МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
Навчально-науковий інститут права та психології
Кафедра інформаційних технологій

105 РОКІВ
НАВС 2026

АКТУАЛЬНІ ПРОБЛЕМИ ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВІ ТА ПСИХОЛОГІЇ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Матеріали круглого столу
(м. Київ, 27 листопада 2025 року)

Київ
2026

УДК 004:[34+159.9](477)(06)
А437

Матеріали круглого столу за загальною редакцією:
Хахановський В.Г. – професор кафедри інформаційних технологій навчально-наукового інституту права та психології Національної академії внутрішніх справ, доктор юридичних наук, професор

Рецензенти:
Звєрєв Володимир Павлович – заступник керівника служби з питань інформаційної безпеки та кібербезпеки – керівник управління інформаційної безпеки Апарату РНБО України, кандидат технічних наук, старший науковий співробітник
Кудінов Вадим Анатолійович – завідувач кафедри інформаційних технологій навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат фізико-математичних наук, доцент

Матеріали схвалено та рекомендовано до друку на засіданні науково-методичної ради Національної академії внутрішніх справ (протокол № 12 від «23» грудня 2025 року)

Усі матеріали надані в авторській редакції та виражають персональну позицію учасників круглого столу

А437 **Актуальні проблеми використання сучасних інформаційних технологій в праві та психології та шляхи їх вирішення**: матеріали круглого столу (м. Київ, НАВС, 27 листопада 2025 р.); за заг. редакцією В. Г. Хахановського. Київ: Нац. акад. внутр. справ, 2026. 44 с.

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на круглий стіл за темою «Актуальні проблеми використання сучасних інформаційних технологій в праві та психології та шляхи їх вирішення», який відбувся на базі навчально-наукового інституту права та психології Національної академії внутрішніх справ 27 листопада 2025 року.

Для здобувачів вищої освіти, науково-педагогічних працівників закладів вищої освіти, практичних працівників органів та підрозділів системи МВС України.

УДК 004:[34+159.9](477)(06)

ЗМІСТ

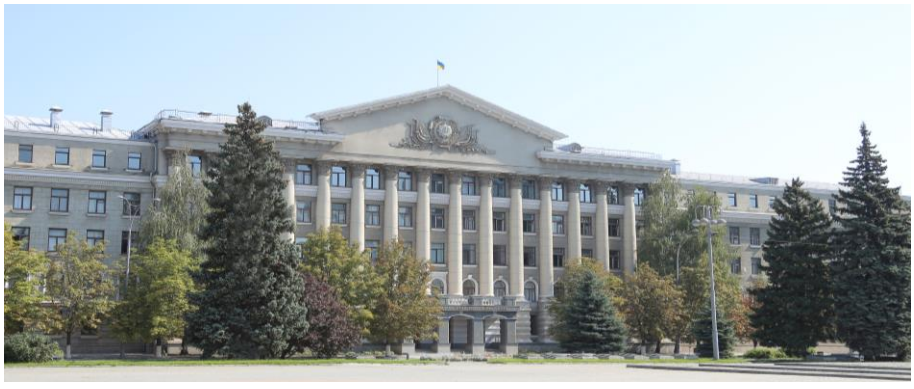
МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
Навчально-науковий інститут права та психології
Кафедра інформаційних технологій

П Р О Г Р А М А

проведення круглого столу на тему:

АКТУАЛЬНІ ПРОБЛЕМИ ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВІ ТА ПСИХОЛОГІЇ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

(*27 листопада 2025 року*)



Київ – 2025

Дата проведення: **27 листопада 2025 року**

Початок роботи: **14.00**

Місце проведення: Національна академія внутрішніх справ (м. Київ, пл. Солом'янська 1, Цифровий Hub) та ZOOM.

Регламент: доповіді – *до 5 хв.*; обговорення – *до 3 хв.*

Відкриває захід директор ННІ права та психології НАВС, кандидат юридичних наук, доцент **Кульчицька Оксана Вікторівна**.

Вступне слово завідувача кафедри інформаційних технологій ННІ права та психології НАВС, кандидата фізико-математичних наук, доцента **Кудінова Вадима Анатолійовича**.

Модератор заходу: професор кафедри інформаційних технологій ННІ права та психології НАВС, доктор юридичних наук, професор **Хахановський Валерій Георгійович**.

ДОПОВІДІ:

1. Студентка 105СПД н.гр. **Стрельцова Кіра Юріївна** «Міжнародний досвід створення систем інформаційно-аналітичного забезпечення правоохоронної діяльності» (д.ю.н. Хахановський В.Г.).
2. Студентка 105СПД н.гр. **Червінська Ксенія Олегівна** «Актуальні проблеми використання сучасних інформаційних технологій в праві та психології та шляхи їх вирішення» (д.ю.н. Хахановський В.Г.).
3. Студент 117СПД н.гр. **Демченко Максим Володимирович** «Політика конфіденційності та захист персональних даних» (к.ф.-м.н. Тарасенко В.П.).
4. Студентка 117СПД н.гр. **Убога Сніжана Сергіївна** «Інноваційний потенціал та найкращі практики застосування інформаційних технологій для підвищення ефективності права та психології» (к.ф.-м.н. Тарасенко В.П.).

5. Студентка 117СПД н.гр. **Ходосок Карина Юріївна** «Етичні та правові виклики інтеграції сучасних інформаційних технологій у правозастосовну практику та психологічну допомогу» (к.ф.-м.н. Тарасенко В.П.).
6. Студентка 103СПД н.гр. **Горенчук Євгенія Андріївна** «Інформаційно-аналітичне забезпечення правоохоронних органів» (д.ю.н. Хахановський В.Г.).
7. Студентка 103СПД н.гр. **Левченко Дарина Олександрівна** «Кібербезпека персональних даних клієнтів у роботі юриста та психолога: сучасні загрози та технологічні рішення» (д.ю.н. Хахановський В.Г.).
8. Студентка 301СПС н.гр. **Савотєєва Анастасія Олександрівна** «Вплив надмірного захоплення цифровими пристроями на розвиток психологічних проблем у дітей» (к.т.н. Пакриш О.Є.).
9. Студентка н.гр. 101СПД **Шинкаренко Ангеліна Юріївна** «Шляхи вирішення актуальних проблем використання сучасних інформаційних технологій в правовій сфері та психології (к.ф.-м.н. Кудінов В.А.).
10. Студент н.гр. 102СПД **Шуляк Богдан Андрійович** «Потенційні ризики для фінансової документації в цифровому форматі освітніх установ системи МВС України» (к.ф.-м.н. Кудінов В.А.).
11. Студент н.гр. 102СПД **Богатир Артем Юрійович** «Цифрова трансформація правосуддя та психологічної безпеки: виклики штучного інтелекту, deepfakes та віртуальних середовищ» (к.ф.-м.н. Кудінов В.А.).

Стрельцова Кіра Юріївна,
студентка н.гр. 105_ СПД ННІ права та психології НАВС

Науковий керівник:
Хахановський Валерій Георгійович
доктор юридичних наук, професор, професор кафедри інформаційних технологій ННІ права та психології НАВС

МІЖНАРОДНИЙ ДОСВІД СТВОРЕННЯ СИСТЕМ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

Конвенція Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою даних особистого характеру» (Страсбург, 28 січня 1981 р.) визначила, що автоматизоване оброблення даних – це процес, що включає такі операції, які здійснюються повністю або частково за допомогою автоматизованих засобів зберігання даних, виконання логічних і/або арифметичних операцій із цими даними, змінення, знищення, обрання або поширення даних. Слід зазначити, що цю Конвенцію було ратифіковано у 2010 р. Законом України «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних» від 06.07.2010 № 2438-VI.

Розглядаючи питання використання досвіду окремих країн щодо нормативно-правового регулювання створення й використання баз та банків даних правоохоронних органів, слід зазначити, що ця проблема пов'язана із проблемою нормативно-правового регулювання процесу збирання інформації про злочини.

У Кримінальному процесуальному кодексі України дискусійними залишаються питання щодо розширення переліку перевірочних дій (що дають первинну інформацію про злочин), а додаткові фактичні дані з'ясовувати вже в межах розслідування.

Ці проблеми вирішуються у деяких країнах по-різному.

Так, у Німеччині, якщо прокуратура на основі донесення або іншим шляхом отримує відомості про підозру у вчиненні злочину, то для прийняття рішення про висування публічного обвинувачення вона має дослідити обставини справи. У німецькому законодавстві взагалі не йдеться про здійснення перевірних дій.

Останнім часом у рамках міжнародної співпраці в боротьбі зі злочинністю правоохоронцями всього світу дедалі ширше використовуються можливості Міжнародної організації кримінальної поліції – Інтерполу.

Організація має забезпечувати широку взаємодію всіх органів (установ) кримінальної поліції в рамках чинного законодавства країни і в дусі Загальної декларації прав людини, створювати й розвивати установи, які можуть успішно сприяти запобіганню кримінальній злочинності та підтримувати боротьбу з нею. У зв'язку з прийняттям України до Міжнародної організації кримінальної поліції – Інтерполу в 1993 р. Кабінетом Міністрів України було прийнято Постанову (від 25.03.1993 р. № 220) «Про Національне центральне бюро Інтерполу».

У 1995 році відповідно до наказу МВС України від 15.02.1995 було створено підрозділи Укрбюро Інтерполу, затверджено типові завдання та функції цих підрозділів.

У 1997 році спільним наказом МВС, Генпрокуратури, СБ, Держкомітету у справах охорони державного кордону, Державної митної служби, ДПА було затверджено Інструкцію «Про порядок використання правоохоронними органами можливостей НЦБ Інтерполу в Україні у попередженні, розкритті та розслідуванні злочинів».

27 травня 2009 р. у Сан-Марино відбулася Європейська регіональна конференція Інтерполу «Стратегічний підхід у боротьбі із загрозами світовій безпеці». Були присутні близько 130 делегатів, які представляли 49 країн та 10 міжнародних організацій. У роботі конференції взяли участь перший заступник Міністра внутрішніх справ України та керівник Укрбюро Інтерполу. Однією із ключових проблем, що обговорювались під час конференції, було питання збільшення обсягів обміну важливою поліцейською інформацією та активізація використання ДНК-аналізу й дактилоскопії для розкриття транснаціональних злочинів, а також встановлення місцезнаходження і затримання злочинців, які намагаються уникнути відповідальності.

Серед завдань Генерального секретаріату Інтерполу зазначено, що він виступає як міжнародний центр боротьби зі злочинністю й діє як спеціалізований та інформаційний центр. З огляду на це однією з головних функцій Генерального секретаріату Інтерполу є створення та забезпечення функціонування міжнародних банків даних інформації криміналістичного й розшукового характеру.

Характерними особливостями цих банків даних є те, що інформація туди вноситься усіма країнами – членами Інтерполу (на сьогодні це 188 країн) та є доступною для правоохоронних органів усіх країн – членів Організації. Це дає підстави вважати банки даних Інтерполу глобальним інструментом з протидії злочинності, зокрема, для попередження, розкриття та розслідування злочинів, розшуку осіб (підозрюваних, обвинувачених, підсудних, засуджених, безвісті відсутніх), автотранспорту, речей та предметів, ідентифікації осіб (які не можуть повідомити про себе відомості, у тому числі й хворих та дітей, невпізнаних трупів) тощо.

Сьогодні існують такі банки даних Інтерполу: БД «Особи»; БД викрадених або втрачених документів; БД викрадених транспортних засобів; БД викрадених творів мистецтва; БД ДНК-профілів; БД відбитків пальців рук; БД порнографічних зображень, створених із залученням неповнолітніх.

Отримання інформації або перевірка відомостей за банками даних Інтерполу здійснюються в режимі On-line через комунікаційну систему Інтерполу «I-24/7» шляхом надсилання запиту до Генерального секретаріату Інтерполу (банки даних ДНК, порнографічних зображень, відбитків пальців).

Для забезпечення цільового використання правоохоронними органами держав-членів банків даних Інтерполу їх функціонування організовано так, що країна-власник інформації про об'єкт, розміщений у БД, автоматично отримує повідомлення про факт перевірки цього об'єкта іншою державою. Отримання такого повідомлення для країни-власника інформації є підставою для звернення до країни, що перевіряла об'єкт у банку даних, з приводу з'ясування необхідності проведення відповідної перевірки, запитування відомостей про місцезнаходження об'єкта тощо.

Невід'ємною частиною банків даних Інтерполу є Система міжнародних повідомлень Інтерполу (повідомлень із кольоровим кутком). Системою міжнародних повідомлень передбачено такі категорії інформаційних повідомлень/карток, які видаються державами-членами (НЦБ) та розміщуються на закритій частині web-сайту Генерального секретаріату Інтерполу, доступного правоохоронним органам.

Слід зазначити, що, крім Інтерполу, вже друге десятиліття на території Європи діє ще одна організація – Європол, працівникам якого надано надзвичайно широкі повноваження.

У процесі формування системи інформаційно-аналітичної системи правоохоронних органів можна скористатися досвідом створення таких систем у деяких країнах світу, зокрема, в частині захисту конфіденційної інформації та прав людини. Так, останнім часом поліція Великобританії працює над створенням Національної бази даних ДНК для потреб боротьби зі злочинністю.

Слід зазначити, що поліція Великобританії отримує більше зразків ДНК на одиницю населення, ніж будь-яка інша країна. У національній базі даних ДНК цієї країни знаходиться більш ніж 7 % населення (для порівняння, в Австрії у такій БД поліції знаходиться трохи більш ніж 1% населення).Подібна база даних США за загальною кількістю зразків є дещо більшою.

Отже, застосування світового досвіду створення та використання баз і банків даних буде корисним в процесі створення та впровадження системи інформаційно-аналітичного забезпечення правоохоронних органів України.

Ведучи мову про застосування кращого закордонного досвіду, не можна не згадати про програму «I2», яку вважають світовим лідером серед програмних засобів для візуального аналізу даних в процесі розслідування кримінальних правопорушень, її використовують аналітики та слідчі всього світу.

Список використаних джерел:

1. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Amendment to Convention ETS No. 108 allowing the European Communities to accede. – Режим доступу: //www.convention.coe.int/treaty/en/Treaties/Html/108.htm.
2. Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних: Закон України від 6 липня 2010 року № 2438-VI // Відомості Верховної Ради України (ВВР), 2010, № 46, ст. 542.
3. Система інформаційно-аналітичного забезпечення правоохоронних органів в умовах електронного урядування: монографія / В.В. Дурдинець, А.М. Іщенко, В.Г. Хахановський та ін. Київ: Нац. акад. внутр. справ, 2018. 352 с.
4. Хахановський В.Г. Міжнародний досвід нормативно-правового регулювання створення та використання баз і банків даних правоохоронних органів. *Актуальні проблеми правоохоронної діяльності: матер. Всеукр. наук.-практ. Інтернет конф.*; м. Сєвєродонецьк, 23 грудня 2016 р., Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка, 2017. С. 350–354.

Червінська Ксенія Олегівна,
студентка н.гр. 105_СПД ННІ
права та психології НАВС

Науковий керівник:
Хахановський Валерій Георгійович
доктор юридичних наук, професор, професор кафедри інформаційних технологій ННІ права та психології НАВС

АКТУАЛЬНІ ПРОБЛЕМИ ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВІ ТА ПСИХОЛОГІЇ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Інформаційні технології стали невід'ємною складовою нашого повсякденного життя і суттєво змінили спосіб функціонування людства. Інформатизація суспільства дозволяє збільшувати продуктивність роботи та навчання, крім того – організувати їх в домашніх умовах.

Однак, разом з перевагами, існують і серйозні недоліки, зокрема вплив технологій на фізичне та психічне здоров'я. Надмірне використання технологій Надмірне використання технологій пов'язане з різними негативними наслідками, серед яких особливо важливою є проблема психологічної залежності від інформаційних технологій.

Проведені дослідження свідчать про широкий спектр форм залежності від інформаційних технологій, таких як комп'ютерна, інтернет-залежність, цифрова, технологічна, електронна, соціальномедіа залежність та ін.

Основними напрямами застосування інформаційних технологій у юридичній сфері є;

- електронний суд та електронний документообіг (ЄСІТС);
- Єдиний державний реєстр судових рішень;
- автоматизовані аналітичні системи для правоохоронних органів;
- відеофіксація, онлайн-засідання в умовах воєнного стану;
- системи розпізнавання облич, аналітика даних, криміналістичні бази даних.

Актуальними проблемами застосування інформаційних та комунікайійних технологій в праві нині є:

- загрози кібербезпеці – злам державних інформаційних систем, витік персональних даних;
- недостатня захищеність електронних доказів – проблема автентичності цифрових файлів;
- недостатня цифрова грамотність працівників – труднощі з використанням ІТ у судах та поліції;
- технічні збої систем – підвійне навантаження у період війни, нестабільність зв'язку:
- нормативно-правова невизначеність – законодавство часто не встигає за розвитком технологій:
- етичні ризики – використання штучного інтелекту (ШІ) у кримінальних розслідуваннях може впливати на права людини.

Використання інформаційних технологій у психології.

Основні напрями застосування ІТ у психології є:

- онлайн-консультування та дистанційна психотерапія;
- використання мобільних додатків для моніторингу психічного стану;
- психодіагностика за допомогою комп'ютерних тестів;
- нейротехнології, віртуальна реальність (VR-терапія);
- застосування ШІ для аналізу поведінкових патернів.

Актуальними проблемами використання ІТ у психології сьогодні є:

- ризик порушення конфіденційності пацієнтів – зберігання чутливої інформації онлайн;
- низька достовірність деяких онлайн-тестів – відсутність валідності та стандартизації;
- залежність від технічної якості зв'язку – вплив на якість терапії;
- проблеми ідентифікації особи під час онлайн-консультації;
- етичні питання використання ШІ для психологічної діагностики;
- недостатня підготовка фахівців до роботи з цифровими інструментами.

На наш погляд, шляхами вирішення актуальних проблем у правовій сфері можуть бути:

- розробка й оновлення законодавства, що регулює роботу з цифровими доказами та використання ШІ;

- створення більш захищених реєстрів, модернізація ЄСІТС та інших державних платформ;

- підвищення цифрової грамотності юристів, суддів, слідчих;

- проведення кібераудиту у державних установах;

- стандартизація електронних доказів на рівні кримінального та цивільного процесів.

Список використаних джерел:

1. Коваль Г.С. Характеристики різних категорій користувачів кіберпростору: саноцентричний підхід. *Габітус*. 2023. № 46. С. 152–160. URL: https://doi.org/10.32782/2663-5208.2023.46.24 (дата звернення: 06.03.2024).

2. Лукащук С. Стрес як передумова інтернет-залежності студентів. *Вісник Львівського університету. Серія психологічні науки*. 2022. № 13. С. 87–96. URL: https://doi.org/10.30970/ps.2022.13.11 (дата звернення: 28.02.2024).

3. Максименко Ю.Б., Малюта Ю.С. Психологічні особливості персоніфікації комп'ютера у дітей молодшого шкільного віку. *Актуальні проблеми психології особистості: теорія, досвіт, практика*: матер. Всеукр. наук.-практ. конф. (28-29 квітня 2022 року). ПНПУ ім. К. Д. Ушинського, каф. загальної та диференціальної психології соціально-гуманітарного фак-ту. Одеса, 2022. С. 45-52.

4. Максименко Ю., Мурманова І. Психологічні особливості залежності особистості від впливу сучасних інформаційних технологій // *Актуальні проблеми психології особистості: теорія, досвід, практика* / Зб. матер. Всеукр. наук.-практ. конф. (м.Одеса, 25-26 квітня 2024 року). Одеса: ун-т Ушинського, 2024. С. 162-170.

Демченко Максим Володимирович,
студент н.гр. 117_СПД ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович,
кандидат фіз.-мат наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

ПОЛІТИКА КОНФІДЕНЦІЙНОСТІ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

У сучасному цифровому середовищі персональні дані стали одним із ключових ресурсів, що визначають безпеку, довіру та ефективність функціонування держави й суспільства. З огляду на стрімкий розвиток інформаційних технологій, інтеграцію електронних сервісів і зростання кількості кіберзагроз особливої актуальності набувають питання захисту приватності та дотримання принципів політики конфіденційності. Україна, адаптуючи законодавство до європейських стандартів, зокрема до Загального регламенту ЄС про захист даних (GDPR), створює правові механізми, спрямовані на забезпечення балансу між використанням цифрових технологій та охороною прав громадян.

Політика конфіденційності визначає правила збирання, використання, зберігання та поширення персональних даних, а також гарантує дотримання прав суб'єкта даних. Вона є невід'ємним елементом правовідносин між громадянином, державою та організаціями, які обробляють інформацію. Особливе значення політика конфіденційності має в діяльності публічних органів, що забезпечують надання адмінпослуг, ведення державних реєстрів та впровадження електронного врядування.

Закон України «Про захист персональних даних» визначає персональні дані як будь-яку інформацію, що прямо чи опосередковано ідентифікує особу. Закон встановлює принципи їх обробки, серед яких: законність, прозорість, цілеспрямованість, пропорційність, достовірність та збереження протягом необхідного строку. Ключовою гарантією є згода суб'єкта персональних даних, що надає право органам та організаціям здійснювати їхню обробку, окрім випадків, прямо передбачених законом.

Європейський GDPR посилив підхід до захисту даних, запровадивши такі важливі інструменти, як право на забуття, право на перенесення даних, обов'язок повідомлення про витоки інформації та принцип «privacy by design». Україна поступово впроваджує ці механізми, що підвищує прозорість та відповідальність у сфері обробки даних, особливо в державному секторі.

Проблематика захисту персональних даних ускладнюється зростанням кіберзагроз, зокрема несанкціонованим доступом, фішинговими атаками, витоками з державних реєстрів та зламами електронних систем. У цих умовах важливою є діяльність Державної служби спеціального зв'язку та захисту інформації України (ДССЗЗІ), яка координує кіберзахист державних ресурсів та встановлює вимоги до безпечної обробки інформації. Значна увага приділяється впровадженню комплексної системи захисту інформації (КСЗІ), яка забезпечує технічну та організаційну безпеку даних.

Сучасні цифрові сервіси, такі як «Дія», також здійснюють обробку значного обсягу персональних даних, що вимагає підвищених заходів безпеки. Уряд декларує, що обробка інформації здійснюється відповідно до міжнародних стандартів і в умовах сертифікованих систем захисту. Важливо, що користувач має право контролювати, які саме його дані обробляються, та може отримати відповідну інформацію через офіційні канали.

Окремим викликом є необхідність підвищення цифрової грамотності населення, адже значна частина витоків інформації пов'язана з людським фактором: некоректним використанням паролів, завантаженням шкідливих програм або погодженням на сумнівні умови обробки даних. Тому політика конфіденційності не обмежується лише правовими нормами — вона потребує формування культури захисту даних на рівні всього суспільства.

Таким чином, ефективний захист персональних даних в Україні можливий лише за умови комплексного підходу, що поєднує оновлення законодавства, впровадження сучасних технологій кіберзахисту, посилення відповідальності за порушення та підвищення рівня обізнаності громадян. Політика конфіденційності стає фундаментальним інструментом забезпечення прав людини в цифрову епоху та формує довіру до державних і приватних сервісів.

Список використаних джерел:

1. Закон України «Про захист персональних даних».
2. Загальний регламент Європейського Союзу про захист даних (GDPR).
3. Офіційний сайт Уповноваженого ВРУ з прав людини — Розділ «Захист персональних даних».
4. Офіційний портал ДССЗЗІ — матеріали щодо кіберзахисту.

Ходосок Карина Юріївна,
студентка н.гр. 117_СПД
ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович,
кандидат фіз.-мат наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

ЕТИЧНІ ТА ПРАВОВІ ВИКЛИКИ ІНТЕГРАЦІЇ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРАВОЗАСТОСОВНУ ПРАКТИКУ ТА ПСИХОЛОГІЧНУ ДОПОМОГУ

Сучасні інформаційні технології (ІТ) активно впливають на різні сфери життя, зокрема на правозастосування та надання психологічної допомоги. Інноваційні технології, зокрема штучний інтелект (ШІ), великі дані, блокчейн, цифрові платформи для консультацій, відкривають нові можливості для оптимізації процесів, підвищення ефективності та доступності послуг. Однак одночасно з цими перевагами виникають й етичні та правові виклики, які потребують детального аналізу та відповідного регулювання.

1. Етичні виклики

a. Конфіденційність та захист персональних даних

Одним із основних етичних викликів є забезпечення конфіденційності даних клієнтів. В умовах, коли особиста інформація, медичні записи або дані про психічний стан збираються та обробляються через цифрові платформи, постає питання захисту цих даних від несанкціонованого доступу або витоку. У правозастосуванні та психологічній допомозі ці дані є надзвичайно чутливими, тому зловживання ними може призвести до серйозних наслідків для осіб, що звертаються за допомогою.

b. Психологічні маніпуляції

Інтеграція технологій, зокрема ШІ, у психологічну допомогу створює можливості для маніпулювання емоціями користувачів. Наприклад, чат-боти або автоматизовані системи підтримки можуть виявляти вразливі моменти у психічному стані людини та використовувати їх для змінення її поведінки чи емоцій. Це піднімає важливі етичні питання щодо доцільності використання таких інструментів без належного контролю з боку фахівців.

c. Заміна людського фактору

Хоча ІТ можуть покращити ефективність правозастосування та психологічної допомоги, їх використання не повинно повністю замінювати людський фактор. Важливі аспекти взаємодії з клієнтами, такі як емпатія, розуміння індивідуальних потреб і контексту, не можуть бути повною мірою замінені автоматизованими системами. Це створює етичну дилему: чи можна покладатися на технології в тих випадках, коли людський контакт є необхідним для досягнення успіху?

2. Правові виклики

a. Регулювання використання ІТ в правозастосуванні та психології

Інтеграція ІТ в ці сфери вимагає розробки відповідного законодавства для визначення меж використання технологій. Правове регулювання повинно забезпечити, щоб застосування ШІ, блокчейну, цифрових платформ тощо не порушувало права людини. Наприклад, застосування ШІ для прийняття судових рішень або автоматичне визначення рівня ризику при наданні психологічної допомоги потребує чіткої правової регламентації, аби уникнути можливих помилок або зловживань.

b. Відповідальність за помилки технологій

Інший важливий аспект – визначення відповідальності за помилки, спричинені використанням ІТ. Якщо ШІ або інша технологія зробить помилку в аналізі доказів або визначенні потреб клієнта, хто нестиме відповідальність за такі помилки? Це питання досі залишається відкритим у багатьох країнах і потребує розробки спеціалізованих законів щодо відповідальності за використання технологій у правозастосуванні та психології.

c. Цифровий розрив і доступність

Не всі громадяни мають рівний доступ до новітніх технологій, особливо в країнах з низьким рівнем цифровізації або у віддалених регіонах. Це створює правову проблему щодо забезпечення рівного доступу до правових і психологічних послуг. Відсутність доступу до інтернету або технологічних засобів обмежує можливості деяких громадян скористатися сучасними сервісами.

3. Приклади використання технологій

У правозастосуванні сучасні технології використовуються для автоматизованого аналізу доказів, прогнозування результатів судових справ, розпізнавання та верифікації документів за допомогою ШІ. Одним із прикладів є використання ШІ для автоматичного визначення пріоритетів справ, що дозволяє скоротити час їх розгляду.

У психології технології застосовуються для дистанційного консультування через відеозв’язок, використання чат-ботів для першої психологічної підтримки, а також для моніторингу психічного здоров’я через спеціалізовані додатки. Ці інструменти дозволяють знизити бар'єри для отримання допомоги, але водночас підвищують ризик порушення конфіденційності або неналежного впливу на клієнтів.

Висновок

Інтеграція сучасних інформаційних технологій у правозастосовну практику та психологічну допомогу має значний потенціал для підвищення ефективності та доступності цих послуг. Однак вона також ставить перед суспільством низку етичних та правових викликів, які потребують ретельного аналізу та розробки відповідного регулювання. Необхідно знайти баланс між використанням технологій для поліпшення сервісів та захистом прав людини, збереженням конфіденційності і забезпеченням доступу до допомоги для всіх.

Список використаних джерел:

1. Барбакова, О.В. (2022). "Правові аспекти використання сучасних інформаційних технологій в судовій практиці". *Юридичний вісник*, 8(1), 45-50.
2. Гречанюк, О.О. (2023). "Етичні виклики цифровізації психологічної допомоги". *Психологія та суспільство*, 9(2), 12-18.
3. Ткаченко, В.І. (2021). "Штучний інтелект у правозастосуванні: переваги та ризики". *Право і технології*, 4(3), 55-60.
4. Кучеренко, І.С. (2020). "Захист персональних даних у цифрову епоху". *Правовий журнал*, 6(2), 99-104.
5. Соловйова, Л.Ю. (2021). "Цифрова нерівність: правові наслідки для доступу до психологічних послуг". *Сучасні проблеми права*, 11(4), 42-46.

Горенчук Євгенія Андріївна,
студентка н.гр. 103_СПД
ННІ права та психології НАВС

Науковий керівник:
Хахановський Валерій Георгійович,
доктор юридичних наук, професор, професор кафедри інформаційних технологій ННІ права та психології НАВС

ОСНОВНІ ЗАСАДИ СТВОРЕННЯ СИСТЕМИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННИХ ОРГАНІВ

Підґрунтям для створення єдиної інтегрованої системи інформаційно-аналітичного забезпечення правоохоронних органів слугували розроблені та впроваджені ще у 70-ті роки минулого століття інформаційні системи та підсистеми. Але виникла нагальна потреба наукового обґрунтування, створення та впровадження системи інформаційно-аналітичного забезпечення правоохоронної діяльності, яка базується на новітніх апаратно-програмних засобах, застосовує інтегрований банк даних та охоплює всі рівні управління правоохоронних органів України.

Профілактика, боротьба з кримінальними правопорушеннями, охорона громадського порядку та інші завдання, що вирішуються правоохоронними органами, потребують подальшого вдосконалення техніки і методів управління на основі сучасних досягнень науки й практики, розробки й впровадження комп'ютеризованих систем.

Програма націлена на розроблення та впровадження комп'ютеризованих інформаційних систем у правоохоронних органах. Основною її метою є створення інформаційно-комп'ютерних систем, що забезпечують:

• підвищення рівня управління підрозділами правоохоронних органів;

• зниження впливу суб'єктивних чинників при виробленні рішень, що приймаються за заявами і повідомленнями громадян;

• контроль за дотриманням законності;

• зниження трудомісткості і підвищення культури обробки інформації;

• повніше використання фондів і джерел інформації у запобіганні правопорушенням, розшуку злочинців, що переховуються, розшуку осіб, зниклих безвісти та ін.;

• раціональну розстановку сил і засобів, підвищення ефективності взаємодії підрозділів;

• підвищення якості розробки відомчих нормативних актів та вирішення інших завдань.

Для реалізації цих цілей здійснено і здійснюється:

• розробка теоретичних засад побудови комп'ютеризованої системи оперативного управління в органах внутрішніх справ;

• моделювання вирішення задач синхронізації в складних системах організаційного управління;

• уніфікація документообігу, раціоналізація вирішення завдань оперативного управління;

• розробка методів і засобів вирішення спеціальних пошукових, розпізнавальних та інших задач в інтересах штабів, чергових частин, карного розшуку, профілактики, слідства, боротьби з економічними злочинами, хабарництвом, раціоналізації патрульної служби та інших підрозділів.

Різноманіття і специфічність завдань правоохоронних органів, що часто вирішуються в умовах невизначеності, неповної інформації, наявності випадкових чинників і ризику, соціально-психологічних та інших особливостей осіб, схильних до здійснення правопорушень, а також фактів суб'єктивного тлумачення правових норм, потребують розробки нової методології управління на основі сучасних інформаційних технологій, наукових методів, комп'ютерної техніки та електронних комунікацій.

Розвиток банку даних, системи спілкування та інших засобів комп'ютеризованого управління має послідовність і етапність. Запропонована модель комп'ютеризованої системи оперативного управління є подальшим кроком розвитку бази знань для вирішення конкретних завдань, у тому числі правоохоронних органів.

Використовувані інформаційні системи типу банку даних дозволяють уникнути недоліків і виконують функції інформаційно-пошукових та довідкових систем, що обслуговують входи і виходи системи оперативного управління.

Внаслідок системного аналізу відібрані для вирішення в КСУ завдання і функції: штабу і його підрозділів; служб секретаріату; карного розшуку і профілактики; служб охорони громадського порядку; слідчих апаратів; служби по боротьбі з економічними злочинами; патрульної поліції; служб планування, обліку і аналізу кадрового складу та інших.

Зокрема, галузева комп'ютеризована система управління правоохоронних органів, зважаючи на свою складність, різноплановість, ієрархічність, велику кількість зав'язків, потребує чіткого визначення її структури як на етапі проектування, так і під час функціонування.

При дослідженні функцій, виконуваних підрозділами правоохоронних органів на всіх рівнях управління, і операцій формування рішень виявилася доцільною декомпозиція її за трьома ознаками а саме:

• за функціональним призначенням елементу структури;

• за масштабом діяльності;

• за виконуваним етапом у процесі управління.

При цьому враховуються організаційні і функціональні структури правоохоронних органів, що вже склалися, окремі напрями в їх діяльності і сталі послідовності дій в процесі управління.

Відповідно до функцій, виконуваних органами внутрішніх справ, КСУ МВС України розділена на функціональні підсистеми, що відповідають організаційній структурі МВС.

В окремі підсистеми виділяються методологічне, інформаційно-правове і кадрове забезпечення.

Аналіз існуючої системи управління, потоків інформації і завдань, що вирішуються структурними підрозділами правоохоронних органів на прикладі МВС України, дозволили зробити висновок про створення КСУ з трьома рівнями автоматизованого управління, які найраціональніше забезпечують збирання, накопичення, обробку, аналіз і використання інформації в діяльності правоохоронних органів.

Основними рівнями управління в КСУ МВС України прийняті:

І рівень – центральний. На цьому рівні забезпечується загальна централізація управління і вирішуються завдання планування, оцінки, обліку, аналізу і прогнозування оперативної обстановки, стану боротьби із злочинністю та правопорушеннями в регіонах і в державі, оцінюється ефективність діяльності управлінь і відділів поліції, виробляються і приймаються рішення.

ІІ рівень – управління ОНП в областях. Тут вирішуються завдання з обробки інформації, одержаної в ході оперативно-розшукової і профілактичної діяльності, розробляються рекомендації по боротьбі зі злочинністю і проведенням конкретних оперативних заходів.

ІІІ рівень – міські і районні органи Національної поліції. На цьому рівні ОНП здійснюються функції боротьби із злочинністю, охороняється громадський порядок і т. д. Формується первинна інформація і здійснюється її введення в КСУ.

Нами умовно виділено чотири основних, певною мірою самостійних, етапи (фази), що становлять повний цикл у процесі управління:

I фаза /«Облік»/.

II фаза /«Аналіз»/.

III фаза /«Прогноз»/.

IV фаза /«План»/.

Розділення процесу управління на окремі фази обумовлюється самою логікою управлінської діяльності і може бути віднесено до багатьох систем управління.

Застосування запропонованої методології дозволяє розробляти і комп’ютеризувати вирішення низки завдань. До їх числа відносяться:

• безперервне стеження за оперативною обстановкою;

• облік і аналіз стану боротьби із злочинністю;

• безперервне планування управлінської діяльності і контроль виконання;

• розрахунок потреби сил і засобів, їх раціональна розстановка;

• обробка даних, що містяться в нормативних актах, даних про передовий досвід, листах, заявах, скаргах громадян і з інших питань.

Видаються дані, що відображають процеси в часі, за напрямами діяльності, зокрема: про результати оперативно-розшукової діяльності

правоохоронних органів у боротьбі із злочинністю по всіх службах; про результати роботи із спостереження за особами, прибулими після завершення терміну покарання, і умовно засудженими; про результати боротьби з наркоманією, хуліганством та інші питання.

Комплекс програм, що реалізують обробку і видачу даних про листи, заяви, скарги і пропозиції, що надходять до МВС, забезпечує: підготовку інформації в державні органи; аналіз листів громадян, що надходять; планування діяльності МВС, органів Національної поліції та інших ЦОВВ, які координує Міністр внутрішніх справ через Кабінет Міністрів України; контроль і визначення ефективності проведення заходів.

Комплекс програм з обробки даних, що містяться в нормативних документах, які регламентують діяльність правоохоронних органів (укази, закони, постанови, розпорядження, накази, вказівки, інструкції), забезпечує виконавців і розробників нових нормативних актів різними довідками, потрібними при виконанні ними службових функцій.

Розроблення і впровадження комп'ютеризованої підсистеми централізованого оперативного управління на основі запропонованої моделі оперативного управління, дозволяє скоротити трудовитрати на виконання завдань, оптимізувати вироблення управлінських рішень, знизити вплив суб'єктивних чинників.

Система відомостей про різні об'єкти, що підлягають обліку, є важливим ресурсом у забезпеченні запобігання, виявлення, розкриття та розслідування злочинів. За характером об'єктів, що враховуються, виділяються три групи даних про осіб, події, предмети і об'єкти. Відповідно до цього класифікуються інформаційні фонди, завдання, розроблена структура баз даних.

Інтеграція галузевих інформаційно-комп'ютерних систем МВС, прокуратури, податкової, митної та інших правоохоронних служб дозволяє реалізувати завдання Указу Президента № 80\2006 від 31 січня 2006 року «Про Єдину комп'ютерну інформаційну систему правоохоронних органів з питань боротьби зі злочинністю».

Для функціонування CASE-продуктів у складі САПР треба мати СУБД ORACLE (версія 5.1 і вище), що включає модулі SQL*FORMS та SQL*PLUS. У свій час МВС України у однойменній фірми було придбано та багато років успішно використовується СУБД ORACLE з цими та іншими модулями й постійним оновленням версій. Українські програмісти (працівники МВС та ОНП України) постійно проходять стажування та підвищення кваліфікації, які проводяться представниками фірми «ORACLE».

Система інформаційно-аналітичного забезпечення правоохоронних органів – це високоорганізований логічний комплекс на базі інтегрованого банку даних, де накопичується масиви інформаційних обліків, взаємозв'язаних через центральне ядро даних; використовується загальна технологія оброблення інформації, повномасштабний комплекс засобів забезпечення безпеки й надійності, яка дозволяє забезпечити аналітичною інформацією для оперативно-розшукової діяльності, розслідування і попередження злочинів,

надання аналітичної, статистичної та контрольної інформації для розроблення та прийняття обґрунтованих рішень на всіх рівнях управління правоохоронними органами; ефективної взаємодії з комп'ютерними мережами кримінальної поліції закордонних країн з метою підвищення рівня ефективності правоохоронної діяльності та боротьби з корупцією.

Інтегрований банк даних (ІБД) дозволив об'єднати окремі інформаційні обліки ОВС в єдине ціле. Інтегрованість дозволяє встановлювати і відслідковувати зв'язки між усіма включеними в ІБД об'єктами.

Отже, **с**творення системи інформаційно-аналітичного забезпечення правоохоронних органів дозволило впровадити сучасну організацію та технологію опрацювання даних, що охоплює використання нових методів і засобів, фіксацію та своєчасну підготовку інформації на випадок можливих пошкоджень оригіналу й оперативне надання даних користувачам у потрібних їм аспектах. При цьому пропонуються різноманітні форми надання інформації.

Список використаних джерел:

1. Про Єдину комп'ютерну інформаційну систему правоохоронних органів з питань боротьби зі злочинністю: указ Президента України від 31 січня 2006 року № 80/2006.
2. Джужа О.М. Джерела кримінологічної інформації про стан злочинності в Україні / О. Джужа, Д. Голосніченко, А. Кирилюк // Право України. 2003. № 12. С. 55-69.
3. Задорожній Ю.О., Хахановський В.Г. Інформації багато не буває // Бюл. з обм. досвідом роботи. 2009. № 178. С. 9–14.
4. Інформаційно-довідкове забезпечення кримінальних проваджень: підручн. / В.В. Бірюков, В.Г. Хахановський, В.С. Бондар та ін. Київ: Центр учбової літератури, 2014. 288 с.
5. Хахановський В.Г. Інформатизація управління в органах внутрішніх справ: посіб. / В.Г. Хахановський, П.П. Підюков, В.М. Смаглюк та ін.: заг. ред. проф. Я. Ю. Кондратьева. Київ: НАВСУ, 2003.
6. Хахановський В.Г. Проблеми та перспективи використання автоматизованих дактилоскопічних систем у боротьбі зі злочинністю // Криміналістичний вісник. 2002. Вип. 3. С. 98–104.
7. Хахановський В.Г. Інтегрований банк даних: формування термінології та проблеми впровадження у правоохоронну діяльність // Боротьба з організованою злочинністю і корупцією (теорія і практика): наук.-практ. журнал. 2012. № 1 (27). С. 307–311.
8. Кудінов В.А., Смаглюк В.М., Хахановський В.Г. Інформаційне забезпечення ОВС: навч. посіб. / за заг ред. В.Г. Хахановського. Київ: Нац. акад. внутр. справ, 2015. 108 с.
9. Хахановський В.Г., Чукаєва А.В. Інформаційне право: підручн. / за заг. ред. С.С. Чернявського. Київ: Нац. акад. внутр. справ, 2015. 216 с.

10. Хахановський В.Г. Кудінов В.А., Смаглюк В.М. Інформаційні технології в правозастосовній практиці: навч. посіб. Київ: Нац. акад. внутр. справ, 2015. 112 с.

11. Кондратьєв Я.Ю., Хахановський В.Г. Нормативно-правова база інформаційно-аналітичного забезпечення діяльності оперативних підрозділів міліції // Наук. вісник НАВСУ. 2003. № 3. С. 52–59.

12. Хахановський В.Г. Корзун В.М. Геоінформаційна система як складова єдиної комп'ютерної інформаційної системи правоохоронних органів // Правова інформатика. 2008. № 1 (17). С. 62–66.

13. Хахановський В.Г., Замаруєва І.В. Інформаційні загрози стану інформаційно-аналітичного забезпечення державного управління // Бюл. з обм. досв. роботи. 2001. № 135. С. 3–6.

14. Хахановський В.Г. Проблеми теорії і практики криміналістичної інформатики: монографія. Київ: Вид.Дім «Аванпост-Прим». 2010. 382 с.

15. Хахановський В.Г. Розслідування злочинів як інформаційний процес // Науковий вісник ЛІВС. 2003. № 3 (1). С. 131–135.

16. Хахановський В.Г., Смаглюк В.М. Термінологічні та організаційні аспекти створення інформаційно-аналітичної системи ОВС України // Правова інформатика. 2006. № 1 (9). С. 42–44.

17. Система інформаційно-аналітичного забезпечення правоохоронних органів в умовах електронного урядування: монографія/ В.В. Дурдинець, О.М. Іщенко, В.Г. Хахановський та ін. ; за заг. ред. І.В. Сергієнка, С.С. Чернявського, М.Я. Швеця. Київ: Нац. акад. внутр. Справ, 2018, 352 с.

Левченко Дарина Олександрівна,
студентка н.гр. 103_СПД ННІ права та психології НАВС

Науковий керівник:
Хахановський Валерій Георгійович
доктор юридичних наук, професор, професор кафедри інформаційних технологій ННІ права та психології НАВС

КІБЕРБЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ КЛІЄНТІВ У РОБОТІ ЮРИСТА ТА ПСИХОЛОГА: СУЧАСНІ ЗАГРОЗИ ТА ТЕХНОЛОГІЧНІ РІШЕННЯ

У сучасних умовах цифровізації юридичної та психологічної практики питання захисту персональних даних клієнтів набуває пріоритетного значення. У роботі юриста та психолога обробляється інформація, що належить до категорії конфіденційної, а часто — до чутливої (intimate/sensitive data): медичні дані, психологічний стан, результати тестувань, особисті історії, дані кримінального провадження, фінансова інформація, матеріали адвокатської таємниці тощо. Порушення конфіденційності може спричинити юридичну відповідальність, професійну дискваліфікацію, моральну шкоду для клієнта, втрату репутації фахівця.

Водночас збільшення кількості онлайн-консультацій, використання хмарних сервісів, електронних доказів, дистанційних платформ та месенджерів значно підвищує ризики несанкціонованого доступу до інформації. Важливим є впровадження комплексних технічних і організаційних заходів, що забезпечують відповідність законодавству України, загальним стандартам кібербезпеки та міжнародним практикам (GDPR, NIST, ISO/IEC 27001).

Нормативно-правове підґрунтя захисту персональних даних у юридичній та психологічній практиці:

Закон України «Про захист персональних даних» (№2297-VI).

Закон визначає:

- поняття персональних даних та їхні категорії;
- обов’язки володільців і розпорядників даних;
- вимоги до згоди суб’єкта;
- принципи обробки: законність, пропорційність, мінімізація, точність, обмеження строків;
- необхідність впровадження організаційних і технічних заходів безпеки.

Для юриста та психолога визначальними є статті щодо чутливих даних, адже інформація клієнтів належить до категорій, які потребують підвищеного захисту.

Загальний регламент ЄС із захисту даних (GDPR) – як міжнародний орієнтир.

Хоча Україна формально не підпадає під дію GDPR, його принципи є міжнародним стандартом:

- «privacy by design» та «privacy by default»;
- необхідність Data Protection Impact Assessment (DPIA) при роботі з ризиковими даними;
- право клієнта на стирання, перенесення, доступ;
- вимоги до безпечної передачі даних.

Адвокатська таємниця (Закон України «Про адвокатуру та адвокатську діяльність»)

Юрист зобов'язаний забезпечити конфіденційність:

- матеріалів справи;
- електронних документів;
- листування з клієнтом;
- чернеток та нотаток;
- файлів у смартфоні, ноутбуці та хмарних сховищах.

Порушення конфіденційності є дисциплінарним проступком.

Етичні стандарти психолога

Кодекси етики забороняють розкривати інформацію про клієнта, окрім випадків загрози життю.

Це накладає технологічні зобов'язання:

- безпечне зберігання записів сесій;
- недопущення використання небезпечних месенджерів;
- обмеження доступу сторонніх осіб.

Сучасні кіберзагрози для юристів і психологів.

Фішинг і соціальна інженерія

Близько 90% кібератак у світі починаються з фішингу. Атакувальники можуть:

- видавати себе за клієнта;
- надсилати «документи справи» або «результати тестів» як заражені файли;
- використовувати месенджери та соціальні мережі;
- підробляти email встановленого домену.

Юристи та психологи – ідеальні цілі, бо працюють із приватною інформацією.

Злам месенджерів і електронної пошти

Більшість випадків витоку конфіденційних даних відбувається через:

- слабкі паролі;
- відсутність двофакторної автентифікації (MFA);
- збереження паролів у браузері;
- синхронізацію на незахищених пристроях.

Витоки через незахищені онлайн-платформи

Небезпеку становлять:

- безкоштовні сервіси відеозв'язку без end-to-end шифрування;
- застарілі або «піратські» програми;
- неперевірені онлайн-тести й додатки для психологів;
- CRM-системи з низьким рівнем захисту.

Атаки на хмарні сховища

Проблеми виникають через:

- неправильно налаштовані права доступу;
- слабкі корпоративні паролі;
- відсутність контролю активності;
- сторонні підключення.

Ransomware (віруси-вимагачі)

Шифрування файлів клієнтів із вимогою викупу стало головною загрозою для приватних кабінетів.

Ризики:

- повна втрата бази клієнтів;
- витік документів справи;
- шантаж;
- кримінальна відповідальність за недбале зберігання персональних даних.

Інсайдерські загрози

До них належать:

- доступ помічників до конфіденційних матеріалів;
- випадкові витоки через копіювання файлів;
- неправильна передача документів у messengers;
- робота з документами у спільних Google-дисках.

Принципи кіберзахисту для юристів і психологів.

Мінімізація даних

Збирати лише те, що потрібно.

Психологу не потрібно знати адресу клієнта; юристу – сімейний стан, якщо це не має значення для справи.

Розмежування доступу

- кожен співробітник має доступ лише до тих файлів, які потрібні для роботи;
- заборонено передавати дані через особисті акаунти;
- не дозволяти сім'ї або друзям користуватися робочим ноутбуком.

Шифрування

- шифрування диска: BitLocker, FileVault, VeraCrypt;
- шифрування листування: E2EE;
- шифрування архівів із паролем;
- шифрування резервних копій.

MFA/2FA — основа сучасного захисту

Вести професійну діяльність без MFA — критична помилка.

Захист мобільних пристроїв

Оскільки психологи та юристи часто працюють зі смартфона:

- PIN 6+ цифр;

- біометрія;
- вимкнення push-сповіщень для месенджерів, де обговорюються справи;
- заборона автоматичного створення скрінів.

Технологічні рішення для безпечної практики.

Безпечні месенджери

Рекомендовані: Signal, Threema, WhatsApp (E2EE).

Умовно дозволені з певними застереженнями:

- Telegram (НЕ E2EE у чатах за замовчуванням, немає E2EE у групах).

Заборонені для конфіденційної роботи:

- Instagram Direct
- Facebook Messenger
- Viber (немає перевірки ключів і слабка реалізація E2EE).

Відеозв'язок для онлайн-консультацій

Психологам:

- Google Meet (якщо підключено корпоративний Google Workspace),
- Zoom (лише в корпоративній версії з E2EE),
- VSee (медично орієнтована платформа),
- Doxy.me (для телемедицини).

Юристам: Microsoft Teams, Google Meet, Zoom з E2EE.

Не рекомендовано: Telegram-дзвінки, Skype, Facebook Messenger Rooms.

Хмарні сховища

Найбезпечніші:

- Google Workspace (корпоративний рівень)
- Microsoft OneDrive for Business
- Tresorit (повне шифрування)
- Proton Drive

Заборонені для конфіденційних даних:

- безкоштовні Google-диски без обмеження доступу;
- iCloud без MFA;
- Dropbox Basic.

Менеджери паролів.

Варто використовувати: Bitwarden, 1Password, KeePassXC.

НЕ рекомендується: зберігати паролі у браузері, паролі у нотатках телефону.

Антивірус і захисне ПЗ

Рекомендовані рішення:

- Bitdefender
- Kaspersky (тільки якщо немає законодавчих обмежень)
- ESET
- Microsoft Defender (вбудований, але надійний)

Також важливі: фільтрація вкладень у пошті, блокування небезпечних сайтів, функція виявлення ransomware.

Організаційні заходи

Політика безпеки

Має містити:

• правила доступу; правила зберігання документів; порядок резервного копіювання; обов'язки співробітників; порядок реагування на інциденти; порядок ведення онлайн-консультацій.

Навчання персоналу

Щонайменше раз на рік проводиться навчання щодо: фішингу; використання робочих пристроїв; заборонених сервісів; алгоритму реагування при атаці.

Угоди про нерозголошення (NDA)

Підписуються: з помічниками; адміністраторами; перекладачами; технічним персоналом.

Оцінка впливу DPIA

Проводиться при: використанні нових платформ; обробці чутливих медичних/психологічних даних; перенесенні даних у хмару.

Рекомендації для психолога.

Психолог працює з даними: про психічний стан; діагностичні тести; результати терапії; історії травм; записи сесій.

Це особливо чутлива інформація.

Психолог зобов'язаний:

1. Використовувати окремий робочий пристрій.
2. Не проводити консультації через небезпечні месенджери.
3. Заборонити запис екрана у смартфоні.
4. Зберігати записи сесій у зашифрованому вигляді.
5. Обмежувати доступ до календаря з розкладом клієнтів.
6. Використовувати платформи, адаптовані до медичної конфіденційності (VSee, Doxy).

Рекомендації для юриста.

Юрист працює з: документами кримінальних проваджень; персональними даними сторін; фінансовими документами; доказами; відео/аудіоматеріалами; матеріалами з обмеженим доступом.

Юристу необхідно:

1. Шифрувати досьє та усі резервні копії.
2. Використовувати електронний підпис тільки через сертифіковані сервіси.
3. Уникати пересилання документів клієнта через месенджери.
4. Створити захищений канал обміну файлами (ProtonDrive, Tresorit).
5. Заборонити ведення справи через особисту пошту (тільки корпоративна).

План реагування на інциденти

Алгоритм

У разі підозри на витік:

1. Негайно ізолювати пристрій.
2. Змінити паролі та закрити сесії входів.
3. Перевірити журнали активності у хмарі.

4. Повідомити керівництво або клієнта (залежно від законодавства).
5. Оцінити масштаб витоку.
6. Відновити дані з резервної копії.
7. Оформити інцидент у внутрішньому журналі.

Висновок.

Юрист і психолог працюють із вразливими категоріями інформації, тому зобов'язані забезпечити найвищий рівень кіберзахисту. Сучасні загрози – фішинг, соціальна інженерія, ransomware, злом месенджерів, вразливі онлайн-платформи – вимагають комплексного підходу:технічного (шифрування, MFA, безпечні пристрої), організаційного (політики, навчання, NDA) та правового (дотримання Закону України, рекомендацій міжнародних стандартів).

Ефективна стратегія кібербезпеки – це не одноразова дія, а системна робота, яка підвищує захист професіонала та довіру клієнтів.

Список використаних джерел:

1. Закон України «Про захист персональних даних» №2297-VI.
2. Закон України «Про адвокатуру та адвокатську діяльність».
3. GDPR — General Data Protection Regulation (Regulation (EU) 2016/679).
4. NIST SP 800-122. Guide to Protecting the Confidentiality of Personally Identifiable Information.
5. ISO/IEC 27001:2022 — Information Security Management Systems.
6. OWASP Top 10 Web Application Security Risks.
7. National Cyber Security Centre (NCSC). Cyber Security Guidance.
8. American Psychological Association (APA). Guidelines for Telepsychology.
9. LawTech Today. Cybersecurity Best Practices for Attorneys.
10. European Federation of Psychologists' Associations. Ethical Guidelines for Online Therapy.

Савотєєва Анастасія Олександрівна,
студентка н.гр. 301_СПС
ННІ права та психології НАВС

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

ВПЛИВ НАДМІРНОГО ЗАХОПЛЕННЯ ЦИФРОВИМИ ПРИСТРОЯМИ НА РОЗВИТОК ПСИХОЛОГІЧНИХ ПРОБЛЕМ У ДІТЕЙ

Під впливом надмірного захоплення цифровими пристроями на розвиток психологічних проблем у дітей слід розуміти сукупність негативних змін у емоційному, когнітивному та поведінковому розвитку дитини, що виникають унаслідок тривалого та неконтрольованого користування гаджетами.

Узагальнюючи думки провідних науковців, це поняття може бути визначене так: «Надмірне та тривале використання цифрових пристроїв у дитячому віці може “перепрошивати” (перебудовувати) природний хід розвитку, роблячи дітей більш тривожними, емоційно нестабільними та вразливими до депресії й залежної поведінки» - на основі висновків Джонатана Гайдта [1].

Проблема впливу гаджетів на здоров’я дітей є надзвичайно актуальною для сучасного суспільства, коли спостерігається їх масштабне та динамічне проникнення в усі сфери життєдіяльності людини та значною мірою відображається на її соціальному самопочутті і орієнтаціях.

Взаємодія особистості з гаджетом неоднозначно впливає на здоров’я дитини та соціальне становлення. З одного боку, гаджет надає величезні можливості для спілкування, читання книг, відвідування онлайн музеїв та перегляду кіно, а з іншого - містить віртуальні загрози, які можуть мати негативні наслідки для дітей шкільного віку та їх близьких у реальному житті.

В багатьох сім`ях батьки за допомогою гаджетів відвертають увагу дітей, щоб зайнятися побутовими справами. Безперечно, це дуже зручно, але надмірне захоплення цифровими пристроями шкодить, в першу чергу, психічному здоров’ю дитини.

Найголовнішою віковою «втратою» є відсутність «живої» гри, як засобу комунікації, соціалізації та в загальному втрата навички гратися. Надмірно тривале перебування перед комп’ютерним екраном заважає дітям латентного віку вчитися гратися. На початку періоду латентності діти перебувають на стадії «гри поряд», тобто граються один біля одного, але зазвичай не разом. Це відбувається тому, що соціальні аспекти гри, зокрема співучасть і вміння домовлятися для них ще складні [2].

Гра має вирішальне значення у розвитку дитини латентного віку. Існує безліч свідчень того, що саме гра є основним способом за допомогою якого діти навчаються та соціалізуються. Якщо діти не набувають повної сукупності навичок гри, оскільки забагато часу проводять перед екраном комп'ютера, їм буде важко вчитися в школі. Діти, які багато часу проводять перед екраном, схильні часто переключатися з одного заняття на інше, і їм буває важко зосередитися на запропонованому завданні, оскільки для цього потрібні більш розвинені навички гри, ніж ті, які вони мають. Ці діти не набули вміння гратися у творчі ігри на рівні, якого досягають їхні однолітки. Багато дітей дошкільного віку, які змалечку проводять багато часу з гаджетами, схильні й досі гратися у прості, нехитрі ігри, характерні для зовсім маленьких дітей, і це має свої причини та наслідки.

Такі діти можуть подовгу збирати докупи дві речі або щось чимось наповнювати і випорожняти замість того, щоб взяти участь у грі, яка потребує застосування уяви, або у рольовій грі, що зображує реальне життя. Це може викликати сильне роздратування, тому що дитині важко долучитися до запропонованого заняття, також це означає, що вона з великою ймовірністю порушуватиме дисципліну на заняттях і їй нелегко буде завести друзів [3].

У процесі розвитку діти занурюються у навколишній світ, водночас маючи за собою сім'ю як підтримку й опору. Та дедалі частіше зустрічаються випадки, коли вся сім'я є залежна від гаджетів, чи є блогерами, вони весь час прикуті до телефонів і втрачають основні етапи та закономірності розвитку. Сталий емоційний зв'язок (прихильність), що має бути сформований у дитини з близькою дорослою людиною набуває ознак ізольованості та депривації. Діти не відчувають опори в собі та підтримки від значимих дорослих, не вміють спілкуватися та вибудовувати стабільні емоційні зв'язки, не розуміють соціальних маркерів.

Виділяють найпоширеніші наслідки надмірного захоплення школярів ґаджетами: порушення режиму сну, залежність від девайсів, депресія, стрес, зниження фізичної активності та ожиріння, психічні розлади, агресивність, цифрова деменція, віддалення дітей від реальності, шкідливе випромінювання [3].

У сучасних реаліях діти отримують доступ до інтернету значно раніше, ніж це було ще десять років тому. Дошкільники нерідко користуються смартфонами вже у 2–3 роки. Такий ранній доступ створює кілька суттєвих ризиків, що включає у себе : нездатність критично оцінювати інформацію; сприйнятливість до небажаного та агресивного контенту; формування залежності від яскравих стимулів; порушення процесів раннього розвитку, які потребують взаємодії з реальним світом, а не зі швидкими цифровими образами. Діти раннього віку не можуть самостійно регулювати час, проведений у мережі, тому раннє знайомство з інтернетом без супроводу дорослих збільшує ймовірність розвитку страхів, збудливості, порушення сну та проблем з емоційною саморегуляцією.

Дитяча психіка є надзвичайно пластичною та вразливою. Мозок ще перебуває на стадії активного розвитку, тому будь-які сильні або тривалі стимули мають більший вплив, ніж на дорослу людину. Діти не вміють фільтрувати інформацію і тому вони часто сприймають усе побачене буквально та емоційно [4].

Дитяча психіка не має сформованих механізмів психологічного захисту, тому лякаючий, агресивний або надмірно яскравий контент може викликати тривогу, нічні страхи, дратівливість. Діти не мають життєвого досвіду, через що рідко можуть відрізнити реальність від вигадки.

Таким чином, цифрове середовище може впливати на формування характеру, моделей поведінки, самооцінки та навіть світогляду. Несформована психіка «вбирає» інформацію без бар'єрів, що підвищує ризик психологічних травм.

Сучасною проблемою є активне публікування батьками фотографій своїх дітей у соціальних мережах. Це порушує приватність дитини, а також наражає на небезпеку, формує викривлену самооцінку, що тягне за собою психологічний тиск та формування залежності від схвалення. У підлітковому віці це може призвести до сором'язливості, тривожності та почуття втрати контролю над власною особистою інформацією.

Ранній доступ дитини до мережі ще з дитинства занурює їх у світ «ідеальності» та «глянцевості», вони починають оцінювати себе через штучні стандарти. Це може сформувати у дитини враження, що вона гірше за інших, якщо її життя не схоже на життя людей з мереж. До небезпек можна віднести також : заниження самооцінки, втрату інтересу до реального життя, формування нереалістичних очікувань.

Окремим пунктом необхідно винести роль соціальних мереж у провокуванні розладу харчової поведінки, депресії та тривожності. Маючи ще несформоване тіло, діти можуть порівнювати себе з «ідеальними картинками», що вони бачать на щоденній основі та відчути необхідність досягти того самого. Перебування у конкуруючому середовищі, де дитина щодня бачить нереалістично гарних, щасливих, заможніх людей може призвести до почуття меншовартості, думки «я не такий хороший» і подальшої ізоляції. Дитина може вигадати собі штучний образ у соціальних мережах і тому уникати реального життя. Це у свою чергу підвищує ризик депресії і тривожності [5].

Надмірний і ранній доступ дітей до цифрових пристроїв створює значні ризики для їхнього емоційного, когнітивного та соціального розвитку. Несформована психіка особливо вразлива до швидкого та інколи агресивного цифрового контенту, що може призводити до тривожності, депресивності та порушень поведінки. Публікація дитячих фото та раннє порівняння себе з іншими в інтернеті формують викривлену самооцінку та підвищують ризик психологічних розладів. Тому контроль цифрового середовища, участь батьків та формування здорових онлайн-звичок є критично важливими для безпечного розвитку дитини.

Список використаних джерел:

1. Haidt, J. The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness. Penguin Press. 2024. 400 с.

2. Золотова Г. Д. Сутність і зміст ігрової залежності дітей / Г. Д. Золотова // Вісник Луганського національного університету імені Тараса Шевченка. Педагогічні науки. - 2012. - № 19(2). - С. 204-212. - Режим доступу: http://nbuv.gov.ua/UJRN/vlup_2012_19(2)__27.

3. Сбітнєва І. С. Діагноз – інтернет-залежність підлітка / І. С. Сбітнєва // Педагогічний альманах. - 2015. - Вип. 27. - С. 223-227. - Режим доступу: http://nbuv.gov.ua/UJRN/pedalm_2015_27_38

4. Abdoli, Maryam; Khoshgoftar, Mohadeseh1; Jadidi, Hosin2; Daniali, Seyede Shahrbanoo3; Kelishadi, Roya3. Screen Time and Child Behavioral Disorders During COVID-19 Pandemic: A Systematic Review. International Journal of Preventive Medicine 15():9, February 2024. DOI: 10.4103/ijpvm.ijpvm_78_23

5. Colak M, Bingol OS, Dayi A. Self-esteem and social media addiction level in adolescents: The mediating role of body image. Indian J Psychiatry. 2023 May;65(5):595-600. doi: 10.4103/indianjpsychiatry.indianjpsychiatry_306_22. Epub 2023 May 15. PMID: 37397839; PMCID: PMC10309264.

Шинкаренко Ангеліна Юріївна,
студентка н.гр. 101_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

ШЛЯХИ ВИРІШЕННЯ АКТУАЛЬНИХ ПРОБЛЕМ ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВОВІЙ СФЕРІ ТА ПСИХОЛОГІЇ

Сучасний етап цифрової трансформації суттєво змінює як правову сферу, так і практику психології. Інформаційні технології (штучний інтелект (ШІ), великі дані, цифрові платформи, системи електронного урядування, онлайн-комунікація) відкривають широкі можливості для підвищення ефективності професійної діяльності, однак водночас формують низку юридичних, етичних та психологічних ризиків. У зв'язку з цим виникає потреба в комплексному аналізі проблем та у визначенні шляхів їх вирішення.

Актуальні проблеми використання ІТ у правовій сфері

1. *Нормативна невизначеність щодо штучного інтелекту.* Розвиток ШІ випереджає формування відповідної правової бази. В Україні поки відсутній спеціальний закон щодо використання штучного інтелекту, що створює складнощі у визначенні відповідальної особи за наслідки роботи алгоритмів. Окремою проблемою є відсутність правового статусу автономних систем, що використовуються у правозастосовній діяльності (системи аналізу доказів, прогнозування судових рішень, електронне правосуддя).

2. *Проблеми кібербезпеки та захисту персональних даних*. Поширення електронного судочинства, електронних реєстрів та дистанційних сервісів підвищує ризики несанкціонованого доступу до інформації. Частими залишаються кіберінциденти, пов'язані зі зламом державних інформаційних ресурсів, що створює загрозу витоку персональних даних та підробки інформації.

3. *Докази цифрової природи та їхня оцінка*. Цифрові докази (листування, метадані, логи, відео, цифрові сліди поведінки) є складними для збирання, збереження та верифікації. Проблемою є можливість швидкої модифікації або фальсифікації таких доказів, зокрема за допомогою технологій deepfake.

4. *Недостатня цифрова компетентність працівників правових інституцій*. Потреба у застосуванні електронних систем вимагає від юристів нових навичок: роботи з базами даних, розуміння принципів обробки інформації, алгоритмів та цифрових ризиків. Водночас рівень цифрової грамотності кадрів у багатьох органах залишається недостатнім.

Актуальні проблеми використання IT у психології

1. *Використання невалідних та не стандартизованих онлайн-тестів*. Значна частина психологічних онлайн-інструментів не проходить належної наукової експертизи. Це може призводити до хибних діагнозів, некоректного трактування результатів або неправомірного використання персональних даних респондентів.

2. *Ризики онлайн-психологічного консультування*. Дистанційна взаємодія ускладнює контроль за дотриманням конфіденційності, а також створює ризики несанкціонованого доступу до записів сеансів. Крім того, онлайн-формат не завжди дозволяє адекватно оцінити емоційний стан клієнта.

3. *Психологічний вплив цифрового середовища*. У молоді та дорослих спостерігається підвищення рівня тривожності, залежності від соціальних мереж, інформаційної перевантаженості. Поширення гаджетів та цифрових платформ змінює комунікативну поведінку, інколи погіршує міжособистісні взаємини та формує нові види девіантної поведінки (кібербулінг, тролінг).

4. *Алгоритмічна упередженість*. Системи профайлінгу та автоматизованого прийняття рішень у сфері освіти, підбору персоналу або соціальної допомоги можуть відтворювати соціальні стереотипи. Це має як психологічні, так і правові наслідки (може порушувати принцип рівності).

Міждисциплінарні проблеми на перетині права та психології в умовах цифровізації

1. *Кіберзлочинність і психологічні чинники*. Більшість кіберзлочинів має виражений психологічний компонент (маніпуляція, соціальна інженерія, довіра, емоційний тиск). Розуміння психології кіберзлочинця й жертви є необхідним для ефективного розслідування.

2. *Цифрові сліди поведінки як джерело для юридичного аналізу*. Поведінкові профілі, створені на основі цифрової активності користувача, можуть бути важливими для юридичних процедур, але одночасно ставлять питання про межу між приватністю та інтересами правосуддя.

3. *Інтернет-булінг та його правове регулювання*. Кібербулінг може мати тяжкі психологічні наслідки, а правова база України ще перебуває у стадії розвитку. Виникає потреба уточнення відповідальності та вдосконалення механізмів захисту неповнолітніх.

Шляхи вирішення проблем

1. *Розробка комплексного законодавства щодо ШІ та цифрових технологій*. Потрібне створення нормативної бази, яка враховуватиме:

- вимоги до прозорості алгоритмів;
- механізми аудиту систем;
- визначення відповідальності за автоматизовані рішення.

2. *Підвищення кваліфікації юристів і психологів*. Необхідне впровадження:

- курсів із кібербезпеки;
- навчання цифровій етиці;
- практики роботи з електронними доказами;
- програм перепідготовки щодо застосування ШІ.

3. *Технічні заходи захисту інформації*. Рекомендовано впроваджувати багаторівневу аутентифікацію, шифрування даних, блокчейн-технології для фіксації доказів, а також регулярний моніторинг безпеки інформаційних систем.

4. *Етичне регулювання використання цифрових технологій*. Доцільно створити міждисциплінарні комітети для оцінки ризиків роботизованих і цифрових систем, а також розробити національні стандарти надання онлайн-психологічних послуг.

Висновки. Цифрові технології стають ключовим елементом функціонування правової та психологічної сфер. Їхнє впровадження відкриває нові можливості, але потребує ретельного аналізу ризиків та вдосконалення законодавчого, етичного і організаційного забезпечення. Ефективне вирішення окреслених проблем можливе лише за умови тісної співпраці юристів, психологів, ІТ-фахівців та державних інституцій.

Список використаних джерел:

1. Про захист персональних даних : Закон України від 01 черв. 2010 р. № 2297-VI // Відомості Верховної Ради України. 2010. № 34. Ст. 481.
2. Про електронні довірчі послуги : Закон України від 05 жовт. 2017 р. № 2155-VIII // Відомості Верховної Ради України. 2017. № 45. Ст. 400.
3. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII // Відомості Верховної Ради України. 2017. № 45. Ст. 403.
4. Журавель В.А. Кіберзлочинність: кримінально-правові та кримінологічні аспекти. Харків: «Право», 2021.
5. Оніщенко Н.М. Право та інформаційні технології: сучасні виклики. Київ: НАН України, 2020.
6. Ткалич О.В. Психологія інформаційного суспільства. Дніпро: Вид-во ДНУ, 2019.
7. Чепа М.Д. Психологічна безпека особистості в цифровому середовищі. Київ: КНУ ім. Т. Шевченка, 2021.
8. Петрова Н.В. Етичні аспекти онлайн-психологічного консультування // Психологічні перспективи, 2022.
9. Жданова І.Є. Цифровізація судочинства: проблеми та перспективи розвитку в Україні. Київ: Алерта, 2023.

Шуляк Богдан Андрійович,
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

ПОТЕНЦІЙНІ РИЗИКИ ДЛЯ ФІНАНСОВОЇ ДОКУМЕНТАЦІЇ В ЦИФРОВОМУ ФОРМАТІ ОСВІТНІХ УСТАНОВ СИСТЕМИ МВС УКРАЇНИ

Сьогодні спостерігається інтенсивна цифровізація середовища освітніх установ системи МВС України, яке, спираючись на відповідну нормативно-правову базу, активно діджиталізується. Активно впроваджуються різноманітні платформи для онлайн-навчання та ведення електронного документообігу, що підвищує ефективність освітнього процесу закладів вищої освіти (далі – ЗВО) та зменшує витрати часу/ресурсів на підтримку його функціонування.

Але цифровізація освітньої системи МВС України супроводжується новими ризиками. Серед ключових загроз виділяють:

1) вразливість цифрових платформ: більшість платформ, що використовуються в ЗВО, мають низький рівень кіберзахисту (не оновлене програмне забезпечення та слабкі алгоритми шифрування);
2) використання недостатньо захищених каналів для передачі даних між структурними підрозділами ЗВО. Тому стають можливими кібератаки типу «ransomware», які блокують доступ до баз даних, вимагаючи викуп за їх відновлення. Також серед ризиків – застосування фішингових схем, які спрямовані на отримання доступу до паролів або інших конфіденційних даних [1].

Таким чином, викрадення фінансової інформації може призвести до втрати коштів або їх використання для незаконних операцій, а розголошення персональних даних викликає репутаційні та юридичні ризики.

До ризиків слід також обов’язково віднести і можливі технічні збої – у такому разі відсутність резервного копіювання електронних баз даних може призвести до повної втрати інформації.

Отже, в сучасних реаліях хакерські атаки можуть завдати значної шкоди фінансовим процесам ЗВО. Вплив таких кібератак охоплює кілька аспектів:

1) економічні наслідки: втрата доступу до баз даних може спричинити затримки у виплаті заробітних плат, що вплине на якість роботи персоналу, а також існує ризик розкрадання коштів з рахунків ЗВО або благодійних фондів;

2) збої в управлінні: відсутність доступу до фінансових звітів унеможливлює оперативне прийняття рішень щодо витрат, а порушення звітності перед органами управління освітою може призвести до санкцій або призупинення фінансування;
3) репутаційні ризики: втрата довіри з боку персоналу та здобувачів вищої освіти освітньої установи, потенційних абітурієнтів, які можуть відмовитися від вступу на навчання до ЗВО, а також негативний імідж закладу освіти в інформаційному просторі.

Питання захисту освітніх баз даних у країнах ЄС, США, Канаді стало актуальним ще в середині 1990-х років, коли почали використовуватися перші автоматизовані програмні продукти для діловодства у закладах освіти, що відповідали стандартам FERPA (Family Educational Rights and Privacy Act) [2].

У Німеччині, Великобританії, Канаді та Австралії електронні журнали в освітній системі стали обов'язковими з 2000-х років, а в Швеції – з 2005 року [3]. Поряд з їх впровадженням завжди актуальним було питання гарантій захисту даних і наразі в країнах ЄС діють чіткі вимоги для роботи з освітніми платформами відповідно до регламенту GDPR (General Data Protection Regulation), а в скандинавських країнах всі навчальні заклади користуються інтегрованими державними платформами, які забезпечують збереження усієї звітності [4].

Таким чином, захист фінансових даних закладів вищої освіти системи МВС України є основою для забезпечення стабільної роботи освітньої системи, оскільки це дозволить уникнути непередбачуваних витрат, забезпечить відшкодування збитків у разі порушення роботи систем. Автоматизація фінансових процесів із захищеними системами забезпечує більшу прозорість та зручність управління.

Слід зазначити, що для підвищення рівня захисту інформації необхідно формувати цифрову компетентність з питань кібергігієни (уникнення підозрілих посилань, створення складних паролів тощо) науково-педагогічного складу, адміністрації та бухгалтерії закладів вищої освіти системи МВС України.

Список використаних джерел:

1. Бендер Ю. В. Вплив кіберзлочинності на фінансову сферу: проблеми та можливі рішення. Економіка і фінанси. 2017. № 6. С. 112-120.

2. Власенко С. Ю. Основи кіберстрахування: теорія та практика: книга для фахівців з фінансів та ІТ. 2020.

3. Броннер Д. Захист даних у цифрових платформах: принципи та підходи до страхування. Економіка та інновації. 2020. № 3(8). С. 65-70.

4. Огляд Європейського агентства з кібербезпеки: безпека електронних платформ для закладів освіти. ENISA : [сайт]. URL: http://www.enisa.europa.eu (дата звернення: 18.10.2025).

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.

Штучний інтелект впливає на всі сфери людського життя сьогодні, і з часом цей вплив лише зростатиме, зокрема, це стосується й навчання дітей. Розглянемо переваги та недоліки використання штучного інтелекту в освітньому процесі.

До переваг використання штучного інтелекту можна віднести:

– швидкість роботи ШІ. Ви можете майже миттєво отримати необхідні пояснення, приклади, підказки. ШІ може швидко обробляти велику кількість інформації. Він допоможе знайти відповіді на запитання, які вас цікавлять, або чомусь навчить;

– точність розрахунків. ШІ використовує спеціальні алгоритми й формули, які дозволяють йому швидко та точно обчислювати різні завдання;

– можливість забезпечити доступ до навчання для людей, які мають особливі потреби або людей, що в силу певних обставин вимушені навчатися дистанційно;

– використання засобів перекладу в режимі реального часу на основі алгоритмів штучного інтелекту сприяє безперешкодному спілкуванню, незважаючи на мовні бар'єри;

– можливості застосування ШІ у творчих проєктах щодо отримання ідей для малюнків, музики або твору;

– учні та студенти можуть брати участь у інтерактивних іграх та вправах, які дають їм можливість розвивати навички та вміння, а також забезпечують позитивний досвід навчання.

– посилення безпеки, виявлення шахрайства та недоброчесності в межах участі в освітньому процесі;

– штучний інтелект може забезпечити студентам доступ до більш різноманітних та актуальних джерел інформації, що дозволить їм отримувати повну та корисну інформацію, необхідну для навчання.

Але використання ШІ в освітньому процесі має і суттєві недоліки:

– ШІ робить учнів та студентів більш лінивими, автоматизуючи значну частину роботи за допомогою своїх можливостей;

– надмірна довіра до систем штучного інтелекту призводить до залежності та втрати контролю і критичного осмислення отриманих результатів, що несе в собі потенційні пастки;

– застосування штучного інтелекту може призвести до збору та використання персональних даних студентів без їх згоди або без належної захисту цих даних;

– штучному інтелекту не завжди вдається враховувати людські емоції, контекст або інші нюанси, які можуть бути важливими для ухвалення правильного рішення. Зокрема якщо це стосується етичних питань;

– ШІ не завжди розуміє задачу, яку ви йому ставите. Це залежить від того, наскільки повно і правильно ви формулюєте запитання та описуєте проблематику. Відповідь ШІ може розчарувати або ввести в оману;

– Штучний інтелект "знає" лише те, що йому “згодували”. Тож він обмежений в ухваленні оптимальних рішень. Він має купу обмежень, встановлених його розробниками, що може призвести до генерації рішень та рекомендацій далеких від оптимальних;

– використання штучного інтелекту може призвести до залежності від смарт технологій та втрати навичок, які можуть бути корисними в реальному житті;

– штучний інтелект може призвести до зміни спілкування між вчителями та студентами, а також між студентами. Це може вплинути на соціальну взаємодію та розвиток навичок спілкування.

У підсумку, можимо зазначити, що ШІ є потужним інструментом, який може значно покращити освітній процес, але ефективність його застосування залежить від балансу між технологічними можливостями та педагогічними цінностями, а також від збереження провідної ролі людини у навчанні. В будь-якому разі, розповсюдження ШІ не можна ігнорувати. Його розвиток призведе до революції в усіх галузях. Нам лишається спостерігати, як з його розвитком буде змінюватися світ.

Список використаних джерел:

1. Про переваги та недоліки штучного інтелекту у навчальному процесі. 2 березня 2024 року. URL: https://behindthenews.ua/spetsproiekti/po-toy-bik-novin-kids/pro-perevagi-ta-nedoliki-shtuchnogo-intelektu-u-navchalnomu-protsesi-720/. (дата звернення: 15.11.2025).
2. Приймаченко І. Штучний інтелект в освіті: можливості, виклики та перші кроки великої адаптації. 4 серпня 2023 року. URL: https://life.pravda.com.ua/columns/2023/08/4/255650/ (дата звернення: 17.11.2025).
3. Покатілова В. Штучний інтелект в освіті: як технологія впливає на навчання в українських школах. 20 грудня 2023 року. URL: https://fakty.com.ua/ua/ukraine/suspilstvo/20231220-shtuchnyj-intelekt-v-osviti-yak-tehnologiya-vplyvaye-na-navchannya-v-ukrayinskyh-shkolah/ (дата звернення: 19.11.2025).
4. Вишнякова О. AI та освіта: як штучний інтелект вплине на шкільну освіту. 2 березня 2023 року. URL: https://lb.ua/blog/olena_vyshniakova/547626_ai_osvita_yak_shtuchniy_intelekt.html (дата звернення: 19.11.2025).
5. https://www.researchgate.net/publication/390234239_Perevagi_ta_problemi_vikoristanna_stucnogo_intelektu_v_osvitnomu_procesi
6. Шумілова К. Переваги та проблеми використання штучного інтелекту в освітньому процесі // Матеріали конференції: ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОСВІТУ – ВИКЛИКИ ТА МОЖЛИВОСТІ. 11 квітня 2025 року. DOI: https://doi.org/10.36059/978-966-397-477-4-246 URL: https://www.researchgate.net/publication/390234239_Perevagi_ta_problemi_vikoristanna_stucnogo_intelektu_v_osvitnomu_procesi (дата звернення: 23.11.2025).

Наукове видання

ХАХАНОВСЬКИЙ Валерій Георгійович

АКТУАЛЬНІ ПРОБЛЕМИ ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВІ ТА ПСИХОЛОГІЇ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Матеріали круглого столу

(м. Київ, 27 листопада 2025 року)

Комп’ютерна верстка: *В.Г. Хахановського*

Підписано до друку 02.03.2026. Формат 60х84/16. Папір офсетний.
Обл.-вид. арк. 2,75. Ум. друк. арк. 2,56.
Тираж 50 прим.

Редакційно-видавниче відділення
Національної академії внутрішніх справ
03035, Київ, пл. Солом’янська, 1

Друк: ФОП Поліщук О.В.
Свідоцтво суб’єкта видавничої справи ДК № 2142 від 31.03.2015
07400, м. Бровари, вул. Незалежності, 2, кв. 148
тел. (044) 592-13-49