Богатир Артем Юрійович,
студент н.гр. 102_СПД
ННІ права та психології НАВС

Науковий керівник:
Кудінов Вадим Анатолійович,
кандидат фізико-математичних наук, доцент, завідувач кафедри інформаційних технологій ННІ права та психології НАВС

ЦИФРОВА ТРАНСФОРМАЦІЯ ПРАВОСУДДЯ ТА ПСИХОЛОГІЧНОЇ БЕЗПЕКИ: ВИКЛИКИ ШТУЧНОГО ІНТЕЛЕКТУ, DEEPFAKES ТА ВІРТУАЛЬНИХ СЕРЕДОВИЩ

Стрімка еволюція цифрових технологій у третьому десятилітті XXI століття спричинила фундаментальний зсув парадигми у правоохоронній діяльності та судочинстві. Ми спостерігаємо перехід від класичної моделі «людина-людина» до складної системи взаємодії «людина-алгоритм-людина». Інформаційні технології перестали бути лише інструментарієм фіксації даних; вони трансформувалися в активних учасників процесу аналізу, оцінки та навіть прийняття рішень. Метою даного дослідження є висвітлення гострих проблем валідності, етичності та процесуальної допустимості використання інноваційного IT-інструментарію у практиці розслідування злочинів та проведення судово-психологічних експертиз.

Алгоритмічний профайлінг та автоматизована детекція неправди. Одним із найбільш амбітних напрямів Legal Tech є створення систем автоматизованого аналізу поведінки особи (Automated Behavioral Analysis). Сучасні алгоритми машинного навчання (Machine Learning) здатні аналізувати мікровирази обличчя, тремор голосу, розширення зіниць та лексичні конструкції. Проте, з погляду фундаментальної психології, такий підхід містить критичні ризики:

1. *Проблема контексту*. ШІ часто ігнорує культурні та ситуативні особливості. Стресова реакція підозрюваного може бути викликана не фактом брехні, а страхом перед самою процедурою допиту, що алгоритм може хибно інтерпретувати як ознаку вини (хибний позитив / false positive).

2. *«Ефект чорної скриньки» (Black Box Problem)*. Глибокі нейронні мережі не надають пояснення своїм висновкам. У судовому процесі, де кожне твердження має бути верифікованим, висновок типу «система визначила вірогідність брехні на рівні 87%» без пояснення причин є процесуально нікчемним та порушує право на захист.

Загроза синтетичного контенту: Deepfakes та «Дивіденд брехуна». Розвиток генеративних змагальних мереж (GAN) зробив можливим створення гіперреалістичних підробок аудіо- та відеозаписів. Це створює безпрецедентний виклик для судової експертизи. Психологічний аспект проблеми полягає у двох площинах:

1. *Маніпуляція свідомістю*. Фейкові відео можуть бути використані для дискредитації свідків, шантажу (сексторшн) або створення хибного алібі. Людська психіка еволюційно схильна довіряти візуальній інформації, тому deepfake сприймається як істина швидше, ніж текст.

2. *«Дивіденд брехуна» (Liar's Dividend)*. Злочинці отримують можливість ставити під сумнів будь-які справжні докази, апелюючи до того, що вони можуть бути згенеровані ШІ. Це призводить до ерозії довіри до цифрових доказів як таких. Вирішенням цієї проблеми має стати обов'язкове впровадження криптографічного підпису медіафайлів на етапі їх створення (технологія C2PA) та використання спеціалізованого ПЗ для виявлення артефактів генерації.

Імерсивні технології (VR/AR) у криміналістиці та психології. Віртуальна реальність відкриває нові горизонти для слідчих експериментів та судових засідань.

1. *Реконструкція подій*: VR дозволяє відтворити обстановку місця злочину з фотограмметричною точністю. Це дає змогу суду та присяжним «зануритися» в обставини справи, перевірити видимість, дистанцію та сектори огляду.

2. *Психологічна підготовка*: VR-симулятори є незамінними для тренування працівників поліції (стресостійкість, переговори, звільнення заручників), дозволяючи відпрацьовувати алгоритми дій у безпечному середовищі. Водночас, існує ризик сугестивного впливу віртуальної реконструкції на пам'ять свідків. Створення «ідеальної картинки» злочину у VR може витіснити реальні, фрагментарні спогади особи, створюючи феномен помилкової пам'яті.

Кіберпсихологія та протидія соціальній інженерії. Сучасна злочинність зміщується в кіберпростір, де головним інструментом злочинця стає не фізична сила, а знання психології. Соціальна інженерія використовує когнітивні викривлення жертв (страх, жадібність, авторитет) для отримання доступу до даних. Правоохоронні органи повинні розуміти психологічні механізми, які лежать в основі фішингу та вішингу, для ефективної профілактики та розслідування кібершахрайств. Необхідна розробка нових методик психологічної експертизи жертв кіберзлочинів, які часто переживають специфічну травматизацію та почуття провини.

Блокчейн як гарант цілісності інформації. В умовах легкості модифікації цифрових даних, технологія розподіленого реєстру (Blockchain) стає ключовим елементом забезпечення довіри. Хешування файлів (протоколів допитів, відеозаписів з бодікамер) у блокчейні унеможливлює їх непомітну зміну «заднім числом». Це знімає психологічну напругу недовіри між сторонами захисту та обвинувачення щодо автентичності матеріалів справи.

Висновки. Інтеграція ІТ у право та психологію несе як колосальні можливості, так і екзистенційні загрози. Для гармонізації цього процесу необхідні рішучі кроки:

1. *Законодавча регламентація*. Внести зміни до КПК України, визначивши статус алгоритмічно отриманих даних. Закріпити правило, що результати роботи ШІ мають статус «орієнтуючої інформації», а не прямого доказу, до моменту їх верифікації експертом-людиною.

2. *Стандартизація та сертифікація*. Створити національний реєстр сертифікованого програмного забезпечення для судової експертизи. Програми, що використовуються для аналізу психіки чи доказів, мають проходити регулярний аудит на предмет відсутності упередженості (bias audit).

3. *Освіта*. Впровадити в систему підготовки кадрів МВС міждисциплінарні курси з «Legal Tech» та «Кіберпсихології», щоб слідчі та експерти розуміли природу цифрових слідів.

Технології мають слугувати ствердженню верховенства права, а не його підміні алгоритмічною доцільністю. Людина, її права та психологічний комфорт повинні залишатися в центрі цифрової трансформації правосуддя.

Список використаної літератури:

1. Європейська етична хартія про використання штучного інтелекту в судових системах та правосудді. Європейська комісія з питань ефективності правосуддя (CEPEJ). Страсбург, 2018.

2. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI.

3. Хахановський В.Г. Актуальні проблеми кібербезпеки та використання інформаційних технологій у правоохоронній діяльності : монографія. Київ : НАВС, 2021.

Євженко Дарія Дмитрівна,
студентка н.гр. 101_СПС
ННІ права та психології НАВС

Науковий керівник:
Пакриш Олександр Євгенійович,
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій ННІ права та психології НАВС

ПОЗИТИВНІ ТА НЕГАТИВНІ АСПЕКТИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОСВІТНЬОМУ ПРОЦЕСІ

Штучний інтелект (ШІ) – це технологія, що швидко розвивається, яка намагається імітувати людський інтелект за допомогою інформаційних технологій, що виконують широкий спектр завдань різноманітної складності.