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

СУЧАСНИЙ СТАН ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ УКРАЇНИ

Матеріали науково-практичного семінару
(м. Київ, 15 травня 2025 року)

Київ
2025

УДК 004.9:352/354](477)(06)
С916

Матеріали науково-практичного семінару за загальною редакцією:
Кудінов В.А. – кандидат фізико-математичних наук, доцент, завідувач кафедри інформаційних технологій навчально-наукового інституту права та психології Національної академії внутрішніх справ

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;
Хахановський Валерій Георгійович – професор кафедри інформаційних технологій навчально-наукового інституту права та психології Національної академії внутрішніх справ, доктор юридичних наук, професор

Матеріали схвалено та рекомендовано до друку на засіданні науково-методичної ради Національної академії внутрішніх справ (протокол № 6 від 19 червня 2025 року)

Усі матеріали надані в авторській редакції та виражають персональну позицію учасників науково-практичного семінару

С916 **Сучасний стан використання інформаційних технологій в органах державної влади України**: матеріали наук.-практ. семінару (м. Київ, НАВС, 15 травня 2025 р.); за заг. редакцією В. А. Кудінова. Київ: Нац. акад. внутр. справ, 2025. 68 с.

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на науково-практичний семінар на тему «Сучасний стан використання інформаційних технологій в органах державної влади України», який відбувся на базі навчально-наукового інституту права та психології Національної академії внутрішніх справ 15 травня 2025 року.

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

УДК 004.9:352/354](477)(06)

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 науково-практичного семінару на тему:

«СУЧАСНИЙ СТАН ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ УКРАЇНИ»

(*15 травня 2025 року*)

Київ – 2025

Дата проведення: **15 травня 2025 року**
Початок роботи: 14:00
Місце проведення: Національна академія внутрішніх справ (м. Київ, пл. Солом'янська 1, ауд. 402) 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** та модератора заходу, доцента кафедри інформаційних технологій ННІ права та психології НАВС, кандидата технічних наук, доцента **Пакриша Олександра Євгенійовича.**

ДОПОВІДІ:

1. Студентка 3 н.гр. 4-КВ курсу ІЗДН НАВС **Калінченко Вікторія Костянтинівна** «Проблеми використання інформаційних технологій в органах державної влади України та шляхи їх вирішення» (к.ф.-м.н. Кудінов В.А.).
2. Student of academic group 102_SPS, Institute of Law and Psychology, NAIA **Humenyuk Victoria Olegivna** "Use of pr-technologies in public administration" (Ph. D. Pakrysh O.Y.).
3. Студентка 205_СПД н.гр. ННІПП НАВС **Петровська Надія Анатоліївна** «Цифрова держава: впровадження та перспективи розвитку платформами «Дія» в Україні» (к.ф.-м.н. Тарасенко В.П.).
4. Студентка 205_СПД н.гр. ННІПП НАВС **Юроца Наталія Ігорівна** «Доступність державних послуг онлайн: інклюзивність та цифрова грамотність» (к.ф.-м.н. Тарасенко В.П.).
5. Студентка 204_СПД н.гр. ННІПП НАВС **Дегтяренко Анастасія Андріївна** «Використання інформаційних технологій у Міністерстві охорони здоров'я України» (к.ф.-м.н. Тарасенко В.П.).
6. Студентка 204_СПД н.гр. ННІПП НАВС **Портненко Дарія Сергіївна** «Використання інформаційних технологій в Міністерстві освіти і науки України» (к.ф.-м.н. Тарасенко В.П.).
7. Студент 2 н.гр. 3-КВ курсу ІЗДН НАВС **Маленко Андрій Олександрович «**Штучний інтелект в діяльності публічних службовців» (к.ф.-м.н. Кудінов В.А.).
8. Студентка 206_СПД н.гр. ННІПП НАВС **Ноздренко Яна Валентинівна** «Загальний огляд програм штучного інтелекту для персональних комп'ютерів (платні та безкоштовні версії)» (Грищенко О.І.).
9. Студентка 205_СПД н.гр. ННІПП НАВС **Градюк Іванна Миколаївна** «Використання ШІ для виявлення фейків і дезінформації в системах державної інформаційної безпеки» (к.ф.-м.н. Тарасенко В.П.).
10. Student of academic group 102_SPS, Institute of Law and Psychology, NAIA **Slepko Angelina Ivanivna** «Manipulation of Public Consciousness During War Using Artificial Intelligence» (Ph. D. Pakrysh O.Y.).
11. Студентка 102_СПС н.гр. ННІПП НАВС **Федорова Людмила Федорівна** «Fake-засоби психології масової дезинформації» (к.т.н. Пакриш О.Є.).
12. Студентка 205_СПД н.гр. ННІПП НАВС **Доброгорська Валерія Сергіївна** «Використання чат-ботів для швидкої обробки запитів громадян» (к.ф.-м.н. Тарасенко В.П.).
13. Студентка 204_СПД н.гр. ННІПП НАВС **Герасимова Катерина Олександрівна** «Роль інформаційних технологій у забезпеченні відкритості та прозорості діяльності Національної поліції» (к.ф.-м.н. Тарасенко В.П.).

14. Студентка 205_СПД н.гр. ННІПП НАВС **Чалбишева Віталіна Русланівна** «Роль інформаційних систем у протидії корупції в державному секторі України» (к.ф.-м.н. Тарасенко В.П.).
15. Студентка 205_СПД н.гр. ННІПП НАВС **Калашникова Карина Ігорівна** «Електронний документообіг як основа цифрової трансформації державного управління» (к.ф.-м.н. Тарасенко В.П.).
16. Студентка 205_СПД н.гр. ННІПП НАВС **Кононіченко Ірина Олександрівна** «Кібербезпека державних інформаційних систем» (к.ф.-м.н. Тарасенко В.П.).
17. Студентка 103_СПД н. гр. ННІПП НАВС **КіцакСофія Андріївна** «Правові та організаційні аспекти забезпечення інформаційної безпеки органів та підрозділів Національної поліції» (к.ф.-м.н. Кудінов В.А.).
18. Студентка 202_СПД н.гр. ННІПП НАВС **Нікітенко Марія Богданівна** «Розумні презентації: огляд нейромережевих програм для створення презентацій» (Грищенко О.І.).

https://www.navs.edu.ua/news/informacijni-tehnologiyi-v-diyi-molod-navs-obgovorila-cifrove-majbutnye-derzhavi.html

ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО КАФЕДРУ

Історія становлення кафедри містить цікавий та насичений різними подіями шлях, який пов'язаний з історією становлення провідного вищого навчального закладу системи Міністерства внутрішніх справ України (далі – МВС) – Національної академії внутрішніх справ (далі – НАВС).

ДАТА	***НАЗВА КАФЕДРИ***	
25.06.1988	кафедра технічних засобів попередження та розкриття злочинів	Київської вищої школи МВС СРСР ім. Ф.Е. Дзержинського
01.05.1990	кафедра інформаційно-обчислювальної техніки	
01.09.1991	кафедра технічних засобів попередження та розкриття злочинів	
27.01.1992	кафедра технічних засобів попередження та розкриття злочинів	Української академії внутрішніх справ
10.01.1996	кафедра оперативної техніки	
20.12.1996	кафедра оперативної техніки	Національної академії внутрішніх справ України
30.08.1999	кафедра інформаційних технологій	Інституту підготовки управлінських кадрів НАВС України
21.07.2000		Інституту управління НАВС України
15.01.2003		НАВС України
08.09.2005		Київського національного університету внутрішніх справ
27.08.2010		НАВС
19.07.2013		навчально-наукового інституту підготовки фахівців для підрозділів слідства та кримінальної міліції НАВС
07.11.2015		навчально-наукового інституту № 1 НАВС
01.09.2017	кафедра інформаційних технологій та кібернетичної безпеки	навчально-наукового інституту № 1 НАВС
17.10.2018	кафедра інформаційних технологій та кібербезпеки	
01.09.2024	кафедра інформаційних технологій	навчально-наукового інституту права та психології НАВС

ЗМІСТ

Калінченко Вікторія Костянтинівна
Студентка 3 н.гр. 4-КВ курсу ІЗДН НАВС

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

ПРОБЛЕМИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ УКРАЇНИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

У сучасних умовах інформаційні технології (далі – ІТ) відіграють ключову роль у трансформації державного управління, забезпечуючи підвищення ефективності, прозорості та доступності адміністративних послуг. В Україні, починаючи з 2019 року, цифрова трансформація стала одним із пріоритетів державної політики, що реалізується через ініціативи Міністерства цифрової трансформації [2]. Цей процес, відомий як концепція «Держава у смартфоні», спрямований на цифровізацію державних послуг, впровадження електронного урядування та модернізацію інформаційної інфраструктури. Також, з метою систематизації підходів до цифрового розвитку інноваційної діяльності та забезпечення стратегічного планування у цій сфері, у 2024 році Кабінетом Міністрів України було схвалено Стратегію цифрового розвитку інноваційної діяльності України на період до 2030 року та затверджено операційній план заходів з її реалізації у 2025–2027 роках [4]. Цей документ визначає основні напрями та цілі цифрового розвитку, передбачає комплекс заходів щодо впровадження цифрових технологій в інноваційний сектор, а також сприяє інтеграції України у світовий цифровий простір.

Метою даного дослідження є оцінка сучасного стану використання ІТ в органах державної влади України, визначення ключових досягнень, проблем та перспектив розвитку з урахуванням наукового підходу.

1. Цифрова трансформація та електронне урядування.

Одним із основних напрямів цифровізації в Україні є розвиток електронного урядування, яке включає автоматизацію документообігу, інтеграцію державних реєстрів та надання електронних адміністративних послуг. Портал «Дія», впроваджений у 2020 році, став центральним інструментом для реалізації цих завдань.

Станом на сьогодні через «Дію» доступно понад 100 електронних послуг, зокрема оформлення паспортів, реєстрація бізнесу та отримання соціальних виплат [2]. Це сприяє спрощенню взаємодії громадян із державою та зменшенню бюрократичних процедур.

Проте інтеграція інформаційних систем між різними органами влади залишається викликом. Лише близько 60% державних реєстрів підключено до єдиної системи електронної взаємодії, що ускладнює обмін даними та знижує ефективність надання послуг [5]. Відсутність єдиних стандартів для розробки та впровадження ІТ-систем є однією з причин цієї проблеми. Для її вирішення необхідна розробка уніфікованих протоколів та стандартів, які б забезпечували сумісність систем.

2. Застосування сучасних інформаційних технологій.

Органи державної влади України активно впроваджують сучасні ІТ-рішення, такі як хмарні технології, аналітика великих даних (big data) та елементи штучного інтелекту (ШІ). Наприклад, Державна податкова служба України використовує аналітичні системи для виявлення податкових правопорушень, що підвищує ефективність фіскального контролю [7]. Хмарні технології застосовуються для зберігання даних та забезпечення віддаленого доступу до інформаційних ресурсів, що особливо актуально в умовах децентралізації.

Водночас широке використання ШІ обмежене через брак кваліфікованих кадрів у державному секторі та недостатнє фінансування. Розробка та впровадження складних ІТ-систем потребують значних інвестицій, які наразі не завжди доступні, особливо на місцевому рівні [7]. Це створює нерівномірність у цифровізації між центральними та регіональними органами влади.

3. Інформаційна безпека.

Забезпечення кібербезпеки є критично важливим аспектом використання ІТ в органах державної влади, особливо в умовах гібридних загроз. Кібератаки 2022-2023 років на державні інформаційні ресурси України виявили вразливості у захисті даних [1]. У відповідь Україна посилила заходи з кібербезпеки, зокрема через співпрацю з міжнародними партнерами, такими як Європейська консультативна місія (EUAM) та НАТО. Було впроваджено нові стандарти шифрування та системи моніторингу кіберзагроз.

Проте залишаються проблеми з недосконалістю законодавчої бази та відсутністю національного програмного забезпечення для захисту інформації [3]. Залежність від іноземних антивірусних рішень підвищує ризики вразливості. Для вирішення цих питань необхідно розробити власні програмні продукти та гармонізувати національне законодавство з міжнародними стандартами в галузі ІТ, такими як ISO/IEC 27001.

4. Проблеми та бар'єри.

Незважаючи на досягнення, використання ІТ в органах державної влади України стикається з низкою бар'єрів.

По-перше, низький рівень цифрової грамотності державних службовців ускладнює впровадження нових технологій. Більшість працівників потребують додаткового навчання для ефективного використання ІТ-систем [6]. *По-друге*, брак фінансування обмежує модернізацію інформаційної інфраструктури, особливо в регіонах [7]. *По-третє*, відсутність уніфікованих стандартів для ІТ-систем створює труднощі в їх інтеграції та масштабуванні.

Ці проблеми посилюються нерівномірним доступом до високошвидкісного Інтернету в сільських регіонах, що ускладнює цифровізацію на місцевому рівні [7]. Таким чином, подолання цифрової нерівності є одним із ключових завдань для забезпечення рівномірного розвитку ІТ в органах влади.

5. Перспективи розвитку.

Для подальшого вдосконалення використання ІТ в органах державної влади України необхідно зосередитися на кількох напрямах.

По-перше, розширення програм навчання цифрової грамотності для державних службовців сприятиме ефективнішому використанню технологій [6]. *По-друге*, залучення приватного сектору до розробки ІТ-рішень може компенсувати брак кадрів та ресурсів у державному секторі. *По-третє*, впровадження технологій «мобільного уряду» дозволить спростити доступ громадян до державних послуг, особливо в умовах зростання популярності мобільних пристроїв [2].

Крім того, гармонізація стандартів інформаційної безпеки з міжнародними нормами та розвиток національних програмних продуктів посилять захист державних інформаційних ресурсів [3]. Інвестиції в модернізацію інфраструктури, зокрема в регіонах, сприятимуть подоланню цифрової нерівності та забезпечать рівний доступ до електронних послуг.

Висновки. Отже, використання інформаційних технологій в органах державної влади України демонструє значний прогрес, зокрема в розвитку електронного урядування та наданні адміністративних послуг. Портал «Дія», інтеграція реєстрів та застосування сучасних технологій, таких як big data та ШІ, свідчать про амбітний підхід до цифрової трансформації. Водночас проблеми, пов'язані з фінансуванням, кібербезпекою, цифровою грамотністю та стандартизацією, залишаються значними бар'єрами. Подолання цих викликів через системний підхід, залучення міжнародного досвіду та співпрацю з приватним сектором сприятиме підвищенню ефективності державного управління, прозорості та довіри громадян до державних інституцій. Таким чином, цифрова трансформація залишається стратегічним напрямом для розвитку сучасної української держави.

Список використаних джерел:

1. Звіт про кібербезпеку в державному секторі України. URL: https://www.euam-ukraine.eu (дата звернення 30.04.2025).
2. Звіт про цифрову трансформацію України 2023–2024. *Міністерство цифрової трансформації України*. URL: https://thedigital.gov.ua/news/rezultati-tsifrovoi-transformatsii-v-regionakh-ukraini-za-2024-rik (дата звернення 28.04.2025).
3. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05 липня 1994 року № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення 28.04.2025).
4. Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025-2027 роках : Розпорядження Кабінету Міністрів України від 31 грудня 2024 року № 1351-р. URL: https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text (дата звернення 30.04.2025).
5. Кравченко О. В. Електронне урядування в Україні: сучасний стан та перспективи розвитку. *Державне управління: удосконалення та розвиток*. 2024. № 1(6). С. 45–52.
6. Сидоренко Т. М. Цифрова грамотність державних службовців: виклики та шляхи вирішення. *Науковий вісник Ужгородського університету*. 2024. № 1. С. 78–85.
7. Стан цифровізації регіонів України: статистичний огляд. *Державна служба статистики України.* URL: https://www.ukrstat.gov.ua/ (дата звернення 28.04.2025).

Humenyuk Victoria Olegivna
Student of academic group 102_SPS,
Institute of Law and Psychology, NAIA

Scientific supervisor:
Pakrysh Oleksandr Yevheniiovych
Candidate of Technical Sciences,
Associate Professor, Associate Professor of the Department of Information Technologies, Institute of Law and Psychology, NAIA

USE OF PR-TECHNOLOGIES IN PUBLIC ADMINISTRATION

In the modern era, public administration increasingly relies on Public Relations (PR) technologies to effectively communicate with citizens, manage information dissemination, and build trust. Ukraine's experience, especially amid ongoing challenges, illustrates the critical role of PR in governance. PR in public administration serves as a bridge between the government and the public. By employing strategic communication, governments can convey policies, respond to public concerns, and foster a transparent environment. In Ukraine, the integration of PR strategies has been pivotal in enhancing transparency, fostering public trust, and countering misinformation, especially amidst ongoing geopolitical challenges.

The advent of digital technologies has revolutionized PR practices within public administration. Tools such as social media platforms, official websites, and digital newsletters enable real-time communication and broader outreach. In Ukraine, the implementation of digital PR strategies has allowed for immediate dissemination of information, crucial during times of crisis or rapid policy changes. Ukraine has established dedicated centers to oversee strategic communication and information security. These centers are tasked with monitoring information flows, combating disinformation, and coordinating communication efforts across various government departments. Their role is vital in maintaining a coherent and unified governmental message. Effective PR strategies are crucial during crises. In Ukraine, PR technologies have been employed to manage public communication during emergencies, ensuring that accurate information is relayed promptly. This approach helps in mitigating panic, directing public behavior, and maintaining order. Through strategic PR campaigns, Ukraine has engaged with international audiences to build a positive national image. By highlighting democratic values and resilience, these efforts aim to garner international support and foster diplomatic relations. The integration of PR technologies into public administration is indispensable for modern governance.

In Ukraine, these tools have enhanced governmental transparency, improved citizen engagement, and strengthened the nation's position on the global stage. As challenges evolve, the continuous development and adaptation of PR strategies will remain a cornerstone of effective public administration.

Therefore, Ukraine's integration of Public Relations (PR) technologies into public administration exemplifies the transformative power of strategic communication in modern governance. By leveraging digital platforms, establishing dedicated communication centers, and engaging in innovative outreach, Ukraine has enhanced transparency, countered misinformation, and fostered public trust. These efforts not only strengthen internal governance but also bolster Ukraine's international standing. As global challenges evolve, the continuous adaptation and advancement of PR strategies will remain essential for effective and resilient public administration.

References:

1. "Strategic Communication: How is Ukraine Managing Its PR Campaign?" Future Center. URL: https://futureuae.com/0.rar/Mainpage/Item/9602/strategic-communication-how-is-ukraine-managing-its-pr-campaign
2. "Transparency for Victory: How Openness Can Improve Ukraine's Public Relations." War on the Rocks. URL: https://warontherocks.com/2024/01/ transparency-for-victory-how-openness-can-improve-ukraines-public-relations/
3. "How Public Relations Can Globally Influence Support for Ukraine." The Hoyt Organization. URL: https://www.hoytorg.com/how-public-relations-can-globally-influence-support-for-ukraine/
4. "Ukraine's Hard-Won Approach to Strategic Communications and Counter-Disinformation." Tech Policy Press. URL: https://www.techpolicy.press/ ukraines-hardwon-approach-to-strategic-communications-and-counterdisinformation-lessons-for-europe-and-beyond/
5. "Centre for Strategic Communication and Information Security." Wikipedia. URL: https://en.wikipedia.org/wiki/Centre_for_Strategic_Communication_and_Information_Security
6. "Public Relations (PR) in Public Governance and Administrative Management in Ukraine." ResearchGate. URL: https://www.researchgate.net/publication/371352767_Public_Relations_PR_in_Public_Governance_and_Administrative_Management_in_Ukraine
7. "Support to Strategic Communication and Awareness Raising on Ukraine's Public Administration Reform." EEAS. URL: https://www.eeas.europa.eu/node/28292_en

Петровська Надія Анатоліївна
Студентка н.гр. 205_СПД ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

ЦИФРОВА ДЕРЖАВА: ВПРОВАДЖЕННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ПЛАТФОРМАМИ «ДІЯ» В УКРАЇНІ

В умовах сучасного інформаційного суспільства цифровізація стає одним із ключових напрямків розвитку державних інститутів. Інформаційні технології допомагають зробити державне управління прозорим, ефективним та доступним для громадян. В Україні основним інструментом для реалізації ідеї цифрової держави є платформа «Дія», що дозволяє надавати громадянам широкий спектр послуг без необхідності фізично відвідувати державні установи. Цей проєкт є важливою частиною загальної стратегії цифровізації в Україні та сприяє підвищенню рівня державних послуг.

Історія та розвиток цифрової держави в Україні

Процес цифровізації в Україні розпочався після 2014 року, коли стало зрозуміло, що традиційні механізми управління не відповідають вимогам часу. У 2019 році був започаткований проєкт «Цифрова держава», спрямований на інтеграцію новітніх інформаційних технологій у всі аспекти державного управління. Одним з найбільших досягнень цієї стратегії стало створення платформи «Дія», що стала основним інструментом у забезпеченні доступу громадян до електронних послуг. Згідно з даними Міністерства цифрової трансформації України, на 2025 рік планується значне розширення функціоналу платформи, що включатиме інтеграцію з міжнародними сервісами, а також додаткові інструменти для поліпшення державного управління.

Платформа «Дія» – основа цифрової держави

Платформа «Дія», запущена у 2020 році, є мобільним додатком і веб-сервісом, який дозволяє українцям отримувати державні послуги без необхідності відвідувати відповідні установи. Вона включає великий набір послуг, таких як реєстрація транспортних засобів, оформлення медичних довідок, подача заяв на соціальні виплати та отримання електронних версій важливих документів. Серед таких документів – паспорт громадянина, водійське посвідчення та технічний паспорт на транспортний засіб.

Це спрощує процеси, значно зменшуючи час, необхідний для отримання тих чи інших послуг. Платформа не лише значно скорочує час на отримання послуг, але й підвищує рівень довіри громадян до державних органів завдяки зручності та прозорості процесів.

Впровадження платформи «Дія» в Україні

Впровадження платформи «Дія» стало важливим кроком для покращення якості обслуговування громадян. Система дозволяє об'єднати всі необхідні дані в одному місці, що знижує потребу у фізичному спілкуванні з бюрократичними інстанціями. Згідно з даними Міністерства цифрової трансформації, в 2020 році було зареєстровано більше 8 мільйонів користувачів платформи, а кількість доступних послуг постійно зростає. Відповідно до Закону України «Про електронні довірчі послуги», що був прийнятий у 2017 році, платформа «Дія» відповідає вимогам для використання електронних підписів та довірчих послуг, що забезпечує правову значущість електронних документів. Перспективи розвитку цифрової держави та платформи «Дія».

Незважаючи на значні досягнення, впровадження цифрової держави в Україні потребує подальших удосконалень. Одним із основних напрямків є розширення функціоналу платформи «Дія». У майбутньому передбачається додавання нових сервісів, таких як електронні суди та взаємодія з міжнародними базами даних. Крім того, платформа має потенціал для інтеграції з іншими країнами Європейського Союзу, що дозволить українцям користуватися державними послугами за кордоном.

Ще одним важливим аспектом є захист персональних даних. Згідно з нормами європейського законодавства, таких як Загальний регламент захисту даних (GDPR), Україна повинна забезпечити високий рівень безпеки і захисту інформації, що є одним із завдань для Міністерства цифрової трансформації.

Проєкт «Дія» є важливим етапом на шляху створення цифрової держави в Україні. Він сприяє підвищенню якості державних послуг, забезпечує зручний доступ до інформації та допомагає знизити бюрократичні перепони. Проте для досягнення повного потенціалу цифрової трансформації необхідно продовжувати роботу над удосконаленням платформи, розширенням спектра послуг та забезпеченням високого рівня захисту даних.

Список використаних джерел:

1. Міністерство цифрової трансформації України. Офіційний сайт. https://thedigital.gov.ua/.

2. Закон України «Про електронні довірчі послуги». Верховна Рада України, 2017. [https://zakon.rada.gov.ua/laws/show/2155-19].

Юроца Наталія Ігорівна
Студентка н.гр. 205_СПД ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

ДОСТУПНІСТЬ ДЕРЖАВНИХ ПОСЛУГ ОНЛАЙН: ІНКЛЮЗИВНІСТЬ ТА ЦИФРОВА ГРАМОТНІСТЬ

У сучасному світі цифровізація стає ключовим фактором розвитку суспільства та держави. Онлайн-доступність державних послуг є важливим кроком на шляху до підвищення ефективності державного управління, зменшення бюрократії та поліпшення взаємодії між громадянами та владою. Однак, поряд із перевагами, існують і виклики, пов'язані з забезпеченням інклюзивності та належного рівня цифрової грамотності серед населення. Ця доповідь має на меті проаналізувати актуальний стан доступності державних послуг онлайн в Україні у період 2024-2025 рр., розглянути ключові аспекти інклюзивності та цифрової грамотності, а також окреслити основні тенденції та перспективи розвитку.

1. Актуальний стан розвитку державних онлайн-послуг в Україні (2024-2025 рр.)

Упродовж останніх років Україна демонструє значний прогрес у сфері цифровізації державних послуг. Платформа "Дія" стала одним із ключових інструментів, що забезпечує доступ громадян до широкого спектра послуг онлайн, включаючи отримання документів, реєстрацію, оплату та інше. Розширюється перелік доступних послуг, удосконалюється інтерфейс та функціональність.

- Зростання кількості користувачів та послуг: Спостерігається тенденція до збільшення кількості громадян, які активно користуються онлайн-сервісами, а також розширення переліку послуг, що стають доступними в цифровому форматі.
- Розвиток мобільних застосунків: Мобільні застосунки державних установ стають важливим каналом доступу до послуг, забезпечуючи зручність та оперативність взаємодії.
- Інтеграція даних та міжвідомча співпраця: активно впроваджуються системи обміну даними між державними органами, що спрощує процедури отримання послуг, зменшує необхідність подання одних і тих самих документів кілька разів.
- Забезпечення кібербезпеки: Питання кібербезпеки та захисту персональних даних залишаються пріоритетними у процесі розвитку онлайн-послуг.

2. Інклюзивність доступу до державних онлайн-послуг

Інклюзивність передбачає забезпечення рівного доступу до державних онлайн-послуг для всіх категорій громадян, незалежно від їхнього соціального статусу, віку, місця проживання, рівня доходу чи фізичних можливостей.

- Проблеми цифрового розриву: Існує значний цифровий розрив між міським та сільським населенням, між різними віковими групами та людьми з інвалідністю, що ускладнює їхній доступ до онлайн-послуг.

- Забезпечення альтернативних каналів доступу: Важливо зберігати та розвивати альтернативні канали отримання державних послуг (офлайн-центри, телефонні гарячі лінії) для тих, хто не має можливості або навичок користування онлайн-сервісами.

- Адаптація інтерфейсів: Веб-сайти та мобільні застосунки державних установ повинні бути розроблені з урахуванням потреб людей з інвалідністю (наприклад, забезпечення можливості використання екранних читачів, збільшення шрифтів, контрастність).

- Підтримка маломобільних груп населення: Необхідно забезпечити фізичну доступність до центрів надання адміністративних послуг, де громадяни можуть отримати допомогу у користуванні онлайн-сервісами.

3. Цифрова грамотність як ключовий фактор доступу до онлайн-послуг

Рівень цифрової грамотності населення є визначальним фактором успішного впровадження та використання державних онлайн-послуг.

- Потреба у підвищенні цифрової грамотності: Значна частина населення України має недостатній рівень цифрових навичок, що перешкоджає повноцінному використанню онлайн-сервісів.

- Ініціативи з підвищення цифрової грамотності: Державні та громадські організації реалізують різноманітні програми та ініціативи, спрямовані на навчання населення базовим цифровим навичкам.

- Роль освіти: Інтеграція елементів цифрової грамотності в систему освіти є важливим кроком для формування цифрової компетентності у майбутніх поколінь.

- Інформаційна підтримка та навчання: Необхідно забезпечити доступність інформаційних матеріалів та навчальних ресурсів, які б допомагали громадянам опановувати користування онлайн-послугами.

4. Основні тенденції та перспективи розвитку

- Подальша цифровізація та розширення спектру послуг: Очікується подальше зростання кількості та різноманітності державних послуг, що будуть доступні онлайн.

- Персоналізація послуг: Розвиток технологій дозволить надавати більш персоналізовані та проактивні державні послуги, враховуючи індивідуальні потреби громадян.

- Використання штучного інтелекту: Впровадження технологій штучного інтелекту може покращити якість обслуговування, автоматизувати рутинні процеси та надавати більш ефективну підтримку користувачам.

- Посилення уваги до кібербезпеки та захисту даних: Питання кібербезпеки та захисту персональних даних залишатимуться ключовими у процесі розвитку онлайн-послуг.

- Поглиблення співпраці з громадським сектором: Залучення громадських організацій до процесу розробки та впровадження онлайн-послуг сприятиме їхній більшій інклюзивності та відповідності потребам громадян.

Висновки

Доступність державних послуг онлайн є важливим кроком на шляху до побудови ефективної та орієнтованої на громадян державності.

Успішна цифровізація державних послуг вимагає комплексного підходу, який враховує потреби всіх категорій громадян, забезпечує безпеку даних та сприяє розвитку цифрової культури в суспільстві.

Давайте ще порівняємо ситуацію з доступністю державних онлайн-послуг та цифровою грамотністю в Україні до війни (до 24 лютого 2022 року) та на даний час (2024-2025 роки) дуже коротко:

До війни:

- Розвиток: Цифровізація державних послуг активно розвивалася, платформа "Дія" вже функціонувала та набирала популярності.

- Інклюзивність: Проблеми цифрового розриву існували, але меншою мірою відчувалися в контексті безпеки та першочергових потреб.

- Цифрова грамотність: Рівень цифрової грамотності потребував підвищення, але не був таким критичним фактором доступу до життєво важливих послуг в умовах війни.

Основний фокус: Зручність та оптимізація адміністративних процесів.

На даний час (2024-2025 роки):

- Прискорення: Війна значно прискорила цифровізацію, зробивши онлайн-послуги критично важливими для безпеки, отримання допомоги, документів та інформації.

- Інклюзивність: Цифровий розрив став гострішим через міграцію, руйнування інфраструктури та нерівномірний доступ до технологій. Забезпечення доступу для всіх, особливо вразливих категорій, стало нагальною потребою.

- Цифрова грамотність: Недостатній рівень цифрової грамотності став серйозною перешкодою для багатьох у отриманні життєво необхідних послуг та інформації онлайн.

- Основний фокус: Забезпечення безперебійного доступу до критично важливих послуг в умовах війни, інформаційна безпека та боротьба з дезінформацією.

Коротко кажучи, війна каталізувала цифровізацію, але також виявила та загострила проблеми інклюзивності та цифрової грамотності, зробивши їх вирішення першочерговим завданням.

Список використаних джерел:

1. Про основні засади кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII.
2. Концепція розвитку електронного урядування в Україні. Розпорядження Кабінету Міністрів України від 13 січня 2016 р. № 10/2016р.
3. Національна стратегія розвитку інформаційного суспільства в Україні на 2013-2020 роки. Указ Президента України від 17 травня 2013 року № 287/2013.
4. Веб-сайт платформи "Дія" (https://diia.gov.ua/).

Дегтяренко Анастасія Андріївна
Студентка н.гр. 204_СПД ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В МІНІСТЕРСТВІ ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ

У XXI столітті інформаційні технології стали невід'ємною частиною функціонування майже всіх галузей суспільного життя, зокрема системи охорони здоров'я. Застосування ІТ дозволяє підвищити ефективність управління ресурсами, забезпечити швидкий доступ до медичних даних, покращити взаємодію між медичними працівниками та пацієнтами, а також забезпечити прозорість у діяльності органів охорони здоров'я. В Україні цей процес має особливу актуальність у контексті загальної трансформації медичної сфери, зокрема завдяки роботі Міністерства охорони здоров'я України (МОЗ) та впровадженню електронної системи охорони здоров'я (ЕСОЗ). Однією з найважливіших реформ, пов'язаних з цифровізацією охорони здоров'я, є створення та впровадження електронної системи охорони здоров'я (ЕСОЗ), яка є основою цифрової трансформації в цій сфері. ЕСОЗ забезпечує централізований облік медичних послуг, електронний документообіг, а також збереження персональних медичних записів пацієнтів у безпечному цифровому середовищі. Ця система дозволяє лікарям реєструвати пацієнтів, створювати електронні медичні записи, призначати лікування, виписувати електронні рецепти, а також направляти пацієнтів на діагностику чи до інших спеціалістів. Ключовим компонентом цієї системи є платформа eHealth — спільний проєкт Міністерства охорони здоров'я України, Національної служби здоров'я України (НСЗУ) та міжнародних донорських організацій. Платформа виконує функцію обміну даними між лікарями, закладами охорони здоров'я, аптеками та НСЗУ. Пацієнти можуть скористатися перевагами електронного обліку, наприклад — перевірити інформацію про надані медичні послуги, отримати електронний рецепт або COVID-сертифікат.

Особливу роль у цифровізації охорони здоров'я відіграє НСЗУ. Вона забезпечує укладення електронних договорів із закладами охорони здоров'я, контролює якість та обсяг наданих послуг, адмініструє виплати за Програмою медичних гарантій. За допомогою аналітичних інструментів, які базуються на IT-рішеннях, НСЗУ має змогу оперативно аналізувати ефективність системи, виявляти зловживання та покращувати розподіл фінансування. Одним із найуспішніших прикладів цифровізації стало впровадження електронного рецепта, який забезпечив автоматизацію призначення, обліку та відпуску лікарських засобів. Це стало основою для реалізації програми «Доступні ліки», в межах якої пацієнти з хронічними захворюваннями можуть отримати необхідні препарати безкоштовно або зі знижкою. Електронна форма рецепта мінімізує можливість зловживань, а також дозволяє МОЗ та НСЗУ здійснювати контроль за розподілом медикаментів у масштабах усієї країни. У період пандемії COVID-19 IT-рішення стали критично важливими для забезпечення оперативної реакції держави. МОЗ реалізувало цифрові інструменти для моніторингу кількості захворювань, ведення реєстрів вакцинованих, формування цифрових COVID-сертифікатів, які згодом стали частиною міжнародної системи сертифікації ЄС. Була створена також система онлайн-запису на вакцинацію через платформу «Дія», що значно спростило доступ населення до медичних послуг у кризовий період. Ще одним важливим напрямом є розвиток телемедицини — сучасного підходу до надання медичних послуг на відстані. Це особливо актуально для сільських регіонів та віддалених населених пунктів, де обмежений доступ до вузькопрофільних спеціалістів. МОЗ заохочує розвиток телемедичних платформ, які дозволяють проводити дистанційні консультації, обмінюватися результатами обстежень та контролювати стан здоров'я пацієнтів за допомогою мобільних додатків чи спеціального обладнання.

Також МОЗ активно працює над впровадженням реєстрів медичних даних, серед яких: реєстр медичних працівників, реєстр пацієнтів, реєстр вакцин та щеплень, реєстр медичних закладів тощо. Наявність цих реєстрів дає змогу забезпечити ефективне управління системою охорони здоров'я, планування державних програм, а також формування стратегій профілактики і лікування хвороб на підставі статистично достовірних даних. Значну увагу приділено відкритим даним, які МОЗ публікує на порталі data.gov.ua. До таких даних належать інформація про ліцензовані заклади охорони здоров'я, статистика захворювань, фінансові показники, державні закупівлі тощо. Це сприяє прозорості, боротьбі з корупцією, покращенню контролю громадськості та підвищенню довіри населення до органів влади. Однак процес цифровізації супроводжується й низкою викликів.

Одним із основних є проблема цифрової грамотності як серед медичного персоналу, так і серед пацієнтів, особливо у старшому віці. Частина лікарів не має достатньої кваліфікації для роботи з електронними системами, а пацієнти іноді не розуміють, як скористатися тими чи іншими цифровими послугами. Крім того, інфраструктура деяких лікарень, особливо в сільській місцевості, застаріла та потребує оновлення — починаючи від комп'ютерної техніки до стабільного інтернет-зв'язку. Не менш важливою є проблема захисту персональних даних. МОЗ, відповідно до законодавства України та європейських стандартів, зобов'язане забезпечити конфіденційність та безпеку інформації, що зберігається в цифрових системах. Для цього впроваджуються засоби шифрування, системи авторизації, цифрові підписи та постійний моніторинг ІТ-систем на предмет уразливостей.

Отже, використання інформаційних технологій у системі охорони здоров'я України є необхідною умовою для її ефективного функціонування та подальшого розвитку. МОЗ України послідовно реалізує політику цифровізації, що охоплює широкий спектр заходів — від створення електронних реєстрів до запуску телемедичних сервісів та впровадження електронного документообігу. Ці зусилля спрямовані на підвищення якості медичних послуг, зручності для пацієнтів та ефективності управління ресурсами галузі. У майбутньому, за належної підтримки з боку держави та міжнародних партнерів, цифрові технології можуть стати основою нової, сучасної та пацієнт-орієнтованої системи охорони здоров'я в Україні.

Список використаних джерел:

1. Міністерство охорони здоров'я України. Офіційний сайт – https://moz.gov.ua.
2. Національна служба здоров'я України. Офіційний сайт – https://nszu.gov.ua.
3. Платформа eHealth — https://ehealth.gov.ua
4. Закон України «Про основи законодавства України про охорону здоров'я»
5. Закон України «Про захист персональних даних» №2297-VI від 01.06.2010.
6. Постанова КМУ №411 від 25 квітня 2018 року «Про реалізацію пілотного проекту щодо впровадження електронного рецепта».

Портненко Дарія Сергіївна
Студентка н.гр. 204 СПД ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук,
доцент кафедри інформаційних технологій ННІ права та психології НАВС

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У МІНІСТЕРСТВІ ОСВІТИ І НАУКИ УКРАЇНИ

У час стрімкого розвитку цифрових рішень та трансформації суспільства, впровадження ІТ у сферу освіти стало не лише бажаним, а й необхідним кроком.

1. Цифровізація освітнього процесу

МОН активно впроваджує цифрові технології в навчальний процес, зокрема:

Електронні щоденники та журнали, які полегшують взаємодію між вчителями, учнями та батьками.

Платформи дистанційного навчання, як-от «Всеукраїнська школа онлайн», яка стала важливим інструментом під час пандемії COVID-19 та продовжує функціонувати в умовах воєнного стану.

Розробка цифрових підручників, що забезпечують рівний доступ до якісного контенту для школярів у будь-якому регіоні України.

2. Єдина освітня екосистема

МОН працює над створенням єдиної цифрової платформи, яка об’єднає:

Базу даних про учнів, студентів, педагогів.

Електронні кабінети вступників (через систему ЄДЕБО – Єдина державна електронна база з питань освіти).

Інструменти для аналітики та моніторингу якості освіти на національному рівні.

Це дозволяє забезпечити прозорість, зменшити бюрократію та посилити управлінські рішення.

3. Автоматизація адміністративних процесів

Міністерство активно використовує ІТ для автоматизації:

Вступних кампаній (через електронні заяви).

Атестації педагогічних працівників.

Звітування закладів освіти.

Реєстрації на ЗНО/НМТ.

Такі інструменти зменшують корупційні ризики, економлять час і покращують обслуговування громадян.

4. Кібербезпека та захист даних

У зв'язку з активною цифровізацією, важливим напрямом роботи є захист персональних даних та забезпечення кібербезпеки в освітніх установах. У співпраці з профільними органами впроваджуються протоколи захисту та резервного зберігання інформації.

5. Співпраця з міжнародними партнерами

МОН співпрацює з такими організаціями, як ЮНЕСКО, ЮНІСЕФ, ЄС які надають як технічну підтримку, так і освітні ресурси, допомагаючи розвивати цифрові навички учнів та вчителів.

6. Виклики та перспективи

Серед головних викликів: 1. Нерівний доступ до інтернету та техніки в окремих регіонах. 2. Недостатня цифрова компетентність деяких педагогів. 3. Потреба в оновленні законодавчої бази для повноцінної цифрової трансформації. Однак уже сьогодні видно позитивні результати: підвищення якості освіти, доступності знань, розширення можливостей для дітей з особливими освітніми потребами.

Висновки. Впровадження інформаційних технологій у сферу освіти – це не лише вимога часу, а й стратегічна інвестиція в майбутнє країни. Міністерство освіти і науки України робить реальні кроки в цьому напрямі, і наше завдання - підтримати, удосконалити та масштабувати ці ініціативи.

Список використаних джерел:

1. Міністерство освіти і науки України. Офіційний сайт – https://mon.gov.ua
2. Єдина державна електронна база з питань освіти (ЄДЕБО) – https://info.edbo.gov.ua
3. Всеукраїнська школа онлайн – https://lms.e-school.net.ua
4. Постанова Кабінету Міністрів України № 800 від 13 липня 2011 р. «Про затвердження Положення про ЄДЕБО».
5. Національне агентство із забезпечення якості вищої освіти – https://naqa.gov.ua
6. Стратегія цифрової трансформації освіти і науки України до 2026 року – https://mon.gov.ua/ua/news/strategiya-cifrovoyi-transformaciyi-osviti-i-nauki-ukrayini-do-2026-roku.
7. ЮНЕСКО. Цифрова освіта: міжнародні практики та рекомендації – https://unesdoc.unesco.org
8. UNICEF Україна – Освітні ініціативи в умовах війни – https://www.unicef.org/ukraine
9. Google for Education – https://edu.google.com
10. Microsoft Education – https://education.microsoft.com

Маленко Андрій Олександрович
Студент 2 н.гр. 3-КВ курсу ІЗДН НАВС

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

ШТУЧНИЙ ІНТЕЛЕКТ В ДІЯЛЬНОСТІ ПУБЛІЧНИХ СЛУЖБОВЦІВ

Представлено дослідження застосування штучного інтелекту (ШІ) в процесі вибору обладнання для потреб установи. Метою роботи є оцінка ефективності використання безоплатної моделі ШІ Copilot від Microsoft для швидкого опрацювання ринкового асортименту на основі заданих критеріїв. Описано процес формування порівняльних таблиць, встановлення критеріїв відбору та параметрів відображення. Отримані результати верифіковано з використанням відкритих джерел, виявлено окремі невідповідності у даних, наданих ШІ, чим обґрунтовано необхідність критичного підходу до інформації, згенерованої ШІ.

Штучний інтелект (ШІ) став об'єктивною реальністю і несе можливості, ігнорування яких не дає змоги встояти на ескалаторах сучасних трендів [1]. Доступність засобів ШІ дозволяє користуватись ними практично будь-кому і, у такому контексті, представникам органів влади з метою забезпечення максимальної ефективності своєї роботи слід застосовувати ШІ у всіх можливих випадках для скорочення часу на рутинні процедури та інші непродуктивні дії [2].

Поштовхом до дослідження стала потреба проведення аналізу ринку з метою встановлення оптимальних для придбання установою мережевих сховищ (NAS) та дискових вінчестерів (HDD) для таких сховищ. Виконання аналізу наявного асортименту безпосередньо службовцем вимагає попереднього тривалого накопичення потрібної інформації від підприємств торгівлі та даних про технічні засоби, що надаються їх виробниками. Іншим шляхом є звернення до зовнішнього експерта (консультанта), проте останній може бути зацікавленим у придбанні замовником товарів певного бренду або моделі, таким чином існує імовірність необ'єктивності результатів.

У нашому випадку використано безоплатну модель ШІ Copilot від Microsoft, доступну у браузері MS Edge, вбудованого у операційну систему MS Windows. Встановлено початкові критерії для пошуку NAS: підтримка технології RAID-1, інтерфейсу SATAIII, низька шумність роботи, інтерфейс Ethernet 1Gb, наявність від 2 до 4 шахт для вінчестерів, контроль мережевого доступу, гаряча заміна вінчестерів, автоматичний перехід у "сплячий" режим з відімкненням живлення вінчестерів, доступність для придбання в Україні.

Кількість пристроїв для виводу в інтерфейс користувача запропоновано обмежити чотирма. В процесі "спілкування" з ШІ вимоги доповнено: живлення від стандартної мережі змінного струму, підтримка дискових вінчестерів форм-фактору 3,5" (оскільки деякі моделі виявились орієнтованими на SSD-тип) та файлових систем ext4 та Btrfs для внутрішніх дисків (оскільки моделі дозволяють підключати зовнішні вінчестери і переліки підтримуваних файлових систем зовнішніми і змінними внутрішніми вінчестерами не збігаються). Також, у цьому ітераційному процесі користувач щоразу пропонував виводити набір тих чи інших характеристик, не охоплених пошуковим запитом, або щодо яких у запиті були вказані діапазони: у остаточних даних (таблиця 1) оптимальною виявилась присутність лише таких індикативних характеристик: модель, кількість шахт для вінчестерів, показники вартості.

Таблиця 1

Відомості про NAS

Модель	Кількість шахт	Діапазон цін, грн	Середньозважена вартість, грн
Synology DiskStation DS923+	4	29,450 – 65,612	47,531
QNAP TS-216G	2	12,999 – 16,893	14,946
Synology DiskStation DS224+	2	16,610 – 31,256	23,933
Asustor Nimbustor 2 Gen2 (AS5402T)	2	18,574 – 22,499	20,536 *
QNAP TS-432X-4G	4	34,650	34,650 *

Аналогічний підхід застосовано до пошуку можливих для придбання вінчестерів, для NAS, кількість моделей для виводу обмежена 8-ма.

Час, витрачений ШІ на опрацювання кожного із запитів, не перевищував однієї хвилини. Слід відмітити, що "спілкування" із ШІ велось простою повсякденною мовою без застосування будь-яких конструкцій з галузі програмування. Таким чином підтверджено можливість використання доступних засобів ШІ публічними службовцями у повсякденній діяльності, без потреби володіння спеціальними навичками, що значно скорочує строк виконання роботи та підвищує їхню ефективність.

Результати піддані перевірці з відкритих джерел і виявлено окремі невідповідності даних, запропонованих ШІ, зокрема похибки у вартості, параметрі напрацювання на відмову та швидкості обертання шпинделю (у таблицях позначено зірочками). Нами не було внесено до ШІ власних (вивірених чи авторитетних) наборів даних, серед яких вівся пошук – він здійснювався серед доступних ресурсів Інтернет. З одного боку такий підхід значно пришвидшив і спростив процедуру, з іншого – результати потребували додаткової перевірки.

Методику надзвичайно легко застосувати для оптимізації пошуку та порівняння різних видів обладнання, суттєві характеристики яких опубліковано. Виявлені розбіжності в даних, наданих ШІ, підкреслюють важливість обмеження повної довіри до інформації, отриманої від ШІ, навіть у випадку використання передових інструментів. Пошук у відкритих джерелах в Інтернет без залучення спеціалізованих чи перевірених наборів даних, відображає типовий сценарій використання подібних інструментів користувачами, але водночас демонструє потенційні ризики отримання неточної або застарілої інформації. Таким чином, хоча ШІ може значно прискорити процес збору інформації, відповідальність за перевірку її достовірності та прийняття обґрунтованих рішень залишається за людиною.

ШІ є потужним інструментом для допомоги користувачам у виборі технічних засобів, забезпечуючи швидкий та відносно точний аналіз даних та надання рекомендацій. Незважаючи на певні обмеження, такі як необхідність перевірки отриманої інформації, використання ШІ має значні переваги, особливо в контексті економії часу та зусиль при первинному зборі даних. Навчання користувачів ефективній взаємодії з цими інструментами дозволить значно підвищити їхню ефективність та корисність в органах влади.

Список використаних джерел:

1. Artificial Intelligence Index Report 2025. Stanford Institute for Human-Centered AI. [Електронний ресурс]. URL: https://hai.stanford.edu/ai-index/2025-ai-index-report (дата звернення: 05.05.2025).

2. Пархомчук О.С. Штучний інтелект як мегатренд глобального розвитку // Політикус. 2023. № 4. С. 191-196. [Електронний ресурс]. URL: http://dspace.pdpu.edu.ua/bitstream/ 123456789/18661/1/ Parkhomchuk%20Olena%20Stanislavivna.pdf (дата звернення: 09.05.2025).

Ноздренко Яна Валентинівна
Студентка н.гр. 206_СПД ННІ права та психології НАВС

Науковий керівник:
Грищенко Олег Ігорович
старший викладач кафедри інформаційних технологій ННІ права та психології НАВС

ЗАГАЛЬНИЙ ОГЛЯД ПРОГРАМ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПЕРСОНАЛЬНИХ КОМП'ЮТЕРІВ (ПЛАТНІ ТА БЕЗКОШТОВНІ ВЕРСІЇ)

Сучасний світ переживає глибокі трансформації, спричинені стрімким розвитком цифрових технологій, де центральне місце посідає штучний інтелект (ШІ). Це не просто технологічна новинка, а революційний інструмент, що змінює майже всі сфери людської діяльності: від медицини до бізнесу, освіти та, що особливо актуально, юриспруденції та правоохоронної діяльності. Застосування ШІ на персональних комп'ютерах відкриває безпрецедентні можливості як для досвідчених професіоналів, так і для початківців. Сьогодні доступ до інструментів ШІ, від простих мовних моделей до складних систем аналізу даних, стає все ширшим. Проте, як і будь-яка потужна технологія, ШІ несе не лише обіцянки, а й виклики та ризики. Особливо це стосується чутливих сфер, де рішення, прийняті на основі ШІ, можуть впливати на долі людей, їхні права та свободи. Питання приватності, упередженості алгоритмів, прозорості рішень та відповідальності стають ключовими. Для майбутніх фахівців у правоохоронній діяльності критично важливо розуміти не тільки технічні можливості ШІ, але й його правові та етичні аспекти. Ця доповідь надасть системний огляд сутності ШІ, доступних інструментів, а також розкриє його роль та виклики у формуванні майбутнього правосуддя.

1. Сутність та класифікація штучного інтелекту

Штучний інтелект (ШІ) — це галузь комп'ютерних наук, що створює системи, здатні виконувати завдання, які традиційно потребують людського інтелекту: навчання, розпізнавання мови, прийняття рішень, обробка даних та логічне мислення. Важливо розуміти, що сучасний ШІ не "мислить" у людському розумінні, а є високопродуктивним алгоритмічним інструментом для обробки та аналізу інформації.

ШІ поділяється на кілька типів за рівнем можливостей:

Вузький (слабкий) ШІ (Narrow AI): Найпоширеніший тип, призначений для конкретних, обмежених завдань, як-от голосові помічники (Siri), системи розпізнавання облич або чат-боти. Більшість існуючих ШІ-систем належать до цієї категорії.

Загальний ШІ (General AI): Гіпотетична система, здатна виконувати будь-яке інтелектуальне завдання на людському рівні.

Надлюдський ШІ (Superhuman AI): Ще більш гіпотетичний рівень, де ШІ перевершує людський інтелект у всіх аспектах.

Прорив у сфері ШІ в останні десятиліття зумовлений стрімким зростанням обчислювальних потужностей, доступністю величезних обсягів даних та розробкою передових алгоритмів, зокрема глибинного навчання, що використовує багатошарові нейронні мережі.

2. Програми ШІ для ПК: вибір інструментів та їх застосування

Програми штучного інтелекту для персональних комп'ютерів (ПК) розрізняються за своєю доступністю та функціоналом, поділяючись на платні (комерційні) та безкоштовні. Вибір залежить від бюджету, вимог до функціональності, рівня підтримки та можливостей інтеграції.

Платні програми: Професійні рішення з комплексним функціоналом та підтримкою

Комерційні рішення пропонують повну екосистему, широкий набір інструментів та професійну підтримку, що робить їх оптимальним вибором для корпоративного сегмента та спеціалізованих застосувань.

Adobe Sensei: Інтегрована платформа ШІ в продуктах Adobe Creative Cloud. Використовує комп'ютерний зір та машинне навчання для автоматизації редагування фото/відео, розпізнавання об'єктів та облич. Корисна для аналізу відеодоказів (покращення якості, ідентифікація осіб у складних умовах).

IBM Watson: Потужна хмарна платформа для когнітивних обчислень та аналізу Big Data. Застосовується в медицині, фінансах, та особливо в юриспруденції, аналізуючи тисячі судових прецедентів, законів та нормативних актів. Це значно прискорює пошук релевантної інформації та формування аргументації для юристів і слідчих.

NVIDIA Deep Learning AI (CUDA, cuDNN, TensorRT): NVIDIA, лідер у виробництві графічних процесорів (GPU), розробляє повний програмний стек для глибинного навчання. Їхні інструменти оптимізують роботу нейронних мереж на GPU, прискорюючи процеси навчання та використання ШІ-моделей. Ці технології є основою для систем відеоаналітики в реальному часі, автоматичного розпізнавання облич на великих масивах відеоданих та 3D-реконструкції місць злочинів у криміналістиці.

Платні рішення забезпечують максимальну надійність, продуктивність та безпеку, що є критично важливим для відповідальних завдань.

Безкоштовні програми: Доступність, гнучкість та освітній потенціал

Відкриті рішення та інструменти з відкритим кодом є фундаментом для наукових досліджень, освітніх проєктів та стартапів, дозволяючи широкому колу розробників та дослідників експериментувати з ШІ без значних початкових інвестицій.

Google Colaboratory (Colab): Хмарне середовище для розробки та виконання коду Python, що підтримує популярні бібліотеки машинного навчання. Надає безкоштовний доступ до GPU/TPU від Google, що робить його ідеальним для навчання, експериментів та швидкого прототипування без потреби у потужному локальному обладнанні.

TensorFlow: Одна з найпопулярніших бібліотек для машинного та глибинного навчання з відкритим кодом (розроблена Google). Надає потужні інструменти для побудови та навчання нейронних мереж для розпізнавання мови, комп'ютерного зору, генерації тексту. Це чудовий інструмент для студентів та дослідників.

OpenAI GPT (API та відкриті моделі): Хоча флагманські моделі OpenAI є комерційними, існують відкриті аналоги та API для доступу. Моделі GPT є потужними інструментами для обробки природної мови (NLP): генерації тексту, перекладу, узагальнення документів та відповідей на запитання. У правоохоронній діяльності можуть бути корисними для автоматичного узагальнення протоколів допитів або перекладу документів.

Безкоштовні рішення, хоч і можуть мати функціональні обмеження та вимагати більшої технічної експертизи, є доступними та ідеальними для освоєння технології, пілотних проєктів та для розробників, що цінують відкритість та гнучкість.

Вибір програми ШІ повинен ґрунтуватися на ретельному аналізі потреб, доступного бюджету, необхідності технічної підтримки та можливості інтеграції.

3. Штучний інтелект у правоохоронній діяльності: можливості та правові/етичні виклики

Застосування ШІ у правоохоронній діяльності є однією з найбільш перспективних, але водночас і контроверсійних сфер. Ця технологія має потенціал значно підвищити ефективність та швидкість реагування, але породжує низку складних правових та етичних питань, що вимагають ретельного аналізу та законодавчого регулювання.

Можливості та переваги застосування ШІ:

Аналіз великих обсягів даних (Big Data Analytics): ШІ здатен оперативно обробляти, індексувати та виявляти приховані закономірності, зв'язки та аномалії у колосальних масивах інформації (відео, соцмережі, фінансові транзакції), що допомагає у розслідуваннях та розкритті злочинних мереж.

Прогнозування злочинності (Predictive Policing): Системи ШІ можуть аналізувати історичні дані для прогнозування ймовірних місць і часу майбутніх правопорушень, дозволяючи ефективніше розподіляти патрульні ресурси та запобігати злочинам.

Розпізнавання осіб та об'єктів (Facial and Object Recognition): Системи комп'ютерного зору на основі ШІ автоматично ідентифікують обличчя підозрюваних, номерні знаки, зброю на відеозаписах, прискорюючи пошук доказів.

Автоматизація рутинних завдань: ШІ прискорює складання звітів, сортування документів, пошук інформації, звільняючи час співробітників для складніших аналітичних завдань.

Криміналістична експертиза: ШІ інтегрується в процеси аналізу ДНК, відбитків пальців, балістичних даних, підвищуючи швидкість та точність експертних висновків.

Правові та етичні виклики:

Використання ШІ у правоохоронній діяльності тісно пов'язане з фундаментальними правами людини, принципами верховенства права та конфіденційністю. Необдумане або неврегульоване впровадження ШІ може призвести до серйозних порушень.

Приватність та захист персональних даних: ШІ-системи потребують великих обсягів чутливих даних (біометричні дані, геолокація). Це викликає занепокоєння щодо втручання у приватне життя та масового стеження. Закон України "Про захист персональних даних" (№ 2297-VI) є основоположним, вимагаючи згоди на обробку, обмеження цілей та забезпечення безпеки даних.

Упередженість та дискримінація: Моделі ШІ навчаються на існуючих даних. Якщо ці дані містять історичні упередження, ШІ може їх відтворювати та посилювати, призводячи до дискримінації та порушення принципу рівності перед законом (Конституція України). Це може проявлятись у несправедливих "прогнозуваннях злочинності" для певних груп або районів.

Прозорість та пояснюваність: Багато складних ШІ-моделей функціонують як "чорні скриньки" – їхня логіка прийняття рішень незрозуміла. У правоохоронній діяльності, де рішення мають серйозні наслідки, необхідно розуміти, як ШІ дійшов до висновку. Це є критичним для права на справедливий судовий розгляд. Розвиток пояснюваного ШІ (XAI) має вирішальне значення.

Відповідальність: Хто несе відповідальність за помилки, допущені ШІ? Наразі відповідальність, як правило, покладається на людину-оператора або юридичну особу, що використовує ШІ, оскільки ШІ розглядається як інструмент.

Нагляд та контроль: Для запобігання зловживанням необхідні надійні механізми нагляду та контролю за використанням ШІ. Це включає розробку спеціалізованого законодавства (як, наприклад, EU AI Act в ЄС), етичних кодексів та регулярний аудит систем ШІ.

4. Перспективи розвитку ШІ та його інтеграція у суспільство

Перспективи розвитку ШІ є надзвичайно широкими. Постійне зростання обчислювальних потужностей, доступність величезних обсягів даних та удосконалення алгоритмів сприяють швидкому прогресу. Гібридні моделі ШІ та інтеграція з іншими технологіями (наприклад, Інтернет речей, блокчейн) лише посилюють його вплив.

ШІ продовжить трансформувати:

Бізнес: Оптимізація процесів, персоналізація маркетингу, автоматизація клієнтської підтримки.

Медицина: Автоматизована діагностика, розробка ліків, персоналізовані плани лікування.

Освіта: Адаптивні навчальні програми, автоматична перевірка знань.

Безпека та кібербезпека: Виявлення загроз, прогнозування кібератак, автоматизація реагування.

Демократизація ШІ через безкоштовні та відкриті рішення дозволяє ширшому колу фахівців, дослідників та ентузіастів використовувати потужні інструменти, що прискорює інновації та підвищує загальний рівень технологічної грамотності.

Висновок: Штучний інтелект вже перестав бути концепцією майбутнього і став реальністю, що має величезний потенціал для трансформації сучасного світу. Від глобальних економічних систем до щоденних завдань на персональному комп'ютері, ШІ переформатовує наші підходи до роботи, навчання та взаємодії з інформацією. Залежно від конкретних потреб, бюджетних обмежень та цілей, користувачі мають широкий вибір між потужними платними й гнучкими безкоштовними програмами та фреймворками. Для ефективного використання ШІ, як індивідуального, так і інституційного, надзвичайно важливо визначити конкретні завдання, ретельно обрати оптимальний інструмент та інвестувати у відповідне навчання та інфраструктуру. Впровадження цієї технології у сфері правосуддя та безпеки вимагає не лише розуміння її технічних можливостей, а й усвідомлення потенційних ризиків для фундаментальних прав людини, приватності та справедливості. Розробка та імплементація адекватного законодавства, що відповідає викликам XXI століття (наприклад, регулювання захисту персональних даних у контексті масового аналізу ШІ, забезпечення прозорості алгоритмів, боротьба з упередженістю в даних та моделях, чітке визначення юридичної відповідальності за дії ШІ), є критично важливими завданнями для будь-якої держави, що прагне побудувати правове та справедливе суспільство. Україна, як держава, що активно інтегрується у світовий простір та розвиває цифрові технології, стоїть перед викликом ефективного впровадження ШІ, зберігаючи при цьому демократичні цінності та верховенство права.

Майбутні фахівці у правоохоронній сфері повинні бути не лише компетентними користувачами нових технологій, а й активними учасниками дискусії щодо їхнього етичного та правового регулювання. Лише за умови збалансованого підходу, що поєднує технологічні інновації з дотриманням прав людини, демократичних принципів та верховенства права, штучний інтелект зможе повною мірою реалізувати свій величезний потенціал на благо українського суспільства та його безпеки.

Список використаних джерел:

1. Закон України "Про захист персональних даних" від 01 червня 2010 року № 2297-VI.
2. Закон України "Про електронні довірчі послуги" від 05 жовтня 2017 року № 2155-VIII.
3. Офіційний сайт Міністерства цифрової трансформації України.
4. Сайт Уряду України (Кабінет Міністрів України).
5. Adobe Sensei. Офіційний вебсайт продукту: https://www.adobe.com/sensei.html
6. IBM Watson. Офіційний вебсайт продукту: https://www.ibm.com/watson
7. NVIDIA Deep Learning AI. Офіційний вебсайт продукту: https://developer.nvidia.com/deep-learning
8. Google Colaboratory. Офіційний вебсайт: https://colab.research.google.com/
9. TensorFlow. Офіційний вебсайт: https://www.tensorflow.org/
10. OpenAI. Офіційний вебсайт: https://openai.com/

Градюк Іванна Миколаївна
Студентка н.гр. 205_СПД ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

ВИКОРИСТАННЯ «ШІ» ДЛЯ ВИЯВЛЕННЯ ФЕЙКІВ І ДЕЗІНФОРМАЦІЇ В СИСТЕМАХ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У сучасному світі інформаційні потоки стали однією з головних арен боротьби за вплив. Фейки, дезінформація та інформаційні маніпуляції використовуються як інструменти гібридної війни, що становить серйозну загрозу національній безпеці. Особливо це актуально для України, яка вже понад десятиліття перебуває під інформаційним тиском з боку агресора. У таких умовах критично важливо мати ефективні інструменти для протидії дезінформації. Штучний інтелект (ШІ) відкриває нові можливості для автоматизованого виявлення неправдивих повідомлень, фейкових джерел та координованих інформаційних атак.

Безперечно, впровадження технологій штучного інтелекту знаменує собою якісно новий етап у боротьбі з загрозами інформаційній безпеці. Інтелектуальні системи отримують можливість у режимі реального часу здійснювати глибокий аналіз величезних масивів даних, що надходять з різних інформаційних джерел – від соціальних мереж до новинних агрегаторів та медіа-платформ. Завдяки цьому стає можливим оперативно виявляти стрімко розповсюджувані фейкові повідомлення, розпізнавати маніпулятивні інформаційні конструкції, спрямовані на руйнування суспільної єдності та довіри до інститутів, а також розкривати організовані дезінформаційні атаки, метою яких є дестабілізація внутрішньої ситуації в країні.

Штучний інтелект здатний не лише реагувати на вже виявлені випадки дезінформації, а й аналізувати потоки інформації для виявлення потенційних загроз на ранніх стадіях їхнього формування. Це досягається шляхом виявлення певних лінгвістичних патернів, різких змін у тематиці обговорень або активності певних груп користувачів, що може свідчити про підготовку або початок інформаційної атаки.

Штучний інтелект може використовуватися:

1) для автоматичного аналізу великої кількості даних, що надходять з різних джерел,

2) для виявлення неправдивої інформації,

3) для розпізнавання змінених (підроблених) зображень шляхом порівняння їх з оригінальними,

4) для встановлення принципів, схем і способів поширення дезінформації,

5) для блокування виявленої дезінформації [1].

В умовах глобального інформаційного простору дезінформація часто поширюється різними мовами. Системи штучного інтелекту, навчені на багатомовних даних, здатні аналізувати та виявляти неправдиву інформацію незалежно від мови її поширення, що є критично важливим для протидії зовнішньому інформаційному впливу. Розробка передових багатомовних моделей ШІ дозволяє здійснювати раннє виявлення фейків та надавати прозорі пояснення щодо прийнятих рішень, що сприяє ефективній перевірці інформації людиною. Важливо, щоб такі системи ШІ розроблялися та використовувалися з дотриманням принципів справедливості, прозорості, підзвітності та безпеки, що забезпечує довіру суспільства та ефективність контрзаходів проти дезінформації [2].

Одним із найнебезпечніших інструментів поширення дезінформації є синтетичний медіаконтент, зокрема фальшиві зображення, відео та аудіофайли, створені за допомогою технологій штучного інтелекту, таких як deepfake. Ці технології дозволяють маніпулювати зовнішністю або голосом людини, створюючи реалістичні, але неправдиві матеріали, які можуть дискредитувати публічних осіб, викривляти факти або сіяти паніку в суспільстві.

У відповідь на ці загрози, сучасні алгоритми ШІ розвиваються у напрямку детектування ознак підробки та маніпуляцій. Це включає аналіз метаданих, виявлення невідповідностей у тінях, звукових частотах або глибинах зображення. Наприклад, нейронні мережі, спеціально навчені на великій кількості справжніх та фальшивих зразків, можуть з високою точністю виявляти використання штучно згенерованих облич або голосів. Це відкриває нові можливості для протидії аудіовізуальній дезінформації, знижуючи ймовірність успішного поширення фейкових матеріалів через соціальні мережі та месенджери.

В Україні вже впроваджуються практичні рішення для боротьби з дезінформацією. Зокрема, платформа Mantis Analytics, розроблена українськими фахівцями, використовує штучний інтелект для моніторингу інформаційного простору в режимі реального часу. Ця система аналізує тисячі повідомлень з медіа та соціальних мереж, виявляючи фейки та інформаційно-психологічні операції (ІПСО), що дозволяє оперативно реагувати на загрози інформаційній безпеці держави. Сучасні виклики інформаційної безпеки вимагають нових технологічних рішень, і штучний інтелект уже сьогодні доводить свою ефективність у боротьбі з дезінформацією.

Його здатність швидко обробляти великі обсяги даних, виявляти приховані зв’язки, аналізувати медіаконтент та розпізнавати фейки значно підсилює можливості держави в інформаційній протидії.

Запровадження ШІ в системи державної інформаційної безпеки дозволяє не лише оперативно реагувати на загрози, а й діяти на випередження – виявляючи інформаційні атаки ще на етапі їхнього поширення. Водночас важливо враховувати етичні, правові та технічні аспекти використання таких технологій, щоб забезпечити баланс між безпекою та правами громадян.

Список використаних джерел:

1. Штучний інтелект в системі інформаційної безпеки України в умовах російсько - української війни//Воропаєва Т. С., Авер'янова Н. М.//ст. 62-65 // URL: https://previous.scientia.report/index.php/archive/article/view/2026/2042

Slepko Angelina Ivanivna
Student of academic group 102_SPS,
Institute of Law and Psychology, NAIA

Scientific supervisor:
Pakrysh Oleksandr Yevheniiovych
Candidate of Technical Sciences,
Associate Professor, Associate Professor of the Department of Information Technologies,
Institute of Law and Psychology, NAIA

MANIPULATION OF PUBLIC CONSCIOUSNESS DURING WAR USING ARTIFICIAL INTELLIGENCE

In the modern world, artificial intelligence (AI) technologies are rapidly developing, penetrating various spheres of life, including military affairs and information warfare. During military conflicts, information becomes a powerful weapon capable of influencing the course of events, the moral state of the population, and international public opinion. The use of AI for creating and spreading disinformation opens new opportunities for manipulating public consciousness, which can have serious consequences for state security and stability.

The application of AI for manipulating public consciousness during war is an extremely relevant issue. Modern technologies allow the creation of realistic fake news, images, and videos that are difficult to distinguish from real ones. This complicates the process of detecting and debunking disinformation, undermines trust in the media and official sources, and contributes to the spread of panic and chaos among the population. Understanding the mechanisms of AI-driven information attacks is essential for developing effective countermeasures and protecting the information space.

The issue of using AI to manipulate public consciousness during war has been studied by many scientists and experts. In Ukraine, in particular, this issue has been analyzed by specialists from the Ukrainian Institute for the Future, who examined the potential of AI in analytical work and its impact on various spheres of life [1]. Additionally, experts from the Ukrainian Helsinki Human Rights Union have studied the influence of AI on society, considering the possible risks and challenges associated with its use during wartime. The experts of the Ukrainian Helsinki Human Rights Union emphasize: “The use of AI technologies must ensure compliance with fundamental human rights and adhere to certain principles that can mitigate potential risks associated with their application” [2].

AI technologies enable the automation of processes for creating and disseminating disinformation. In particular, generative neural networks can produce fake images and videos that are difficult to distinguish from real ones. Such materials can be used to discredit military leaders, spread panic among the population, or mislead the international community. Social networks, governed by AI algorithms, can facilitate the rapid spread of disinformation, amplifying its influence on public consciousness. Algorithms that analyze user behavior can select content that triggers strong emotional reactions, contributing to societal polarization and intensifying conflicts.

I believe that using AI to manipulate public consciousness during war is a serious threat that requires immediate attention. It is necessary to develop and implement technologies for detecting disinformation, enhance media literacy among the population, and establish ethical standards for AI usage. Only a comprehensive approach will minimize the negative impact of disinformation on society.

To minimize the risks associated with AI-driven manipulation of public consciousness, certain measures should be taken:

1. Increasing media literacy – conducting educational programs that teach critical evaluation of information and the identification of fake news.
2. Developing technologies for detecting disinformation – creating AI algorithms that can automatically identify and block fake content.
3. Implementing ethical standards for AI usage – developing international norms and regulations on the ethical use of AI, especially in the context of information warfare.
4. Cooperation between states and technology companies – joint efforts to detect and combat disinformation, as well as the exchange of experience and technologies.

The use of artificial intelligence to manipulate public consciousness during war is one of the greatest threats to the modern information space. AI technologies enable the creation of realistic fakes that affect people's emotional states, undermine trust in official sources, and exacerbate social conflicts. Social media algorithms contribute to the rapid dissemination of disinformation, shaping a distorted perception of reality and increasing psychological pressure on the population. The ability of AI to generate visual and textual content creates risks for military and political stability, as disinformation can be used for propaganda, demoralization of military personnel and civilians, and influencing the international community. Additionally, constant information overload leads to the phenomenon of "information fatigue," reducing people's ability to think critically and analyze incoming data. However, the increase in threats does not mean their inevitability. To counteract manipulations, it is necessary to develop media literacy among the population, create effective fake detection algorithms, and implement ethical standards for AI use. It is crucial that governments, civil organizations, and technology companies cooperate in the field of information security, preventing AI from being used as a tool for manipulation and information attacks.

Ultimately, artificial intelligence is merely a tool, and its impact on society depends on how it is utilized. If humanity learns to use AI responsibly, these technologies can become not only a means of disinformation but also a powerful mechanism for exposing falsehoods, contributing to the formation of a more resilient and aware society.

References:

1.“Battle of Approaches: Human Intelligence vs. Artificial Intelligence in Predicting the Future Until 2028” (29.01.25). Ukrainian Institute for the Future. URL: https://uifuture.org/publications/lyudskyy-intelekt-proty-shtuchnogo-u-prognozuvanni-maybutnogo-do-2028-roku/

2.“Artificial Intelligence and Human Rights: Guidelines and Restrictions in the Context of National Security and Defense” (14.05.24). Ukrainian Helsinki Human Rights Union. URL: https://www.helsinki.org.ua/articles/shtuchnyy-intelekt-ta-prava-liudyny-oriientyry-ta-obmezhennia-u-konteksti-natsionalnoi-bezpeky-ta-oborony/

Федорова Людмила Федорівна
Студентка групи 102_СПС ННІ права та психології НАВС

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

FAKE-ЗАСОБИ ПСИХОЛОГІЇ МАСОВОЇ ДЕЗІНФОРМАЦІЇ

У наш час інформація стала одним з найпотужніших інструментів впливу на суспільство. Завдяки розвитку цифрових технологій ми маємо миттєвий доступ до новин, думок, фактів і подій з усього світу. Проте разом із цим зростає загроза масової дезінформації, яка використовує численні психологічні механізми для маніпулювання свідомістю людей. Особливо небезпечними є так звані fake-засоби, які створюються не лише для введення в оману, а й для формування хибної картини реальності.

Fake-засоби – це вигадані, перекручені або навмисно спотворені матеріали, що подаються як достовірна інформація. Їхня мета – змусити людину повірити в неправду, спровокувати емоційну реакцію або змінити її поведінку. Часто такі засоби використовують механізми психологічного впливу, як-от ефект повторення, емоційне зараження, авторитет джерела, ефект більшості, а також когнітивні упередження. Наприклад, коли людина постійно бачить ту саму інформацію з різних джерел, навіть якщо вона неправдива, її мозок схильний вважати її правдою – це називається «ілюзія правди». Якщо до фейкової інформації додається посилання на «експерта» або «свідка», що нібито підтверджує її, це викликає більшу довіру.

Масова дезінформація найчастіше поширюється через соціальні мережі, месенджери та інтернет-медіа. Особливість таких платформ полягає в швидкості розповсюдження новин та відсутності контролю за достовірністю інформації. Алгоритми соціальних мереж часто підсилюють контент, який викликає сильні емоції – обурення, страх, співчуття – що сприяє вірусному ефекту поширення фейків.

Ще один аспект дії fake-засобів – це їхній вплив на суспільну думку та політичну стабільність. За допомогою маніпуляцій можна розпалити ворожнечу, дестабілізувати суспільство, підірвати довіру до офіційних джерел інформації, науки або державних інституцій.

У кризових ситуаціях, наприклад, під час війни або пандемії, фейкова інформація може викликати паніку, масові порушення порядку або відмову від реальних заходів безпеки.

Захист від fake-засобів дезінформації полягає у розвитку критичного мислення, медіаграмотності та усвідомлення того, як працює людська психіка в умовах інформаційного навантаження. Важливо навчитися перевіряти джерела, ставити під сумнів надто емоційні повідомлення та розуміти, що не вся інформація в інтернеті є правдивою. Окрім цього, держава, освітні заклади та медіа мають сприяти формуванню стійкого імунітету до інформаційних маніпуляцій.

Отже, fake-засоби психології масової дезінформації – це складне і небезпечне явище, що вимагає уваги не лише спеціалістів, а й кожного свідомого громадянина. В умовах інформаційної війни здатність розрізняти правду і маніпуляцію є не менш важливою, ніж фізична безпека. Тому завдання сучасного суспільства – навчитися захищати свою свідомість так само, як і свою територію.

Список використаних джерел:

1. О. Батрименко, Д. Неліпа, Фейк-ньюз у соціальних мережах як маніпулятивний засіб інформаційної війни //Вісник Львівського університету. Серія філос.-політолог. студії. 2022. Випуск 44, С. 86-91.

2. Данилик В., Висоцька В., Назаркевич М. Методи ідентифікації дезінформації, фейків та пропаганди в засобах масової інформації на основі машинного навчання. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *1*(25). 2024. С. 449–467. URL: https://doi.org/10.28925/2663-4023.2024.25.449467

3. Zhang, Z., Chen, Y., & Chen, L. (2020). Methods for detecting fake news: A survey. ACM Computing Surveys, 53(6), С. 1–37.

Доброгорська Валерія Сергіївна
Студентка н.гр. 205_СПД ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

ВИКОРИСТАННЯ ЧАТ-БОТІВ ДЛЯ ШВИДКОЇ ОБРОБКИ ЗАПИТІВ ГРОМАДЯН

Впровадження сучасних інформаційних технологій у державному секторі є одним із ключових напрямів цифрової трансформації, що сприяє підвищенню ефективності управління та покращенню якості обслуговування громадян. Серед таких технологій особливе місце займають чат-боти — автоматизовані системи, які дозволяють оперативно відповідати на запити користувачів, знижуючи навантаження на персонал та забезпечуючи доступність інформації 24/7. У даній роботі розглянуто можливості використання чат-ботів у державних установах для швидкої обробки запитів громадян, визначено їх переваги, виклики та перспективи впровадження.

Суть технології чат-ботів у державних установах

Чат-боти — це програмні агенти, які імітують людську комунікацію за допомогою текстових або голосових повідомлень. У державних установах вони можуть бути впроваджені для вирішення таких завдань:

- **Консультаційна підтримка:** Надання відповідей на типові питання громадян, наприклад, про графік роботи установи, порядок отримання документів, контактну інформацію тощо.
- **Обробка заявок:** Автоматичний прийом заявок на отримання довідок, запис на прийом, інформування про статус обробки документів.
- **Зворотний зв’язок:** Збір відгуків та пропозицій від громадян щодо якості обслуговування.
- **Інформаційна підтримка:** Інформування про нові законодавчі акти, зміни у процедурі надання послуг, запобігання шахрайським діям.
- **Навчання громадян:** Чат-боти можуть бути використані для проведення інформаційних кампаній, наприклад, щодо цифрової грамотності, доступу до електронних сервісів тощо.

Для реалізації цих завдань чат-боти використовують попередньо визначені сценарії, алгоритми машинного навчання та технології обробки природної мови (NLP). Вони можуть бути простими, які працюють за принципом розпізнавання ключових слів, або складними — такими, що застосовують штучний інтелект для аналізу та обробки контексту запиту.

Переваги використання чат-ботів у державних установах

Застосування чат-ботів у державних установах має низку переваг, серед яких:

1. **Оперативність:** Чат-боти можуть надавати відповіді миттєво, без черг та затримок, що особливо актуально у періоди підвищеного навантаження на контактні центри.
2. **Масштабованість:** Один чат-бот здатний обробляти велику кількість запитів одночасно, що дозволяє уникнути перевантаження операторів та скоротити час очікування.
3. **Цілодобова доступність:** Чат-боти працюють 24/7, що забезпечує громадянам можливість отримати інформацію у будь-який зручний для них час.
4. **Зменшення витрат:** Використання чат-ботів знижує витрати на утримання великої кількості операторів, а також на організацію кол-центрів.
5. **Аналітика та моніторинг:** Чат-боти можуть зберігати історію взаємодій із громадянами, аналізувати типові запити та формувати рекомендації щодо покращення роботи установи.

Виклики та ризики впровадження чат-ботів

Попри значний потенціал чат-ботів, їх впровадження у державних установах пов’язане з певними викликами:

- **Захист персональних даних:** Взаємодія з чат-ботом передбачає обробку конфіденційної інформації. Неналежний захист даних може призвести до витоку або неправомірного використання інформації.
- **Технічні обмеження:** Стандартні чат-боти здатні обробляти лише типові запити. Відповіді на складні або нестандартні питання можуть бути некоректними або взагалі відсутніми.
- **Сприйняття громадянами:** Частина користувачів може скептично ставитися до відповідей чат-бота, вважаючи їх менш надійними у порівнянні з консультацією оператора.
- **Мовний бар’єр:** Чат-боти повинні враховувати мовні та культурні особливості користувачів для уникнення непорозумінь

Розробка автоматизованої системи для надання першої медичної допомоги з використанням чат-бота

Окремим напрямом розвитку чат-ботів є їх впровадження для надання першої медичної допомоги. Такі системи можуть значно підвищити швидкість реагування у випадках невідкладних ситуацій. Основні можливості таких чат-ботів включають:

- **Оцінка стану пацієнта:** Чат-бот може провести швидке опитування про симптоми (наприклад, біль у грудях, задишка, втрата свідомості) та визначити необхідність термінової медичної допомоги.
- **Надання інструкцій:** Система може інформувати користувача про основні кроки надання першої допомоги до прибуття медиків (штучне дихання, зупинка кровотечі, стабілізація потерпілого).
- **Навчальні матеріали:** Чат-бот може надавати інформацію про алгоритми дій у разі серцевого нападу, інсульту, опіків, травм тощо.
- **Інтеграція з екстреними службами:** У випадку критичних ситуацій, чат-бот може автоматично передати інформацію про стан пацієнта до диспетчерського центру.

Такі системи вже реалізовані у багатьох країнах. Наприклад, чат-боти, що працюють на базі штучного інтелекту, використовуються у Великій Британії для дистанційного медичного консультування через додаток NHS 111. В Україні впровадження таких рішень може значно скоротити час реагування на екстрені випадки та підвищити рівень обізнаності громадян щодо основ першої допомоги.

Використання чат-ботів у період воєнного стану

В умовах війни в Україні, чат-боти стали важливим інструментом для надання оперативної інформації та забезпечення безпеки громадян. Основні напрями використання чат-ботів у цей період включають:

- **Попередження про небезпеку:** Чат-боти можуть інформувати громадян про загрози ракетних ударів, евакуаційні шляхи, місця укриття. Наприклад, чат-бот "Повітряна тривога" миттєво сповіщає про небезпеку в конкретному регіоні.
- **Психологічна підтримка:** В умовах стресу та паніки, чат-боти можуть забезпечувати психологічну підтримку громадян, надавати поради з подолання тривожності, контакти кризових центрів та гарячих ліній.
- **Контроль за фейковими новинами:** Чат-боти можуть використовуватись для перевірки достовірності інформації, що поширюється в мережі, що особливо актуально у період інформаційних атак.
- **Надання медичної інформації:** Чат-боти можуть консультувати громадян з питань першої медичної допомоги, зокрема при пораненнях, контузіях, опіках. Вони можуть також надавати контакти медичних закладів, що працюють у зоні бойових дій.

Таким чином, чат-боти є не лише інструментом комунікації, але й важливою складовою системи безпеки та підтримки громадян під час воєнного стану.

Впровадження чат-ботів у державних установах: досвід України та інших країн

У багатьох країнах світу державні установи вже успішно впроваджують чат-боти:

- **Україна:** У рамках програми цифровізації державних послуг було створено чат-бота "Дія". Він допомагає громадянам у вирішенні питань, пов'язаних з отриманням електронних документів, перевіркою статусу заявок, повідомленням про зміни у законодавстві.
- **США:** IRS (Internal Revenue Service) використовує чат-боти для консультацій з податкових питань, що дозволяє суттєво знизити навантаження на операторів кол-центрів.
- **Естонія:** В межах програми "E-stonia" запроваджено чат-боти для комунікації з громадянами у сфері соціального забезпечення, охорони здоров'я та електронного урядування.
- **Сінгапур:** Чат-боти використовуються для інформування громадян про зміни у міграційних правилах, отримання дозволів на роботу та інші адміністративні процедури.

Висновки:

Використання чат-ботів у державних установах є важливим кроком до впровадження сучасних інформаційних технологій у державне управління. Вони дозволяють оперативно та ефективно обробляти запити громадян, забезпечують цілодобову підтримку та зменшують витрати на утримання контактних центрів. Водночас успішне впровадження цієї технології потребує комплексного підходу, включаючи забезпечення кібербезпеки, адаптацію сценаріїв відповідей до потреб громадян та постійний моніторинг якості обслуговування.

Список використаних джерел:

1. Борисенко В. В., Сидоренко М. І. Використання чат-ботів у державних установах: перспективи та виклики // Інформаційні технології в управлінні. – 2024. – №2. – С. 12-18.
2. Коваленко А. Сучасні інформаційні технології у державному управлінні // Збірник наукових праць НУ "Львівська політехніка". – 2023. – №3. – С. 45-50.
3. Official Website of "Diia" – https://diia.gov.ua
4. IRS Chatbot Implementation Report. – https://www.irs.gov
5. Міністерство цифрової трансформації України. (2023). Використання чат-ботів у державних установах: Аналітичний огляд.
6. Мінцифра України. (2023). Чат-бот "Повітряна тривога" як інструмент оперативного сповіщення громадян.

Герасимова Катерина Олександрівна
Студентка н.гр. 204_СПД ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

РОЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ЗАБЕЗПЕЧЕННІ ВІДКРИТОСТІ ТА ПРОЗОРОСТІ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Сучасне суспільство перебуває на етапі активної цифрової трансформації, яка проникає в усі сфери життя, включаючи державне управління та правоохоронну діяльність. В умовах прагнення до демократизації та підвищення рівня довіри громадян до державних інституцій, забезпечення відкритості та прозорості діяльності Національної поліції України набуває особливої ваги. У цьому контексті інформаційні технології (ІТ) виступають не просто інструментом, а ключовим фактором, що визначає якісно новий рівень взаємодії між поліцією та суспільством.

Основні аспекти впливу інформаційних технологій

Інформаційні технології забезпечують відкритість та прозорість діяльності Національної поліції через низку ключових механізмів:

1. Забезпечення доступу до інформації:

Офіційний веб-сайт Національної поліції: Є центральним онлайн-ресурсом, що надає оперативну інформацію про діяльність поліції, новини, аналітичні матеріали, контакти керівництва, інформацію про структуру та функції підрозділів. Регулярне оновлення та зручна навігація сайту забезпечують легкий доступ громадян до необхідних відомостей.

Оприлюднення нормативно-правових актів та внутрішніх регламентів: Забезпечення відкритого доступу до законодавчих актів, на основі яких діє поліція, а також до внутрішніх інструкцій та положень, підвищує рівень правової обізнаності громадян та сприяє розумінню принципів роботи правоохоронців.

2. Оптимізація внутрішніх процесів та зменшення корупційних ризиків:

Системи електронного документообігу (СЕД): Автоматизація процесів реєстрації звернень, руху документів, контролю виконання завдань значно підвищує ефективність роботи поліції, мінімізує бюрократію та унеможливлює втрату документів. Прозорість документообігу знижує ризики корупційних дій та зловживань службовим становищем.

Автоматизовані системи управління нарядами (АСУН): Оптимізація розподілу патрулів та реагування на виклики за допомогою ІТ дозволяє підвищити оперативність реагування на правопорушення та забезпечити більш справедливий розподіл навантаження між співробітниками.

Системи внутрішнього аудиту та контролю: Впровадження ІТ-систем для моніторингу діяльності співробітників, аналізу службових порушень та проведення внутрішніх розслідувань сприяє підвищенню дисципліни та відповідальності в лавах поліції.

3. Забезпечення ефективної комунікації та зворотного зв'язку з громадянами:

Сервіси для електронних звернень: Можливість подання заяв, скарг, пропозицій через онлайн-платформи та електронну пошту значно спрощує процес взаємодії громадян з поліцією, економить час та забезпечує фіксацію звернення.

Онлайн-запис на прийом: Запровадження онлайн-запису на прийом до керівництва або профільних спеціалістів поліції робить комунікацію більш зручною та організованою.

Чат-боти та інтерактивні помічники: Використання чат-ботів на веб-сайті та в соціальних мережах дозволяє надавати оперативні консультації з типових питань, інформувати про порядок дій у різних ситуаціях та розвантажувати операторів телефонної лінії "102".

4. Підвищення рівня підзвітності та контролю за діями поліцейських:

Використання боді-камер: Обов'язкове використання боді-камер працівниками патрульної поліції та інших підрозділів фіксує їхні дії під час виконання службових обов'язків, що забезпечує об'єктивність у спірних ситуаціях, запобігає зловживанням та підвищує рівень довіри до поліцейських.

Системи відеоспостереження в публічних місцях: Встановлення камер спостереження в містах та інших публічних місцях сприяє фіксації правопорушень, допомагає в розкритті злочинів та може слугувати стримуючим фактором. Доступ до відеозаписів у встановленому законом порядку забезпечує прозорість розслідувань.

5. Взаємодія з суспільством через соціальні мережі:

Активне ведення сторінок у соціальних мережах (Facebook, Instagram): Поліція використовує соціальні мережі для оперативного інформування населення про події, проведення інформаційних кампаній, роз'яснення законодавства, реагування на запити та коментарі громадян. Це створює прямий канал комунікації та підвищує рівень відкритості.

Виклики та перспективи

Незважаючи на значний потенціал інформаційних технологій у забезпеченні відкритості та прозорості, існують і певні виклики, серед яких:

Цифровий розрив: Необхідно забезпечити рівний доступ до інформаційних технологій для всіх громадян, незалежно від їхнього соціального статусу та місця проживання.

Кібербезпека: Захист інформаційних систем поліції від кібератак є критично важливим для забезпечення безпеки даних та безперебійної роботи сервісів.

Захист персональних даних: При впровадженні нових технологій необхідно суворо дотримуватися законодавства про захист персональних даних громадян.

Етичні питання: Використання технологій розпізнавання облич, аналізу великих даних тощо потребує ретельного етичного обґрунтування та законодавчого регулювання.

Подальший розвиток інформаційних технологій у діяльності Національної поліції має бути спрямований на:

Впровадження інтегрованих інформаційних систем: Створення єдиної інформаційної екосистеми, що об'єднує різні підрозділи та бази даних, підвищить ефективність роботи та забезпечить кращу координацію.

Використання штучного інтелекту та машинного навчання: Застосування ШІ для аналізу даних, прогнозування злочинності та оптимізації оперативного реагування може значно підвищити ефективність правоохоронної діяльності.

Розвиток онлайн-сервісів та мобільних додатків: Надання громадянам ширшого спектру онлайн-послуг та зручних мобільних інструментів для взаємодії з поліцією.

Підвищення рівня цифрової грамотності співробітників: Навчання та підвищення кваліфікації поліцейських у сфері використання сучасних інформаційних технологій є необхідною умовою ефективного впровадження ІТ.

Висновки

Інформаційні технології є потужним інструментом для досягнення якісно нового рівня відкритості та прозорості в діяльності Національної поліції України. Їхнє ефективне впровадження сприяє не лише підвищенню ефективності роботи правоохоронців, оптимізації внутрішніх процесів та покращенню якості надання послуг громадянам, але й, що найважливіше, зміцненню довіри суспільства до поліції.

Подальший розвиток та інтеграція інноваційних ІТ-рішень у діяльність Національної поліції є стратегічно важливим напрямком для побудови відкритої, підзвітної та ефективної правоохоронної системи, яка служить інтересам громадян та сприяє зміцненню демократичного правового суспільства в Україні.

Список використаних джерел:

1. Про Національну поліцію : закон України від 02 липня 2015 р. Відомості Верховної Ради України. 2015. № 40–41. Ст. 379.

2. Про доступ до публічної інформації: закон України від 13 січня 2011 р. №2939-VI.

3. Національна безпека України : навч. посібник / Ситник Г. П. та ін.; за заг. ред. Г. П. Ситника. Київ : Кондор, 2007. 616 с.

4. Основи інформаційного права України : навч. посіб. / В. С. Цимбалюк та ін.; за ред. М. Я. Швеця. Київ : Знання, 2009. Вид. 2-ге, переробл. і допов. 414 с.

5. Ващенко Л. О., Єфімов О. М. Тлумачний словник – мінімум української мови. Київ : Довіра, 2000. Вид. 2-ге. 546 с.

6. Правова інформатика : підручник. У 2 т. Київ : Парлам. вид-во, 2004. Т. 1. 416 с.

Чалбишева Віталіна Русланівна
Студентка н.гр. 205_СПД ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

РОЛЬ ІНФОРМАЦІЙНИХ СИСТЕМ У ПРОТИДІЇ КОРУПЦІЇ В ДЕРЖАВНОМУ СЕКТОРІ УКРАЇНИ

1. Актуальність теми

Корупція є однією з найбільш деструктивних загроз демократичному розвитку, ефективному функціонуванню державних інституцій і довірі громадян до влади. Особливо гостро ця проблема стоїть в Україні, яка водночас веде масштабну війну та прагне інтегруватися до ЄС. Протидія корупції стає не просто завданням правоохоронних органів, а елементом національної безпеки. У цьому контексті важливо не лише карати за зловживання, а й створити ефективну систему запобігання та моніторингу.

Інформаційні системи (ІС), побудовані на засадах відкритості, доступності та автоматизованого аналізу, є потужним інструментом у досягненні цієї мети. Їх застосування у сфері державного управління дозволяє зробити процеси публічного адміністрування більш прозорими, а діяльність посадовців — підзвітною.

2. Теоретичні засади: поняття та класифікація ІС

Інформаційна система – це сукупність організаційних, технічних і програмних засобів, які забезпечують збір, обробку, зберігання, передачу та аналіз інформації з метою підтримки прийняття управлінських рішень. У державному секторі такі системи відіграють роль інструменту цифрового врядування, підвищують якість публічних послуг, а також виступають бар'єром для корупційних практик.

Ключові типи ІС, що використовуються для протидії корупції в Україні:

• Електронне врядування (e-Government) — комплекс систем, що дозволяє автоматизувати публічні послуги та обмежити людський фактор (платформа «Дія»).

• ІС фінансової прозорості — системи відкритих бюджетів та публічних закупівель (Prozorro, E-Data, Spending.gov.ua), які дозволяють громадськості контролювати витрати бюджетних коштів.

• Антикорупційні реєстри — системи електронного декларування (реєстр НАЗК), публічні бази даних про бенефіціарів, судові рішення тощо.

• Аналітичні ІС — автоматизовані модулі аналізу нормативно-правових актів, що дозволяють виявляти корупційні ризики ще до ухвалення рішень (модуль НАЗК з оцінки проєктів актів).

3. Реалізація інформаційних систем в Україні

Після Революції Гідності Україна почала активне впровадження цифрових інструментів у сфері антикорупційної політики. Зокрема:

• Prozorro — електронна система публічних закупівель, яка забезпечує доступ усіх громадян до тендерної інформації. За даними Prozorro, (https://prozorro.gov.ua/) у 2024 році вона охопила понад 95% державних закупівель, а економія державних коштів перевищила 50 млрд грн.

• E-Data — платформа відкритих фінансів, яка дозволяє відслідковувати кожну гривню бюджетних витрат, забезпечуючи прозорість руху коштів у реальному часі.

• Єдиний державний реєстр декларацій осіб, уповноважених на виконання функцій держави — дає змогу перевіряти майновий стан посадовців. У 2024 році НАЗК провело понад 1 200 повних перевірок декларацій.

• Платформа «Дія» — забезпечує доступ до понад 100 публічних послуг без необхідності відвідувати органи влади. Це значно знижує побутову корупцію, пов’язану з отриманням дозволів, довідок та ліцензій.

4. Результати впровадження ІС у боротьбі з корупцією

Реалізація ІС у сфері антикорупційної політики вже демонструє позитивні результати:

• Зростання прозорості: громадяни мають змогу стежити за витратами держави, діями посадовців, змінами в законодавстві.

• Зменшення корупційних ризиків: зменшення «ручного» втручання з боку чиновників та зниження суб’єктивного фактору у прийнятті рішень.

• Активізація громадського контролю: журналісти, аналітики та громадські організації використовують відкриті дані для викриття порушень (наприклад, аналітика Bihus.info, антикорупційна діяльність DOZORRO тощо).

• Формування культури підзвітності: посадовці змушені декларувати свої доходи, майно, родинні зв’язки; державні органи — оприлюднювати звіти та бюджети.

5. Проблеми та виклики

Однак ефективність інформаційних систем стримується низкою факторів:

• Недостатня цифрова грамотність службовців, що ускладнює впровадження нових систем у регіонах.

• Нерівномірність технічного забезпечення: частина ОМС (органів місцевого самоврядування) не має ресурсів для впровадження ІС належного рівня.

• Опір корупціонерів: чиновники, які втратили контроль над потоками ресурсів, можуть гальмувати цифрові реформи.

• Кібератаки та загрози інформаційній безпеці: у 2022–2024 роках урядові ІС зазнали сотень хакерських атак, що вимагає постійного посилення захисту.

• Правова невизначеність у сфері використання великих даних, алгоритмічного управління тощо.

6. Перспективи розвитку

Подальша цифровізація державного управління в Україні повинна включати:

• Інтеграцію штучного інтелекту у систему ризик-менеджменту — наприклад, для виявлення аномальних витрат у бюджетах або зв'язків між компаніями.

• Автоматичне визначення конфліктів інтересів — шляхом перехресного аналізу відкритих реєстрів (ЄДР, декларації, дані про тендери тощо).

• Розширення функціоналу «Дії» — зокрема, щодо моніторингу соціальних виплат, реконструкції об'єктів, цифрових бюджетів громад.

• Формування «єдиного цифрового вікна» контролю громадськості — зведена антикорупційна платформа для аналітики, реєстрації скарг, запитів, перевірки даних

Висновки:

Інформаційні системи є не лише технічним, а насамперед інституційним засобом протидії корупції. Вони сприяють зменшенню зловживань, підвищенню підзвітності, розвитку демократичного врядування. В умовах трансформації публічного сектору ІС стають критично важливими для збереження довіри до влади, ефективного управління ресурсами та інтеграції до європейських стандартів доброчесності.

Однак для сталого ефекту необхідно забезпечити синхронний розвиток правової, організаційної та технічної складових, а також посилити роль громадянського суспільства у використанні цифрових інструментів контролю.

Список використаних джерел:

1. Transparency International Україна. Індекс сприйняття корупції – 2024. – https://cpi.ti-ukraine.org (https://cpi.ti-ukraine.org/).

2. Державна антикорупційна програма 2023–2025. – https://nazk.gov.ua (https://nazk.gov.ua/).

3. Prozorro – https://prozorro.gov.ua (https://prozorro.gov.ua/).

4. Портал E-Data – https://spending.gov.ua (https://spending.gov.ua/).

5. Міністерство цифрової трансформації України – https://thedigital.gov.ua (https://thedigital.gov.ua/).

6. Верховна Рада України. Аналітичні публікації – https://research.rada.gov.ua (https://research.rada.gov.ua/).

Калашникова Катерина Ігорівна
Студентка н.гр. 205_СПД ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ ЯК ОСНОВА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ДЕРЖАВНОГО УПРАВЛІННЯ

Ключові слова: електронний документообіг, ЕДО, цифрова трансформація, державне управління, адміністративні послуги, ефективність, прозорість, електронний уряд, інформаційні технології.

Анотація. У доповіді розглядається роль електронного документообігу (ЕДО) як ключового елемента цифрової трансформації державного управління. Аналізуються переваги впровадження ЕДО, його вплив на ефективність роботи державних органів, якість надання адміністративних послуг та рівень прозорості. Досліджуються сучасні тенденції розвитку систем ЕДО в Україні та світі, а також існуючі виклики та перспективи їх подальшого вдосконалення в контексті загальної цифрової трансформації державного сектору.

Вступ

У сучасному світі інформаційні технології стрімко проникають у всі сфери суспільного життя, не оминаючи й державне управління. Цифрова трансформація стає не просто трендом, а нагальною необхідністю для підвищення ефективності, прозорості та підзвітності державних органів, а також для покращення якості взаємодії держави з громадянами та бізнесом. Однією з фундаментальних основ цієї трансформації є впровадження систем електронного документообігу (ЕДО).

Перехід від традиційного паперового документообігу до електронного є стратегічним кроком, що відкриває нові можливості для оптимізації управлінських процесів, скорочення витрат часу та ресурсів, мінімізації корупційних ризиків та підвищення рівня задоволеності громадян якістю державних послуг. ЕДО виступає не просто інструментом для обміну інформацією, а й каталізатором глибоких організаційних змін у структурі та функціонуванні державних установ.

Основна частина

Електронний документообіг являє собою автоматизовану систему створення, обробки, передачі, зберігання та використання електронних документів у рамках діяльності організації. У контексті державного управління, впровадження ЕДО передбачає переведення основних документоорієнтованих процесів у цифровий формат, від реєстрації вхідної кореспонденції до формування архівних справ.

Переваги впровадження ЕДО в державному управлінні є численними та вагомими

1. Підвищення ефективності роботи: ЕДО значно скорочує час на обробку документів, усуває необхідність фізичного переміщення паперів між підрозділами, автоматизує рутинні операції (реєстрація, розсилка, погодження), що дозволяє державним службовцям зосередитися на більш важливих аналітичних та стратегічних завданнях.
2. Зниження витрат: Відмова від паперових носіїв, витрат на друк, копіювання, транспортування та зберігання документів призводить до значної економії бюджетних коштів. Електронні архіви є більш компактними та вимагають менших витрат на утримання.
3. Покращення якості надання адміністративних послуг: ЕДО забезпечує швидший та зручніший доступ громадян та бізнесу до необхідної інформації та послуг. Можливість подання документів в електронному вигляді, відстеження статусу їх розгляду онлайн, отримання електронних витягів та довідок значно спрощує взаємодію з державою.
4. Підвищення прозорості та підзвітності: Електронна фіксація всіх етапів руху документа забезпечує чіткість та контрольованість адміністративних процесів, ускладнює можливість втрати або фальсифікації документів, сприяє боротьбі з корупцією.
5. Покращення міжвідомчої взаємодії: ЕДО забезпечує оперативний та стандартизований обмін інформацією між різними державними органами, що сприяє координації їхньої діяльності та підвищує ефективність вирішення міжвідомчих питань.
6. Створення єдиного інформаційного простору: Впровадження ЕДО сприяє формуванню інтегрованої системи управління інформаційними ресурсами держави, що є необхідною умовою для прийняття обґрунтованих управлінських рішень на основі аналізу великих обсягів даних.

Сучасні тенденції розвитку систем ЕДО в Україні та світі

В Україні процес впровадження ЕДО в державних органах активно триває. Приймаються відповідні нормативно-правові акти, розробляються та впроваджуються національні стандарти електронного документообігу, створюються централізовані платформи для обміну електронними документами між державними установами.

Важливим кроком є розвиток систем електронної ідентифікації та автентифікації громадян (наприклад, BankID, MobileID, КЕП), що забезпечують безпечний доступ до електронних державних послуг.

У світовій практиці спостерігаються такі тенденції розвитку ЕДО в державному управлінні

1. Перехід до хмарних технологій: Хмарні рішення забезпечують гнучкість, масштабованість та економічність систем ЕДО.
2. Використання штучного інтелекту (ШІ): Технології ШІ можуть бути використані для автоматизації рутинних завдань (наприклад, класифікація документів, розпізнавання тексту), аналізу документів, підтримки прийняття рішень.
3. Інтеграція з іншими державними електронними системами: Розвиток екосистеми електронних державних послуг передбачає інтеграцію систем ЕДО з іншими платформами (наприклад, порталами адміністративних послуг, системами електронного урядування).
4. Забезпечення кібербезпеки: Зростання обсягів електронної інформації вимагає посилення заходів щодо захисту від кіберзагроз та забезпечення конфіденційності даних.
5. Впровадження принципів відкритого урядування: ЕДО може бути інструментом для забезпечення прозорості діяльності державних органів шляхом публікації відкритих даних та електронних документів (за винятком інформації з обмеженим доступом).

Виклики та перспективи подальшого вдосконалення ЕДО в контексті цифрової трансформації

Незважаючи на значні досягнення у сфері впровадження ЕДО в Україні, існують певні виклики, які потребують вирішення:

1. Недостатній рівень інтеграції між різними системами ЕДО: Відсутність єдиних стандартів та протоколів обміну даними ускладнює міжвідомчу взаємодію.
2. Проблеми з кібербезпекою та захистом даних: Необхідне постійне вдосконалення механізмів захисту електронної інформації.
3. Недостатній рівень цифрової грамотності державних службовців та громадян: Потрібні програми навчання та підвищення кваліфікації у сфері використання електронних інструментів.

4. Необхідність подальшого удосконалення нормативно-правової бази: Законодавство у сфері електронного документообігу потребує постійного оновлення з урахуванням новітніх технологій та міжнародного досвіду.

Перспективи подальшого розвитку ЕДО в Україні пов'язані з інтеграцією з іншими компонентами цифрової трансформації державного управління, такими як електронні реєстри, системи електронної ідентифікації, платформи відкритих даних. Подальше впровадження хмарних технологій, використання ШІ та розвиток мобільних державних послуг зроблять взаємодію громадян та бізнесу з державою ще більш зручною та ефективною.

Висновки:

Електронний документообіг є невід'ємною основою успішної цифрової трансформації державного управління. Його впровадження забезпечує значні переваги у підвищенні ефективності, зниженні витрат, покращенні якості послуг, забезпеченні прозорості та міжвідомчої взаємодії. Подальший розвиток систем ЕДО в Україні має бути спрямований на інтеграцію з іншими цифровими інструментами, забезпечення кібербезпеки, підвищення цифрової грамотності та вдосконалення нормативно-правової бази. Успішна реалізація цих завдань сприятиме побудові ефективної, прозорої та орієнтованої на потреби громадян системи державного управління.

Список використаних джерел:

1. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV. (Актуальна редакція).

2. Постанова Кабінету Міністрів України «Про затвердження Порядку роботи з електронними документами в діловодстві та їх архівного зберігання» від 17.01.2018 № 55. (Актуальна редакція).

Кононіченко Ірина Олександрівна
Студентка н.гр. 205_СПД ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, доцент кафедри інформаційних технологій ННІ права та психології НАВС

КІБЕРБЕЗПЕКА ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

У сучасних умовах розвитку інформаційного суспільства та цифровізації державного управління питання кібербезпеки набуває особливого значення. Державні інформаційні системи зберігають величезні обсяги важливої інформації — персональні дані громадян, інформацію про національну безпеку, діяльність органів влади, критичну інфраструктуру тощо. Будь-яке порушення безпеки цих систем може мати серйозні наслідки для держави й громадян. Тому кібербезпека державних інформаційних систем є однією з ключових складових національної безпеки України.

Кібербезпека – це стан захищеності кіберпростору, при якому забезпечується стійке функціонування інформаційних систем, запобігається несанкціонований доступ, втручання, пошкодження або знищення інформації. Державна інформаційна система — це система, що створена державним органом для автоматизованої обробки інформації, яка використовується для виконання ним повноважень.

Основні нормативно-правові акти, які регулюють сферу кібербезпеки в Україні:

- Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII;
- Закон України «Про інформацію»;
- Постанова КМУ № 518 «Про затвердження Порядку функціонування державної системи кіберзахисту»;
- Національна стратегія кібербезпеки України (Указ Президента № 47/2021 від 26.03.2021).

Кіберпростір — це середовище, яке виникає в результаті взаємодії людей, програм, даних і цифрових пристроїв через глобальні мережі. Кібербезпека охоплює технічні, організаційні та правові заходи, спрямовані на захист цифрового середовища.

Особливістю законодавства України є врахування міжнародних стандартів у сфері кібербезпеки, зокрема документів Європейського Союзу, стандартів ISO/IEC 27001, 27032

Загрози кібербезпеці державних інформаційних систем

Основні загрози:

- кібератаки з боку хакерських угруповань (у т.ч. державних);
- розповсюдження шкідливого програмного забезпечення (віруси, трояни);
- несанкціонований доступ до інформаційних ресурсів;
- внутрішні порушення (недбалість персоналу, помилки адміністраторів);
- фішингові атаки та соціальна інженерія.

Загрози кібербезпеці

Крім вірусу Petya, прикладом масштабної загрози є атака BlackEnergy (2015 рік), яка спричинила збої в енергетичних системах України.

Серед сучасних загроз — використання бот-мереж (botnets), DDoS-атаки, криптографічні атаки, порушення в системах автентифікації. Фішингові атаки стають дедалі витонченішими, використовують елементи штучного інтелекту для імітації офіційних ресурсів держави.

Система забезпечення кібербезпеки в Україні

Головні суб'єкти забезпечення кібербезпеки:

- Рада національної безпеки і оборони України;
- Державна служба спеціального зв'язку та захисту інформації;
- Служба безпеки України;
- Національний координаційний центр кібербезпеки;
- Кіберполіція.

Також діє державна система кіберзахисту, яка включає систему моніторингу, виявлення, запобігання та реагування на кіберінциденти. Державні органи зобов’язані впроваджувати політики інформаційної безпеки, проводити аудит, навчання персоналу та технічне зміцнення інфраструктури.

Система забезпечення кібербезпеки

Національний координаційний центр кібербезпеки (НКЦК) при РНБО здійснює стратегічне управління. Він координує обмін інформацією між суб’єктами кібербезпеки, розробляє сценарії реагування. Держспецзв’язку виконує функції технічного захисту інформації та сертифікації. СБУ через департамент кібербезпеки виконує контррозвідувальні та захисні функції. Також розвиваються центри реагування на комп’ютерні інциденти (CERT-UA).

Перспективи та виклики

В умовах війни з Російською Федерацією Україна стала однією з головних цілей кібератак. Це вимагає зміцнення національного кіберзахисту, розвитку власного програмного забезпечення, підготовки фахівців з кібербезпеки. Також актуальним є розширення міжнародного співробітництва з ЄС, НАТО, США та іншими партнерами.

Перспективи

У майбутньому необхідно:

- посилити нормативно-правову базу щодо відповідальності за кіберзлочини;
- розширити мережу кіберполіції та забезпечити її ресурсами;
- впровадити обов'язкову сертифікацію критичних інформаційних систем;
- проводити загальнонаціональні навчання з кіберзахисту;
- інтегруватися в європейський кіберпростір та долучатись до колективних систем захисту (як-от платформа ЄС по реагуванню на кіберінциденти).

Висновки:

Кібербезпека державних інформаційних систем є критично важливою складовою національної безпеки. Надійний захист інформації, впровадження новітніх технологій, навчання персоналу та координація дій між державними структурами – запорука безпеки цифрової держави.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 року № 2163-VIII.
2. Про Стратегію кібербезпеки України: Указ Президента від від 14.05.2021 року № 447/2021.
3. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова КМУ від 19.06.2019 № 518.
4. Матеріали Національного координаційного центру кібербезпеки URL: https://ncscc.gov.ua

Кіцак Софія Андріївна
Студентка н.гр. 103_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

ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІВ ТА ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Забезпечення інформаційної безпеки для органів і підрозділів Національної поліції (далі – НП) відіграє важливу роль у національній безпеці України. Ефективний захист даних, стабільність службових процесів та підтримання довіри громадян до правоохоронних органів суттєво залежать від правових і організаційних аспектів цієї діяльності.

Актуальність. У сучасних умовах, коли зростають кіберзагрози та активізуються гібридні впливи, питання інформаційної безпеки органів і підрозділів НП України стає вкрай важливим. Необхідно забезпечити ефективну правову та організаційну підтримку для захисту службової інформації, сприяння оперативній діяльності та зміцнення загальної безпеки держави.

Метою дослідження є аналіз правових та організаційних аспектів забезпечення інформаційної безпеки в органах і підрозділах НП України. У процесі дослідження передбачено вивчення чинних нормативно-правових актів, оцінка ефективності існуючих механізмів захисту інформації та визначення актуальних проблем у цій сфері.

Інформаційна система НП України включає підсистеми, що здійснюють облік на основі таких вимог: наявність нормативно-правової бази; забезпечення інформаційних підрозділів персоналом; організація навчання та перепідготовки кадрів; наявність необхідних технічних, програмних й електронно-комунікаційних технологій; матеріально-технічне та фінансове забезпечення.

Основоположними завданнями цієї системи є: 1) забезпечення можливості оперативного отримання інформації у повному, систематизованому та зручному для користування вигляді; 2) збір, обробка та узагальнення інформації для оцінки ситуації та прийняття обґрунтованих оптимальних рішень на всіх рівнях управління; 3) забезпечення динамічної та ефективної інформаційної взаємодії

органів Національної поліції, інших правоохоронних органів та державних установ; 4) забезпечення захисту інформації [1, с. 32].

Інформаційно-аналітичне забезпечення діяльності НП України залежно від підпорядкування здійснюється на трьох рівнях [2, с. 2]. *Перший рівень* є центральним і об'єднує інформаційні підсистеми поліції загальнонаціонального значення та галузевих служб НП України. На цьому рівні інтегрується інформація, що використовується для аналізу, планування, прийняття рішень і здійснення дій в межах оперативно-розшукових, слідчих та інших спеціальних заходів з протидії злочинності. *Другий рівень* – це регіональний рівень, де охоплюються інформаційні обліки, які є частинами загальнонаціональних інформаційних підсистем і застосовуються обласними службами НП України. *Третій рівень* – місцевий, включає інформаційні обліки, що є складовими загальнонаціональних інформаційних підсистем і використовуються у міських, районних підрозділах, а також у слідчих та інших підрозділах НП України.

Згідно ч. 2 ст. 25 Закону України «Про Національну поліцію» поліція в рамках інформаційно-аналітичної діяльності: 1) формує реєстри та бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ (далі – МВС) України; 2) користується реєстрами та базами (банками) даних МВС України та інших органів державної влади; 3) здійснює інформаційно-пошукову та інформаційно-аналітичну роботу; 4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями. Згідно ч.3 ст. 25 цього Закону поліція може створювати власні реєстри та бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також бази даних, що формуються в процесі здійснення оперативно-розшукової діяльності відповідно до закону, та інформаційно-аналітичні системи (у тому числі міжвідомчі), необхідні для виконання покладених на неї повноважень [3].

Національна поліція України має доступ до баз даних: 1) єдиної інформаційної системи МВС України; 2) інших правоохоронних органів України; 3) Генерального секретаріату Інтерполу; 4) інших державних інформаційних ресурсів України [1, с. 35].

Станом на сьогодні поліція забезпечує наповнення та актуальність баз даних, що є частиною єдиної інформаційної системи МВС України, з наступних питань: 1) осіб, щодо яких поліцейські здійснюють профілактичну роботу; 2) виявлених кримінальних та адміністративних правопорушень, осіб, які їх учинили, руху кримінальних проваджень; обвинувачених, обвинувальний акт щодо яких направлено до суду; 3) розшуку підозрюваних, обвинувачених (підсудних) осіб, які ухиляються від відбування покарання або вироку суду, або від виконання обов'язків, визначених законом для суб'єктів пробації; 4) розшуку осіб, зниклих безвісти; 5) установлення особи невпізнаних трупів та людей, які не можуть

надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком; 6) зареєстрованих в органах внутрішніх справ і поліції кримінальних або адміністративних правопорушень, подій, які загрожують особистій чи публічній безпеці, надзвичайних ситуацій; 7) осіб, стосовно яких поліцією застосовано адміністративне затримання, затримання в порядку, передбаченому Кримінальним процесуальним кодексом України, або інше законне затримання; осіб, підданих адміністративному арешту, домашньому арешту; осіб, яким повідомлено про підозру в учиненні кримінального правопорушення; 8) осіб, які скоїли адміністративні правопорушення, провадження у справах за якими здійснюється поліцією або територіальними центрами комплектування та соціальної підтримки; 9) зареєстрованих корупційних кримінальних правопорушень, адміністративних правопорушень, пов'язаних з корупцією, а також осіб, які їх учинили, та результатів розгляду цих правопорушень у судах; 10) іноземців та осіб без громадянства, затриманих поліцією за порушення визначених правил перебування в Україні; 11) викрадених номерних речей, цінностей та іншого майна, які мають характерні ознаки для ідентифікації, або речей, пов'язаних із учиненням правопорушень, відповідно до заяв громадян; 12) викрадених (втрачених) документів за зверненням громадян; 13) знайдених, вилучених предметів і речей, у тому числі заборонених або обмежених в обігу, а також документів з ознаками підробки, які мають індивідуальні (заводські) номери; 14) транспортних засобів, які розшукуються, у тому числі у зв'язку з безвісним зникненням особи, виявлених безхазяйних транспортних засобів, а також викрадених, втрачених номерних знаків; 15)виданих дозвільних документів у сфері безпеки дорожнього руху та дозволів на рух окремих категорій транспортних засобів [3].

Поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади з обов'язковим дотриманням Закону України «Про захист персональних даних». Інформація про доступ до реєстру та бази (банку) даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про особу, яка отримала доступ, та про обсяг даних, доступ до яких було отримано. Кожна дія особи, яка отримує доступ до інформації, фіксується в електронному архіві. Там зберігаються дані про користувача, час доступу та обсяг отриманої інформації (передбачених статтями 25-27 Закону України «Про Національну поліцію» [3]). В електронному архіві фіксуються прізвище, ім'я, по батькові, посада та номер спеціального жетона (в разі наявності), вид отриманої інформації, реєстр, з якого отримувалася інформація, час отримання інформації та інші дані, необхідні для ідентифікації особи, яка отримувала інформацію з інформаційних ресурсів, реєстрів та баз (банків) даних [3].

Поліція вживає необхідні заходи щодо недопущення будь-яких порушень прав і свобод людини, пов'язаних з обробкою інформації. Поліцейські та особи, які мають доступ до інформаційних ресурсів єдиної інформаційної системи МВС

України та інших інформаційно-комунікаційних систем (інформаційних ресурсів), несуть персональну дисциплінарну, адміністративну та кримінальну відповідальність за вчинені ними діяння, що призвели до порушень прав і свобод людини, пов'язаних з обробкою інформації.

Міністерство внутрішніх справ України у межах компетенції здійснює контроль за дотриманням вимог законів та інших нормативно-правових актів під час формування та користування поліцейськими інформаційними реєстрами та базами (банками) даних у порядку, визначеному у статтях 26, 27 Закону України «Про Національну поліцію» [3].

Висновки. Правові та організаційні аспекти забезпечення інформаційної безпеки органів і підрозділів Національної поліції України є фундаментальними для ефективного функціонування всієї системи правоохоронних органів. Інформаційна система поліції базується на наявності нормативно-правової бази, належному кадровому забезпеченні, організації професійної підготовки, використанні сучасних інформаційно-комунікаційних технологій та стабільному матеріально-фінансовому забезпеченні.

Основними завданнями у сфері інформаційно-аналітичної діяльності НП України є: забезпечення можливості оперативного доступу до систематизованої та повної інформації; здійснення збору, обробки та узагальнення інформації для оцінки оперативної обстановки; налагодження ефективної інформаційної взаємодії між підрозділами поліції та іншими правоохоронними і державними органами; забезпечення надійного захисту інформації від несанкціонованого доступу.

Завдяки чіткій організації багаторівневої інформаційної структури та постійному контролю за дотриманням відповідних законодавчих вимог, Національна поліція України забезпечує ефективну інформаційну безпеку в діяльності своїх органів та підрозділів.

Список використаних джерел:

1. Кудінов В. А., Яровий К. В. Інформаційне забезпечення правоохоронної діяльності: навч.-практ. посіб. Київ: Національна академія внутрішніх справ, 2024. 120 с. URL: https://elar.navs.edu.ua/items/67587163-1e25-48d4-ba8b-ff6b12004434 (дата звернення 02.05.2025).

2. Нікулін Є. Ю. Зміст інформаційного забезпечення органів Національної поліції України. Юридична наука: 2020. 9 с. URL: https://journal-nam.com.ua/index.php/journal/article/download/157/151 (дата звернення 05.05.2025)

3. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII // Відомості Верховної Ради. 2015. № 40-41. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення 06.05.2025)

Нікітенко Марія Богданівна
Студентка н.гр. 202_СПД ННІ права та психології НАВС

Науковий керівник:
Грищенко Олег Ігорович
старший викладач кафедри інформаційних технологій ННІ права та психології НАВС

РОЗУМНІ ПРЕЗЕНТАЦІЇ: ОГЛЯД НЕЙРОМЕРЕЖЕВИХ ПРОГРАМ ДЛЯ СТВОРЕННЯ ПРЕЗЕНТАЦІЙ

Актуальність: допомога в розумінні, які сервіси доступні для створення презентацій, як їх використовувати та які переваги вони мають.

Мета: показати, як нейромережеві сервіси оптимізують процес створення презентацій, зробити його ефективнішим, швидшим та простішим.

Вступ

Існує багато програм для створення презентацій, кожна з яких має свої особливості та призначення.

Однак, я можу надати загальну інформацію про програми для створення презентацій та їх типове призначення.

Загальне призначення програм для створення презентацій:

Програми для створення презентацій, такі як Microsoft PowerPoint, Google Slides, Apple Keynote та інші, є потужними інструментами, призначеними для створення візуально привабливих та інформативних презентацій. Їх основна мета – допомогти користувачам ефективно донести інформацію до аудиторії, використовуючи поєднання тексту, зображень, графіків, відео та інших мультимедійних елементів.

Основні функції та можливості програм для створення презентацій:

- **Створення слайдів:** Основною функцією є створення окремих слайдів, які складають презентацію. Кожен слайд може містити заголовок, текст, зображення, графіки, відео та інші об'єкти.
- **Редагування та форматування:** Програми надають широкі можливості для редагування та форматування тексту, зображень та інших об'єктів на слайдах. Можна змінювати шрифти, кольори, розміри, вирівнювання, додавати тіні, рамки та інші ефекти.
- **Вставка мультимедійних елементів:** Можна легко вставляти зображення, графіки, аудіо- та відеофайли, щоб зробити презентацію більш цікавою та захопливою.

- **Анімація та переходи:** Додавання анімації до об'єктів та переходів між слайдами дозволяє зробити презентацію динамічною та привернути увагу аудиторії.
- **Шаблони та теми:** Програми зазвичай пропонують широкий вибір готових шаблонів та тем, які можна використовувати як основу для створення презентації. Це значно спрощує процес розробки та дозволяє створити професійно виглядаючу презентацію за короткий час.
- **Спільна робота:** Багато сучасних програм для створення презентацій, особливо хмарні сервіси, підтримують спільну роботу над презентацією. Це дозволяє кільком користувачам одночасно редагувати та коментувати презентацію, що робить процес створення більш ефективним.
- **Показ презентації:** Програми надають різні можливості для показу презентації аудиторії, включаючи перегляд на екрані комп'ютера, проектування на великий екран, показ онлайн та інші.
- **Експорт та імпорт:** Можна експортувати презентацію в різні формати, такі як PDF, зображення, відео та інші. Також можна імпортувати презентації з інших форматів, що дозволяє обмінюватися презентаціями з користувачами, які використовують різні програми.

Призначення програм для створення презентацій в різних сферах:

- **Бізнес:** Для представлення продуктів та послуг, демонстрації результатів роботи, проведення навчальних семінарів та тренінгів, представлення стратегії компанії та інше.
- **Освіта:** Для проведення лекцій, семінарів, захисту дипломних робіт та інших навчальних заходів.
- **Наука:** Для представлення результатів досліджень на конференціях та симпозіумах.
- **Державне управління:** Для представлення звітів, планів та інших документів.
- **Інші сфери:** Для особистого використання, наприклад, для представлення фотографій з подорожей, сімейних подій та інше.

Штучний інтелект став важливим інструментом для автоматизації створення презентацій;

використання AI-інструментів значно спрощує процес розробки контенту, зекономити час та підвищити якість презентації;

Представлено популярні безкоштовні та платні нейромережеві сервіси для створення презентацій.

1. Переваги використання AI-інструментів у PowerPoint:

- Автоматичне оформлення та генерація креативних ідей.
- Спрощення роботи для студентів та викладачів.
- Створення якісних презентацій без дизайнерських навичок

2. Безкоштовні AI-сервіси для створення презентацій:

- Autoppt - автоматично створює презентації на основі теми або документу.
- ChatGPT - генерує VBA-код, який імпортується в PowerPoint для створення презентації.
- Canva - має інтуїтивні інструменти редагування, великий вибір шаблонів та функцію для спільної роботи.

3. Платні AI-інструменти для створення презентацій:

- Gamma - створення презентацій за допомогою готових шаблонів, імпорту тексту та інтеграції з Google Docs.
- Beautiful:ai - генерує макети з узгодженим дизайном, підтримує спільну роботу та імпорт файлів з інших серверів.
- Tome - пропонує динамічне формування структури презентації, інтеграцію з різними платформами та спільне редагування.

Висновок:

- Нейромережеві сервіси полегшують процес створення презентацій, автоматизуючи дизайн, зміст та структуру.
- Безкоштовні варіанти будуть корисні для базових завдань, тоді як платні пропонують розширені можливості для спільного та професійного використання.
- Вибір залежить від потреб: якщо потрібне швидке рішення, можна використати безкоштовні сервіси; якщо потрібна висока якість контенту - є можливість розглянути платні варіанти.

ДЛЯ НОТАТОК

Наукове видання

КУДІНОВ Вадим Анатолійович

СУЧАСНИЙ СТАН ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ УКРАЇНИ

Матеріали науково-практичного семінару

(м. Київ, 15 травня 2025 року)

Комп’ютерна верстка: *В.А. Кудінова*

Підписано до друку 19.06.2025. Формат 60х84/16. Папір офсетний.
Обл.-вид. арк. 4,25. Ум. друк. арк. 3,95.
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