інформації. Відтак програма вважатиме, що він становить меншу загрозу для суспільства.

Україна динамічно рухається у цьому напрямку. Так, задля забезпечення громадської безпеки, збору доказів злочину, пошуку і затримання злочинців, охорони власності, дотримання правил дорожнього руху Національна поліція України використовує системи відеоспостереження силових структур і приватних власників [10]. У вересні 2020 року Міністерство юстиції України анонсувало сучасний пілотний проект, у рамках якого запроваджується програмне забезпечення з елементами штучного інтелекту для того, щоб аналізувати злочинців та визначити, чи можуть вони в майбутньому знову порушувати закон. Нова розробка Мін’юсту з елементами штучного інтелекту під назвою “Касандра” використовується з метою аналізу ймовірності повторного порушення закону певним злочинцем. Програмне забезпечення “Касандра” – це не окрема програма, а фактично одна з вкладок єдиного реєстру засуджених і взятих під варту, яка включає в собі оцінку ризиків і потреб.

Ця розробка фактично автоматизує процес створення досудової доповіді, де характеризується особистість обвинуваченого та його схильність до повторного скоєння злочинів. Наразі розглядається можливість аналізування “Касандрою” реєстрів не лише Міністерства юстиції, а й інших відомств. На даний час програма не лише поповнюється даними з реєстру, а здійснює попередню обробку анкет людей, виставляючи їм бали. З роками “Касандра” стане більш оперативною та, маючи великі масиви даних, почне перевіряти, чи адекватно надано оцінку ймовірності рецидиву в кожному конкретному випадку. В сучасних умовах “Касандра” формується вручну, але при наповненні реєстру максимально можливими даними, цей процес буде відбуватиметься автоматично. Можливості для подальшого використання цього інструменту є дуже широкими як і для контролю за правопорушниками, так і для запобіжних аспектів. Йдеться про належне проведення з ними спеціальної виховної роботи тощо. Таким чином, програмне забезпечення “Касандра” працює у форматі підсистеми Єдиного реєстру засуджених осіб та осіб, взятих під варту.

Висновки.

Впровадження штучних нейронних мереж в різноманітні сфери життя здатне якісно його змінити, що сприятиме підвищенню результативності будь-якої діяльності, у тому числі й правоохоронної. Найбільш активно застосовуються штучні нейронні технології в таких країнах, як США, Японія, Китай, Німеччина. Інтелектуальна реальність сьогодні передбачає широку практику застосування, зміст якої формує низку перспективних напрямків розвитку розумних технологій. Очікується, що довіра до інтелектуальних технологій в рамках діяльності правоохоронних органів буде активно зростати і стимулювати появу нових унікальних рішень.

Ключовим аспектом у реалізації інноваційних проєктів стане розуміння представниками влади необхідності зміцнення співпраці з дослідницькими і науковими центрами, а також доцільності належного фінансування сфери інновацій. Саме штучні нейронні системи за допомогою відповідних програм, камер і датчиків руху здатні стежити за порядком на вулицях міста і в місцях масового скупчення людей, прогнозувати виникнення небезпечних та кризових ситуацій і навіть впізнавати обличчя злочинців. Також розумні системи штучного інтелекту здатні з точністю проводити звірку документів, запобігаючи крадіжкам персональних даних.

Штучний інтелект неможливо забезпечити від помилок і впливу зовнішніх чинників. Не можна недооцінювати роль та значення сучасних розробок штучного інтелекту та передових цифрових технологій, які впроваджуються у зарубіжних країнах з метою профілактики та боротьби зі злочинністю.

Враховуючи таку динаміку, міжнародними експертами прогнозується, що до 2030 року у світі будуть мінімізовані прояви поширення злочинності. Отже, технічні та технологічні досягнення, зокрема штучні нейронні мережі, суттєво допомагають та спрощують роботу правоохоронців в усьому світі. Окрім того, вони захищають правоохоронців від нещасних випадків чи надмірної агресії. До того ж штучний інтелект працює над алгоритмами пошуку серійних вбивць та маніяків для того, щоб зробити людське життя більш безпечнішим та комфортнішим.

Вбачається, що ключовими напрямками підвищення конкурентоздатності цифрових інформаційних та комунікаційних технологій мають стати: стимулювання створення організацій та суб'єктів господарювання, які здійснюють діяльність, спрямовану на розвиток усього спектру сервісів цифрової економіки (екосистеми економіки); забезпечення трансферу іноземних технологій та застосування кращих практик зарубіжного досвіду у сфері впровадження інформаційних технологій у правоохоронну діяльність. У зв'язку з великою швидкістю та інтенсивністю еволюційних процесів більшість інформаційних систем вітчизняних правоохоронних органів, що були створені понад 10 років, потребують модернізації. Це, наприклад, Інтегрована міжвідомча інформаційно-телекомунікаційна система контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон.

Основними напрямками такої модернізації має стати використання засобів електронної ідентифікації, захищених електронних каналів передачі даних, систем контролю якості інформації, систем аналізу даних, систем управління інформаційною безпекою. Безумовно, передовий зарубіжний досвід у сфері інформаційного забезпечення заходів у сфері боротьби зі злочинністю доцільно адаптувати у роботі вітчизняних правоохоронних органів. Також потребує прискорення запровадження дієвий механізм взаємодії та налагодження конструктивної співпраці між правоохоронними органами та науково-дослідними установами, спеціалізованими у ІТ-промисловості. В даному контексті вважається доцільним впровадити в поліцейську діяльність відповідне

програмне забезпечення систем штучного інтелекту, у тому числі й з використанням системи трансферу технологій.

Саме штучні нейронні мережі та сучасні цифрові технології допоможуть швидко обробляти великі масиви інформації, які доцільно опрацьовувати під час здійснення розслідування та попередження будь-якої злочинної діяльності. Також доцільно визначити на державному рівні перелік потенційних ІТ-компаній, які виступають розробниками відповідних програм штучного інтелекту та аналізуватимуть інформаційні системи правоохоронних органів, державних реєстрів, інших інформаційних джерел з метою пошуку потенційних злочинців. Впровадження цифрових технологічних досягнень в діяльність правоохоронних органів надасть змогу значно підвищити ефективність їхньої роботи, забезпечити громадську безпеку.

Використана література

1. Брижко В.М. Фурашев В.Н. Конвергенція новітніх технологій: стан і перспективи змін у інформаційних відносинах. *Інформація і право*. № 1(20)/2017. С. 51-67.
2. Бусол О.Ю. Потенційна небезпека штучного інтелекту. *Інформація і право*. № 2(14)/2015. С. 121-127.
3. Савченко В.А., Шаповаленко О.Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. *Сучасний захист інформації*. 2020. № 4 (44). С. 6-11.
4. Баранов О.А. Інтернет речей (ІоТ): робот зі штучним інтелектом у правовідносинах. *Юридична Україна*. 2018. № 5-6. С. 75-95.
5. Бежевець А.М. Правовий статус роботів: проблеми та перспективи визначення. *Інформація і право*. № 1(28)/2019. С. 61-67.
6. Косілова О.І. Солодовнікова Х.К. Права і свободи людини і громадянина v.s. штучний інтелект: проблемні аспекти. *Інформація і право*. № 4(35)/2020. С. 56-66.
7. Кривецький О. До проблеми правового регулювання штучного інтелекту. *Громадська думка про правотворення*. 2018. № 14. С. 15-19. URL: http://nbuviar.gov.ua/index.php?option=com_content&view=article&id=3728:do-problemi-pravovogoregulyuvannya-shtuchnogo-intelektu&catid=8&Itemid=350
8. Радутний О.Е. Кримінальна відповідальність штучного інтелекту. *Інформація і право*. № 2(21)/2017. С. 124-132.
9. Американський стартап таємно випробував систему передбачення злочинів. URL: <https://techno.nv.ua/ukr/innovations/velikij-brat-amerikanskij-startap-tajemno-viprobuvav-u-novomu-orleani-sistemu-peredbachennja-zlochiv-2455319.html>
10. Мордвинцев М.В. Хлестков О.В., Ницюк С.П. Сучасний стан систем інтелектуального відеоспосереження які використовуються в діяльності Національної поліції України: зб. матеріалів круглого столу *Застосування інформаційних технологій у діяльності правоохоронних органів*, м. Харків, 9 грудня 2020 р. – (МВС України, Харк. нац. ун-т внутр. справ). Харків: ХНУВС, 2020. С. 88-90.

~~~~~ \* \* \* ~~~~~