Отже, потенціал OSINT в українській системі інформаційної безпеки є надзвичайно значним, але його реалізація вимагає системного підходу: нормативного врегулювання, інституційного зміцнення, технічного переоснащення, кадрової підготовки й інтеграції міжвідомчого обміну. За наявності політичної волі, координації із західними партнерами та підтримки цифрових ініціатив знизу, OSINT може перетворитися з фрагментарного інструменту в один із ключових елементів національної інформаційної оборони, що забезпечить гнучкість, превентивність і прозорість дій у сфері державної безпеки.

Заєць Наталія,
викладач кафедри №23,
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

Жилінський Ігор,
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

Коваленко Іван,
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У РОЗВІДУВАЛЬНО-АНАЛІТИЧНІЙ ДІЯЛЬНОСТІ: СУЧАСНІ МОЖЛИВОСТІ ТА МАЙБУТНІ ВЕКТОРИ РОЗВИТКУ

У сучасних умовах змін глобального безпекового середовища, коли традиційні підходи до ведення розвідки підсилюються інформаційними та кіберзагрозами, особливої актуальності набуває використання високотехнологічних рішень. Однією з провідних технологій, що визначає перспективи розвитку оборонного сектору, є штучний інтелект (ШІ). Його здатність до швидкої обробки великих обсягів даних, виявлення прихованих закономірностей і формування прогнозів надає розвідувальній діяльності нового виміру.

Сьогодні провідні країни світу вже впроваджують ШІ для реалізації таких завдань, як обробка відкритих джерел інформації (OSINT), аналіз контенту соціальних мереж, відео- та аудіозаписів; класифікація об’єктів на зображеннях, отриманих із супутників і БПЛА; автоматизований переклад, транскрипція і аналіз мовлення; виявлення відхилень у поведінці інформаційних суб’єктів; оцінка ризиків та підтримка ухвалення рішень у режимі реального часу.

Системи глибокого навчання (Deep Learning) і нейронні мережі забезпечують розпізнавання образів, класифікацію подій і моделювання сценаріїв розвитку ситуацій, що суттєво підвищує рівень ситуаційної обізнаності. Особливо важливими такі можливості є в умовах бойових дій, де критичною є оперативна перевірка достовірності отриманої інформації з метою мінімізації ризику впливу дезінформації.

Подальше вдосконалення застосування ШІ у розвідувально-аналітичній сфері пов’язане з розвитком таких напрямів, як ситуаційне моделювання, інтеграція мультисенсорної інформації та пояснюваний штучний інтелект (Explainable AI). Завдяки цьому можливо моделювати складні сценарії із врахуванням численних змінних, поєднувати дані з різних джерел (супутникові системи, радари, БПЛА, сигнали зв’язку) в єдину інформаційно-аналітичну платформу, а також зберігати контроль аналітика над процесом ухвалення рішень, що підвищує прозорість і надійність систем.

Однак паралельно з перевагами виникають і суттєві виклики. Це етичні аспекти використання алгоритмів у критичних сферах, можливість маніпуляції внаслідок викривлених вхідних даних, зростання кіберризиків через вразливість цифрової інфраструктури, а також нагальна потреба у підготовці нового покоління фахівців, здатних поєднувати технічні, аналітичні та етичні компетенції.

Штучний інтелект не може повністю замінити людський фактор у розвідці, однак його інтеграція вже сьогодні суттєво трансформує розвідувально-аналітичну діяльність. Ефективне використання цих технологій вимагає не лише технічної модернізації, але й формування нової стратегії управління інформаційними ресурсами. Необхідними умовами є впровадження скоординованої державної політики, розвиток цифрової інфраструктури, оновлення нормативно-правової бази, а також підготовка висококваліфікованих кадрів, які здатні працювати з сучасними інтелектуальними системами. Такий підхід відповідає принципам євроатлантичної інтеграції, сприяє підвищенню ефективності функціонування безпекового сектору та забезпечує збалансоване впровадження інновацій із дотриманням етичних і правових норм.

Зінченко Сергій,
старший викладач кафедри тактики та тактико-спеціальної підготовки,
Київський інститут Національної гвардії України

АНАЛІЗ ЧИННИКІВ, ЯКІ ВПЛИВАЮТЬ НА ЕФЕКТИВНІСТЬ ОЦІНЮВАННЯ ЯКОСТІ ВИКОНАННЯ ІНФОРМАЦІЙНИХ ДОКУМЕНТІВ В СИСТЕМІ РОЗВІДКИ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Аналіз чинників, які впливають на ефективність оцінювання якості виконання інформаційних документів в системі розвідки Національної гвардії України, можна провести за кількома ключовими критеріями: якість джерел інформації, методологія оцінювання, командний склад, системи автоматизації, зворотний зв'язок та коригування процесів, інфраструктура та технології, регламентуюча база. Всі ці фактори взаємопов’язані і повинні бути враховані комплексно для досягнення високої якості виконання інформаційних документів.

Розглянемо більш детально кожний із цих факторів окремо.