технічного університету імені Івана Пулюя, 14-15 грудня 2011 р. – Тернопіль: ТНТУ, 2011. – С. 247.

2. Бойко О. Б. Управління чинниками відродження інноваційної діяльності в умовах промислового підприємства у повоєнний період. (Контексти імплементації сучасних інформаційно-аналітичних технологій в коноко-фінансову діяльність підприємства)». \ Бойко О, Б. – Тернопіль: Осадца Ю.В., 2023.-266 с.

3. Бешта О. С. Принципи підвищення енергоефективності виробничих комплексів геотехнічних систем / О. С. Бешта. // Науковий вісник Національного гірничого університету. – 2012. – № 6. – С. 99–106.

4. Гагалюк О. І. Управління трансформаційними процесами гермінативного розвитку в Україні у повоєнний період (Адміністративно-територіальні аспекти адаптації економіки до екологічних вимог ЄС. – Тернопіль: Осадца Ю. В., 2024,, -280 с.

5. Інноваційні засоби розвитку нетрадиційних джерел енергії та організація ресурсовикористання в соціогуманітарному комплексі України: монографія / Б. Андрушків, О. Бойко, Ю. Вовк ін./– Тернопіль: Терно-граф, 2016. – 816 с.

6. Кирич Наталія. Від стабілізації виробництва – до сталого розвитку суспільства. – Тернопіль: ТДТУ ім. І Пулюя, 2003. – 201 с.

7. Кузьмін О. Є. Тимощук М. Р., Фещур Р. В. Методи оцінювання потенціалу розвитку підприємств.//Економіка: проблеми теорії і практики – Харків: ХЕУ. 2005. – С. 374 –383.

8. Сердак С. Е. Принципи ефективного управління ресурсами суб'єктів господарювання / С. Е. Сердак // Академічний огляд. –2008. – № 2. – С. 83-88.

9. Управління сервісною інфраструктурою в умовах добровільного об'єднання територіальних громад, Ратинський Вадим. -. – Тернопіль: Осадца Ю. В., 2022,, - 496 с.

10. Управління потенціалом підприємства / І. З. Должанський, Т. О. Загорна, О. О. Удалих та ін.- К.: Центр навчальної літератури, 2006. – 362 с.

11. Шерстюк Р. П. Інноваційні шляхи активізації природоохоронного провайдингу в умовах підприємства (Європейські акценти) / Р. П. Шерстюк, Н. Б. Кирич, І. Б. Гевко. та ін.; за ред. проф. Б. М. Андрушківа. – Тернопіль: Тернограф. – 2011. – 576 с.

УДК 355.451 + 004.056 (477)

Войтко О., д. військ. наук, доц.; Федорієнко В., канд. техн. наук
Національний університет оборони України, Україна

ІНФОРМАЦІЙНА МОДЕЛЬ ПІДТРИМКИ РЕІНТЕГРАЦІЙНИХ ЗАХОДІВ ЗВІЛЬНЕНИХ ОБОРОНЦІВ УКРАЇНИ

Анотація. *Звільнені оборонці України (ЗОУ) є носіями колосального обсягу інформації про ворога, обставини потрапляння до ізоляції, умови утримування та факти воєнних злочинів. Проблемне завдання полягає у критичному розриві між обсягом даних, які потребують опрацювання, та наявними спроможностями державної системи. В умовах масових звільнень кількість осіб, які потребують допомоги, багаторазово перевищує чисельність підготовлених фахівців. Традиційна модель «As Is», що базується на розрізнених файлах та ручній обробці, не забезпечує необхідної оперативності та комплексності.*

Дане дослідження присвячене розробці та обґрунтуванню інноваційної «To Be» моделі, яка базується на використанні геоінформаційних систем (ГІС) та інтелектуального аналізу даних для забезпечення повного постізоляційного відновлення військовослужбовців. Актуальність цієї теми виходить за межі суто медичної реабілітації, оскільки вона безпосередньо стосується національної безпеки та спроможності держави захищати свій людський потенціал в умовах гібридної агресії.

Ключові слова: *інформаційна модель, Звільнені оборонці України, реінтеграція, ГІС, когнітивна безпека*

Voitko O., Dr. (Mil. Sci.), Assoc. Prof.; Vitalii Fedoriienko, Ph.D. (Eng.)
National Defence University of Ukraine, Ukraine

INFORMATION MODEL OF SUPPORT FOR REINTEGRATION MEASURES OF RELEASED DEFENDERS OF UKRAINE

Abstract. *Abstract. Released defenders of Ukraine (DFU) are carriers of a huge amount of information about the enemy, the circumstances of their isolation, the conditions of detention and the facts of war crimes. The problem lies in the critical gap between the volume of data that needs to be processed and the state system's available capabilities. In conditions of mass releases, the number of people in need of assistance often exceeds the number of trained specialists. The traditional "As Is" model, based on disparate files and manual processing, does not provide the necessary efficiency and comprehensiveness.*

This study is devoted to the development and justification of the innovative "To Be" model, which uses geographic information systems (GIS) and intelligent data analysis to ensure the full post-isolation recovery of servicemen. The relevance of this topic goes beyond purely medical rehabilitation, since it directly concerns national security and the state's ability to protect its human potential in conditions of hybrid aggression.

Keywords: *information model, Released Ukrainian Defense Forces, reintegration, GIS, cognitive security*

Сучасний етап російсько-української війни характеризується безпрецедентним поєднанням кінетичних методів впливу з агресивними когнітивними операціями. У цьому контексті питання відновлення персоналу трансформується з суто гуманітарної чи медичної процедури у стратегічно важливий елемент національної безпеки.

Актуальність теми зумовлена специфікою сучасної російсько-української війни, де кінетичні методи поєднуються з агресивними когнітивними операціями. Ворог використовує питання полонених як важіль маніпулятивного впливу на українське суспільство та родини захисників. Станом на кінець 2025 року кількість звільнених осіб перевищила 5000. Повернення такої значної кількості людей із важким досвідом ізоляції потребує не просто уваги, а науково обґрунтованої системи, здатної опрацьовувати колосальні масиви даних у реальному часі. Проблема полягає у необхідності одночасного вирішення трьох завдань: надання медико-психологічної допомоги, збору розвідувальних даних та документування воєнних злочинів для міжнародних судів. Традиційні підходи «As Is», сформовані в умовах конфліктів низької інтенсивності, виявилися неспроможними перед нинішніми масштабами.

Психологічний аспект актуальності зумовлений явищем «психоінформаційного розвантаження», коли інформація підсвідомо «виливається» з людини через перевантаження психіки. Хоча цей процес є природним чинником постізоляційної декомпресії, він робить військовослужбовця надзвичайно вразливим. Тому виникає потреба у створенні таких інформаційних моделей, які дозволяють структурувати спогади без ризику ретравматизації, одночасно трансформуючи травматичний досвід у внутрішній ресурс.

Інформаційна безпека додає ще один функціональний рівень: російська федерація систематично використовує тему полонених як важіль маніпулятивного впливу на ЗОУ, їхні родини та все суспільство. Це вимагає від української системи реінтеграції переходу до проактивного аналізу даних та впровадження контурів когнітивної безпеки.

Аналіз поточної ситуації (As Is) виявив низку системних недоліків. По-перше, це фрагментованість даних: інформація зберігається у розрізнених файлах MS Office (Word/Excel) або паперових анкетах. Це призводить до затримок, дублювання функцій різними відомствами та ризику втрати контексту. По-друге, це висока частка ручної праці: фахівці витрачають значний час на перенабір текстів та ручне геокодування об'єктів. По-третє, відсутня наскрізна геопросторова прив'язка, що ускладнює аналіз маршрутів переміщення ворога та локалізацію місць утримання. Застосовуючи закон Літтла, ми бачимо,

що при зростанні інтенсивності повернення полонених, черга на обробку даних зростає експоненційно, що загрожує колапсом системи.

Розроблення інтегрованої інформаційної моделі (To Be) на основі геоінформаційних систем (ГІС) та інтелектуального моніторингу є передумовою для: забезпечення когнітивної стійкості особового складу та суспільства; максимізації інформаційного виграшу через аналіз маршрутів переміщення ворога та місць примусової ізоляції; створення верифікованої доказової бази воєнних злочинів для міжнародних інституцій.

Майбутня модель To Be демонструє перехід від фрагментованого збору даних до цілісної екосистеми підтримки, здатної ефективно функціонувати в умовах високої невизначеності та інтенсивного інформаційного тиску гібридної війни.

Запропонована модель вирішує ієрархію цілей на трьох рівнях:

1. Стратегічний рівень: Забезпечення повного відновлення ЗОУ та збереження кадрового потенціалу ЗСУ.
2. Оперативний рівень: Реалізація конкретних заходів на трьох етапах: підготовчому, основному та етапі супроводу (до 12 місяців). Ключовим завданням моделі є перехід до Data-Driven Protection — захисту на основі даних, де кожне управлінське рішення підкріплене верифікованою аналітикою.
3. Тактичний рівень: Розбудова інфраструктури реінтеграції та налагодження міжвідомчої координації (МОУ, СБУ, МВС) на основі єдиних стандартів НАТО.

Методологічним фундаментом моделі є підхід щодо узагальнення досвіду (Lessons Learned), що відповідає спільній доктрині НАТО з проведення операцій. В аспекті реінтеграції ЗОУ пропонуються для його реалізації п’ять кроків: ідентифікація - документування - аналіз - збереження - удосконалення. Для візуалізації та автоматизації процесів використано нотацію BPMN (Business Process Model and Notation). Це дозволило деталізувати бізнес-процеси від моменту зустрічі ЗОУ на пункті обміну до завершення їхньої реабілітації, зробивши перехід від «As Is» до «To Be» керованим і вимірюваним.

Особлива увага в моделі приділена процесу психоінформаційного розвантаження. Людина, яка повернулася з полону, має підсвідоме прагнення «скинути» інформаційний тиск. Варто враховувати, що розповідь може бути нехронологічною, емоційно забарвленою та містити повтори. Замість традиційних дебрифінгів пропонується впровадження постізоляційного опитування з використанням засобів цифровізації за алгоритмом, який мінімізує ретравматизацію. Використання часових шкал (timeline) допомагає людині структурувати спогади, трансформуючи травматичний досвід у внутрішній ресурс.

Розроблена модель передбачає автоматизований 15-кроковий алгоритм збору інформації. Процес починається з ідентифікації військовослужбовця та визначення початку ізоляційної події. Далі система веде фахівця через серію блоків: переміщення, перебування в конкретних локаціях (L1…Ln), умови утримання, факти катувань та воєнних злочинів. Завдяки використанню розумних форм (Smart-forms) у ArcGIS Survey123, дані вносяться оперативно, а логічні перевірки на вході виключають грубі помилки та дублювання.

Центральним елементом моделі є ГІС-платформа (ArcGIS), яка реалізує функції збирання просторових даних про локації примусового утримання та маршрути етапування; просторового аналізу, кластеризації та виявлення закономірностей. ГІС дозволяє створити «карту реабілітації», візуалізувати «гарячі зони» воєнних злочинів та оптимізувати логістику надання допомоги залежно від місця проживання ЗОУ.

Гібридний характер війни вимагає включення в модель контуру моніторингу інформаційного простору. Для обґрунтування було введено поняття «інформаційного тиску» – динамічного впливу потоків пропаганди рф на ЗОУ та їхні родини. Розроблена математична модель індексу тиску враховує кількість публікацій, залученість аудиторії та наявність маніпулятивних наративів. Це дозволяє системі працювати як предиктор навантаження: зростання медіа-атак ворога сигналізує про необхідність посилення психологічної підтримки та уточнення дебрифінгів.

Практичне застосування ArcGIS Survey123 на планшетах дебриферів підтвердило високу стійкість системи до навантажень та зручність для персоналу. Використання ГІС-модуля дозволило скоротити невизначеність даних за рахунок інформаційного виграшу, зменшуючи ентропію при класифікації подій ізоляції.

Запропонована інформаційна модель забезпечує перехід від фрагментованого збору даних до цілісної інтелектуальної системи. Впровадження моделі дозволяє:

1. Двократно підвищити швидкість опрацювання інформації.
2. Сформувати потужну доказову базу щодо воєнних злочинів агресора.
3. Забезпечити когнітивну безпеку звільнених захисників через моніторинг загроз.

За рахунок технологічного оновлення може бути створено проактивну державну систему, де кожен захисник відчуває реальну підтримку, а держава отримує інструменти для ефективної відсічі в інформаційній та правовій площинах для притягнення рф до відповідальності за воєнні злочини.

Джерела та література

1. Герман Дж. Психологічна травма та шлях до видужання. Наслідки насильства – від знущань у сім'ї до політичного терору. Львів: Видавництво Старого Лева, 2015. 416 с.

2. Ukrinform. Як Росія використовує акції родичів військовополонених в інформаційній війні. *Укрінформ - актуальні новини України та світу*. URL: https://www.ukrinform.ua/rubric-ato/3925824-ak-rosia-vikoristovue-akcii-rodiciv-vijskovopolonenih-v-informacijnij-vijni.html (дата звернення: 03.09.2025).

3. Allied Joint Publication. AJP-3(C). Allied Joint Doctrine for the Conduct of Operations. – Brussels: NATO Standardization Office, 2019. – 240 p.

4. Vitalii Fedoriienko, Oleksandr Koshlan, Serhii Kravchenko, Andrii Shyshatskyi, Nataliia Vasiukova, Oleksandr Trotsko, Oksana Havryliuk, Oleksandr Sovik, Oleksandr Alieinik, & Yurii Svyryda. (2021). Development of a methodological approach for processing different types of data in systems of special purpose. Technology Audit and Production Reserves, 6(2(62)), 18–24. DOI: 10.15587/2706-5448.2021.243950.

УДК 355.4:004.8:007.5

Гаврилечко Ю., канд. наук з держ. упр., доц.
Заклад вищої освіти «Університет трансформації майбутнього», Україна

РИЗИКИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ІНФОРМАЦІЙНІЙ СКЛАДОВІЙ СУЧАСНИХ ВОЄННИХ КОНФЛІКТІВ

Анотація. *Тези присвячено аналізу ризиків застосування штучного інтелекту в інформаційній складовій сучасних воєнних конфліктів. Ідентифіковано п'ять категорій загроз: генерація дипфейків, автоматизована дезінформація, кібератаки на критичну інфраструктуру, алгоритмічна упередженість та підрив суспільної стійкості. Окреслено нормативну відповідь ЄС і запропоновано три напрями протидії для України.*

Ключові слова: *штучний інтелект, воєнний конфлікт, державна інформаційна політика, публічне управління, дезінформація, кібербезпека, кібератака.*

Gavrilechko Yu., Ph.D. (Publ. Adm.), Assoc. Prof.
Higher Education Institution "University of Future Transformation", Ukraine

RISKS OF ARTIFICIAL INTELLIGENCE USE IN THE INFORMATION COMPONENT OF MODERN MILITARY CONFLICTS

Abstract. *The theses examine the risks of artificial intelligence (AI) application in the information component of modern armed conflicts. Five categories of threats are identified: deepfake generation and synthetic content production, automated disinformation campaigns, cyberattacks on critical digital infrastructure, algorithmic bias of AI systems, and erosion of societal resilience. The EU regulatory response through the AI Act, NIS2 Directive and Cyber*