РОЛЬ ШІ В ЗАБЕЗПЕЧЕННІ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Іщук Андрій,
студент Інституту права
Львівського державного університету внутрішніх справ

На сьогоднішній день наш світ перебуває на шляху революційних перетворень, пов'язаних через стрімкий розвиток інформаційних технологій, які призвели до масштабної цифровізації всього людства. З кожним днем ми спостерігаємо тенденцію коли інноваційні розробки поступово впроваджуються в усі сфери життєдіяльності: медицині, економіці, освіті, сільське господарство, правоохоронна діяльність, тощо. Тобто, це означає, що ІТ технології являється невід'ємною частиною нашого життя, які можуть допомогти у вирішенні складних задач. Незважаючи на військові події, в Україні продовжуються інтеграційні процеси в сфері цифрової трансформації, що відображається у створенні мобільного застосунку **«Дія»**, де можна мати доступ до цифровізованих документів (внутрішній та закордонний паспорт, водійське посвідчення, тощо) у своєму смартфоні. Також, важливо звернути увагу на те, що Україна першою у світі розробила варіант COVID-сертифікату, систему **«Prozzoro»** (електронна система закупівель, яка має на меті підвищити рівень прозорості та ефективності процесів державних закупівель), **«Електронний суд»** (проєкт, який надає можливість суб'єкту подання документів в електронному форматі, приймати участь в судових засіданнях через відеоконференції, а також доступ до платформи з рішеннями суду в онлайн варіанті). Безумовно, цифровізація відіграє велику роль у розвитку економічного напрямку та інтеграції нашої держави в європейське співтовариство. Вона не тільки сприяє ефективному управлінню ресурсами, але й поліпшує рівень якості державних послуг, роблячи їх доступнішими для громадян України. Важливим є те, що цифровізація допомагає країні наблизитися до європейських критеріїв, що є одним із пріоритетних напрямків зовнішньої політики України.

Проте, процес розвитку цифрової ери має і негативні наслідки, а саме: поява кіберзлочинів, хакерські атаки на державні установи, інформаційні шахрайства. чинний цілях, істотне зростання кібератак. Так, наприклад, за даними американської компанії McAfee хакерські атаки протягом 2020 року коштували світовій економіці понад трильйон доларів або 820 мільярдів євро, що становлять понад один відсоток світового ВВП. Причому об'єктом посягання кіберзлочинців є як пересічні громадяни, так і критично важливі ІТ-інфраструктури.

Згадаймо лише вірусу Petya від якого, зокрема, постраждали: уряд України, національна пошта, метрополітен Києва, міжнародний аеропорт «Бориспіль», Чорнобильська АЕС, а також низка ЗМІ, банків, комерційних структур. За даними експертів Міжнародного валютного фонду, економічні втрати від атаки вірусу становили майже 850 млн доларів [1]. Усе вищезазначене потребує негайної протидії з боку правоохоронців і наразі як діючим інструментом боротьби з цими явищами є ***штучний інтелект*** (далі – ШІ). Тому, що розкриття злочину з кожним днем стає все важче і потребує дуже багато часу та використання ресурсів, щоб дійти до успішного результату. Тобто, сучасна правоохоронна система вимагає загального оновлення та введення у її діяльність сучасних технологій, таким чином ШІ являє собою яскравим прикладом для вищевказаного. У міжнародній практиці є чимало прикладів успішного впровадження штучного інтелекту в правоохоронній діяльності. Так, наприклад, у США Федеральне Бюро Розслідувань (FBI) використовує штучний інтелект для розпізнавання правопорушників на відео з камер спостереження в режимі реального часу. За допомогою штучного інтелекту агенти FBI можуть отримувати доступ до великих обсягів даних та аналізувати їх, щоб виявляти правопорушників та спрогнозувати місце та час наступного злочину [2].

Введення ШІ у роботі правоохоронних органів, зокрема у напрямі протидії кіберзлочинності, є суспільно необхідним та актуальним. Можливості інноваційних технологій в забезпеченні правопорядку дають велику користь щодо фіксації правопорушення. На даний момент, в Україні правоохоронні органи використовують ШІ в різних напрямах.

1. Основним напрямком є і**дентифікація особи**. На цьому етапі, використовуються технології, які базуються на основі ШІ, дозволяючи розпізнавати осіб. Цей процес починається з аналізу зображень, які надходять до системи ШІ з камер відеоспостережень та гаджету. Потім зображення набирає максимальної чіткої якості, щоб мати змогу чітко визначити ключові позиції (губи, колір очей, розмір носа, форма лиця), після отримання відповідних даних, система автоматично створює пошук осіб. В кінці даного етапу, ШІ в разі знаходження відповідності, може ідентифікувати особу. В Україні правоохоронці широко використовують даний напрям в разі ідентифікації особи, захист державних кордонів, в також зниклих громадян.

2. **Кібербезпека**. Під час воєнного стану в Україні, наша держава постійно зазнає шкоди від кібератак з боку росії, тому це питання набуло широкого дискурсу серед суспільства. Україна виділяє значні кошти на розвиток кібербезпеки, внаслідок цього було створено у

2021 році Національний координаційний центр кібербезпеки. На сьогодні, ШІ дозволяє оперативно реагувати та точно виявляти загрози. Таким чином, аналізує трафік мереж, а також активність суб'єктів у реальному часі, щоб завчасно реагувати на загрозу. ШІ може автоматизувати процес реагування кіберзагрози у разі прослідковування підозрілого трафіка, блокуючи його без людського втручання. Після попередніх атак, система робить її аналіз, щоб передбачити майбутні загрози, щоб уникнути вторгненню.

Завдяки цьому, ШІ є ефективний у вказаному процесі, роблячи кібербезпеки на максимально високому рівні.

3. **Дрони для спостереження**. Правоохоронні органи можуть використовувати безпілотний літальний апарат (далі – БПЛА) штучного інтелекту для розвідки, збору даних у своїх областях. На практиці БПЛА (наприклад, під час пожежі)слугують заміною сучасним гелікоптерам, через свої функції він може вести огляд критичних ситуаціях з висоти пташиного польоту .За їх допомогою, наприклад, поліцейські з підрозділу протидії наркозлочинності у 2020 році знайшли в Дніпропетровській області 36 ділянок, засіяних коноплями. Також роботи можуть виявляти браконьєрів, фіксувати незаконний видобуток корисних копалин, незаконні рубки лісу, знаходити осередки лісових пожеж, допомагати шукати заблукалих в лісі чи горах [3].

4. **Прогнозування кримінальних правопорушень**, це інноваційна технологія, яка бере за основу аналітику даних та сукупність алгоритмів ШІ для передбачення подій. Основним завданням є допомогти правоохоронцям успішно використовувати свої ресурси, підвищити рівень забезпечення правопорядку.

Спершу система збирає всі відомості про минулі скоєні злочини (місце, час, обставини, погодні умови, тощо). Також дані можуть збиратися із соціальних мереж. На основі виявлених причин ШІ робить прогноз щодо ймовірності майбутнього кримінального правопорушення. Внаслідок цього правоохоронні органи отримують результат у формі звітів, що дозволяє їм запровадити превентивні заходи. Наприклад, у США активно використовується система «PredPol». Вона робить аналіз даних про попередні злочини та прогнозує місця, де може відбутися нове правопорушення.

Отже, ШІ поступово розвивається як потужний інструмент у протидії злочинності. Ми бачимо те, що він відіграє ключову роль у трансформації діяльності правоохоронних органів, підвищуючи їхню ефективність та точність. Перш за все, його роль буде і надалі зростати, адже має амбітні перспективи. Завдяки ШІ правоохоронці можуть аналізувати великі обсяги даних, використовувати БПЛА штучного

інтелекту, прогнозувати злочини та покращувати кібербезпеку. Технології ШІ дозволяють краще розпізнавати осіб, захищати мережі від кібератак з боку рф і виявляти підозрілу активність осіб у режимі реального часу. Однак, важливо використовувати ШІ відповідально, зберігаючи баланс між безпекою та захистом прав і свобод громадян. Тому, що в демократичній державі важливо, щоб кожна людина, хто вчинила кримінальне правопорушення, була притягнута до відповідною відповідальності, а також важливо пам'ятати про презумпцію невинуватості.

Література:

1. ЄС уперше покарав Росію за хакерські атаки. URL: https://www.dw.com/uk/єс-уперше-покарав-росію-за-хакерські-атаки/a54384562 (дата звернення: 22.04.2022).

2. Зачек О.І., Дмитрик Ю.І., Сеник В.В., Роль штучного інтелекту в «Підвищенні ефективності правоохоронної діяльності науковий вісник» // Львівського державного університету внутрішніх справ 2023 р. URL:https://doi.org/10.32782/2311-8040/2023-3-19.

3. Штучний інтелект і робототехніка на службі поліції // Matrix-divergent : сайт.URL:https://matrix-info.com/shtuchnyj-intelekt-i-robototehnika-na-sluzhbi-politsiyi (дата звернення: 14.09.2021).

ОСНОВНІ НАПРЯМИ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА СБ УКРАЇНИ У ГАЛУЗІ СУДОВО-ЕКСПЕРТНОЇ ДІЯЛЬНОСТІ

Капелюха Артемій,
аспірант відділу аспірантури і докторантури
Національної академії Служби безпеки України

Останніми роками, в умовах повномасштабної війни з російською федерацією дещо змінилися напрямки міжнародного співробітництва СБ України. Найбільш активно розвивається співробітництво СБ України зі спецслужбами й правоохоронними органами, експертними установами країн НАТО та ЄС. Зокрема спостерігається активізація взаємодії за такими напрямами:

– партнерство у галузі судово-експертної діяльності;
– протидія міжнародному тероризму та транснаціональній організованій злочинності;
– розвиток євроатлантичного партнерства у сфері кібербезпеки;
– – протидія гібридним загрозам;